



User Guide

AWS IAM Identity Center



AWS IAM Identity Center: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist das IAM Identity Center?	1
Warum sollten Sie IAM Identity Center verwenden?	1
Umbenennen von IAM Identity Center	3
Ältere Namespaces bleiben unverändert	3
Erste Schritte	5
Voraussetzungen und Überlegungen zu IAM Identity Center	7
Auswahl eines AWS-Region	8
Verwenden Sie IAM Identity Center nur für Anwendungen	15
Von IAM Identity Center erstellte IAM-Rollen	16
IAM Identity Center und AWS Organizations	17
IAM Identity Center-Instanzen	18
AWS-Konto Typen, die IAM Identity Center aktivieren können	18
Organisationsinstanzen von IAM Identity Center	20
Konto-Instances von IAM Identity Center.	23
Löschen Sie Ihre IAM Identity Center-Instanz	28
IAM Identity Center aktivieren	31
Um eine Instanz von IAM Identity Center zu aktivieren	32
Bestätigen Sie Ihre Identitätsquellen	36
Aktualisieren Sie Firewalls und Gateways	38
Überlegungen zum Zulassen von Domains und URL-Endpunkten	41
Tutorials zur Identitätsquelle	42
Active Directory	43
CyberArk	46
Voraussetzungen	46
Überlegungen zu SCIM	47
Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center	47
Schritt 2: Konfigurieren Sie die Bereitstellung in CyberArk	48
(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute CyberArk für die Zugriffskontrolle (ABAC) im IAM Identity Center	49
(Optional) Übergabe von Attributen für die Zugriffskontrolle	50
Google Workspace	51
Überlegungen	52
Schritt 1: Google WorkSpace: Konfigurieren Sie die SAML-Anwendung	53

Schritt 2: IAM Identity Center und Google WorkSpace: Ändern Sie die IAM Identity Center-Identitätsquelle und richten Sie sie ein Google WorkSpace als SAML-Identitätsanbieter	54
Schritt 3: Google WorkSpace: Aktivieren Sie die Apps	55
Schritt 4: IAM Identity Center: Richten Sie die automatische Bereitstellung von IAM Identity Center ein	56
Schritt 5: Google WorkSpace: Konfigurieren Sie die automatische Bereitstellung	57
Übergabe von Attributen für die Zugriffskontrolle - Optional	59
Weisen Sie den Zugriff zu AWS-Konten	59
Nächste Schritte	62
Fehlerbehebung	63
JumpCloud	63
Voraussetzungen	64
Überlegungen zu SCIM	65
Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center	65
Schritt 2: Konfigurieren Sie die Bereitstellung in JumpCloud	66
(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute JumpCloud für die Zugriffskontrolle im IAM Identity Center	67
(Optional) Übergabe von Attributen für die Zugriffskontrolle	68
Microsoft Entra ID	69
Voraussetzungen	69
Überlegungen	70
Schritt 1: Bereiten Sie Ihren Microsoft-Tenant vor	72
Schritt 2: Bereite deine vor AWS Konto	74
Schritt 3: Konfigurieren und testen Sie Ihre SAML-Verbindung	77
Schritt 4: Konfigurieren und testen Sie Ihre SCIM-Synchronisierung	82
Schritt 5: ABAC konfigurieren - Optional	86
Weisen Sie den Zugriff zu AWS-Konten	88
Microsoft Entra IDKonfiguration für den Zugriff auf zusätzliche Regionen	90
Fehlerbehebung	91
Okta	93
Überlegungen	95
Schritt 1: Okta: Besorgen Sie sich die SAML-Metadaten von Ihrem Okta Konto	96
Schritt 2: IAM Identity Center: Konfigurieren Okta als Identitätsquelle für IAM Identity Center	96
Schritt 3: IAM Identity Center und Okta: Bereitstellung Okta users	98
Schritt 4: Okta: Synchronisieren Sie Benutzer von Okta mit IAM Identity Center	99

Übergabe von Attributen für die Zugriffskontrolle - Optional	101
Weisen Sie Zugriff zu AWS-Konten	102
OktaKonfiguration für den Zugriff auf zusätzliche Regionen	104
Nächste Schritte	105
Fehlerbehebung	105
OneLogin	108
Voraussetzungen	109
Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center	109
Schritt 2: Konfigurieren Sie die Bereitstellung in OneLogin	110
(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute OneLogin für die Zugriffskontrolle im IAM Identity Center	111
(Optional) Übergabe von Attributen für die Zugriffskontrolle	112
Fehlerbehebung	113
Ping Identity	114
PingFederate	114
PingOne	122
Identity-Center-Verzeichnis	129
Video-Tutorials	136
Einrichten Ihrer Arbeitskräfte	137
Benutzer, Gruppen und Bereitstellung	137
Eindeutigkeit von Benutzernamen und E-Mail-Adresse	137
Gruppen	138
Bereitstellung für Benutzer und Gruppen	138
Deprovisionierung für Benutzer und Gruppen	138
Verwaltung Ihrer Identitätsquelle	139
Überlegungen zum Ändern Ihrer Identitätsquelle	139
Ändern Sie Ihre Identitätsquelle	145
Benutzer- und Gruppenattribute in IAM Identity Center	147
Externe Identitätsanbieter	149
Microsoft AD directory	169
Benutzer im Identity Center-Verzeichnis verwalten	192
Bereitstellung, wenn sich Benutzer im IAM Identity Center befinden	192
Ändern Sie Ihre Identitätsquelle	192
Hinzufügen von Benutzern	193
Fügen Sie Gruppen hinzu	196
Fügen Sie Benutzer zu Gruppen hinzu	197

Gruppen löschen	198
Löschen von Benutzern	200
Benutzer aus Gruppen entfernen	201
Benutzereigenschaften bearbeiten	202
Zugang für Mitarbeiter	204
Grundlegendes zu Authentifizierung	204
Arten von Authentifizierungssitzungen	205
Möglichkeiten, Benutzersitzungen zu beenden	207
Was passiert mit dem Benutzerzugriff, wenn Sie eine Sitzung beenden	207
Einmaliges Abmelden	213
Bewährte Methoden für das Sitzungsmanagement	213
Konfigurieren Sie die Sitzungsdauer	213
Interaktive Benutzersitzungen	214
Benutzersitzungen im Hintergrund	215
Erweiterte Sitzungen für Kiro	217
Beenden Sie aktive Sitzungen für Workforce-Benutzer	218
Überlegungen zu Identitätsquellen, AWS CLI und AWS SDKs	219
Deaktivieren Sie den Benutzerzugriff	223
Benutzerzugriff verweigern	224
Verwaltung des Zugriffs für Benutzer im Identity Center-Verzeichnis	226
Verwaltung von Kennwörtern	226
MFA	226
Benutzerpasswörter einrichten	227
Multifaktor-Authentifizierung	230
Anwendungszugriff	245
AWS verwaltete Anwendungen	246
Steuerung des Zugriffs auf Anwendungen	246
Weitergabe von Identitätsinformationen	247
Einschränkung der Verwendung von AWS verwaltete Anwendungen	248
Anwendungen, die Sie mit IAM Identity Center verwenden können	249
Einrichtung von IAM Identity Center zum Testen AWS verwalteter Anwendungen	254
Bewerbungsdetails anzeigen und ändern	261
Deaktivierung einer AWS verwaltete Anwendung	261
Aktivieren von Konsolensitzungen mit verbesserter Identität	262
Vom Kunden verwaltete Anwendungen	266
SAML 2.0- und OAuth 2.0-Anwendungen	267

Einrichtung der SAML 2.0-Anwendung	272
Kontozugriff aktivieren	276
Weitergabe von vertrauenswürdigen Identitäten	280
Vorteile der Verbreitung vertrauenswürdiger Identitäten	280
Aktivierung der Verbreitung vertrauenswürdiger Identitäten	280
So funktioniert die Propagierung vertrauenswürdiger Identitäten	281
Voraussetzungen und Überlegungen	282
Anwendungsfälle	284
Autorisierungsdienste	311
Richten Sie Ihre eigene OAuth 2.0-Anwendung ein	322
Richten Sie vom Kunden verwaltete Anwendungen ein	322
Geben Sie vertrauenswürdige Anwendungen an	327
Vertrauenswürdiger Token-Aussteller	328
Zertifikate rotieren	345
Überlegungen vor der Rotation eines Zertifikats	345
Rotieren Sie ein IAM Identity Center-Zertifikat	345
Indikatoren für den Ablaufstatus des Zertifikats	348
Verstehen Sie die Anwendungseigenschaften	349
URL zum Starten der Anwendung	349
Status weiterleiten	350
Sitzungsdauer	350
Weisen Sie Anwendungen Benutzerzugriff zu	351
Entfernen Sie den Benutzerzugriff auf Anwendungen	352
Ordnen Sie Attribute zu	353
AWS-Konto Zugriff	354
AWS-Konto Typen	356
Status "Assigning" AWS-Konto access	359
End-user Erfahrung	359
Durchsetzung und Beschränkung des Zugriffs	360
Delegieren und Durchsetzen des Zugriffs	360
Beschränken Sie den Zugriff auf den Identitätsspeicher von Mitgliedskonten aus	361
Delegierte Verwaltung	362
Bewährte Methoden	363
Voraussetzungen	368
Registrieren Sie ein Mitgliedskonto	368
Aufheben der Registrierung eines Mitgliedskontos	369

Konten für delegierte Administratoren anzeigen	370
Temporärer erhöhter Zugang	371
Single-Sign-On-Zugriff auf AWS-Konten	372
Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten	373
Entfernen Sie den Benutzer- und Gruppenzugriff auf eine AWS-Konto	376
Benutzerzugriff widerrufen	377
Delegieren Sie, wer den Single-Sign-On-Zugriff gewähren kann	379
Berechtigungssätze	381
Erstellen Sie einen Berechtigungssatz, der Berechtigungen mit geringsten Rechten anwendet	382
Vordefinierte Berechtigungen	384
Benutzerdefinierte Berechtigungen	385
Berechtigungssätze erstellen, verwalten und löschen	388
Konfigurieren Sie die Eigenschaften von Berechtigungssätzen	402
Referenzieren von Berechtigungssätzen	409
Empfehlungen zur Vermeidung von Zugriffsunterbrechungen	412
Beispiel für eine benutzerdefinierte Vertrauensrichtlinie	413
Attribute-based Zugriffskontrolle	414
Vorteile	415
Checkliste: Konfiguration von ABAC in AWS mithilfe von IAM Identity Center	416
Attribute für Zugriffskontrolle	418
Service-linked Rollen	427
AWS auf das Portal zugreifen	429
Erste Schritte mit dem AWS auf das Portal zugreifen	429
Konfigurieren Sie das AWS auf das Portal zugreifen	430
Was können Sie konfigurieren	430
Aktivierung des Zugriffsportals AWS	431
Anpassen der AWS auf die URL des Portals zugreifen	431
Bestätigen Sie, dass sich Benutzer bei der anmelden können AWS auf das Portal zugreifen	432
Verwenden Sie das AWS auf das Portal zugreifen	434
Wie benutzt man den AWS auf das Portal zugreifen	434
Melden Sie sich bei der an AWS auf das Portal zugreifen	435
Ihr Benutzerkennwort zurücksetzen	437
AWS CLI und AWS SDK-Zugriff	439
Verknüpfungen erstellen	445

Registrieren Sie Ihr Gerät für MFA	448
Beenden Sie Ihre aktive Sitzung	450
Verwenden von IAM Identity Center auf mehreren AWS-Regionen	452
Vorteile der Unterstützung mehrerer Regionen	452
Voraussetzungen und Überlegungen	452
Eine zusätzliche Region auswählen	454
Replizieren Sie IAM Identity Center in eine zusätzliche Region	454
Schritt 1: Erstellen Sie einen Replikatschlüssel	455
Schritt 2: Fügen Sie die Region hinzu	455
Schritt 3 (nur externe Identitätsanbieter): Aktualisieren Sie das externe IdP-Setup	457
Schritt 4: Bestätigen Sie die Zulassungslisten für Firewall und Gateway	457
Schritt 5: Stellen Sie Ihren Benutzern Informationen zur Verfügung	458
Die Region ändert sich über das Hinzufügen der ersten Region hinaus	458
Welche Daten werden repliziert?	458
Zugang zu Arbeitskräften über eine zusätzliche Region	459
Benutzersitzungen über mehrere AWS-Regionen	460
AWS Greifen Sie auf die Portal-Endpunkte im primären und zusätzlichen Bereich zu AWS-Regionen	460
ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen	462
Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs	464
Failover zu einer zusätzlichen Region für den Zugriff AWS-Konto	465
AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu	466
Bereitstellung und Verwaltung von Anwendungen auf mehreren AWS-Regionen	467
Bereitstellung und Verwaltung AWS verwalteter Anwendungen auf mehreren AWS-Regionen	467
Bereitstellung und Verwaltung von kundenverwalteten Anwendungen in mehreren AWS-Regionen	469
Eine Region aus dem IAM Identity Center entfernen	469
Schritt 1: Aktualisieren Sie die externe IdP-Konfiguration (falls zutreffend)	469
Schritt 2: Entfernen Sie die Region	470
Schritt 3: Löschen Sie den Replikatschlüssel	471
Zusätzlich werden Service-APIs unterstützt AWS-Regionen	471
CloudTrail Ereignisse in der primären und zusätzlichen Region	472
IAM Identity Center-Anwendungsfälle in der primären und zusätzlichen Region	472
Resilienzdesign und regionales Verhalten	476
Auf Verfügbarkeit ausgelegt	477

Richten Sie den Notfallzugriff auf das ein AWS-Managementkonsole	477
Zusammenfassung der Konfiguration des Notfallzugriffs	479
Wie gestalten Sie Ihre kritischen Operations-Rollen	479
Wie planen Sie Ihr Zugriffsmodell	480
Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle	481
So erstellen Sie Ihre Notfallzugriffskonfiguration	482
Aufgaben zur Notfallvorbereitung	483
Failover-Prozess für Notfälle	484
Kehren Sie zum normalen Betrieb zurück	484
One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta	484
One-time Einrichtung einer direkten IAM-Verbundanwendung mit ADFS	488
Sicherheit	495
Identitäts- und Zugriffsmanagement für IAM Identity Center	496
Authentifizierung	496
Zugriffskontrolle	496
Übersicht über die Verwaltung von Zugriffsberechtigungen	497
Identity-based Beispiele für Richtlinien	501
Resource-based Beispiel für eine Richtlinie	510
AWS verwaltete Richtlinien	513
Verwenden von servicegebundenen Rollen	534
IAM Identity Center-Konsole und API-Autorisierung	542
API-Aktionen nach November 2023	543
API-Aktionen nach Oktober 2020	544
AWS STS Bedingungsschlüssel für IAM Identity Center	546
UserId	547
IdentityStoreArn	547
ApplicationArn	548
CredentialId	548
InstanceArn	549
Protokollieren und Überwachen	549
Protokollierung von IAM Identity Center-API-Aufrufen mit AWS CloudTrail	549
Protokollierung von IAM Identity Center SCIM mit AWS CloudTrail	591
Amazon EventBridge	598
Protokollierung konfigurierbarer AD-Synchronisierungsfehler	599
Compliance-Validierung	602
Unterstützte Compliance-Standards	602

Ausfallsicherheit	604
Sicherheit der Infrastruktur	605
Datenschutz	606
Verschlüsselung während der Übertragung	606
Datenschutz	607
Datenaufbewahrung	607
Verschlüsselung im Ruhezustand	607
IAM Identity Center-Verschlüsselungskontext	609
Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den kundenseitig verwalteten Schlüssel	610
Überwachung Ihrer Verschlüsselungsschlüssel für IAM Identity Center	610
AWS Speicherung, Verschlüsselung und Löschung von IAM Identity Center- Identitätsattributen durch verwaltete Anwendungen	610
Implementierung von kundenverwalteten KMS-Schlüsseln	611
Grundlegende KMS-Schlüsselrichtlinie	622
Erweiterte KMS-Grundsatzserklärungen	627
Taggen von Ressourcen	638
Tag-Einschränkungen	639
Verwalten Sie Tags mit der Konsole	639
AWS CLI Beispiele	640
Zuweisen von Tags	640
Anzeigen von Tags	641
Entfernen von Tags	641
Anwenden von Tags beim Erstellen eines Berechtigungssatzes	642
API-Aktionen	642
Integration von AWS CLI mit IAM Identity Center	643
So integrieren Sie AWS CLI in IAM Identity Center	643
Überlegungen zum privaten Zugriff	644
Kontingente	645
Kontingente für Anwendungen	645
AWS-Konto Kontingente	646
Active Directory-Kontingente	647
Kontingente für den IAM Identity Center-Identitätsspeicher	647
Drosselungsgrenzen für IAM Identity Center	647
Kontingente für OIDC-Dienstanfragen	649
Zusätzliche Kontingente	650

Fehlerbehebung	652
Probleme beim Erstellen einer Kontoinstanz von IAM Identity Center	652
Sie erhalten eine Fehlermeldung, wenn Sie versuchen, die Liste der Cloud-Anwendungen anzuzeigen, die für die Verwendung mit IAM Identity Center vorkonfiguriert sind	652
Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden ..	654
Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden	654
Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter	656
Benutzer können sich nicht anmelden, wenn ihr Benutzername im UPN-Format ist	657
Beim Ändern einer IAM-Rolle erhalte ich die Fehlermeldung „Der Vorgang kann für die geschützte Rolle nicht ausgeführt werden“	658
Verzeichnisbenutzer können ihr Passwort nicht zurücksetzen	658
Auf meinen Benutzer wird in einem Berechtigungssatz verwiesen, er kann jedoch nicht auf die zugewiesenen Konten oder Anwendungen zugreifen	659
Ich kann meine Anwendung aus dem Anwendungskatalog nicht korrekt konfigurieren	660
Fehler „Ein unerwarteter Fehler ist aufgetreten“, wenn ein Benutzer versucht, sich mit einem externen Identitätsanbieter anzumelden	660
Fehler 'Die Attribute für die Zugriffskontrolle konnten nicht aktiviert werden'	661
Ich erhalte die Meldung „Browser wird nicht unterstützt“, wenn ich versuche, ein Gerät für MFA zu registrieren	661
Die Active Directory-Gruppe „Domänenbenutzer“ wird nicht ordnungsgemäß mit dem IAM Identity Center synchronisiert	662
Fehler bei den ungültigen MFA-Anmeldeinformationen	662
Ich erhalte die Meldung „Ein unerwarteter Fehler ist aufgetreten“, wenn ich versuche, mich mit einer Authenticator-App zu registrieren oder anzumelden	662
Ich erhalte die Fehlermeldung „Du bist es nicht, das sind wir“, wenn ich versuche, mich im IAM Identity Center anzumelden	663
Meine Benutzer erhalten keine E-Mails vom IAM Identity Center	663
Fehler: Sie können nicht delete/modify auf die im Verwaltungskonto bereitgestellten Berechtigungssätze remove/assign zugreifen	664
Fehler: Das Sitzungstoken wurde nicht gefunden oder ist ungültig	664
Gruppenmitglieder aus vertrauenswürdigen Domänen werden nicht mit IAM Identity Center synchronisiert	664
Beheben Sie Probleme mit vom Kunden verwalteten Schlüsseln in AWS IAM Identity Center ..	665
Zugriff verweigert: Problem mit der KMS-Entschlüsselungsberechtigung	665

AWS Fehler bei der Anmeldung verwalteter Anwendungen mit einem vom Kunden verwalteten Schlüssel, der im IAM Identity Center aktiviert ist	665
AWS Fehler bei der and/or Benutzerzuweisung bei der Installation verwalteter Anwendungen, wenn ein vom Kunden verwalteter Schlüssel im IAM Identity Center aktiviert ist	666
KMS-Berechtigungsproblem: Konfiguration des vom Kunden verwalteten Schlüssels mit AWS IAM Identity Center	666
AWS auf Anmeldefehler im Portal zugreifen, wenn ein vom Kunden verwalteter Schlüssel im IAM Identity Center aktiviert ist	667
Beheben Sie Probleme bei der Einrichtung mehrerer Regionen in AWS IAM Identity Center	667
Die Region, in die ich meine IAM Identity Center-Instance replizieren möchte, ist in der IAM Identity Center-Konsole nicht verfügbar	667
AWS Fehler bei der Anmeldung verwalteter Anwendungen in einer weiteren Region	667
Probleme beim Aktivieren einer Instanz von IAM Identity Center mit mehreren Regionen	668
Die Schlüsselerstellung ist fehlgeschlagen	668
Die Schlüsselreplikation ist fehlgeschlagen	668
Die Instanzerstellung ist fehlgeschlagen	669
Dokumentverlauf	670
AWS Glossar	685
.....	dclxxxvi

Was ist das IAM Identity Center?

AWS IAM Identity Center ist die AWS Lösung, um die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Kiro und Amazon Quick und anderen AWS Ressourcen zu verbinden. Sie können Ihren bestehenden Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt im IAM Identity Center erstellen und verwalten. Anschließend können Sie IAM Identity Center für eine oder beide der folgenden Aufgaben verwenden:

- Benutzerzugriff auf Anwendungen
- Benutzerzugriff auf AWS-Konten

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den [Verbund mit IAM](#) für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-Konten Weise zugreifen, wie sie es immer getan haben, und Sie können Ihre vorhandenen Workflows weiterhin verwenden, um diesen Zugriff zu verwalten.

Warum sollten Sie IAM Identity Center verwenden?

IAM Identity Center optimiert und vereinfacht den Benutzerzugriff der Mitarbeiter auf Anwendungen oder AWS-Konten beides mithilfe der folgenden Schlüsselfunktionen.

Integration mit verwalteten Anwendungen AWS

[AWS verwaltete Anwendungen](#) wie Kiro und Amazon Redshift lassen sich in IAM Identity Center integrieren. IAM Identity Center bietet AWS verwalteten Anwendungen eine gemeinsame Ansicht von Benutzern und Gruppen.

Vertrauenswürdige Identitätsverbreitung zwischen Anwendungen

Durch die Verbreitung vertrauenswürdiger Identitäten können AWS verwaltete Anwendungen wie Amazon Quick die Identität eines Benutzers auf sichere Weise mit anderen AWS verwalteten Anwendungen teilen, z. B. Amazon Redshift den Zugriff auf AWS Ressourcen auf der Grundlage der Benutzeridentität autorisieren. Sie können Benutzeraktivitäten einfacher überwachen, da CloudTrail Ereignisse auf der Grundlage des Benutzers und der vom Benutzer

initiierten Aktionen protokolliert werden. Dadurch ist es einfacher zu verstehen, wer auf was zugegriffen hat. Informationen zu den unterstützten Anwendungsfällen, einschließlich einer umfassenden Anleitung zur Konfiguration, finden Sie unter [Anwendungsfälle für vertrauenswürdige Identitätsverbreitung](#).

Ein Verbundpunkt zur Vereinfachung des Benutzerzugriffs auf AWS

Durch die Bereitstellung eines Verbundpunkts reduziert IAM Identity Center den Verwaltungsaufwand, der für die Verwendung mehrerer AWS verwalteter Anwendungen und AWS-Konten erforderlich ist. Mit IAM Identity Center führen Sie einen Verbund nur einmal durch, und Sie müssen nur ein Zertifikat verwalten, wenn Sie einen [SAML 2.0](#) Identitätsanbieter verwenden. IAM Identity Center bietet AWS verwalteten Anwendungen eine gemeinsame Ansicht von Benutzern und Gruppen für Anwendungsfälle, in denen vertrauenswürdige Identitäten verbreitet werden, oder wenn Benutzer den Zugriff auf AWS Ressourcen gemeinsam mit anderen Personen nutzen.

Informationen zur Konfiguration häufig verwendeter Identitätsanbieter für die Zusammenarbeit mit IAM Identity Center finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#). Wenn Sie noch keinen Identitätsanbieter haben, können Sie Benutzer direkt im IAM Identity Center [erstellen und verwalten](#).

Möglichkeit, den Zugriff der Belegschaft auf mehrere AWS-Konten

IAM Identity Center bietet Ihnen Optionen zur zentralen Verwaltung des Zugriffs Ihrer Mitarbeiter auf AWS-Konten:

- Ihre Teams können ihre IAM-Rollen in IAM Identity Center-Benutzern AWS-Konten und -Gruppen mithilfe der IAM [Account Access Manager-Funktion erstellen und die Rollenzuweisungen für Benutzer und Gruppen im IAM Identity Center zentral verwalten](#). Weitere Informationen finden Sie [im IAM-Benutzerhandbuch unter](#) [Warum sollten Sie den Account Access Manager verwenden](#).
- Sie können IAM Identity Center-Berechtigungssätze auch verwenden, um zentral Berechtigungen für allgemeine Berufsfunktionen wie Admin zu erstellen, sie übergreifend AWS-Konten bereitzustellen und sie Benutzern und Gruppen zuzuweisen. Diese optionale Funktion ist nur für Organisationsinstanzen von IAM Identity Center verfügbar.

Zwei Instanztypen

IAM Identity Center unterstützt zwei Arten von Instanzen: Organisationsinstanzen und Kontoinstanzen. Eine Organisationsinstanz ist die beste Methode. Sie ist die einzige Instanz, mit der Sie den Zugriff auf Anwendungen verwalten können, AWS-Konten und sie wird für alle

Produktionsanwendungen empfohlen. Eine Organisationsinstanz wird im AWS Organizations Verwaltungskonto bereitgestellt und bietet Ihnen einen zentralen Punkt, von dem aus Sie den Benutzerzugriff verwalten können AWS.

Kontoinstanzen sind an die Instanz gebunden, AWS-Konto in der sie aktiviert sind. Verwenden Sie Kontoinstanzen von IAM Identity Center nur, um isolierte Bereitstellungen ausgewählter AWS verwalteter Anwendungen zu unterstützen. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

User-friendly Zugriff auf das Webportal für Ihre Benutzer

Das AWS Zugangsportal ist ein benutzerfreundliches Webportal, das Ihren Benutzern einen nahtlosen Zugriff auf alle ihnen zugewiesenen Anwendungen oder beides bietet. AWS-Konten

Multi-Region Zugriff auf AWS-Konten und Anwendungen

Wenn Sie Ihre IAM Identity Center-Instance in weitere Regionen replizieren, können Ihre Mitarbeiter über alle aktivierten Regionen auf ihre zugewiesenen AWS-Konten Anwendungen zugreifen und AWS verwaltete Anwendungen in jeder aktivierten Region bereitstellen.

Umbenennen von IAM Identity Center

Am 26. Juli 2022 Sign-On wurde AWS Single umbenannt in. AWS IAM Identity Center

Ältere Namespaces bleiben unverändert

Die Namespaces sso und die identitystore API-Namespace sowie die folgenden verwandten Namespaces bleiben aus Gründen der Abwärtskompatibilität unverändert.

- CLI-Befehle
 - [aws configure sso](#)
 - [identitystore](#)
 - [sso](#)
 - [sso-admin](#)
 - [sso-oidc](#)
- [Verwaltete Richtlinien, die](#) Präfixe AWSSSO und AWSIdentitySync Präfixe enthalten
- [Dienstendpunkte](#), die und enthalten sso identitystore

- [CloudFormation](#)-Ressourcen, die AWS : : SS0-Präfixe enthalten
- [Service-linked Rolle](#), die enthält AWSServiceRoleForSSO
- Konsolen-URLs, die sso und enthalten singlessignon
- URLs zur Dokumentation, die singlessignon enthalten

Erste Schritte mit IAM Identity Center

Im Folgenden wird beschrieben, wie Sie mit IAM Identity Center beginnen können.

1. IAM Identity Center aktivieren

Wenn Sie IAM Identity Center [aktivieren](#), wählen Sie zwischen zwei Typen von IAM Identity Center-Instanzen. Diese Typen sind: [Organisationsinstanzen](#) (empfohlen) und [Kontoinstanzen](#). Weitere Informationen zu den verschiedenen Funktionen dieser Instanztypen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Note

Nachdem IAM Identity Center aktiviert wurde, können Sie sich anmelden und die [IAM Identity Center-Konsole öffnen](#), indem Sie einen der folgenden Schritte ausführen:

- Organisationsinstanz — Melden Sie sich mit AWS Anmeldeinformationen mit Administratorrechten im Verwaltungskonto an.
- Kontoinstanz — Melden Sie sich mit AWS Anmeldeinformationen mit Administratorrechten in dem Bereich an, in AWS-Konto dem IAM Identity Center aktiviert ist.

2. Verbinden Sie Ihre Identitätsquelle mit IAM Identity Center

Bestätigen Sie in der IAM Identity Center-Konsole die Identitätsquelle, die Sie verwenden möchten. Im Folgenden finden Sie Informationen zu Identitätsquellen:

- Externer Identitätsanbieter — Wenn Sie bereits über einen Identitätsanbieter verfügen, der die Benutzer Ihrer Belegschaft verwaltet, können Sie ihn mit dem IAM Identity Center verbinden. Weitere Informationen zur Konfiguration häufig verwendeter Identitätsanbieter für die Zusammenarbeit mit IAM Identity Center finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#)
- Active Directory — Wenn Sie Active Directory zur Verwaltung Ihrer Mitarbeiterbenutzer verwenden, können Sie es mit dem IAM Identity Center verbinden. Weitere Informationen finden Sie unter [Verwenden von Active Directory als Identitätsquelle](#).
- IAM Identity Center — Alternativ können Sie Benutzer und Gruppen direkt im IAM Identity Center [erstellen und verwalten](#).

 Note

Um die Vorteile einer Einrichtung mit mehreren Regionen nutzen zu können, müssen Sie einen externen Identitätsanbieter oder das Identity Center-Verzeichnis als Identitätsquelle für Ihr IAM Identity Center verwenden. Multi-Region Unterstützung ist für Active Directory nicht verfügbar. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

3. Richten Sie den Benutzerzugriff ein auf AWS-Konten (nur Organisationsinstanz)

Wenn Sie eine Organisationsinstanz von IAM Identity Center verwenden, können Sie Benutzern oder Gruppen Zugriff darauf [zuweisen AWS-Konten](#), indem Sie [Berechtigungssätze verwenden](#), um Ihren Benutzern Zugriff auf Ressourcen zu AWS-Konten gewähren.

4. Richten Sie den Benutzerzugriff auf Anwendungen ein

Mit IAM Identity Center können Sie Benutzern Zugriff auf zwei Arten von Anwendungen gewähren:

a. [AWS verwaltete Anwendungen](#)

- Sie können IAM Identity Center mit AWS verwalteten Anwendungen wie Amazon Q Business und Amazon AWS CLI Redshift verwenden. Weitere Informationen erhalten Sie unter [AWS verwaltete Anwendungen](#) und [Integration von AWS CLI mit IAM Identity Center](#).

b. [Vom Kunden verwaltete Anwendungen](#)

- Sie können eine der folgenden Arten von kundenverwalteten Anwendungen in IAM Identity Center integrieren:
 - [Anwendungen, die im IAM Identity Center-Katalog aufgeführt sind](#)
 - [Ihre benutzerdefinierten Anwendungen](#)
- Nachdem Sie Ihre Anwendung konfiguriert haben, können Sie Ihren Benutzern Zugriff auf die Anwendung [zuweisen](#).

5. Stellen Sie Ihren Benutzern Anweisungen zur Anmeldung für das AWS Zugangsportal zur Verfügung

Das AWS Zugriffsportal ist ein Webportal, das Ihren Benutzern einen nahtlosen Zugriff auf alle ihnen zugewiesenen Anwendungen oder beides bietet. AWS-Konten Neue Benutzer im IAM Identity Center müssen ihre Benutzeranmeldeinformationen aktivieren, bevor sie sich beim AWS Zugriffsportal anmelden können.

Informationen zur Anmeldung beim AWS Access Portal finden Sie im AWS-Anmeldung Benutzerhandbuch unter Beim AWS Access Portal <https://docs.aws.amazon.com/signin/latest/userguide/iam-id-center-sign-in-tutorial.html> anmelden. Weitere Informationen zum Anmeldevorgang für das AWS Access Portal finden Sie unter [Anmelden beim AWS Access Portal](#).

Voraussetzungen und Überlegungen zu IAM Identity Center

Sie können IAM Identity Center nur für den Zugriff auf AWS verwaltete Anwendungen, AWS-Konten nur oder für beides verwenden. Wenn Sie den IAM-Verbund zur Verwaltung des Zugriffs auf verwenden AWS-Konten, können Sie dies weiterhin tun und gleichzeitig IAM Identity Center für den Anwendungszugriff verwenden.

Bevor Sie IAM Identity Center aktivieren, sollten Sie Folgendes beachten:

- AWS Region

Sie aktivieren IAM Identity Center zunächst in einer einzelnen, [unterstützten](#) Region für jede Instanz von IAM Identity Center. Wenn Sie IAM Identity Center für den Single-Sign-On-Zugriff auf AWS Konten verwenden möchten, muss die Region für alle Benutzer in Ihrer Organisation zugänglich sein. Wenn Sie planen, IAM Identity Center für den Anwendungszugriff zu verwenden, beachten Sie, dass einige AWS verwaltete Anwendungen, wie Amazon SageMaker AI, nur in den Regionen ausgeführt werden können, die sie unterstützen. Außerdem muss IAM Identity Center für die meisten AWS verwalteten Anwendungen in derselben Region wie die Anwendung verfügbar sein. Dies kann erreicht werden, indem sie sich in derselben Region befinden, oder, sofern dies unterstützt wird, indem die IAM Identity Center-Instanz in die gewünschte Bereitstellungsregion einer verwalteten Anwendung repliziert wird. AWS Weitere Informationen finden Sie unter [Überlegungen zur Auswahl eines AWS-Region](#).

- Nur Anwendungszugriff

Sie können IAM Identity Center nur für den Benutzerzugriff auf Anwendungen wie Kiro verwenden, indem Sie Ihren vorhandenen Identitätsanbieter verwenden. Weitere Informationen finden Sie unter [IAM Identity Center nur für den Benutzerzugriff auf Anwendungen verwenden](#).

 Note

Der Zugriff auf Anwendungsressourcen wird unabhängig vom Anwendungseigentümer verwaltet.

- Kontingent für IAM-Rollen

IAM Identity Center erstellt IAM-Rollen, um Benutzern Berechtigungen für Kontoressourcen zu erteilen. Weitere Informationen finden Sie unter [Von IAM Identity Center erstellte IAM-Rollen](#).

- IAM Identity Center und AWS Organizations

AWS Organizations wird für die Verwendung mit IAM Identity Center empfohlen, ist aber nicht erforderlich. Wenn Sie noch keine Organisation eingerichtet haben, müssen Sie das auch nicht tun. Wenn Sie IAM Identity Center bereits eingerichtet haben AWS Organizations und zu Ihrer Organisation hinzufügen möchten, stellen Sie sicher, dass alle AWS Organizations Funktionen aktiviert sind. Weitere Informationen finden Sie unter [IAM Identity Center und AWS Organizations](#).

Die Webschnittstellen von IAM Identity Center, einschließlich des Zugriffsportals und der IAM Identity Center-Konsole, sind für den menschlichen Zugriff über unterstützte Webbrowser vorgesehen. Zu den kompatiblen Browsern gehören die neuesten drei Versionen von Microsoft Edge, Mozilla Firefox, Google Chrome und Apple Safari. Der Zugriff auf diese Endpunkte über nicht browserbasierte Pfade wird nicht unterstützt. Für den programmatischen Zugriff auf IAM Identity Center-Dienste empfehlen wir, die in den API-Referenzhandbüchern für IAM Identity Center und Identity Store APIs verfügbaren Dokumente zu verwenden.

Überlegungen zur Auswahl eines AWS-Region

Sie können IAM Identity Center in einem einzigen Gerät aktivieren, das AWS-Region Ihrer Wahl unterstützt wird und Benutzern weltweit zur Verfügung steht. Diese globale Verfügbarkeit erleichtert Ihnen die Konfiguration des Benutzerzugriffs auf mehrere AWS-Konten Anwendungen. Im Folgenden finden Sie wichtige Überlegungen zur Auswahl eines AWS-Region.

- Geografischer Standort Ihrer Benutzer — Wenn Sie eine Region auswählen, die der Mehrheit Ihrer Endbenutzer geografisch am nächsten liegt, haben diese eine geringere Latenz beim Zugriff auf das AWS Zugriffsportal und AWS verwaltete Anwendungen wie Amazon SageMaker AI.
- Opt-in Regionen (Regionen, die standardmäßig deaktiviert sind) — Eine Opt-in-Region ist eine Region AWS-Region , die standardmäßig deaktiviert ist. Um eine Opt-in-Region zu verwenden,

müssen Sie sie aktivieren. Weitere Informationen finden Sie unter IAM Identity Center in einer Opt-in-Region [verwalten](#).

- IAM Identity Center in weitere Regionen replizieren — Wenn Sie IAM Identity Center in weitere Regionen replizieren möchten, müssen Sie eine Region auswählen AWS-Regionen, die standardmäßig aktiviert ist. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).
- Auswahl von Bereitstellungsregionen für AWS verwaltete Anwendungen — AWS verwaltete Anwendungen können nur in den Regionen ausgeführt werden, AWS-Regionen in denen sie verfügbar sind. Viele AWS verwaltete Anwendungen können auch nur in einer Region ausgeführt werden, in der IAM Identity Center aktiviert oder repliziert ist (primäre oder zusätzliche Region). Um zu überprüfen, ob Ihre IAM Identity Center-Instanz die Replikation in weitere Regionen unterstützt, finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#). Wenn Replikation keine Option ist, sollten Sie erwägen, IAM Identity Center in der Region zu aktivieren, in der Sie AWS verwaltete Anwendungen verwenden möchten.
- Digitale Souveränität — Vorschriften zur digitalen Souveränität oder Unternehmensrichtlinien können die Verwendung einer bestimmten AWS-Region Komponente vorschreiben. Konsultieren Sie die Rechtsabteilung Ihres Unternehmens.
- Identitätsquelle — Wenn Sie ein selbstverwaltetes Verzeichnis in [Active Directory \(AD\)](#) als Identitätsquelle verwenden [AWS Managed Microsoft AD](#), muss die Heimatregion mit der Region übereinstimmen, AWS-Region in der Sie IAM Identity Center aktiviert haben.
- Cross-Region E-Mails mit Amazon Simple Email Service — In einigen Regionen ruft IAM Identity Center möglicherweise [Amazon Simple Email Service \(Amazon SES\)](#) in einer anderen Region an, um E-Mails zu senden. Bei diesen regionsübergreifenden Aufrufen sendet IAM Identity Center bestimmte Benutzerattribute an die andere Region. Weitere Informationen finden Sie unter [Cross-Region E-Mails mit Amazon SES](#).
- AWS Control Tower— Wenn Sie eine Organisationsinstanz von IAM Identity Center von aus aktivieren AWS Control Tower, wird die Instance in derselben Region wie die AWS Control Tower Landing Zone erstellt.

Themen

- [Datenspeicher und -betrieb in der IAM Identity Center-Region](#)
- [Umschalten AWS-Regionen](#)
- [Deaktivierung einer AWS-Region wo IAM Identity Center aktiviert ist](#)

Datenspeicher und -betrieb in der IAM Identity Center-Region

Erfahren Sie, wie IAM Identity Center die Datenspeicherung und den Betrieb in allen Bereichen abwickelt. AWS-Regionen

Erfahren Sie, wie IAM Identity Center Daten speichert

Wenn Sie IAM Identity Center aktivieren, werden alle Daten, die Sie in IAM Identity Center konfigurieren, in der Region gespeichert, in der Sie sie aktiviert haben. Zu diesen Daten gehören Verzeichniskonfigurationen, Berechtigungssätze, Anwendungsinstanzen und Benutzerzuweisungen zu AWS-Konto Anwendungen. Wenn Sie den IAM Identity Center-Identitätsspeicher verwenden, werden alle Benutzer und Gruppen, die Sie in IAM Identity Center erstellen, ebenfalls in derselben Region gespeichert. Wenn Sie Ihre IAM Identity Center-Instanz in weitere Regionen replizieren, repliziert IAM Identity Center automatisch Benutzer, Gruppen, Berechtigungssätze und ihre Zuweisungen sowie andere Metadaten und Konfigurationen in diese Regionen.

Cross-Region E-Mails mit Amazon SES

IAM Identity Center verwendet [Amazon Simple Email Service \(Amazon SES\)](#), um E-Mails an Endbenutzer zu senden, wenn diese versuchen, sich mit einem Einmalkennwort (OTP) als zweitem Authentifizierungsfaktor anzumelden. Diese E-Mails werden auch bei bestimmten Ereignissen zur Identitäts- und Anmeldeinformationsverwaltung versendet, z. B. wenn der Benutzer aufgefordert wird, ein erstes Passwort einzurichten, eine E-Mail-Adresse zu verifizieren und sein Passwort zurückzusetzen. Amazon SES ist in einer Teilmenge verfügbar AWS-Regionen , die IAM Identity Center unterstützt.

IAM Identity Center ruft lokale Amazon SES-Endpunkte auf, wenn Amazon SES lokal in einem verfügbar ist. AWS-Region Wenn Amazon SES nicht lokal verfügbar ist, ruft IAM Identity Center die Amazon SES-Endpunkte auf einem anderen Weg auf AWS-Region, wie in der folgenden Tabelle angegeben.

IAM Identity Center-Regionalcode	Name der IAM Identity Center-Region	Amazon SES-Regionalcode	Name der Amazon SES-Region
ap-east-1	Asien-Pazifik (Hongkong)	ap-northeast-2	Asien-Pazifik (Seoul)
ap-east-2	Asien-Pazifik (Taipeh)	ap-northeast-1	Asien-Pazifik (Tokio)

IAM Identity Center-Regionalcode	Name der IAM Identity Center-Region	Amazon SES-Regionalcode	Name der Amazon SES-Region
ap-south-2	Asien-Pazifik (Hyderabad)	ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-4	Asien-Pazifik (Melbourne)	ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-5	Asien-Pazifik (Malaysia)	ap-southeast-1	Asien-Pazifik (Singapur)
ap-southeast-6	Asien-Pazifik (Neuseeland)	ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-7	Asien-Pazifik (Thailand)	ap-northeast-3	Asien-Pazifik (Osaka)
ca-west-1	Kanada West (Calgary)	ca-central-1	Kanada (Zentral)
eu-south-2	Europa (Spain)	eu-west-3	Europa (Paris)
eu-central-2	Europa (Zürich)	eu-central-1	Europa (Frankfurt)
mx-central-1	Mexiko (Zentral)	us-east-2	USA Ost (Ohio)
me-central-1	Naher Osten (VAE)	eu-central-1	Europa (Frankfurt)
us-gov-east-1	AWS GovCloud (US-East)	us-gov-west-1	AWS GovCloud (US-West)

Bei diesen regionsübergreifenden Aufrufen sendet IAM Identity Center möglicherweise die folgenden Benutzerattribute:

- E-Mail-Adresse
- Vorname
- Nachname
- Konto in AWS Organizations

- AWS auf die URL des Portals zugreifen
- Username
- Verzeichnis-ID
- Benutzer-ID

Verwaltung des IAM Identity Center in einer Opt-in-Region (Region, die standardmäßig deaktiviert ist)

Die meisten AWS-Regionen sind standardmäßig für den Betrieb in allen AWS Diensten aktiviert, aber Sie müssen die folgenden [Opt-in-Regionen aktivieren](#), wenn Sie IAM Identity Center verwenden möchten:

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Taipeh)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Neuseeland)
- Asien-Pazifik (Thailand)
- Kanada West (Calgary)
- Europa (Milan)
- Europa (Spain)
- Europa (Zürich)
- Israel (Tel Aviv)
- Mexiko (Zentral)
- Middle East (Bahrain)
- Naher Osten (VAE)

Wenn Sie IAM Identity Center in einer Opt-in-Region bereitstellen, müssen Sie diese Region in allen Konten aktivieren, für die Sie den Zugriff auf IAM Identity Center verwalten möchten. Alle Konten

benötigen diese Konfiguration, unabhängig davon, ob Sie Ressourcen in dieser Region erstellen. Sie können eine Region für die aktuellen Konten in Ihrer Organisation aktivieren und müssen diese Aktion wiederholen, wenn Sie neue Konten hinzufügen. Eine Anleitung finden Sie im AWS Organizations Benutzerhandbuch unter [Aktivieren oder Deaktivieren einer Region](#) in Ihrer Organisation. Um zu vermeiden, dass diese zusätzlichen Schritte wiederholt werden, können Sie Ihr IAM Identity Center in einer [Region bereitstellen, die standardmäßig](#) aktiviert ist.

 Note

Ihr AWS Mitgliedskonto muss in derselben Region angemeldet sein wie die Opt-in-Region, in der sich Ihre IAM Identity Center-Instanz befindet, damit Sie vom Zugangsportal aus auf das AWS Mitgliedskonto zugreifen können. AWS

Metadaten, die in den Opt-in-Regionen gespeichert sind

Wenn Sie IAM Identity Center für ein Verwaltungskonto in einem Opt-In aktivieren AWS-Region, werden die folgenden IAM Identity Center-Metadaten für alle Mitgliedskonten in der Region gespeichert.

- Konto-ID
- Account name (Kontoname)
- E-Mail-Adresse des Kontos
- Amazon-Ressourcennamen (ARNs) der IAM-Rollen, die IAM Identity Center im Mitgliedskonto erstellt

AWS-Regionen die standardmäßig aktiviert sind

Die folgenden Regionen sind standardmäßig aktiviert, und Sie können IAM Identity Center in diesen Regionen aktivieren.

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Oregon)
- USA West (Nordkalifornien)
- Europa (Paris)

- Südamerika (São Paulo)
- Asien-Pazifik (Mumbai)
- Europa (Stockholm)
- Asia Pacific (Seoul)
- Asien-Pazifik (Tokio)
- Europa (Irland)
- Europa (Frankfurt)
- Europa (London)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Kanada (Zentral)
- Asien-Pazifik (Osaka)

Umschalten AWS-Regionen

Wir empfehlen, IAM Identity Center in einer Region zu installieren, die Sie weiterhin für Benutzer verfügbar halten möchten, und nicht in einer Region, die Sie möglicherweise deaktivieren müssen. Weitere Informationen finden Sie unter [Überlegungen zur Auswahl eines AWS-Region](#).

Sie können Ihre IAM Identity Center-Region nur wechseln, indem Sie Ihre aktuelle IAM Identity Center-Instanz [löschen](#) und eine Instance in einer anderen Region erstellen. Wenn Sie bereits eine AWS verwaltete Anwendung mit Ihrer vorhandenen IAM Identity Center-Instanz aktiviert haben, deaktivieren Sie die Anwendung, bevor Sie IAM Identity Center löschen. Anweisungen zum Deaktivieren AWS verwalteter Anwendungen finden Sie unter [Deaktivierung einer AWS verwaltete Anwendung](#).

Note

Wenn Sie erwägen, Ihre IAM Identity Center-Region zu wechseln, um die Bereitstellung einer AWS verwalteten Anwendung in einer anderen Region zu ermöglichen, sollten Sie erwägen, Ihre IAM Identity Center-Instance stattdessen auf diese Region zu replizieren. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Überlegungen zur Konfiguration in der neuen Region

Sie müssen Benutzer, Gruppen, Berechtigungssätze, Anwendungen und Zuweisungen in der neuen IAM Identity Center-Instanz neu erstellen. Sie können die IAM Identity [Center-APIs für Konto- und Anwendungszuweisungen verwenden](#), um einen Snapshot Ihrer Konfiguration zu erhalten, und diesen Snapshot dann verwenden, um Ihre Konfiguration in einer neuen Region neu aufzubauen. Wenn Sie zu einer anderen Region wechseln, ändert sich auch die URL für das [AWS Zugriffsportal](#), das Ihren Benutzern Single-Sign-On-Zugriff auf ihre AWS-Konten Anwendungen bietet. Möglicherweise müssen Sie auch einige IAM Identity Center-Konfigurationen über die Management Console Ihrer neuen Instance neu erstellen.

Deaktivierung einer AWS-Region wo IAM Identity Center aktiviert ist

Wenn Sie eine deaktivieren, AWS-Region in der IAM Identity Center installiert ist, wird IAM Identity Center ebenfalls deaktiviert. Nachdem IAM Identity Center in einer Region deaktiviert wurde, haben Benutzer in dieser Region keinen Single-Sign-On-Zugriff auf Anwendungen. AWS-Konten

Um IAM Identity Center im [Opt-In erneut zu aktivieren AWS-Regionen](#), müssen Sie die Region erneut aktivieren. Da IAM Identity Center alle unterbrochenen Ereignisse erneut verarbeiten muss, kann die erneute Aktivierung von IAM Identity Center einige Zeit in Anspruch nehmen.

Note

IAM Identity Center kann nur den Zugriff auf diejenigen verwalten, die für AWS-Konten die Verwendung in einem aktiviert sind. AWS-Region Um den Zugriff für alle Konten in Ihrer Organisation zu verwalten, aktivieren Sie IAM Identity Center im Verwaltungskonto in einem Konto AWS-Region , das automatisch für die Verwendung mit IAM Identity Center aktiviert wird.

Weitere Informationen zum Aktivieren und Deaktivieren finden Sie AWS-Regionen [in der AWS-RegionenAWS Allgemeinen Referenz unter](#) Verwalten.

IAM Identity Center nur für den Benutzerzugriff auf Anwendungen verwenden

Sie können IAM Identity Center für den Benutzerzugriff auf Anwendungen wie Kiro oder beides verwenden. AWS-Konten Sie können Ihren bestehenden Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Benutzer direkt in IAM Identity Center

[erstellen und verwalten](#). Informationen darüber, wie Sie Ihren vorhandenen Identitätsanbieter mit IAM Identity Center verbinden, finden Sie im [Tutorials zu Identitätsquellen im IAM Identity Center](#)

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den [Verbund mit IAM](#) für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-Konten Weise zugreifen, wie sie es immer getan haben, und Sie können Ihre vorhandenen Workflows weiterhin verwenden, um diesen Zugriff zu verwalten.

Von IAM Identity Center erstellte IAM-Rollen

Wenn Sie einem AWS Konto einen Benutzer zuweisen, erstellt IAM Identity Center IAM-Rollen, um Benutzern Berechtigungen für Ressourcen zu erteilen.

Wenn Sie einen Berechtigungssatz zuweisen, erstellt IAM Identity Center in jedem Konto die entsprechenden, vom IAM Identity Center kontrollierten IAM-Rollen und fügt diesen Rollen die im Berechtigungssatz angegebenen Richtlinien zu. IAM Identity Center verwaltet die Rolle und ermöglicht es den von Ihnen definierten autorisierten Benutzern, die Rolle über das Zugriffsportal oder zu übernehmen. AWS CLI Wenn Sie den Berechtigungssatz ändern, stellt IAM Identity Center sicher, dass die entsprechenden IAM-Richtlinien und -Rollen entsprechend aktualisiert werden. Die Replikation Ihrer IAM Identity Center-Instanz in weitere Regionen hat keine Auswirkungen auf bestehende IAM-Rollen und es werden keine neuen IAM-Rollen erstellt.

Note

Berechtigungssätze werden nicht verwendet, um Anwendungen Berechtigungen zu erteilen.

Wenn Sie in Ihrem bereits IAM-Rollen konfiguriert haben, empfehlen wir Ihnen AWS-Konto, zu überprüfen, ob sich Ihr Konto dem Kontingent für IAM-Rollen nähert. Das Standardkontingent für IAM-Rollen pro Konto beträgt 1000 Rollen. Weitere Informationen finden Sie unter [IAM-Objektkontingente](#).

Wenn Sie sich dem Kontingent nähern, sollten Sie erwägen, eine Erhöhung des Kontingents zu beantragen. Andernfalls könnten Probleme mit IAM Identity Center auftreten, wenn Sie Berechtigungssätze für Konten bereitstellen, die das IAM-Rollenkontingent überschritten haben. Informationen dazu, wie Sie eine Kontingenterhöhung [beantragen können, finden Sie unter Eine Kontingenterhöhung](#) beantragen im Service Quotas User Guide.

 Note

Wenn Sie die IAM-Rollen in einem Konto überprüfen, das bereits IAM Identity Center verwendet, fallen Ihnen möglicherweise Rollennamen auf, die mit beginnen. "AWSReservedSSO_" Dies sind die Rollen, die der IAM Identity Center-Dienst für das Konto erstellt hat. Sie stammen aus der Zuweisung eines Berechtigungssatzes für das Konto.

IAM Identity Center und AWS Organizations

AWS Organizations wird für die Verwendung mit IAM Identity Center empfohlen, ist aber nicht erforderlich. Wenn Sie noch keine Organisation eingerichtet haben, müssen Sie das auch nicht tun. Wenn Sie IAM Identity Center aktivieren, wählen Sie aus, ob Sie den Dienst mit AWS Organizations aktivieren möchten. Wenn Sie eine Organisation einrichten, wird die Organisation, AWS-Konto die die Organisation einrichtet, zum Verwaltungskonto der Organisation. Der Root-Benutzer von AWS-Konto ist jetzt der Besitzer des Organisationsverwaltungskontos. Alle weiteren, die AWS-Konten Sie zu Ihrer Organisation einladen, sind Mitgliedskonten. Das Verwaltungskonto erstellt die Ressourcen, Organisationseinheiten und Richtlinien der Organisation, mit denen die Mitgliedskonten verwaltet werden. Berechtigungen werden vom Verwaltungskonto an Mitgliedskonten delegiert.

 Note

Wir empfehlen, dass Sie IAM Identity Center mit aktivieren AWS Organizations, wodurch eine Organisationsinstanz von IAM Identity Center erstellt wird. Eine Organisationsinstanz ist unsere empfohlene bewährte Methode, da sie alle Funktionen von IAM Identity Center unterstützt und zentrale Verwaltungsfunktionen bietet. Weitere Informationen finden Sie unter [Organisationsinstanzen von IAM Identity Center](#).

Wenn Sie IAM Identity Center bereits eingerichtet haben AWS Organizations und es Ihrer Organisation hinzufügen möchten, stellen Sie sicher, dass alle AWS Organizations Funktionen aktiviert sind. Wenn Sie eine Organisation erstellen, werden standardmäßig alle Funktionen aktiviert. Weitere Informationen finden Sie unter [Aktivieren aller Funktionen in Ihrer Organisation](#) im AWS Organizations Benutzerhandbuch.

Um eine Organisationsinstanz von IAM Identity Center zu aktivieren, müssen Sie sich beim anmelden, AWS-Managementkonsole indem Sie sich mit Ihrem AWS Organizations Verwaltungskonto als Benutzer mit Administratoranmeldedaten oder als Root-Benutzer anmelden

(nicht empfohlen, sofern keine anderen Administratorbenutzer vorhanden sind). Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter [AWS Organisation erstellen und verwalten](#).

Wenn Sie mit Administratoranmeldedaten von einem AWS Organizations Mitgliedskonto aus angemeldet sind, können Sie eine Kontoinstanz von IAM Identity Center aktivieren. Kontoinstanzen haben eingeschränkte Funktionen und sind an ein einziges AWS Konto gebunden.

Organisations- und Kontoinstanzen von IAM Identity Center

Eine Instanz ist eine einzelne Bereitstellung von IAM Identity Center. Für IAM Identity Center sind zwei Arten von Instanzen verfügbar: Organisationsinstanzen und Kontoinstanzen.

- Organisationsinstanz (empfohlen)

Eine Instanz von IAM Identity Center, die Sie im AWS Organizations Verwaltungskonto aktivieren. Organisationsinstanzen unterstützen alle Funktionen von IAM Identity Center. Wir empfehlen, eine Organisationsinstanz anstelle von Kontoinstanzen bereitzustellen, um die Anzahl der Verwaltungspunkte zu minimieren.

- Kontoinstanz

Eine Instanz von IAM Identity Center, die an eine einzelne AWS-Konto Instanz gebunden ist und die nur innerhalb der AWS-Konto AWS Region sichtbar ist, in der sie aktiviert ist. Verwenden Sie eine Kontoinstanz für einfachere Szenarien mit nur einem Konto. Sie können eine Kontoinstanz auf eine der folgenden Arten aktivieren:

- Und AWS-Konto das wird nicht verwaltet von AWS Organizations
- Ein Mitgliedskonto in AWS Organizations

AWS-Konto Typen, die IAM Identity Center aktivieren können

Um IAM Identity Center zu aktivieren, melden Sie sich je nach Instanztyp, den Sie erstellen möchten, mit einem der folgenden Anmeldeinformationen an: AWS-Managementkonsole

- Ihr AWS Organizations Verwaltungskonto (empfohlen) — Erforderlich, um eine [Organisationsinstanz](#) von IAM Identity Center zu erstellen. Verwenden Sie eine Organisationsinstanz für Berechtigungen und Anwendungszuweisungen für mehrere Konten in der gesamten Organisation.

- Ihr AWS Organizations Mitgliedskonto — Wird verwendet, um eine [Kontoinstanz](#) von IAM Identity Center zu erstellen, um Anwendungszuweisungen innerhalb dieses Mitgliedskontos zu ermöglichen. In einer Organisation können ein oder mehrere Konten mit einer Instanz auf Mitgliedsebene existieren.
- Eine eigenständige Instanz AWS-Konto — Wird verwendet, um eine [Organisations](#) - oder [Kontoinstanz](#) von IAM Identity Center zu erstellen. Die eigenständige Version AWS-Konto wird nicht von AWS Organizations verwaltet. Sie können einem eigenständigen Gerät nur eine Instanz von IAM Identity Center zuordnen AWS-Konto und diese Instanz für Anwendungszuweisungen innerhalb dieses AWS-Konto Standalone-Geräts verwenden.

Verwenden Sie die folgende Tabelle, um die vom Instanztyp bereitgestellten Funktionen zu vergleichen:

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Version AWS-Konto
Benutzer verwalten	✔Ja	✔Ja	✔Ja
AWS Zugriffsportal für den Single-Sign-On-Zugriff auf Ihre AWS verwalteten Anwendungen	✔Ja	✔Ja	✔Ja
Von Kunden verwaltete OAuth 2.0 (OIDC) - Anwendungen	✔Ja	✔Ja	✔Ja
Multi-account Berechtigungen	✔Ja	✘Nein	✘Nein
AWS Zugangsportal für den Single-Sign-On-Zugriff auf Ihre AWS-Konten	✔Ja	✘Nein	✘Nein

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Version AWS-Konto
Von Kunden verwaltete SAML 2.0-Anwendungen	✔Ja	✘Nein	✘Nein
Ein delegierter Administrator kann die Instanz verwalten	✔Ja	✘Nein	✘Nein
Verschlüsselung im Ruhezustand mithilfe eines vom Kunden verwalteten KMS-Schlüssels	✔Ja	✘Nein	✘Nein
Replizieren von IAM Identity Center auf weitere Regionen	✔Ja	✘Nein	✘Nein

Weitere Informationen zu AWS verwalteten Anwendungen und IAM Identity Center finden Sie unter [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#)

Themen

- [Organisationsinstanzen von IAM Identity Center](#)
- [Konto-Instances von IAM Identity Center.](#)
- [Löschen Sie Ihre IAM Identity Center-Instanz](#)

Organisationsinstanzen von IAM Identity Center

Wenn Sie IAM Identity Center zusammen mit aktivieren AWS Organizations, erstellen Sie eine Organisationsinstanz von IAM Identity Center. Ihre Organisations-Instance muss in Ihrem Verwaltungskonto aktiviert sein. Sie können den Zugriff von Benutzern und Gruppen mit einer

einigen Organisations-Instanz zentral verwalten. Sie können für jedes Verwaltungskonto nur eine Organisationsinstanz einrichten. AWS Organizations

Wenn Sie IAM Identity Center vor dem 15. November 2023 aktiviert haben, verfügen Sie über eine Organisationsinstanz von IAM Identity Center.

Informationen zum Aktivieren einer Organisationsinstanz von IAM Identity Center finden Sie unter.

[Um eine Instanz von IAM Identity Center zu aktivieren](#)

Wann sollte eine Organisationsinstanz verwendet werden

Eine Organisationsinstanz ist die primäre Methode zur Aktivierung von IAM Identity Center, und in der Regel wird eine Organisationsinstanz empfohlen. Organisationsinstanzen bieten die folgenden Vorteile:

- Unterstützung für alle Funktionen von IAM Identity Center — einschließlich der Verwaltung von Berechtigungen für mehrere Benutzer AWS-Konten in Ihrem Unternehmen, der Zuweisung von Zugriffen auf vom Kunden verwaltete Anwendungen und der Replikation in mehreren Regionen.
- Reduzierung der Anzahl der Verwaltungspunkte — Eine Organisationsinstanz hat einen einzigen Verwaltungspunkt, das Verwaltungskonto. Wir empfehlen, eine Organisationsinstanz anstelle einer Kontoinstanz zu aktivieren, um die Anzahl der Verwaltungspunkte zu reduzieren.
- Zentrale Steuerung der Erstellung von Kontoinstanzen — Sie können steuern, ob Kontoinstanzen von Mitgliedskonten in Ihrer Organisation erstellt werden können, solange Sie Ihrer Organisation in einer Opt-in-Region (AWS-Region die standardmäßig deaktiviert ist) keine Instanz von IAM Identity Center bereitgestellt haben.

Anweisungen zum Aktivieren einer Organisationsinstanz von IAM Identity Center finden Sie unter.

[Um eine Instanz von IAM Identity Center zu aktivieren](#)

Optionen für die Instanzkonfiguration

Wenn Sie eine Organisationsinstanz in einer aktivieren [AWS-Region , die standardmäßig aktiviert ist](#), wählen Sie eine Instanzkonfiguration. In anderen Regionen wird Ihre Instanz mit Standardeinstellungen erstellt.

Note

Mit den Optionen **Multi-Region Instanz** und **Benutzerdefinierte Instanz** (neuen Schlüssel erstellen) wird ein vom Kunden verwalteter KMS-Schlüssel erstellt, der mit dem Tag

versehen ist, CreatedBy: IAM Identity Center und replizieren ihn in Ihrem Namen in der zusätzlichen Region. Stellen Sie sicher, dass Ihr IAM-Principal zusätzlich zu den `kms:ReplicateKey` für die Aktivierung von IAM [Identity Center erforderlichen Berechtigungen auch über Berechtigungen verfügt. `kms:CreateKeykms:TagResource`](#)

Single-Region Instanz

Ihre Instanz wird in der aktuellen Region erstellt.

- Verschlüsselung im Ruhezustand — Ihre Daten werden mit einem AWS eigenen Schlüssel verschlüsselt. Sie können später auf der Seite „Einstellungen“ zu einem vom Kunden verwalteten Schlüssel wechseln.
- Berechtigungssätze — Standardmäßig aktiviert, sodass Sie den AWS-Konto Zugriff für Benutzer und Gruppen verwalten können. Dies kann nicht deaktiviert werden, sobald es aktiviert ist.
- Primäre Region — Ihre Instance wird in der aktuellen Region erstellt. Dieser kann nach der Erstellung nicht mehr geändert werden.
- Zusätzliche Regionen — Es sind keine zusätzlichen Regionen konfiguriert. Sie können Regionen später auf der Seite „Einstellungen“ hinzufügen.

Multi-Region Instanz

Ihre Instance wird in der aktuellen Region erstellt und in eine weitere Region repliziert, um Ausfallsicherheit AWS-Konto und Anwendungszugriff zu gewährleisten.

- Verschlüsselung im Ruhezustand — Ihre Daten werden mit einem vom Kunden verwalteten Schlüssel für mehrere Regionen verschlüsselt, der in Ihrem Konto mit einer Schlüsselrichtlinie erstellt wurde, die Replikation unterstützt. Der Schlüssel ist mit einem Tag versehenCreatedBy: IAM Identity Center, sodass Sie ihn in Ihrem Konto leicht identifizieren können. Der Schlüssel kann später geändert werden. AWS KMS Es fallen Gebühren an.
- Berechtigungssätze — Standardmäßig aktiviert, sodass Sie den AWS-Konto Zugriff für Benutzer und Gruppen verwalten können. Dies kann nicht deaktiviert werden, sobald es aktiviert ist.
- Primäre Region — Ihre Instance wird in der aktuellen Region erstellt. Dieser kann nach der Erstellung nicht mehr geändert werden.
- Zusätzliche Regionen — Ihre Instance wird in eine zusätzliche Region repliziert, um Ausfallsicherheit AWS-Konto und Anwendungszugriff zu gewährleisten. Sie können die Region ändern oder später weitere Regionen hinzufügen.

Benutzerdefinierte Instanz

Konfigurieren Sie Ihre Instanzeinstellungen individuell.

Verschlüsselung im Ruhezustand

Wählen Sie eine der folgenden Optionen aus. Ein vom Kunden verwalteter Schlüssel ist erforderlich, um weitere Regionen hinzuzufügen.

- **AWS Eigenen Schlüssel verwenden** — Ihre Daten werden mit einem Schlüssel verschlüsselt, der AWS Eigentümer und Verwalter ist. Es fallen keine zusätzlichen Gebühren an.
- **Einen neuen, vom Kunden verwalteten Schlüssel erstellen** — In Ihrem Konto wird ein Schlüssel für mehrere Regionen mit einer grundlegenden Schlüsselrichtlinie erstellt, die die Replikation unterstützt. AWS KMS Es fallen Gebühren an.
- **Wählen Sie einen vorhandenen, vom Kunden verwalteten Schlüssel** — Verwenden Sie einen Schlüssel, der sich bereits in Ihrem Konto befindet. Stellen Sie sicher, dass die Schlüsselrichtlinie die Anforderungen für Ihre Instance erfüllt. AWS KMS Es fallen Gebühren an.

Berechtigungssätze

Sie können sich dafür entscheiden, Berechtigungssätze zu aktivieren, sodass Sie AWS-Konto den Zugriff für Benutzer und Gruppen verwalten können. Dies kann nicht deaktiviert werden, sobald es aktiviert ist.

Zusätzliche Regionen

Fügen Sie Regionen für Resilienz AWS-Konto und Anwendungszugriff hinzu. Der vom Kunden verwaltete AWS KMS Schlüssel muss auch in der ausgewählten Region verfügbar sein.

Anweisungen zum Aktivieren einer Organisationsinstanz finden Sie unter [IAM Identity Center aktivieren](#). Weitere Informationen zur Unterstützung mehrerer Regionen finden Sie unter [Verwenden von IAM Identity Center für mehrere AWS-Regionen](#).

Konto-Instances von IAM Identity Center.

Mit einer Kontoinstanz von IAM Identity Center können Sie unterstützte AWS verwaltete Anwendungen und vom OIDC-based Kunden verwaltete Anwendungen bereitstellen. Account-Instances unterstützen isolierte Bereitstellungen von Anwendungen in einer einzigen AWS-Konto Instanz und nutzen dabei die Funktionen des IAM Identity Center für Mitarbeiteridentität und Zugriff auf das Portal.

Kontoinstanzen sind an eine einzige Instanz gebunden AWS-Konto und werden nur zur Verwaltung des Benutzer- und Gruppenzugriffs für unterstützte Anwendungen im selben Konto und verwendet. AWS-Region Sie sind auf eine Kontoinstanz pro beschränkt AWS-Konto. Sie können eine Kontoinstanz mithilfe einer der folgenden Optionen erstellen: ein Mitgliedskonto in AWS Organizations oder ein eigenständiges Konto AWS-Konto , das nicht von verwaltet wird AWS Organizations.

Anweisungen zum Aktivieren einer Kontoinstanz von IAM Identity Center finden Sie unter [Um eine Instanz von IAM Identity Center zu aktivieren](#) und wählen Sie die Registerkarte Konto aus.

Wann sollte eine Kontoinstanz verwendet werden

In den meisten Fällen wird eine [Organisationsinstanz](#) empfohlen. Verwenden Sie Kontoinstanzen nur, wenn eines der folgenden Szenarien zutrifft:

- Sie möchten eine temporäre Testversion einer unterstützten AWS verwalteten Anwendung ausführen, um festzustellen, ob die Anwendung Ihren Geschäftsanforderungen entspricht.
- Sie haben nicht vor, IAM Identity Center in Ihrem Unternehmen einzuführen, aber Sie möchten eine oder mehrere AWS verwaltete Anwendungen unterstützen.
- Sie haben eine Organisationsinstanz von IAM Identity Center, möchten aber eine unterstützte AWS verwaltete Anwendung für eine isolierte Gruppe von Benutzern bereitstellen, die sich von den Benutzern in Ihrer Organisationsinstanz unterscheiden.
- Sie kontrollieren nicht die AWS Organisation, in der Sie tätig sind. Beispielsweise kontrolliert ein Drittanbieter die AWS Organisation, die Ihre verwaltet AWS-Konten.

Important

Wenn Sie IAM Identity Center verwenden möchten, um Anwendungen in mehreren Konten zu unterstützen, verwenden Sie eine Organisationsinstanz. Kontoinstanzen unterstützen diesen Anwendungsfall nicht.

AWS verwaltete Anwendungen, die Kontoinstanzen unterstützen

Unter erfahren [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#) Sie, welche AWS verwalteten Anwendungen Kontoinstanzen von IAM Identity Center unterstützen. Prüfen Sie, ob die Erstellung von Kontoinstanzen mit Ihrer AWS verwalteten Anwendung möglich ist.

Verfügbarkeitsbeschränkungen für Mitgliedskonten

Um Kontoinstanzen von IAM Identity Center in AWS Organizations Mitgliedskonten bereitzustellen, muss eine der folgenden Bedingungen erfüllt sein:

- In Ihrer Organisation gibt es keine Organisationsinstanz von IAM Identity Center.
- In Ihrer Organisation gibt es eine Organisationsinstanz von IAM Identity Center, und der Instanzadministrator erlaubt die Erstellung von Kontoinstanzen von IAM Identity Center (für Organisationsinstanzen, die nach dem 15. November 2023 erstellt wurden).
- In Ihrer Organisation gibt es eine Organisationsinstanz von IAM Identity Center, und der Instanzadministrator hat die Erstellung von Kontoinstanzen durch Mitgliedskonten in der Organisation manuell aktiviert (für Organisationsinstanzen, die vor dem 15. November 2023 erstellt wurden). Detaillierte Anweisungen finden Sie unter [Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten](#).

Nachdem eine der oben genannten Bedingungen erfüllt ist, müssen alle folgenden Bedingungen erfüllt sein:

- Ihr Administrator hat keine [Service Control-Richtlinie erstellt](#), die verhindert, dass Mitgliedskonten Kontoinstanzen erstellen.
- Sie haben noch keine Instanz von IAM Identity Center in demselben Konto, unabhängig davon AWS-Region.
- Sie arbeiten in einem Land, in AWS-Region dem IAM Identity Center verfügbar ist. Informationen zu Regionen finden Sie unter [Datenspeicher und -betrieb in der IAM Identity Center-Region](#).

Überlegungen zur Kontoinstanz

Eine Kontoinstanz ist für spezielle Anwendungsfälle konzipiert und bietet eine Teilmenge von Funktionen, die einer Organisationsinstanz zur Verfügung stehen. Beachten Sie Folgendes, bevor Sie eine Kontoinstanz erstellen:

- Kontoinstanzen unterstützen keine Berechtigungssätze und unterstützen daher keinen Zugriff auf AWS-Konten.
- Sie können eine Kontoinstanz nicht in eine Organisationsinstanz konvertieren oder zusammenführen.
- Nur ausgewählte [AWS verwaltete Anwendungen](#) unterstützen Kontoinstanzen.

- Verwenden Sie Kontoinstanzen für isolierte Benutzer, die Anwendungen nur in einem einzigen Konto und für die gesamte Lebensdauer der verwendeten Anwendungen verwenden.
- Anwendungen, die an eine Kontoinstanz angehängt sind, müssen mit der Kontoinstanz verknüpft bleiben, bis Sie die Anwendung und ihre Ressourcen löschen.
- Eine Kontoinstanz muss dort verbleiben AWS-Konto , wo sie erstellt wurde.

Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten

Wenn Sie IAM Identity Center vor dem 15. November 2023 aktiviert haben, verfügen Sie über eine [Organisationsinstanz](#) von IAM Identity Center, bei der Mitgliedskonten die Möglichkeit, Kontoinstanzen zu erstellen, standardmäßig deaktiviert ist. Sie können wählen, ob Ihre Mitgliedskonten Kontoinstanzen erstellen können, indem Sie die Kontoinstanzfunktion in der IAM Identity Center-Konsole aktivieren.

Um die Erstellung von Kontoinstanzen durch Mitgliedskonten in Ihrer Organisation zu ermöglichen

Important

Das Aktivieren von Kontoinstanzen von IAM Identity Center für Mitgliedskonten ist ein einmaliger Vorgang. Das bedeutet, dass dieser Vorgang nicht rückgängig gemacht werden kann. Nach der Aktivierung können Sie die Erstellung von Kontoinstanzen einschränken, indem Sie eine Service Control Policy (SCP) erstellen. Anweisungen finden Sie unter [Steuern Sie die Erstellung von Kontoinstanzen mit Services Control-Richtlinien](#).

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie **Einstellungen** und dann die Registerkarte **Verwaltung**.
3. Wählen Sie im Abschnitt **Kontoinstanzen** von IAM Identity Center die Option **Kontoinstanzen von IAM Identity Center aktivieren** aus.
4. Bestätigen Sie im Dialogfeld „Kontoinstanzen von IAM Identity Center aktivieren“, dass Sie Mitgliedskonten in Ihrer Organisation die Erstellung von Kontoinstanzen ermöglichen möchten, indem Sie auf **Aktivieren** klicken.

Verwenden Sie Service Control-Richtlinien, um die Erstellung von Kontoinstanzen zu steuern

Die Fähigkeit von Mitgliedskonten, Kontoinstanzen zu erstellen, hängt davon ab, wann Sie IAM Identity Center aktiviert haben:

- Vor November 2023 — Sie müssen die Erstellung von Kontoinstanzen in [Mitgliedskonten](#) zulassen. Diese Aktion kann nicht rückgängig gemacht werden.
- Nach dem 15. November 2023 können Mitgliedskonten standardmäßig Kontoinstanzen erstellen.

In beiden Fällen können Sie Service Control Policies (SCPs) verwenden, um:

- Verhindern Sie, dass alle Mitgliedskonten Kontoinstanzen erstellen.
- Erlauben Sie nur bestimmten Mitgliedskonten, Kontoinstanzen zu erstellen.

Kontoinstanzen verhindern

Verwenden Sie das folgende Verfahren, um einen SCP zu generieren, der verhindert, dass Mitgliedskonten Kontoinstanzen von IAM Identity Center erstellen.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie auf dem Dashboard im Abschnitt Zentrale Verwaltung die Schaltfläche Kontoinstanzen verhindern.
3. Im Dialogfeld SCP anhängen, um die Erstellung neuer Kontoinstanzen zu verhindern, wird ein SCP für Sie bereitgestellt. Kopieren Sie den SCP und wählen Sie die Schaltfläche Gehe zum SCP-Dashboard. Sie werden zur [AWS Organizations Konsole weitergeleitet, um den SCP](#) zu erstellen oder ihn als Anweisung an einen vorhandenen SCP anzuhängen. SCPs sind eine Funktion von. AWS Organizations Anweisungen zum Anhängen eines SCP finden Sie im Benutzerhandbuch unter [Anhängen und Trennen von Service Control-Richtlinien](#). AWS Organizations

Kontoinstanzen einschränken

Anstatt die gesamte Erstellung von Kontoinstanzen zu verhindern, verweigert diese Richtlinie jeden Versuch, eine Kontoinstanz von IAM Identity Center für alle zu erstellen, AWS-Konten mit Ausnahme der "**<ALLOWED-ACCOUNT-ID>**" explizit im Platzhalter aufgeführten.

Example: Richtlinie zur Beschränkung der Kontoinstanzerstellung ablehnen

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberAccountInstances",
      "Effect": "Deny",
      "Action": "sso:CreateInstance",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
        }
      }
    }
  ]
}
```

- Ersetzen Sie ["<ALLOWED-ACCOUNT-ID>"] durch die tatsächlichen AWS-Konto IDs, denen Sie die Erstellung einer Kontoinstanz von IAM Identity Center erlauben möchten.
- Sie können mehrere zulässige Konto-IDs im Array-Format auflisten: ["111122223333", "444455556666"].
- Hängen Sie diese Richtlinie an den SCP Ihres Unternehmens an, um die zentrale Kontrolle über die Erstellung von IAM Identity Center-Kontoinstanzen durchzusetzen.

Anweisungen zum Anhängen eines SCP finden Sie im Benutzerhandbuch unter [Anhängen und Trennen von Service Control-Richtlinien](#). AWS Organizations

Löschen Sie Ihre IAM Identity Center-Instanz

Wenn eine IAM Identity Center-Instanz gelöscht wird, werden alle Daten in dieser Instanz gelöscht und können nicht wiederhergestellt werden. In der folgenden Tabelle wird anhand des in IAM Identity Center konfigurierten Verzeichnistyps beschrieben, welche Daten gelöscht werden.

Welche Daten werden gelöscht	Verbundenes Verzeichnis — AWS Managed Microsoft AD, AD Connector oder externer Identitätsanbieter	IAM Identity Center-Identitätsspeicher	
Alle Berechtigungsätze, für die Sie konfiguriert haben AWS-Konten	☑Ja	☑Ja	
Alle Anwendungen, die Sie in IAM Identity Center konfiguriert haben	☑Ja	☑Ja	
Alle Benutzerzuweisungen AWS-Konten und Anwendungen, für die Sie konfiguriert haben	☑Ja	☑Ja	
Alle Benutzer und Gruppen im Verzeichnis oder Store	N/A	☑Ja	

Wenn Sie Ihre IAM Identity Center-Instanz in zusätzliche Regionen repliziert haben, müssen Sie diese Regionen entfernen, bevor Sie die Instanz löschen.

Gehen Sie wie folgt vor, um Ihre IAM Identity Center-Instanz zu löschen.

So löschen Sie Ihre IAM Identity Center-Instanz

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Verwaltung“.

4. Wählen Sie im Abschnitt IAM Identity Center-Konfiguration löschen die Option Löschen aus.
5. Markieren Sie im Dialogfeld „IAM Identity Center-Konfiguration löschen“ jedes Kontrollkästchen, um zu bestätigen, dass Sie damit einverstanden sind, dass Ihre Daten gelöscht werden. Geben Sie Ihre IAM Identity Center-Instanz in das Textfeld ein und wählen Sie dann Bestätigen.

IAM Identity Center aktivieren

Wenn Sie IAM Identity Center aktivieren, wählen Sie einen AWS IAM Identity Center Instanztyp aus, den Sie aktivieren möchten. Eine Instanz eines Dienstes ist eine einzelne Bereitstellung eines Dienstes in Ihrer AWS Umgebung. Für IAM Identity Center sind zwei Arten von Instanzen verfügbar: Organisationsinstanzen und Kontoinstanzen. Die Instanztypen, die Sie aktivieren können, hängen vom Kontotyp ab, bei dem Sie angemeldet sind.

In der folgenden Liste sind die Typen von IAM Identity Center-Instanzen aufgeführt, die Sie für jeden Typ von aktivieren können: AWS-Konto

- Ihr AWS Organizations Verwaltungskonto (empfohlen) — Erforderlich, um eine [Organisationsinstanz](#) von IAM Identity Center zu erstellen. Verwenden Sie eine Organisationsinstanz für Berechtigungen und Anwendungszuweisungen für mehrere Konten in der gesamten Organisation. Sie können diesen Instanztyp auf weitere Regionen replizieren, um die Stabilität des Kontozugriffs zu erhöhen und die Flexibilität bei der Auswahl der AWS Anwendungsbereitstellungsregionen zu erhöhen.
- Ihr AWS Organizations Mitgliedskonto — Wird verwendet, um eine [Kontoinstanz](#) von IAM Identity Center zu erstellen, um Anwendungszuweisungen innerhalb dieses Mitgliedskontos zu ermöglichen. In einer Organisation können ein oder mehrere Konten mit einer Instanz auf Mitgliedsebene existieren.
- Eine eigenständige Instanz AWS-Konto — Wird verwendet, um eine [Organisations](#) - oder [Kontoinstanz](#) von IAM Identity Center zu erstellen. Die eigenständige Version AWS-Konto wird nicht von AWS Organizations verwaltet. Sie können einem eigenständigen Gerät nur eine Instanz von IAM Identity Center zuordnen AWS-Konto und diese Instanz für Anwendungszuweisungen innerhalb dieses AWS-Konto Standalone-Geräts verwenden.

Important

Das Organisationsverwaltungskonto kann mithilfe einer Service Control-Richtlinie steuern, ob Mitgliedskonten der [Organisation Kontoinstanzen](#) von IAM Identity Center erstellen können. Wenn Sie ein kostenloses Kontingent verwenden, wird Ihr Konto beim Erstellen einer AWS Organisation automatisch auf einen kostenpflichtigen Tarif mit nutzungsbasierter Bezahlung aktualisiert. Ihre Gutscheine für das kostenlose Kontingent laufen sofort ab.

Weitere Informationen finden Sie unter Häufig gestellte Fragen zum [AWS kostenlosen Kontingent](#).

Einen Vergleich der verschiedenen Funktionen der verschiedenen Instance-Typen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Bevor Sie IAM Identity Center aktivieren, empfehlen wir Ihnen, das [Voraussetzungen und Überlegungen zu IAM Identity Center](#) zu überprüfen.

Um eine Instanz von IAM Identity Center zu aktivieren

Wählen Sie die Registerkarte für den Typ der IAM Identity Center-Instanz, die Sie aktivieren möchten, entweder eine Organisations- oder Kontoinstanz:

Organization (recommended)

1. Gehen Sie wie folgt vor, um sich bei der AWS-Managementkonsole anzumelden.
 - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Wird bereits AWS mit einem Standalone-Gerät verwendet AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
 - Bereits verwendet AWS Organizations (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren Anmeldedaten für das Verwaltungskonto an.
2. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
3. Dieser Schritt gilt nur für diejenigen, [AWS-Regionen die standardmäßig](#) aktiviert sind. Wenn Sie IAM Identity Center in einer anderen Region aktivieren, fahren Sie mit Schritt 4 fort.

Wählen Sie unter Instanzkonfiguration eine der folgenden Optionen aus:

- Single-Region Instanz — Ihre Instanz wird in der aktuellen Region erstellt.
- Multi-Region instance — Ihre Instance wird in der aktuellen Region erstellt und für Resilienz AWS-Konto und Anwendungszugriff in eine weitere Region repliziert. Zur Unterstützung mehrerer Regionen wird automatisch ein vom Kunden verwalteter KMS-Schlüssel für mehrere Regionen erstellt. AWS KMS Es fallen Gebühren an.

- Benutzerdefinierte Instanz — Konfigurieren Sie Ihre Instanzeinstellungen individuell.

Weitere Informationen zu den jeweiligen Optionen finden Sie unter [Optionen für die Instanzkonfiguration](#).

Wählen Sie **Aktivieren**, um Ihre Instanz zu erstellen.

4. (Optional) Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand anstelle des standardmäßigen AWS verwalteten Schlüssels verwenden möchten, konfigurieren Sie den vom Kunden verwalteten Schlüssel im Abschnitt **Schlüssel für die Verschlüsselung von IAM Identity Center-Daten im Ruhezustand**. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).

 Important

Führen Sie diesen Schritt nur aus, wenn Sie die erforderlichen Berechtigungen für die Verwendung des kundenverwalteten KMS-Schlüssels konfiguriert haben. Ohne die richtigen Berechtigungen kann dieser Schritt fehlschlagen oder die Verwaltung von IAM Identity Center und der AWS verwalteten Anwendungen stören.

5. (Optional) Standardmäßig sind für Ihre Instance Berechtigungen für mehrere Konten aktiviert. Wenn Sie IAM Identity Center nur für die Anwendungsauthentifizierung und Benutzerverwaltung verwenden möchten, deaktivieren Sie die Option **Berechtigungen für mehrere Konten** aktivieren.

Wenn Sie sich jetzt dafür entscheiden, die Berechtigungen für mehrere Konten nicht zu aktivieren, wird der **AWS-Konten** Abschnitt nicht in der IAM Identity Center-Konsole angezeigt. IAM Identity Center stellt die serviceverknüpfte Rolle nicht für Mitgliedskonten bereit. Sie können später auf der Seite „Einstellungen“ auf der Registerkarte „Verwaltung“ die Berechtigungen für mehrere Konten aktivieren.

6. Wählen Sie unter IAM Identity Center aktivieren die Option **Aktivieren** aus.
 - Wenn Sie mit dem Verwaltungskonto einer vorhandenen Organisation angemeldet sind, beginnt IAM Identity Center mit der Aktivierung. Fahren Sie mit der Einrichtung Ihrer Umgebung fort.
 - Wenn Sie ein eigenständiges Gerät haben AWS-Konto (das nicht Teil einer Organisation ist), wird die **AWS Organizations** Seite IAM Identity Center aktivieren mit angezeigt.

Mit dieser Option wird eine neue Organisation mit Ihrem Konto als Verwaltungskonto erstellt. Überprüfen Sie die Informationen und wählen Sie „Aktivieren“, um den Vorgang abzuschließen.

 Note

AWS Organizations kann IAM Identity Center nur in einer einzigen AWS Region aktivieren. Wenn Sie nach der Aktivierung von IAM Identity Center die Region ändern müssen, in der IAM Identity Center aktiviert ist, müssen Sie [die aktuelle Instance](#) löschen und eine Instance in der anderen Region erstellen.

 Tip

Wenn Sie ein eigenständiges Konto haben und eine Kontoinstanz anstelle einer Organisationsinstanz erstellen möchten, finden Sie weitere Informationen auf der Registerkarte **Konto**.

Nach der Aktivierung Ihrer Organisationsinstanz empfehlen wir Ihnen, die folgenden Schritte auszuführen, um die Einrichtung Ihrer Umgebung abzuschließen:

- Bestätigen Sie, dass Sie die Identitätsquelle Ihrer Wahl verwenden. Wenn Ihnen bereits eine Identitätsquelle zugewiesen ist, können Sie diese weiterhin verwenden. Weitere Informationen finden Sie unter [Bestätigen Ihrer Identitätsquellen in IAM Identity Center](#).
- Registrieren Sie ein Mitgliedskonto als delegierter Administrator. Weitere Informationen finden Sie unter [Delegierte Verwaltung](#).
- IAM Identity Center bietet Ihnen ein Zugangsportal zu AWS Ressourcen. Wenn Sie den Zugriff auf bestimmte AWS Domänen oder URL-Endpunkte mithilfe einer Lösung zur Filterung von Webinhalten wie Firewalls der nächsten Generation (NGFW) oder Secure Web Gateways (SWG) filtern, finden Sie weitere Informationen unter [Aktualisieren Sie Firewalls und Gateways, um den Zugriff auf die zu ermöglichen AWS-Zugangsportal](#)

Account

1. Gehen Sie wie folgt vor, um sich bei der anzumelden AWS-Managementkonsole.

- Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Bereits verwendet AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
 - Bereits verwendet AWS Organizations (IAM-Anmeldeinformationen) — Melden Sie sich mit den Administratordaten Ihres Mitgliedskontos an.
2. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
 3. Wenn Sie neu bei IAM Identity Center sind AWS oder ein eigenständiges System haben AWS-Konto, wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren aus.

Die Seite „IAM Identity Center aktivieren mit AWS Organizations“ wird angezeigt. Dadurch wird eine Organisationsinstanz erstellt, was wir empfehlen. Wenn Sie jedoch stattdessen eine Kontoinstanz bevorzugen, wählen Sie den Link Eine Kontoinstanz von IAM Identity Center aktivieren.

4. Wenn Sie Administrator eines AWS Organizations Mitgliedskontos sind, wählen Sie unter Eine Kontoinstanz von IAM Identity Center aktivieren die Option Kontoinstanz aktivieren aus.
5. Überprüfen Sie auf der Seite Eine Kontoinstanz von IAM Identity Center aktivieren die Informationen und fügen Sie optional Tags hinzu, die Sie dieser Kontoinstanz zuordnen möchten. Wählen Sie dann Aktivieren aus, um den Vorgang abzuschließen.

 Note

Wenn Ihr AWS Konto Mitglied einer Organisation ist, können Sie möglicherweise eine Kontoinstanz von IAM Identity Center nur eingeschränkt aktivieren.

- Wenn Ihre Organisation IAM Identity Center vor dem 15. November 2023 aktiviert hat, ist die Möglichkeit für Mitgliedskonten, Kontoinstanzen zu erstellen, standardmäßig deaktiviert und muss vom Verwaltungskonto der Organisation aktiviert werden.
- Wenn Ihre Organisation IAM Identity Center nach dem 15. November 2023 aktiviert hat, ist die Möglichkeit für Mitgliedskonten, Kontoinstanzen zu erstellen, standardmäßig aktiviert. Dienststeuerungsrichtlinien können jedoch verwendet

werden, um die Erstellung von Kontoinstanzen von IAM Identity Center innerhalb einer Organisation zu verhindern.

Weitere Informationen erhalten Sie unter [the section called “Erlauben Sie die Erstellung von Kontoinstanzen in Mitgliedskonten”](#) und [the section called “SCPs für die Erstellung von Kontoinstanzen”](#).

Bestätigen Ihrer Identitätsquellen in IAM Identity Center

Ihre Identitätsquelle in IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Nachdem Sie IAM Identity Center aktiviert haben, bestätigen Sie, dass Sie die Identitätsquelle Ihrer Wahl verwenden. Wenn Sie bereits eine zugewiesene Identitätsquelle haben, können Sie diese weiterhin verwenden.

Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen IdP verwalten, empfehlen wir Ihnen, eine Verbindung mit dieser Identitätsquelle in Betracht zu ziehen, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Dies sollte geschehen, bevor Sie Benutzer und Gruppen im Identity Center-Standardverzeichnis erstellen und Zuweisungen vornehmen.

Wenn Sie bereits Benutzer und Gruppen in einer Identitätsquelle in IAM Identity Center verwalten, werden durch den Wechsel zu einer anderen Identitätsquelle möglicherweise alle Benutzer- und Gruppenzuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben. In diesem Fall verlieren alle Benutzer, einschließlich des Administratorbenutzers in IAM Identity Center, den Single-Sign-On-Zugriff auf ihre Anwendungen. Weitere Informationen finden Sie unter [Überlegungen zum Ändern Ihrer Identitätsquelle](#).

Um Ihre Identitätsquelle zu bestätigen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie auf der Dashboard-Seite unter dem Abschnitt Empfohlene Einrichtungsschritte die Option Identitätsquelle bestätigen aus. Du kannst auf diese Seite auch zugreifen, indem du Einstellungen und dann den Tab Identitätsquelle auswählst.
3. Es gibt keine Aktion, wenn Sie Ihre zugewiesene Identitätsquelle behalten möchten. Wenn Sie es vorziehen, sie zu ändern, wählen Sie Aktionen und dann Identitätsquelle ändern aus.

Sie können eine der folgenden Optionen als Identitätsquelle wählen:

Identity-Center-Verzeichnis

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Wenn Sie nicht bereits einen anderen externen Identitätsanbieter verwenden, können Sie mit der Erstellung Ihrer Benutzer und Gruppen beginnen und deren Zugriffsebene Ihren AWS-Konten und Anwendungen zuweisen. Eine Anleitung zur Verwendung dieser Identitätsquelle finden Sie unter [Benutzerzugriff mit dem Standard-IAM Identity Center-Verzeichnis konfigurieren](#).

Active Directory

Wenn Sie bereits Benutzer und Gruppen in Ihrem AWS Managed Microsoft AD Verzeichnis mit Directory Service oder in Ihrem selbstverwalteten Verzeichnis in verwalten, empfehlen wir Active Directory (AD), dass Sie dieses Verzeichnis verbinden, wenn Sie IAM Identity Center aktivieren. Erstellen Sie keine Benutzer und Gruppen im Identity Center-Standardverzeichnis. IAM Identity Center verwendet die von der bereitgestellte Verbindung, AWS Directory Service um Benutzer-, Gruppen- und Mitgliedschaftsinformationen aus Ihrem Quellverzeichnis in Active Directory mit dem IAM Identity Center-Identitätsspeicher zu synchronisieren. Weitere Informationen finden Sie unter [Microsoft AD directory](#).

Note

IAM Identity Center unterstützt SAMBA4-based Simple AD nicht als Identitätsquelle.

Externer Identitätsanbieter

Für externe Identitätsanbieter (IdPs) wie Okta oder können Sie IAM Identity Center verwenden Microsoft Entra ID, um Identitäten nach dem Standard Security Assertion Markup Language (SAML) 2.0 zu authentifizieren. IdPs Das SAML-Protokoll bietet keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Sie machen IAM Identity Center auf diese Benutzer und Gruppen aufmerksam, indem Sie sie im IAM Identity Center bereitstellen. Sie können die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen von Ihrem IAM Identity Center mithilfe des Systems for Cross-domain Identity Management (SCIM) v2.0-Protokoll durchführen, wenn Ihr IdP SCIM unterstützt. Andernfalls können Sie Ihre Benutzer und Gruppen manuell bereitstellen, indem Sie die Benutzernamen, die E-Mail-Adresse und die Gruppen manuell in IAM Identity Center eingeben.

Eine ausführliche Anleitung zum Einrichten Ihrer Identitätsquelle finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#).

 Note

Wenn Sie vorhaben, einen externen Identitätsanbieter zu verwenden, beachten Sie, dass der externe IdP und nicht das IAM Identity Center die Einstellungen für die Multifaktor-Authentifizierung (MFA) verwaltet. MFA im IAM Identity Center wird nicht für die Verwendung durch externe Identitätsanbieter unterstützt. Weitere Informationen finden Sie unter [Benutzer zur MFA auffordern](#).

 Note

Wenn Sie planen, IAM Identity Center in weitere Regionen zu replizieren, müssen Sie einen externen Identitätsanbieter oder das Identity Center-Verzeichnis als Identitätsquelle verwenden. Multi-Region Unterstützung ist für Active Directory nicht verfügbar. Weitere Informationen einschließlich der Voraussetzungen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Aktualisieren Sie Firewalls und Gateways, um den Zugriff auf die zu ermöglichen AWS-Zugangsportale

Das AWS Zugangsportal bietet Benutzern Single-Sign-On-Zugriff auf alle Ihre AWS-Konten und am häufigsten verwendeten Cloud-Anwendungen wie Office 365, Concur, Salesforce und viele mehr. Sie können schnell mehrere Anwendungen starten, indem Sie im Portal einfach auf das Symbol AWS-Konto oder Anwendung klicken.

 Note

AWS verwaltete Anwendungen lassen sich in IAM Identity Center integrieren und verwenden es für Authentifizierung und Verzeichnisdienste, verwenden das AWS Zugriffsportale jedoch möglicherweise nicht für den Anwendungszugriff.

Wenn Sie den Zugriff auf bestimmte AWS Domänen oder URL-Endpunkte mithilfe einer Lösung zur Filterung von Webinhalten wie Firewalls der nächsten Generation (NGFW) oder Secure Web Gateways (SWG) filtern, müssen Sie die Domänen und URL-Endpunkte, die dem Zugriffsportal zugeordnet sind, zulassen. AWS

Die folgende Liste enthält die IPv4- und Dual-Stack-Domains und URL-Endpunkte, die Sie zu Ihren Zulassungslisten für die Filterung von Webinhalten hinzufügen können.

Liste der IPv4-Zulassungen

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.com*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Dual-stack Liste zulassen

- *[Identity Center instance ID].portal.[Region].app.aws*
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws

- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

Kombinierte Zulassungsliste (IPv4 + Dual-stack mit Abwärtskompatibilität)

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *[Identity Centers instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- oidc.*[Region]*.api.aws
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- sso.*[Region]*.api.aws
- *.sso-portal.*[Region]*.amazonaws.com
- portal.sso.*[Region]*.api.aws
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

Überlegungen zum Zulassen von Domains und URL-Endpunkten

Zusätzlich zu den Anforderungen an die Zulassungsliste für das AWS Zugangsportal erfordern die anderen Dienste und Anwendungen, die Sie verwenden, möglicherweise die Zulassung von Domänen.

- Um von Ihrem AWS-Konten Zugriffsportal aus auf die und die IAM Identity Center-Konsole AWS zuzugreifen, müssen Sie zusätzliche Domänen auf die Zulassungsliste setzen. AWS-Managementkonsole Eine Liste der Domänen finden Sie unter [Problembehandlung](#) im Handbuch AWS-Managementkonsole Erste Schritte. AWS-Managementkonsole
- Um von Ihrem Access-Portal aus auf AWS verwaltete Anwendungen AWS zugreifen zu können, müssen Sie die entsprechenden Domänen zulassen. Eine Anleitung finden Sie in der jeweiligen Servicedokumentation.
- Wenn Sie externe Software verwenden, z. B. externe Software IdPs (z. B. Okta und Microsoft Entra ID), müssen Sie deren Domains in Ihre Zulassungslisten aufnehmen.

Tutorials zu Identitätsquellen im IAM Identity Center

Sie können Ihre bestehende Identitätsquelle in Ihrem AWS Organizations Verwaltungskonto mit [einer Organisationsinstanz von IAM Identity Center](#) verbinden. Wenn Sie noch keinen Identitätsanbieter haben, können Sie Benutzer direkt im standardmäßigen IAM Identity Center-Verzeichnis erstellen und verwalten. Sie können eine Identitätsquelle pro Organisation haben.

In den Tutorials in diesem Abschnitt wird beschrieben, wie Sie eine Organisationsinstanz von IAM Identity Center mit einer häufig verwendeten Identitätsquelle einrichten, einen Administratorbenutzer erstellen und ob Sie IAM Identity Center verwenden, um den Zugriff zu verwalten AWS-Konten, Berechtigungssätze zu erstellen und zu konfigurieren. Wenn Sie IAM Identity Center nur für den Anwendungszugriff verwenden, müssen Sie keine Berechtigungssätze verwenden.

In diesen Tutorials wird nicht beschrieben, wie Kontoinstanzen von IAM Identity Center eingerichtet werden. Sie können Kontoinstanzen verwenden, um Benutzern und Gruppen Anwendungen zuzuweisen, aber Sie können diesen Instanztyp nicht verwenden, um den Benutzerzugriff auf diese zu AWS-Konten zu verwalten. Weitere Informationen finden Sie unter [Konto-Instances von IAM Identity Center](#).

Note

Bevor Sie mit einem dieser Tutorials beginnen, aktivieren Sie IAM Identity Center. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).

Themen

- [Verwenden von Active Directory als Identitätsquelle](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [Konfigurieren Sie SAML und SCIM mit Google Workspace und IAM Identity Center](#)
- [Verwenden von IAM Identity Center für die Verbindung mit Ihrer JumpCloud Verzeichnisplattform](#)
- [Konfigurieren Sie SAML und SCIM mit Microsoft Entra ID und IAM Identity Center](#)
- [Konfigurieren Sie SAML und SCIM mit Okta und IAM Identity Center](#)
- [Einrichtung der SCIM-Bereitstellung zwischen OneLogin und IAM Identity Center](#)
- [Ping IdentityProdukte mit IAM Identity Center verwenden](#)

- [Benutzerzugriff mit dem Standard-IAM Identity Center-Verzeichnis konfigurieren](#)
- [Video-Tutorials](#)

Verwenden von Active Directory als Identitätsquelle

Wenn Sie Benutzer in Ihrem AWS Managed Microsoft AD Verzeichnis mithilfe von Active Directory (AD) Directory Service oder Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) verwalten, können Sie Ihre IAM Identity Center-Identitätsquelle so ändern, dass sie mit diesen Benutzern funktioniert. Wir empfehlen Ihnen, eine Verbindung zu dieser Identitätsquelle in Betracht zu ziehen, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Wenn Sie dies tun, bevor Sie Benutzer und Gruppen im standardmäßigen Identity Center-Verzeichnis erstellen, können Sie die zusätzliche Konfiguration vermeiden, die erforderlich ist, wenn Sie Ihre Identitätsquelle später ändern.

Um Active Directory als Identitätsquelle verwenden zu können, muss Ihre Konfiguration die folgenden Voraussetzungen erfüllen:

- Wenn Sie IAM Identity Center verwenden AWS Managed Microsoft AD, müssen Sie es dort aktivieren AWS-Region , wo Ihr AWS Managed Microsoft AD Verzeichnis eingerichtet ist. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der IAM Identity Center konfiguriert ist. Beachten Sie außerdem, dass das AWS Zugriffsportal dieselbe Zugriffs-URL wie Ihr Verzeichnis verwendet.
- Verwenden Sie ein Active Directory, das sich im Verwaltungskonto befindet:

Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis eingerichtet haben AWS Directory Service, und es muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können jeweils nur ein AD Connector Connector-Verzeichnis oder ein Verzeichnis verbinden. AWS Managed Microsoft AD Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie unter:

- [Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#)
- [Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect](#)
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

Wenn Sie planen, einen delegierten IAM Identity Center-Administrator zu aktivieren und Active Directory als Ihre IAM Identity Center-Identitätsquelle zu verwenden, können Sie einen

vorhandenen AD Connector oder ein Verzeichnis verwenden, das im AWS Managed Microsoft AD Verzeichnis eingerichtet ist und sich im AWS delegierten Administratorkonto befindet.

Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle in Active Directory zu ändern oder sie von Active Directory in eine andere Quelle zu ändern, muss sich das Verzeichnis in dem delegierten IAM Identity Center-Administrator-Mitgliedskonto befinden (diesem gehören), falls eines existiert; andernfalls muss es sich im Verwaltungskonto befinden.

Dieses Tutorial führt Sie durch die grundlegenden Einstellungen für die Verwendung von Active Directory als IAM Identity Center-Identitätsquelle.

Schritt 1: Active Directory Connect und einen Benutzer angeben

Wenn Sie Active Directory bereits verwenden, helfen Ihnen die folgenden Themen bei der Vorbereitung der Verbindung Ihres Verzeichnisses mit IAM Identity Center.

Note

Wenn Sie beabsichtigen, ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory zu verbinden und Sie RADIUS MFA nicht mit verwenden AWS Directory Service, aktivieren Sie MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unter [Microsoft AD directory](#)
2. Führen Sie die Schritte unter [Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#) aus.
3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter [Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center](#).

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unter [Microsoft AD directory](#).
2. Führen Sie die Schritte unter [Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect](#) aus.

3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter [Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center](#).

Schritt 2: Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center

Nachdem Sie Ihr Verzeichnis mit IAM Identity Center verbunden haben, können Sie einen Benutzer angeben, dem Sie Administratorrechte gewähren möchten, und diesen Benutzer dann aus Ihrem Verzeichnis mit IAM Identity Center synchronisieren.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, klicken Sie auf „Aktionen“ und anschließend auf „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Gehen Sie unter Hinzugefügte Benutzer und Gruppen wie folgt vor:
 - a. Vergewissern Sie sich, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, angegeben ist.
 - b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.
 - c. Wählen Sie Absenden aus.
7. Auf der Seite „Synchronisation verwalten“ wird der von Ihnen angegebene Benutzer in der Liste „Synchronisierte Benutzer“ angezeigt.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf der Seite Benutzer kann es einige Zeit dauern, bis der von Ihnen angegebene Benutzer in der Liste erscheint. Wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

Zu diesem Zeitpunkt hat Ihr Benutzer keinen Zugriff auf das Verwaltungskonto. Sie richten den Administratorzugriff auf dieses Konto ein, indem Sie einen Administratorberechtigungssatz erstellen und den Benutzer diesem Berechtigungssatz zuweisen. Weitere Informationen finden Sie unter [Erstellen Sie einen Berechtigungssatz](#).

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen aus dem CyberArk Directory Platform IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu lesen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#) Lesen Sie dann im nächsten Abschnitt weitere Überlegungen durch.

Themen

- [Voraussetzungen](#)
- [Überlegungen zu SCIM](#)
- [Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center](#)
- [Schritt 2: Konfigurieren Sie die Bereitstellung in CyberArk](#)
- [\(Optional\) Schritt 3: Konfigurieren Sie Benutzerattribute CyberArk für die Zugriffskontrolle \(ABAC\) im IAM Identity Center](#)
- [\(Optional\) Übergabe von Attributen für die Zugriffskontrolle](#)

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- CyberArkAbonnement oder kostenlose Testversion. Um sich für eine kostenlose Testversion anzumelden, besuchen Sie uns [CyberArk](#).
- Ein IAM Identity Center-fähiges Konto ([kostenlos](#)). Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
- Eine SAML-Verbindung von Ihrem CyberArk Konto zum IAM Identity Center, wie in der [CyberArkDokumentation für IAM Identity Center](#) beschrieben.
- Ordnen Sie den IAM Identity Center-Connector den Rollen, Benutzern und Organisationen zu, denen Sie Zugriff gewähren möchten. AWS-Konten

Überlegungen zu SCIM

Bei der Verwendung von CyberArk Federation für IAM Identity Center sollten Sie Folgendes beachten:

- Nur Rollen, die im Abschnitt Anwendungsbereitstellung zugeordnet sind, werden mit IAM Identity Center synchronisiert.
- Das Provisioning-Skript wird nur in seinem Standardstatus unterstützt. Sobald es geändert wurde, schlägt das SCIM-Provisioning möglicherweise fehl.
 - Es kann nur ein Telefonnummernattribut synchronisiert werden, und die Standardeinstellung ist „Geschäftstelefon“.
- Wenn die Rollenzuweisung in der CyberArk IAM Identity Center-Anwendung geändert wird, wird das folgende Verhalten erwartet:
 - Wenn die Rollennamen geändert werden — keine Änderungen an den Gruppennamen in IAM Identity Center.
 - Wenn die Gruppennamen geändert werden, werden neue Gruppen in IAM Identity Center erstellt. Alte Gruppen bleiben bestehen, haben aber keine Mitglieder.
- Das Benutzersynchronisierungs- und Deprovisionierungsverhalten kann in der CyberArk IAM Identity Center-Anwendung eingerichtet werden. Stellen Sie sicher, dass Sie das richtige Verhalten für Ihre Organisation einrichten. Dies sind die Optionen, die Ihnen zur Verfügung stehen:
 - Benutzer im Identity Center-Verzeichnis mit demselben Prinzipalnamen überschreiben (oder nicht).
 - Heben Sie die Benutzerbereitstellung für IAM Identity Center auf, wenn der Benutzer aus der Rolle entfernt wird. CyberArk
 - Benutzerverhalten aufheben — deaktivieren oder löschen.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung zu aktivieren.

Um die automatische Bereitstellung in IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.

3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpunkt — Zum Beispiel `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mithilfe der CyberArk IAM Identity Center-Anwendung ausführen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren Sie die Bereitstellung in CyberArk

Verwenden Sie das folgende Verfahren in der CyberArk IAM Identity Center-Anwendung, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die CyberArk IAM Identity Center-Anwendung bereits zu Ihrer CyberArk Admin-Konsole unter Web Apps hinzugefügt haben. Falls Sie dies noch nicht getan haben, lesen Sie unter und führen Sie dann dieses Verfahren aus [Voraussetzungen](#), um die SCIM-Bereitstellung zu konfigurieren.

So konfigurieren Sie die Bereitstellung in CyberArk

1. Öffnen Sie die CyberArk IAM Identity Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für hinzugefügt haben CyberArk (Apps > Web-App). Siehe [Voraussetzungen](#).

2. Wählen Sie die IAM Identity Center-Anwendung aus und gehen Sie zum Abschnitt Provisioning.
3. Markieren Sie das Kästchen „Bereitstellung für diese Anwendung aktivieren“ und wählen Sie „Live-Modus“.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert aus dem IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Dienst-URL ein und legen Sie in der CyberArk IAM Identity Center-Anwendung den Autorisierungstyp auf Authorization Header fest.
5. Stellen Sie den Header-Typ auf Bearer-Token ein.
6. Aus dem vorherigen Verfahren haben Sie den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Bearer-Token in der CyberArk IAM Identity Center-Anwendung ein.
7. Klicken Sie auf Überprüfen, um die Konfiguration zu testen und anzuwenden.
8. Wählen Sie unter den Synchronisierungsoptionen das Verhalten aus, für das die ausgehende Bereitstellung funktionieren CyberArk soll. Sie können festlegen, ob bestehende IAM Identity Center-Benutzer mit einem ähnlichen Prinzipalnamen überschrieben (oder nicht) und wie die Bereitstellung aufgehoben werden soll.
9. Richten Sie unter Rollenzuordnung die Zuordnung von CyberArk Rollen im Feld Name zur IAM Identity Center-Gruppe unter Zielgruppe ein.
10. Wenn Sie fertig sind, klicken Sie unten auf Speichern.
11. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von CyberArk werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt Konten zugewiesen werden und können sich innerhalb von IAM Identity Center verbinden.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute CyberArk für die Zugriffskontrolle (ABAC) im IAM Identity Center

Dies ist ein optionales Verfahren für den Fall CyberArk, dass Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre Ressourcen zu verwalten. AWS Die Attribute, die Sie definieren, CyberArk werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, die Sie übergeben haben. CyberArk

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die [Attribute für Zugriffskontrolle](#) Funktion aktivieren. Weitere Information dazu finden Sie unter [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#).

Um Benutzerattribute CyberArk für die Zugriffskontrolle im IAM Identity Center zu konfigurieren

1. Öffnen Sie die CyberArk IAM Identity Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben CyberArk (Apps > Web-Apps).
2. Gehen Sie zur Option SAML Response.
3. Fügen Sie unter Attribute die relevanten Attribute zur Tabelle hinzu. Folgen Sie dabei der folgenden Logik:
 - a. Attributname ist der ursprüngliche Attributname von CyberArk.
 - b. Attributwert ist der Attributname, der in der SAML-Assertion an IAM Identity Center gesendet wird.
4. Wählen Sie Speichern.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das AttributeValue-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Konfigurieren Sie SAML und SCIM mit Google WorkSpace und IAM Identity Center

Wenn Ihre Organisation es verwendet, können Google Workspace Sie Ihre Benutzer Google Workspace in das IAM Identity Center integrieren, um ihnen Zugriff auf Ressourcen zu AWS gewähren. Sie können diese Integration erreichen, indem Sie Ihre IAM Identity Center-Identitätsquelle von der standardmäßigen IAM Identity Center-Identitätsquelle in ändern. Google Workspace

Note

Google Workspaceunterstützt derzeit keine SAML-URLs (Multiple Assertion Consumer Service, ACS) in der Anwendung. AWS IAM Identity Center Diese SAML-Funktion ist erforderlich, um die Unterstützung [mehrerer Regionen in IAM Identity Center](#) in vollem Umfang nutzen zu können. Wenn Sie planen, IAM Identity Center in weitere Regionen zu replizieren, beachten Sie, dass die Verwendung einer einzigen ACS-URL die Benutzererfahrung in diesen zusätzlichen Regionen beeinträchtigen kann. Ihre Hauptregion wird weiterhin normal funktionieren. Wir empfehlen Ihnen, mit Ihrem IdP-Anbieter zusammenzuarbeiten, um diese Funktion zu aktivieren. Weitere Informationen zur Benutzererfahrung in weiteren Regionen mit einer einzigen ACS-URL finden Sie unter [the section called “Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs”](#) und [the section called “AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu”](#).

Benutzerinformationen von Google Workspace werden mithilfe des SCIM 2.0-Protokolls ([System for Cross-domain Identity Management](#)) mit dem IAM Identity Center synchronisiert. Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Sie konfigurieren diese Verbindung, Google Workspace indem Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein IAM Identity Center-Inhaber-Token verwenden. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Google Workspace zu den benannten Attributen in IAM Identity Center. Diese Zuordnung entspricht den erwarteten Benutzerattributen zwischen IAM Identity Center und. Google Workspace Dazu müssen Sie sich Google Workspace als Identitätsanbieter einrichten und eine Verbindung zu Ihrem IAM Identity Center herstellen.

Zielsetzung

Die Schritte in diesem Tutorial helfen Ihnen beim Herstellen der SAML-Verbindung zwischen Google Workspace und AWS. Später werden Sie Benutzer synchronisieren, die SCIM Google Workspace verwenden. Um zu überprüfen, ob alles korrekt konfiguriert ist, melden Sie sich nach Abschluss der Konfigurationsschritte als Google Workspace Benutzer an und überprüfen den Zugriff AWS auf Ressourcen. Beachten Sie, dass dieses Tutorial auf einer Testumgebung für kleine Google Workspace Verzeichnisse basiert. Verzeichnisstrukturen wie Gruppen und Organisationseinheiten sind in diesem Tutorial nicht enthalten. Nach Abschluss dieses Tutorials können Ihre Benutzer mit Ihren Google Workspace Anmeldeinformationen AWS auf das Zugangsportal zugreifen.

Note

Google WorkspaceBesuchen [Google Workspace](#) Sie die Google's Website, um sich für eine kostenlose Testversion von anzumelden.

Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter [IAM Identity Center aktivieren](#).

Überlegungen

- Bevor Sie die SCIM-Bereitstellung zwischen Google Workspace und IAM Identity Center konfigurieren, empfehlen wir Ihnen, dies zunächst zu überprüfen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#)
- Die automatische SCIM-Synchronisierung von Google Workspace ist derzeit auf die Benutzerbereitstellung beschränkt. Die automatische Gruppenbereitstellung wird derzeit nicht unterstützt. Gruppen können manuell mit dem AWS CLI Identity [Store-Befehl](#) create-group oder der AWS Identity and Access Management (IAM) -API erstellt werden. [CreateGroup](#) Alternativ können Sie [ssosync verwenden](#), um Google Workspace Benutzer und Gruppen mit IAM Identity Center zu synchronisieren.
- Für jeden Google Workspace Benutzer müssen ein Wert für Vorname, Nachname, Benutzername und Anzeigename angegeben werden.
- Jeder Google Workspace Benutzer hat nur einen einzigen Wert pro Datenattribut, z. B. E-Mail-Adresse oder Telefonnummer. Alle Benutzer, die mehrere Werte haben, können nicht synchronisiert werden. Wenn es Benutzer gibt, deren Attribute mehrere Werte enthalten, entfernen Sie die doppelten Attribute, bevor Sie versuchen, den Benutzer im IAM Identity Center bereitzustellen. Beispielsweise kann nur ein Telefonnummernattribut synchronisiert werden, da das Standard-Telefonnummernattribut „Geschäftstelefon“ ist. Verwenden Sie das Attribut

„Geschäftstelefon“, um die Telefonnummer des Benutzers zu speichern, auch wenn es sich bei der Telefonnummer des Benutzers um eine Festnetznummer oder ein Mobiltelefon handelt.

- Attribute werden weiterhin synchronisiert, wenn der Benutzer im IAM Identity Center deaktiviert, aber immer noch aktiv in Google Workspace IAM Identity Center ist.
- Wenn im Identity Center-Verzeichnis ein Benutzer mit demselben Benutzernamen und derselben E-Mail-Adresse vorhanden ist, wird der Benutzer überschrieben und mithilfe von SCIM von synchronisiert. Google Workspace
- Beim Ändern Ihrer Identitätsquelle sind weitere Überlegungen zu berücksichtigen. Weitere Informationen finden Sie unter [the section called “Wechsel von IAM Identity Center zu einem externen IdP”](#).

Schritt 1: Google WorkSpace: Konfigurieren Sie die SAML-Anwendung

1. Melden Sie sich mit einem Konto mit Google Superadministratorrechten bei Ihrer Admin-Konsole an.
2. Wählen Sie im linken Navigationsbereich Ihrer Google Admin-Konsole Apps und dann Web- und Mobil-Apps aus.
3. Wählen Sie in der Dropdownliste App hinzufügen die Option Nach Apps suchen aus.
4. Geben Sie in das Suchfeld Amazon Web Services ein und wählen Sie dann die Amazon Web Services (SAML) -App aus der Liste aus.
5. Auf der Seite Google Identity Provider-Details — Amazon Web Services können Sie eine der folgenden Aktionen ausführen:
 - a. Laden Sie die IdP-Metadaten herunter.
 - b. Kopieren Sie die SSO-URL, die Entitäts-ID-URL und die Zertifikatsinformationen.

Sie benötigen entweder die XML-Datei oder die URL-Informationen in Schritt 2.

6. Lassen Sie diese Seite geöffnet und wechseln Sie zur IAM Identity Center-Konsole, bevor Sie mit dem nächsten Schritt in der Google Admin-Konsole fortfahren.

Schritt 2: IAM Identity Center und Google WorkSpace: Ändern Sie die IAM Identity Center-Identitätsquelle und richten Sie sie ein Google WorkSpace als SAML-Identitätsanbieter

1. Melden Sie sich mit einer Rolle mit Administratorrechten bei der [IAM Identity Center-Konsole](#) an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Option „Aktionen“ und dann „Identitätsquelle ändern“ aus.
 - Wenn Sie IAM Identity Center nicht aktiviert haben, finden Sie [IAM Identity Center aktivieren](#) weitere Informationen unter. Nachdem Sie IAM Identity Center zum ersten Mal aktiviert und darauf zugegriffen haben, gelangen Sie zum Dashboard, in dem Sie Wählen Sie Ihre Identitätsquelle aus.
4. Wählen Sie auf der Seite „Identitätsquelle auswählen“ die Option **Externer Identitätsanbieter** aus und klicken Sie dann auf **Weiter**.
5. Die Seite **Externen Identitätsanbieter konfigurieren** wird geöffnet. Um diese Seite und die Google Workspace Seite in Schritt 1 fertigzustellen, müssen Sie die folgenden Schritte ausführen:
 - Im Abschnitt **Identity Provider-Metadaten** in der IAM Identity Center-Konsole müssen Sie eine der folgenden Aktionen ausführen:
 - i. Laden Sie die **Google SAML-Metadaten** als **IdP-SAML-Metadaten** in die IAM Identity Center-Konsole hoch.
 - ii. Kopieren Sie die **Google SSO-URL** und fügen Sie sie in das Feld „**Sign-inIdP-URL**“ ein, fügen Sie die **Google Aussteller-URL** in das Feld „**URL des IdP-Ausstellers**“ ein und laden Sie das **Zertifikat** als **IdP-Zertifikat** hoch. **Google**
6. Nachdem Sie die Google Metadaten im Bereich **Identity Provider-Metadaten** der IAM Identity Center-Konsole eingegeben haben, wählen Sie unter **Dienstanbieter-Metadaten** die Option **Standard-IPv4** oder **Dual-stack**. Wenn Sie Ihre AWS Access-Portal-URL angepasst haben, wählen Sie **Standard-IPv4**. Kopieren Sie die URL des IAM Identity Assertion Consumer Service (ACS) und die URL des IAM Identity Center-Ausstellers. Sie benötigen diese URLs, um die Konfiguration der Google Admin-Konsole im nächsten Schritt abzuschließen. Weitere Informationen zu ACS-URLs finden Sie unter [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#).

7. Lassen Sie die Seite mit der IAM Identity Center-Konsole geöffnet und kehren Sie zur Google Admin-Konsole zurück. Sie sollten sich auf der Seite Amazon Web Services — Service Provider-Details befinden. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite mit den Serviceanbieter-Details die ACS-URL und die Entitäts-ID ein. Sie haben diese Werte im vorherigen Schritt kopiert und sie sind in der IAM Identity Center-Konsole zu finden.
 - Fügen Sie die IAM Identity Center Assertion Consumer Service (ACS) -URL in das ACS-URL-Feld ein
 - Fügen Sie die URL des IAM Identity Center-Ausstellers in das Feld Entitäts-ID ein.
9. Füllen Sie auf der Seite mit den Dienstanbieter-Details die Felder unter Name-ID wie folgt aus:
 - Wählen Sie für das Format der Name-ID die Option E-MAIL aus
 - Wählen Sie für die Name-ID Grundinformationen > Primäre E-Mail-Adresse
10. Klicken Sie auf Weiter.
11. Wählen Sie auf der Seite „Attributzuordnung“ unter „Attribute“ die Option ADD MAPPING aus, und konfigurieren Sie dann diese Felder unter „GoogleVerzeichnisattribut“:
 - Wählen Sie für das `https://aws.amazon.com/SAML/Attributes/RoleSessionName` App-Attribut das Feld Basisinformationen, Primäre E-Mail-Adresse aus den Google Directory Attributen aus.
 - Wählen Sie für das `https://aws.amazon.com/SAML/Attributes/Role` App-Attribut beliebige Google Directory Attribute aus. Ein Google Verzeichnisattribut könnte Abteilung sein.
12. Wählen Sie Fertig stellen
13. Kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Weiter. Überprüfen Sie auf der Seite „Überprüfen und bestätigen“ die Informationen und geben Sie dann ACCEPT in das dafür vorgesehene Feld ein. Wählen Sie Identitätsquelle ändern aus.

Sie sind jetzt bereit, die Amazon Web Services-App zu aktivieren, Google Workspace damit Ihre Benutzer im IAM Identity Center bereitgestellt werden können.

Schritt 3: Google WorkSpace: Aktivieren Sie die Apps

1. Kehren Sie zur Google Admin-Konsole und zu Ihrer AWS IAM Identity Center Anwendung zurück, die Sie unter Apps sowie Web- und Mobil-Apps finden.

2. Wählen Sie im Bereich Benutzerzugriff neben Benutzerzugriff den Abwärtspfeil, um den Benutzerzugriff zu erweitern und das Dienststatusfenster anzuzeigen.
3. Wählen Sie im Bereich Servicestatus die Option FÜR ALLE EIN UND WÄHLEN SIE DANN SPEICHERN.

 Note

Um das Prinzip der geringsten Rechte beizubehalten, empfehlen wir, nach Abschluss dieses Tutorials den Dienststatus für alle auf AUS zu ändern. Der Dienst AWS sollte nur für Benutzer aktiviert sein, die Zugriff auf benötigen. Sie können Google Workspace Gruppen oder Organisationseinheiten verwenden, um Benutzern Zugriff auf eine bestimmte Untergruppe Ihrer Benutzer zu gewähren.

Schritt 4: IAM Identity Center: Richten Sie die automatische Bereitstellung von IAM Identity Center ein

1. Kehren Sie zur IAM Identity Center-Konsole zurück.
2. Suchen Sie auf der Seite „Einstellungen“ das Informationsfeld „Automatische Bereitstellung“ und wählen Sie dann „Aktivieren“. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpunkt- und Zugriffstoken-Informationen werden angezeigt.
3. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Daten jeden der Werte für die folgenden Optionen. In Schritt 5 dieses Tutorials geben Sie diese Werte ein, um die automatische Bereitstellung zu konfigurieren. Google Workspace
 - a. SCIM-Endpunkt — Zum Beispiel
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Dual-stack `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren.

4. Klicken Sie auf Schließen.

Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, konfigurieren Sie im nächsten Schritt die automatische Bereitstellung in Google Workspace.

Schritt 5: Google WorkSpace: Konfigurieren Sie die automatische Bereitstellung

1. Kehren Sie zur Google Admin-Konsole und zu Ihrer AWS IAM Identity Center Anwendung zurück, die Sie unter Apps sowie Web- und Mobil-Apps finden. Wählen Sie im Abschnitt Automatische Bereitstellung die Option Automatische Bereitstellung konfigurieren aus.
2. Im vorherigen Verfahren haben Sie den Zugriffstoken-Wert in die IAM Identity Center-Konsole kopiert. Fügen Sie diesen Wert in das Feld Zugriffstoken ein und wählen Sie Weiter. Außerdem haben Sie im vorherigen Verfahren den SCIM-Endpunkt-Wert in die IAM Identity Center-Konsole kopiert. Fügen Sie diesen Wert in das Feld Endpunkt-URL ein und wählen Sie Weiter.
3. Stellen Sie sicher, dass alle obligatorischen IAM Identity Center-Attribute (die mit * markierten) Attributen zugeordnet Google Cloud Directory sind. Wenn nicht, wählen Sie den Abwärtspfeil und ordnen Sie ihn dem entsprechenden Attribut zu. Klicken Sie auf Weiter.
4. Im Abschnitt Umfang der Bereitstellung können Sie eine Gruppe mit Ihrem Google Workspace Verzeichnis auswählen, um Zugriff auf die Amazon Web Services-App zu gewähren. Überspringen Sie diesen Schritt und wählen Sie Weiter.
5. Im Abschnitt Deprovisionierung können Sie auswählen, wie auf verschiedene Ereignisse reagiert werden soll, die einem Benutzer den Zugriff entziehen. Für jede Situation können Sie angeben, wie lange es dauert, bis mit der Deprovisionierung begonnen wird, um:
 - innerhalb von 24 Stunden
 - nach einem Tag
 - nach sieben Tagen
 - nach 30 Tagen

In jeder Situation gibt es eine Zeiteinstellung, wann der Zugriff auf ein Konto gesperrt und wann das Konto gelöscht werden soll.

 Tip

Stellen Sie vor dem Löschen eines Benutzerkontos immer mehr Zeit ein als für die Sperrung eines Benutzerkontos.

6. Wählen Sie Finish (Abschließen). Sie kehren zur Amazon Web Services-App-Seite zurück.
7. Schalten Sie in Auto-provisioning diesem Abschnitt den Kippschalter ein, um ihn von Inaktiv auf Aktiv zu ändern.

 Note

Der Aktivierungsschieberegler ist deaktiviert, wenn IAM Identity Center für Benutzer nicht aktiviert ist. Wählen Sie Benutzerzugriff und schalten Sie die App ein, um den Schieberegler zu aktivieren.

8. Wählen Sie im Bestätigungsdialogfeld „Einschalten“.
9. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Auf der Seite Benutzer werden die Benutzer aus Ihrem Google Workspace Verzeichnis aufgeführt, die von SCIM erstellt wurden. Wenn Benutzer noch nicht aufgeführt sind, ist die Bereitstellung möglicherweise noch im Gange. Die Bereitstellung kann bis zu 24 Stunden dauern, obwohl sie in den meisten Fällen innerhalb von Minuten abgeschlossen ist. Achten Sie darauf, das Browserfenster alle paar Minuten zu aktualisieren.

Wählen Sie einen Benutzer aus und sehen Sie sich dessen Details an. Die Informationen sollten mit den Informationen im Google Workspace Verzeichnis übereinstimmen.

 Herzlichen Glückwunsch!

Sie haben erfolgreich eine SAML-Verbindung zwischen Google Workspace und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert. Sie können diese Benutzer jetzt Konten und Anwendungen in IAM Identity Center zuweisen. Für dieses Tutorial benennen wir im nächsten Schritt einen der Benutzer zum IAM Identity

Center-Administrator, indem wir ihm Administratorberechtigungen für das Verwaltungskonto gewähren.

Übergabe von Attributen für die Zugriffskontrolle - Optional

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie AWS STS [im IAM-Benutzerhandbuch unter](#) Übergeben von Sitzungs-Tags.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Tag-Schlüssel-Wert-Paar `CostCenter = blue` zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Weisen Sie den Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um Zugriff auf AWS-Konten nur zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

Note

Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Schritt 1: IAM Identity Center: Grant Google WorkSpace Benutzern Zugriff auf Konten

1. Kehren Sie zur IAM Identity Center-Konsole zurück. Wählen Sie im IAM Identity Center-Navigationsbereich unter Multi-account Berechtigungen die Option. AWS-Konten
2. Auf der AWS-Konten Seite „Organisationsstruktur“ wird Ihr Organisationsstamm mit Ihren Konten darunter in der Hierarchie angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:
 - a. Für Schritt 1: Wählen Sie Benutzer und Gruppen aus, wählen Sie den Benutzer aus, der die Administratorfunktion ausführen soll. Klicken Sie anschließend auf Weiter.
 - b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Unterschritte führt, die zum Erstellen eines Berechtigungssatzes erforderlich sind.
 - i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:
 - Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
 - Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

Wählen Sie Weiter aus.

- ii. Für Schritt 2: Geben Sie die Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter.

Mit den Standardeinstellungen wird ein Berechtigungssatz *AdministratorAccess* mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist.

- iii. Stellen Sie für Schritt 3: Prüfen und Erstellen sicher, dass der Berechtigungssatztyp die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen aus. Auf der Seite „Berechtigungssätze“ wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diesen Tab jetzt in Ihrem Webbrowser schließen.
- iv. Auf dem Browser-Tab Benutzer und Gruppen zuweisen befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

- v. Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *AdministratorAccess* Berechtigungssatz wird in der Liste angezeigt. Markieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter aus.
- c. Überprüfen Sie für Schritt 3: Prüfen und Absenden den ausgewählten Benutzer und den ausgewählten Berechtigungssatz und wählen Sie dann Senden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihre gerade konfiguriert AWS-Konto wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. Eine Benachrichtigung informiert Sie darüber, dass Ihre Berechtigungen erneut bereitgestellt AWS-Konto wurden und der aktualisierte Berechtigungssatz angewendet wurde. Wenn sich der Benutzer anmeldet, hat er die Möglichkeit, die Rolle auszuwählen. *AdministratorAccess*

 Note

Die automatische SCIM-Synchronisierung von unterstützt Google Workspace nur die Bereitstellung von Benutzern. Die automatische Gruppenbereitstellung wird derzeit nicht unterstützt. Mit dem können Sie keine Gruppen für Ihre Google Workspace Benutzer erstellen. AWS-Managementkonsole Nach der Bereitstellung von Benutzern können Sie Gruppen mithilfe des AWS CLI Identity [Store-Befehls](#) `create-group` oder der IAM-API erstellen. [CreateGroup](#)

Schritt 2: Google WorkSpace: Bestätigen Google WorkSpace Zugriff der Benutzer auf AWS Ressourcen

1. Melden Sie sich Google mit einem Testbenutzerkonto an. Informationen zum Hinzufügen von Benutzern finden Sie in Google Workspace der [Google Workspace Dokumentation](#).
2. Wählen Sie das Google apps Launcher-Symbol (Waffel) aus.
3. Scrollen Sie zum Ende der Apps-Liste, wo sich Ihre benutzerdefinierten Google Workspace Apps befinden. Die Amazon Web Services-App wird angezeigt.
4. Wählen Sie die Amazon Web Services-App aus. Sie sind im AWS Access-Portal angemeldet und können das AWS-Konto Symbol sehen. Erweitern Sie das Symbol, um die Liste der Objekte anzuzeigen AWS-Konten , auf die der Benutzer zugreifen kann. In diesem Tutorial haben Sie nur

mit einem einzigen Konto gearbeitet. Wenn Sie das Symbol erweitern, wird also nur ein Konto angezeigt.

5. Wählen Sie das Konto aus, um die für den Benutzer verfügbaren Berechtigungssätze anzuzeigen. In diesem Tutorial haben Sie den `AdministratorAccess` Berechtigungssatz erstellt.
6. Neben dem Berechtigungssatz befinden sich Links für die Art des Zugriffs, der für diesen Berechtigungssatz verfügbar ist. Bei der Erstellung des Berechtigungssatzes haben Sie angegeben, dass sowohl die Verwaltungskonsole als auch der programmatische Zugriff aktiviert sein sollen, sodass diese beiden Optionen verfügbar sind. Wählen Sie `Verwaltungskonsole` aus, um die zu öffnen. `AWS-Managementkonsole`
7. Der Benutzer ist an der Konsole angemeldet.

Nächste Schritte

Nachdem Sie die Konfiguration Google Workspace als Identitätsanbieter vorgenommen und Benutzern im IAM Identity Center Zugriffsrechte zugewiesen haben, können Sie:

- Verwenden Sie den AWS CLI Identity [Store-Befehl](#) `create-group` oder die IAM-API, um Gruppen [CreateGroup](#) für Ihre Benutzer zu erstellen.

Gruppen sind nützlich, wenn Sie den Zugriff auf Anwendungen zuweisen möchten. AWS-Konten Anstatt jeden Benutzer einzeln zuzuweisen, erteilen Sie einer Gruppe Berechtigungen. Wenn Sie später Benutzer zu einer Gruppe hinzufügen oder aus einer Gruppe entfernen, erhält oder verliert der Benutzer dynamisch den Zugriff auf Konten und Anwendungen, die Sie der Gruppe zugewiesen haben.

- Konfigurieren Sie Berechtigungen auf der Grundlage von Aufgabenfunktionen, siehe [Erstellen von Berechtigungssätzen](#).

Berechtigungssätze definieren die Zugriffsebene, auf die Benutzer und Gruppen Zugriff haben AWS-Konto. Berechtigungssätze werden im IAM Identity Center gespeichert und können für einen oder mehrere Benutzer bereitgestellt werden. AWS-Konten Sie können einem Benutzer mehrere Berechtigungssätze zuweisen.

Note

Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere IdP-Zertifikate durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein IdP-Zertifikat ersetzen,

wenn sich das Ablaufdatum des Zertifikats nähert. Der Vorgang, bei dem ein älteres Zertifikat durch ein neueres ersetzt wird, wird als Zertifikatsrotation bezeichnet. Lesen Sie unbedingt, wie [Sie die SAML-Zertifikate](#) für Google Workspace verwalten.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit Google Workspace finden Sie in den folgenden Abschnitten:

- [Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden](#)
- [Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden](#)
- [Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter](#)
- Informationen zur Google Workspace Problembehandlung finden Sie in der Dokumentation [Google Workspace](#).

Die folgenden Ressourcen können Ihnen bei der Arbeit mit folgenden Problemen helfen AWS:

- [AWS re:Post](#)- Hier finden Sie häufig gestellte Fragen und Links zu anderen Ressourcen, die Ihnen bei der Behebung von Problemen helfen.
- [AWS Support](#)- Holen Sie sich technischen Support

Verwenden von IAM Identity Center für die Verbindung mit Ihrer JumpCloud Verzeichnisplattform

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen von JumpCloud Directory Platform in IAM Identity Center. Diese Bereitstellung verwendet das SAML 2.0-Protokoll ([Security Assertion Markup Language](#)). Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Sie konfigurieren diese Verbindung JumpCloud mithilfe Ihres IAM Identity Center SCIM-Endpoints und Ihres Zugriffstokens. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine

Zuordnung Ihrer Benutzerattribute JumpCloud zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. JumpCloud

Dieser Leitfaden basiert auf dem JumpCloud Stand von Juni 2021. Die Schritte für neuere Versionen können variieren. Dieses Handbuch enthält einige Hinweise zur Konfiguration der Benutzerauthentifizierung über SAML.

In den folgenden Schritten erfahren Sie, wie Sie mithilfe des SCIM-Protokolls die automatische Bereitstellung von Benutzern und Gruppen von JumpCloud bis zum IAM Identity Center aktivieren.

Note

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu lesen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#) Lesen Sie dann im nächsten Abschnitt weitere Überlegungen durch.

Themen

- [Voraussetzungen](#)
- [Überlegungen zu SCIM](#)
- [Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center](#)
- [Schritt 2: Konfigurieren Sie die Bereitstellung in JumpCloud](#)
- [\(Optional\) Schritt 3: Konfigurieren Sie Benutzerattribute JumpCloud für die Zugriffskontrolle im IAM Identity Center](#)
- [\(Optional\) Übergabe von Attributen für die Zugriffskontrolle](#)

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- JumpCloudAbonnement oder kostenlose Testversion. Um sich für eine kostenlose Testversion anzumelden, besuchen Sie uns [JumpCloud](#).
- Ein IAM Identity Center-fähiges Konto ([kostenlos](#)). Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
- Eine SAML-Verbindung von Ihrem JumpCloud Konto zum IAM Identity Center, wie in der [JumpCloudDokumentation für IAM Identity Center](#) beschrieben.

- Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und von diesen Regionen aus zu ermöglichen. AWS-Konten Weitere Details finden Sie unter [the section called “Schritt 3 \(nur externe Identitätsanbieter\): Aktualisieren Sie das externe IdP-Setup”](#). Weitere Informationen finden Sie in der JumpCloud Dokumentation.
- Ordnen Sie den IAM Identity Center-Connector den Gruppen zu, denen Sie Zugriff auf AWS Konten gewähren möchten.

Überlegungen zu SCIM

Im Folgenden finden Sie Überlegungen zur Verwendung des JumpCloud Verbunds für IAM Identity Center.

- Nur Gruppen, die dem AWS Single Sign-On-Connector zugeordnet sind, JumpCloud werden mit SCIM synchronisiert.
- Es kann nur ein Telefonnummernattribut synchronisiert werden, und die Standardeinstellung ist „Geschäftstelefon“.
- Für Benutzer im JumpCloud Verzeichnis müssen Vor- und Nachnamen so konfiguriert sein, dass sie mit SCIM mit IAM Identity Center synchronisiert werden können.
- Attribute werden weiterhin synchronisiert, wenn der Benutzer in IAM Identity Center deaktiviert, aber trotzdem aktiviert ist. JumpCloud
- Sie können die SCIM-Synchronisierung nur für Benutzerinformationen aktivieren, indem Sie im Connector die Option „Verwaltung von Benutzergruppen und Gruppenmitgliedschaft aktivieren“ deaktivieren.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung zu aktivieren.

Um die automatische Bereitstellung in IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity](#) Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM

Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.

4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpunkt — Zum Beispiel `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mit dem JumpCloud IAM Identity Center Connector erledigen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren Sie die Bereitstellung in JumpCloud

Verwenden Sie das folgende Verfahren im JumpCloud IAM Identity Center Connector, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie den JumpCloud IAM Identity Center-Connector bereits zu Ihrem JumpCloud Admin-Portal und Ihren Gruppen hinzugefügt haben. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen unter diesem Verfahren zur [Voraussetzungen](#) Konfiguration der SCIM-Bereitstellung und führen Sie es anschließend aus.

So konfigurieren Sie die Bereitstellung in JumpCloud

1. Öffnen Sie den JumpCloud IAM Identity Center-Connector, den Sie im Rahmen der Konfiguration von SAML für installiert haben JumpCloud (Benutzerauthentifizierung > IAM Identity Center). Siehe [Voraussetzungen](#).

2. Wählen Sie den IAM Identity Center-Connector und dann die dritte Registerkarte Identity Management.
3. Aktivieren Sie das Kontrollkästchen Verwaltung von Benutzergruppen und Gruppenmitgliedschaften in dieser Anwendung aktivieren, wenn Sie möchten, dass Gruppen mit SCIM synchronisiert werden.
4. Klicken Sie auf Konfigurieren.
5. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Basis-URL im JumpCloud IAM Identity Center-Connector ein.
6. Aus dem vorherigen Verfahren haben Sie den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Token-Schlüssel im JumpCloud IAM Identity Center-Connector ein.
7. Klicken Sie auf Aktivieren, um die Konfiguration zu übernehmen.
8. Vergewissern Sie sich, dass neben Single Sign-On aktiviert eine grüne Anzeige angezeigt wird.
9. Gehen Sie zur vierten Registerkarte Benutzergruppen und markieren Sie die Gruppen, für die Sie SCIM bereitstellen möchten.
10. Wenn Sie fertig sind, klicken Sie unten auf Speichern.
11. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von JumpCloud werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt Konten in IAM Identity Center zugewiesen werden.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute JumpCloud für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für den Fall JumpCloud, dass Sie Attribute für das IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute, die Sie definieren, JumpCloud werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, die Sie übergeben haben. JumpCloud

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zunächst die Funktion „[Attribute für die Zugriffskontrolle](#)“ aktivieren. Weitere Informationen dazu finden Sie unter [Aktivieren und Konfigurieren von Attributen für die Zugriffskontrolle](#).

So konfigurieren Sie Benutzerattribute JumpCloud für die Zugriffskontrolle im IAM Identity Center

1. Öffnen Sie den JumpCloud IAM Identity Center-Connector, den Sie im Rahmen der Konfiguration von SAML für installiert haben JumpCloud (Benutzerauthentifizierung > IAM Identity Center).
2. Wählen Sie den IAM Identity Center-Connector aus. Wählen Sie dann die zweite Registerkarte IAM Identity Center.
3. Unten auf dieser Registerkarte befindet sich die Benutzerattribute-Zuordnung. Wählen Sie Neues Attribut hinzufügen aus, und gehen Sie dann wie folgt vor: Sie müssen diese Schritte für jedes Attribut ausführen, das Sie zur Verwendung in IAM Identity Center für die Zugriffskontrolle hinzufügen möchten.
 - a. Geben Sie im Feld Name des Serviceprovider-Attributs den `https://aws.amazon.com/SAML/Attributes/AccessControl: AttributeName`. Text Replace **AttributeName** durch den Namen des Attributs ein, das Sie in IAM Identity Center erwarten. Beispiel, `https://aws.amazon.com/SAML/Attributes/AccessControl: Email`.
 - b. Wählen Sie im Feld JumpCloudAttributname Benutzerattribute aus Ihrem JumpCloud Verzeichnis aus. Zum Beispiel E-Mail (Arbeit).
4. Wählen Sie Speichern.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl: {TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
```

```
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Konfigurieren Sie SAML und SCIM mit Microsoft Entra ID und IAM Identity Center

AWS IAM Identity Center unterstützt die Integration mit [Security Assertion Markup Language \(SAML\) 2.0](#) sowie die [automatische Bereitstellung](#) (Synchronisation) von Benutzer- und Gruppeninformationen aus Microsoft Entra ID (früher bekannt als Azure Active Directory oder) in IAM Identity Center mithilfe des [Systems for Identity Management \(SCIM\) Azure AD\) 2.0-Protokoll. Cross-domain](#). Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Zielsetzung

In diesem Tutorial richten Sie ein Testlabor ein und konfigurieren eine SAML-Verbindung und SCIM-Bereitstellung zwischen Microsoft Entra ID und IAM Identity Center. Während der ersten Vorbereitungsschritte erstellen Sie sowohl im IAM Identity Center als auch im IAM Identity Center einen Testbenutzer (Nikki Wolf), mit dem Sie die SAML-Verbindung in beide Microsoft Entra ID Richtungen testen. Später erstellen Sie im Rahmen der SCIM-Schritte einen anderen Testbenutzer (Richard Roe), um zu überprüfen, ob neue Attribute erwartungsgemäß mit IAM Microsoft Entra ID Identity Center synchronisiert werden.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie zunächst Folgendes einrichten:

- Ein Microsoft Entra ID Mieter. Weitere Informationen finden Sie [in der Microsoft Dokumentation unter](#) Schnellstart: Einen Mandanten einrichten.
- Ein AWS IAM Identity Center-fähiges Konto. Weitere Informationen finden Sie [im AWS IAM Identity Center Benutzerhandbuch unter IAM Identity Center](#) aktivieren.

Überlegungen

Im Folgenden finden Sie wichtige Überlegungen Microsoft Entra ID, die sich darauf auswirken können, wie Sie die [automatische Bereitstellung](#) mit IAM Identity Center in Ihrer Produktionsumgebung mithilfe des SCIM v2-Protokolls implementieren möchten.

Automatische Bereitstellung

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, dies zunächst zu überprüfen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#)

Attribute für die Zugriffskontrolle

Attribute für die Zugriffskontrolle werden in Berechtigungsrichtlinien verwendet, die festlegen, wer in Ihrer Identitätsquelle auf Ihre AWS Ressourcen zugreifen kann. Wenn ein Attribut von einem Benutzer in entfernt wird Microsoft Entra ID, wird dieses Attribut nicht vom entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung in Microsoft Entra ID. Wenn ein Attribut für einen Benutzer auf einen anderen (nicht leeren) Wert geändert wird, wird diese Änderung mit IAM Identity Center synchronisiert.

Verschachtelte Gruppen

Der Microsoft Entra ID Benutzerbereitstellungsdienst kann Benutzer in verschachtelten Gruppen nicht lesen oder ihnen keine Zugriffsrechte zuweisen. Nur Benutzer, die unmittelbare Mitglieder einer explizit zugewiesenen Gruppe sind, können gelesen und Zugriffsrechte zugewiesen werden. Microsoft Entra ID packt nicht rekursiv die Gruppenmitgliedschaften indirekt zugewiesener Benutzer oder Gruppen (Benutzer oder Gruppen, die Mitglieder einer direkt zugewiesenen Gruppe sind). Weitere Informationen finden Sie in der Dokumentation unter [Assignment-based Geltungsbereich](#). Alternativ können Sie die konfigurierbare AD-Synchronisierung von [IAM Identity Center verwenden](#), um Active Directory Gruppen in IAM Identity Center zu integrieren.

Dynamische Gruppen

Der Microsoft Entra ID Benutzerbereitstellungsdienst kann Benutzer in [dynamischen Gruppen](#) lesen und bereitstellen. Unten finden Sie ein Beispiel, das die Benutzer- und Gruppenstruktur bei der Verwendung dynamischer Gruppen zeigt und zeigt, wie sie im IAM Identity Center angezeigt werden. Diese Benutzer und Gruppen wurden über SCIM Microsoft Entra ID in IAM Identity Center bereitgestellt

Zum Beispiel, wenn die Microsoft Entra ID Struktur für dynamische Gruppen wie folgt lautet:

1. Gruppe A mit den Mitgliedern ua1, ua2
2. Gruppe B mit Mitgliedern ub1
3. Gruppe C mit Mitgliedern uc1
4. Gruppe K mit einer Regel, die Mitglieder der Gruppe A, B, C einschließt
5. Gruppe L mit einer Regel, die Mitglieder der Gruppen B und C einbezieht

Nachdem die Benutzer- und Gruppeninformationen über SCIM aus dem Microsoft Entra ID IAM Identity Center bereitgestellt wurden, sieht die Struktur wie folgt aus:

1. Gruppe A mit den Mitgliedern ua1, ua2
2. Gruppe B mit Mitgliedern ub1
3. Gruppe C mit Mitgliedern uc1
4. Gruppe K mit den Mitgliedern ua1, ua2, ub1, uc1
5. Gruppe L mit den Mitgliedern ub1, uc1

Beachten Sie bei der Konfiguration der automatischen Bereitstellung mithilfe dynamischer Gruppen die folgenden Überlegungen.

- Eine dynamische Gruppe kann eine verschachtelte Gruppe enthalten. Der Microsoft Entra ID Provisioning Service reduziert die verschachtelte Gruppe jedoch nicht. Wenn Sie beispielsweise die folgende Microsoft Entra ID Struktur für dynamische Gruppen haben:
 - Gruppe A ist der Gruppe B übergeordnet.
 - Gruppe A hat ua1 als Mitglied.
 - Gruppe B hat ub1 als Mitglied.

Die dynamische Gruppe, die Gruppe A enthält, umfasst nur die direkten Mitglieder von Gruppe A (d. h. ua1). Mitglieder der Gruppe B werden nicht rekursiv aufgenommen.

- Dynamische Gruppen können keine anderen dynamischen Gruppen enthalten. Weitere Informationen finden Sie [in der Microsoft Dokumentation unter Einschränkungen bei der Vorschau](#).

Schritt 1: Bereiten Sie Ihren Microsoft-Tenant vor

In diesem Schritt erfahren Sie, wie Sie Ihre AWS IAM Identity Center Unternehmensanwendung installieren und konfigurieren und einem neu erstellten Microsoft Entra ID Testbenutzer den Zugriff zuweisen.

Step 1.1 >

Schritt 1.1: Richten Sie die AWS IAM Identity Center Unternehmensanwendung ein in Microsoft Entra ID

In diesem Verfahren installieren Sie die AWS IAM Identity Center Unternehmensanwendung in Microsoft Entra ID. Sie benötigen diese Anwendung später, um Ihre SAML-Verbindung mit AWS zu konfigurieren.

1. Melden Sie sich mindestens [als Cloud-Anwendungsadministrator im](#) Microsoft Entra Admin Center an.
2. Navigieren Sie zu **Identität > Anwendungen > Unternehmensanwendungen** und wählen Sie dann **Neue Anwendung**.
3. Geben Sie auf der Seite „Microsoft Entra Gallery durchsuchen“ den Text **AWS IAM Identity Center** in das Suchfeld ein.
4. Wählen Sie AWS IAM Identity Center aus den Ergebnissen aus.
5. Wählen Sie **Erstellen** aus.

Step 1.2 >

Schritt 1.2: Erstellen Sie einen Testbenutzer in Microsoft Entra ID

Nikki Wolf ist der Name Ihres Microsoft Entra ID Testbenutzers, den Sie in diesem Verfahren erstellen werden.

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu **Identität > Benutzer > Alle Benutzer**.
2. Wählen Sie **Neuer Benutzer** aus und wählen Sie dann oben auf dem Bildschirm **Neuen Benutzer erstellen** aus.
3. Geben Sie **NikkiWolf** im Feld **Benutzerprinzipalname** Ihre bevorzugte Domain und Erweiterung ein und wählen Sie sie aus. Zum Beispiel **NikkiWolf @example.org**.
4. Geben Sie im Feld **Anzeigename** den Wert ein **NikkiWolf**.

5. Geben Sie im Feld **Passwort** ein sicheres Passwort ein, oder wählen Sie das Augensymbol aus, um das automatisch generierte Passwort anzuzeigen. Kopieren Sie den angezeigten Wert, oder notieren Sie ihn.
6. Wählen Sie **Eigenschaften** und geben Sie im Feld **Vorname** den Wert ein **Nikki**. Geben Sie im Feld **Nachname** den Wert ein **Wolf**.
7. Wählen Sie **Überprüfen + erstellen** und dann **Erstellen** aus.

Step 1.3

Schritt 1.3: Teste Nikkis Erfahrung, bevor du ihr ihre Berechtigungen erteilst AWS IAM Identity Center

In diesem Verfahren überprüfst du, wie Nikki sich erfolgreich in ihrem Microsoft [My Account-Portal anmelden kann](#).

1. Öffnen Sie im selben Browser einen neuen Tab, rufen Sie die [Anmeldeseite des Portals](#) „Mein Konto“ auf und geben Sie Nikkis vollständige E-Mail-Adresse ein. Zum Beispiel @. NikkiWolf *example.org*
2. Wenn Sie dazu aufgefordert werden, geben Sie Nikkis Passwort ein und wählen Sie dann **Anmelden**. Wenn es sich um ein automatisch generiertes Passwort handelt, wirst du aufgefordert, das Passwort zu ändern.
3. Wählen Sie auf der Seite **Aktion erforderlich** die Option **Später fragen** aus, um die Aufforderung zur Angabe zusätzlicher Sicherheitsmethoden zu umgehen.
4. Wählen Sie auf der Seite **Mein Konto** im linken Navigationsbereich **Meine Apps** aus. Beachten Sie **Add-ins**, dass derzeit außerdem keine Apps angezeigt werden. Sie fügen eine AWS IAM Identity Center App hinzu, die in einem späteren Schritt hier angezeigt wird.

Step 1.4

Schritt 1.4: Weisen Sie Nikki Berechtigungen zu in Microsoft Entra ID

Nachdem Sie nun bestätigt haben, dass Nikki erfolgreich auf das Portal **Mein Konto** zugreifen kann, gehen Sie wie folgt vor, um ihren Benutzer der AWS IAM Identity Center App zuzuweisen.

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu **Identität > Anwendungen > Unternehmensanwendungen** und wählen Sie dann **AWS IAM Identity Center** aus der Liste aus.

2. Wählen Sie links Benutzer und Gruppen aus.
3. Wählen Sie Hinzufügen user/group aus. Sie können die Meldung ignorieren, dass Gruppen nicht für die Zuweisung verfügbar sind. In diesem Tutorial werden keine Gruppen für Aufgaben verwendet.
4. Wählen Sie auf der Seite „Aufgabe hinzufügen“ unter „Benutzer“ die Option „Keine ausgewählt“ aus.
5. Wählen Sie aus NikkiWolf, und klicken Sie dann auf Auswählen.
6. Wählen Sie auf der Seite „Aufgabe hinzufügen“ die Option Zuweisen aus. NikkiWolf erscheint jetzt in der Liste der Benutzer, die der AWS IAM Identity Center App zugewiesen sind.

Schritt 2: Bereite deine vor AWS Konto

In diesem Schritt erfahren Sie, wie Sie IAM Identity Center Zugriffsberechtigungen (über einen Berechtigungssatz) konfigurieren, manuell einen entsprechenden Nikki Wolf-Benutzer erstellen und ihr die erforderlichen Berechtigungen für die Verwaltung von Ressourcen zuweisen. AWS

Step 2.1 >

Schritt 2.1: Erstellen Sie einen RegionalAdmin Berechtigungssatz unter IAM Identity Center

Dieser Berechtigungssatz wird verwendet, um Nikki die notwendigen AWS Kontoberechtigungen zu gewähren, die für die Verwaltung von Regionen über die Kontoseite innerhalb von erforderlich sind. AWS-Managementkonsole Alle anderen Berechtigungen zum Anzeigen oder Verwalten anderer Informationen für Nikkis Konto werden standardmäßig verweigert.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wähle unter Multi-account Berechtigungen die Option Berechtigungssätze aus.
3. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
4. Wählen Sie auf der Seite Berechtigungssatztyp auswählen die Option Benutzerdefinierter Berechtigungssatz und dann Weiter aus.
5. Wählen Sie Inline-Richtlinie aus, um sie zu erweitern, und erstellen Sie dann mithilfe der folgenden Schritte eine Richtlinie für den Berechtigungssatz:
 - a. Wählen Sie Neue Aussage hinzufügen, um eine Richtlinienerklärung zu erstellen.

- b. Wählen Sie unter Kontoauszug bearbeiten die Option Konto aus der Liste aus und aktivieren Sie dann die folgenden Kontrollkästchen.
 - **ListRegions**
 - **GetRegionOptStatus**
 - **DisableRegion**
 - **EnableRegion**
- c. Wählen Sie neben Eine Ressource hinzufügen die Option Hinzufügen aus.
- d. Wählen Sie auf der Seite Ressource hinzufügen unter Ressourcentyp die Option Alle Ressourcen und dann Ressource hinzufügen aus. Vergewissern Sie sich, dass Ihre Richtlinie wie folgt aussieht:

```
{
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "account:ListRegions",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetRegionOptStatus"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite „Details zum Berechtigungssatz angeben“ unter Name des Berechtigungssatzes den **RegionalAdmin** Text ein, und wählen Sie dann Weiter aus.
8. Wählen Sie auf der Seite Überprüfen und erstellen die Option Erstellen aus. In der Liste der Berechtigungssätze sollte Folgendes RegionalAdmin angezeigt werden.

Step 2.2 >

Schritt 2.2: Erstellen Sie einen entsprechenden NikkiWolf Benutzer in IAM Identity Center

Da das SAML-Protokoll keinen Mechanismus zur Abfrage des IdP (Microsoft Entra ID) und zum automatischen Erstellen von Benutzern hier im IAM Identity Center bietet, gehen Sie wie folgt vor, um manuell einen Benutzer in IAM Identity Center zu erstellen, der die Kernattribute von Nikki Wolfs user in widerspiegelt. Microsoft Entra ID

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Benutzer und dann Benutzer hinzufügen aus, und geben Sie dann die folgenden Informationen ein:
 - a. Sowohl für den Benutzernamen als auch für die E-Mail-Adresse — Geben Sie dasselbe **NikkiWolf** @ ein **yourcompanydomain.extension**, das Sie bei der Erstellung Ihres Microsoft Entra ID Benutzers verwendet haben. Zum Beispiel **NikkiWolf@example.org**.
 - b. E-Mail-Adresse bestätigen — Re-enter die E-Mail-Adresse aus dem vorherigen Schritt
 - c. Vorname — Geben Sie ein **Nikki**
 - d. Nachname — Geben Sie ein **Wolf**
 - e. Anzeigename — Geben Sie ein **Nikki Wolf**
3. Wählen Sie zweimal Weiter und dann Benutzer hinzufügen.
4. Klicken Sie auf Schließen.

Step 2.3

Schritt 2.3: Weisen Sie Nikki der unter festgelegten RegionalAdmin Berechtigung zu IAM Identity Center

Hier finden Sie die Regionen, AWS-Konto in denen Nikki die Regionen verwalten wird, und weisen ihr dann die erforderlichen Berechtigungen zu, damit sie erfolgreich auf das AWS Zugangsportal zugreifen kann.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie unter Multi-account Berechtigungen die Option. AWS-Konten

3. Markieren Sie das Kontrollkästchen neben dem Kontonamen (z. B. *Sandbox*), für den Sie Nikki Zugriff zur Verwaltung von Regionen gewähren möchten, und wählen Sie dann Benutzer und Gruppen zuweisen aus.
4. Wählen Sie auf der Seite „Benutzer und Gruppen zuweisen“ den Tab „Benutzer“, suchen Sie das Kästchen neben Nikki, markieren Sie es und wählen Sie dann Weiter aus.
5.
Example

<caption>On the Wählen Sie Berechtigungssätze aus page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Next.</caption>
6. Überprüfen Sie auf der Seite „Überprüfen und senden“ Ihre Auswahl und wählen Sie dann Senden aus.

Schritt 3: Konfigurieren und testen Sie Ihre SAML-Verbindung

In diesem Schritt konfigurieren Sie Ihre SAML-Verbindung mithilfe der AWS IAM Identity Center Unternehmensanwendung Microsoft Entra ID zusammen mit den externen IdP-Einstellungen im IAM Identity Center.

Step 3.1 >

Schritt 3.1: Erfassen Sie die erforderlichen Dienstanbieter-Metadaten aus dem IAM Identity Center

In diesem Schritt starten Sie den Assistenten zum Ändern der Identitätsquelle von der IAM Identity Center-Konsole aus und rufen die Metadatendatei und die AWS spezifische Anmelde-URL ab, die Sie bei der Konfiguration der Verbindung Microsoft Entra ID im nächsten Schritt eingeben müssen.

1. Wählen Sie in der [IAM Identity Center-Konsole Einstellungen](#) aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Identitätsquelle ändern“.
3. Wählen Sie auf der Seite „Identitätsquelle auswählen“ die Option Externer Identitätsanbieter und dann „Weiter“ aus.
4. Wählen Sie auf der Seite Externer Identitätsanbieter konfigurieren unter Dienstanbieter-Metadaten die Option Standard-IPv4 oder Dual-stack aus. Sie können die Metadatendatei des Dienstanbieters herunterladen, nachdem Sie die Änderung der Identitätsquelle abgeschlossen haben.

5. Suchen Sie im gleichen Abschnitt den Wert der Anmelde-URL für das AWS Access Portal und kopieren Sie ihn. Sie müssen diesen Wert eingeben, wenn Sie im nächsten Schritt dazu aufgefordert werden.
6. Lassen Sie diese Seite geöffnet und fahren Sie mit dem nächsten Schritt (**Step 3.2**) fort, um die AWS IAM Identity Center Unternehmensanwendung in zu konfigurierenMicrosoft Entra ID. Später kehren Sie zu dieser Seite zurück, um den Vorgang abzuschließen.

Step 3.2 >

Schritt 3.2: Konfigurieren Sie die AWS IAM Identity Center Unternehmensanwendung in Microsoft Entra ID

Bei diesem Verfahren wird die Hälfte der SAML-Verbindung auf Microsoft-Seite mithilfe der Werte aus der Metadaten-Datei und der Sign-On URL hergestellt, die Sie im letzten Schritt abgerufen haben.

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann AWS IAM Identity Center
2. Wählen Sie auf der linken Seite 2 aus. Richten Sie Single Sign-On ein.
3. Wählen Sie auf der Seite Single Sign-On mit SAML einrichten die Option SAML aus. Wählen Sie dann Metadaten-Datei hochladen, wählen Sie das Ordnersymbol, wählen Sie die Dienstleister-Metadaten-Datei aus, die Sie im vorherigen Schritt heruntergeladen haben, und klicken Sie dann auf Hinzufügen.
4. Vergewissern Sie sich auf der Seite „Einfache SAML-Konfiguration“, dass sowohl die Werte für Identifier als auch für die Antwort-URL (Assertion Consumer Service URL) jetzt auf Endpunkte in verweisen. AWS
 - Identifier — Dies ist die Aussteller-URL aus dem IAM Identity Center. Derselbe Wert gilt unabhängig davon, ob Sie IPv4-only Dual-Stack-Endpunkte verwenden.
 - Antwort-URL (Assertion Consumer Service URL) — Die Werte hier umfassen IPv4-only sowohl als auch Dual-Stack-Endpunkte aus allen aktivierten Regionen Ihres IAM Identity Center. Sie können die ACS-URL der primären Region als Standardadresse verwenden, sodass Benutzer in die primäre Region umgeleitet werden, wenn sie die Amazon Web Services-Anwendung von dort aus starten. Microsoft Entra ID Weitere Informationen zu ACS-URLs finden Sie unter [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#).

- (Optional) Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, können Sie in jeder weiteren Region auch eine Lesezeichen-App Microsoft Entra ID für das AWS Access Portal erstellen. Auf diese Weise können Ihre Benutzer in weiteren Regionen auf das AWS Zugriffsportal zugreifen. Microsoft Entra ID Stellen Sie sicher, dass Sie Ihren Benutzern Berechtigungen für den Zugriff auf die Lesezeichen-Apps in Microsoft Entra ID gewähren. Weitere Informationen finden Sie in der [Microsoft Entra ID Dokumentation](#). Wenn Sie planen, IAM Identity Center zu einem späteren Zeitpunkt auf weitere Regionen zu replizieren, finden Sie [Microsoft Entra ID Konfiguration für den Zugriff auf zusätzliche Regionen](#) unter Anleitungen, wie Sie den Zugriff auf die zusätzlichen Regionen nach dieser Ersteinrichtung aktivieren.
5. Fügen Sie unter Anmelde-URL (optional) den Wert der Anmelde-URL für das AWS Access Portal ein, den Sie im vorherigen Schritt kopiert haben (**Step 3.1**), wählen Sie Speichern und dann X, um das Fenster zu schließen.
 6. Wenn Sie aufgefordert werden, Single Sign-On mit zu testen AWS IAM Identity Center, wählen Sie Nein, ich werde es später testen. Sie werden diese Überprüfung in einem späteren Schritt durchführen.
 7. Wählen Sie auf der Seite Single Sign-On mit SAML einrichten im Abschnitt SAML-Zertifikate neben Federation Metadata XML die Option Herunterladen aus, um die Metadaten-Datei auf Ihrem System zu speichern. Sie müssen diese Datei hochladen, wenn Sie im nächsten Schritt dazu aufgefordert werden.

Step 3.3 >

Schritt 3.3: Konfigurieren Sie den Microsoft Entra ID externen IdP in AWS IAM Identity Center

Hier kehren Sie zum Assistenten zum Ändern der Identitätsquelle in der IAM Identity Center-Konsole zurück, um die zweite Hälfte der SAML-Verbindung abzuschließen. AWS

1. Kehren Sie in der IAM Identity Center-Konsole zu der Browsersitzung zurück, die Sie geöffnet gelassen haben. **Step 3.1**
2. Wählen Sie auf der Seite „Externen Identitätsanbieter konfigurieren“ im Abschnitt Metadaten des Identitätsanbieters unter IdP-SAML-Metadaten die Schaltfläche „Datei auswählen“, wählen Sie die Metadaten-Datei des Identitätsanbieters aus, aus der Sie Microsoft Entra ID im vorherigen Schritt heruntergeladen haben, und klicken Sie dann auf Öffnen.
3. Wählen Sie Weiter aus.

4. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie Folgendes ein. **ACCEPT**
5. Wählen Sie Identitätsquelle ändern, um Ihre Änderungen zu übernehmen.

Step 3.4 >

Schritt 3.4: Testen Sie, ob Nikki zum AWS Zugangsportal weitergeleitet wird

In diesem Verfahren testen Sie die SAML-Verbindung, indem Sie sich mit Nikkis Anmeldeinformationen beim My Account-Portal von Microsoft anmelden. Nach der Authentifizierung wählen Sie die AWS IAM Identity Center Anwendung aus, die Nikki zum Zugangsportal umleitet. AWS

1. Gehe zur [Anmeldeseite des Portals](#) „Mein Konto“ und gib Nikkis vollständige E-Mail-Adresse ein. Zum Beispiel **NikkiWolf** @ *example.org*.
2. Wenn Sie dazu aufgefordert werden, geben Sie Nikkis Passwort ein und wählen Sie dann Anmelden.
3. Wählen Sie auf der Seite Mein Konto im linken Navigationsbereich Meine Apps aus.
4. Wählen Sie auf der Seite Meine Apps die App mit dem Namen aus AWS IAM Identity Center. Dies sollte Sie zu einer zusätzlichen Authentifizierung auffordern.
5. Wählen Sie auf der Anmeldeseite von Microsoft Ihre NikkiWolf Anmeldeinformationen aus. Wenn Sie ein zweites Mal zur Authentifizierung aufgefordert werden, wählen Sie Ihre NikkiWolf Anmeldeinformationen erneut aus. Dadurch sollten Sie automatisch zum AWS Zugangsportal weitergeleitet werden.

Tip

Wenn Sie nicht erfolgreich weitergeleitet werden, stellen Sie sicher, dass der von Ihnen eingegebene Wert für die Anmelde-URL für das AWS Access Portal mit dem Wert **Step 3.2** übereinstimmt, von **Step 3.1** dem Sie kopiert haben.

6. Vergewissern Sie sich, dass Ihr AWS-Konten Display.

 Tip

Wenn die Seite leer ist und kein AWS-Konten Bildschirm angezeigt wird, vergewissern Sie sich, dass Nikki dem RegionalAdmin Berechtigungssatz erfolgreich zugewiesen wurde (siehe **Step 2.3**).

Step 3.5

Schritt 3.5: Testen Sie Nikkis Zugriffsebene, um sie zu verwalten AWS-Konto

In diesem Schritt überprüfst du, welche Zugriffsrechte Nikki hat, um die Regionseinstellungen für sie zu verwalten. AWS-Konto Nikki sollte nur über ausreichende Administratorrechte verfügen, um Regionen von der Kontoseite aus verwalten zu können.

1. Wählen Sie im AWS Access-Portal den Tab Konten, um die Liste der Konten anzuzeigen. Die Kontonamen, Konto-IDs und E-Mail-Adressen, die allen Konten zugeordnet sind, für die Sie Berechtigungssätze definiert haben, werden angezeigt.
2. Wählen Sie den Kontonamen (z. B. *Sandbox*), auf den Sie den Berechtigungssatz angewendet haben (siehe **Step 2.3**). Dadurch wird die Liste der Berechtigungssätze erweitert, aus denen Nikki wählen kann, um ihr Konto zu verwalten.
3. RegionalAdminWählen Sie als Nächstes Verwaltungskonsole aus, um die Rolle zu übernehmen, die Sie im RegionalAdmin Berechtigungssatz definiert haben. Dadurch werden Sie zur AWS-Managementkonsole Startseite weitergeleitet.
4. Wählen Sie in der oberen rechten Ecke der Konsole Ihren Kontonamen und dann Konto aus. Dadurch gelangst du zur Kontoseite. Beachten Sie, dass in allen anderen Abschnitten auf dieser Seite eine Meldung angezeigt wird, dass Sie nicht über die erforderlichen Berechtigungen zum Anzeigen oder Ändern dieser Einstellungen verfügen.
5. Scrollen Sie auf der Kontoseite nach unten zum Abschnitt AWS Regionen. Wählen Sie in der Tabelle ein Kontrollkästchen für jede verfügbare Region aus. Beachten Sie, dass Nikki über die erforderlichen Berechtigungen verfügt, um die Liste der Regionen für ihr Konto wie vorgesehen zu aktivieren oder zu deaktivieren.

 Gut gemacht!

Die Schritte 1 bis 3 haben Ihnen geholfen, Ihre SAML-Verbindung erfolgreich zu implementieren und zu testen. Um das Tutorial abzuschließen, empfehlen wir Ihnen, mit Schritt 4 zur Implementierung der automatischen Bereitstellung fortzufahren.

Schritt 4: Konfigurieren und testen Sie Ihre SCIM-Synchronisierung

In diesem Schritt richten Sie Microsoft Entra ID die [automatische Bereitstellung](#) (Synchronisation) von Benutzerinformationen aus dem IAM Identity Center mithilfe des SCIM v2.0-Protokolls ein. Sie konfigurieren diese Verbindung, Microsoft Entra ID indem Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Bearer-Token verwenden, das automatisch von IAM Identity Center erstellt wird.

Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Microsoft Entra ID zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. Microsoft Entra ID

In den folgenden Schritten erfahren Sie, wie Sie die automatische Bereitstellung von Benutzern, die sich hauptsächlich in IAM Identity Center befinden Microsoft Entra ID, mithilfe der IAM Identity Center-App in aktivieren. Microsoft Entra ID

Step 4.1 >

Schritt 4.1: Erstellen Sie einen zweiten Testbenutzer in Microsoft Entra ID

Zu Testzwecken erstellen Sie einen neuen Benutzer (Richard Roe) in Microsoft Entra ID. Später, nachdem Sie die SCIM-Synchronisierung eingerichtet haben, testen Sie, ob dieser Benutzer und alle relevanten Attribute erfolgreich mit IAM Identity Center synchronisiert wurden.

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu Identität > Benutzer > Alle Benutzer.
2. Wählen Sie **Neuer Benutzer** aus und wählen Sie dann oben auf dem Bildschirm **Neuen Benutzer erstellen** aus.
3. Geben Sie **RichRoe** im Feld **Benutzerprinzipalname** Ihre bevorzugte Domain und Erweiterung ein und wählen Sie sie aus. Zum Beispiel **RichRoe @example.org**.
4. Geben Sie im Feld **Anzeigename** den Wert ein **RichRoe**.

5. Geben Sie im Feld **Passwort** ein sicheres Passwort ein, oder wählen Sie das Augensymbol aus, um das automatisch generierte Passwort anzuzeigen. Kopieren Sie den angezeigten Wert, oder notieren Sie ihn.
6. Wählen Sie **Eigenschaften** aus, und geben Sie dann die folgenden Werte ein:
 - Vorname — Geben Sie ein **Richard**
 - Nachname - Geben Sie ein **Roe**
 - Berufsbezeichnung — Geben Sie ein **Marketing Lead**
 - Abteilung — Geben Sie ein **Sales**
 - Mitarbeiter-ID — Geben Sie ein **12345**
7. Wählen Sie **Überprüfen + erstellen** und dann **Erstellen**.

Step 4.2 >

Schritt 4.2: Aktivieren Sie die automatische Bereitstellung im IAM Identity Center

In diesem Verfahren verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung von Benutzern und Gruppen zu aktivieren, die aus dem Microsoft Entra ID IAM Identity Center kommen.

1. Öffnen Sie die [IAM Identity Center-Konsole](#) und wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Beachten Sie, dass auf der Seite „Einstellungen“ auf der Registerkarte „Identitätsquelle“ die Option „Bereitstellungsmethode“ auf „Manuell“ gesetzt ist.
3. Suchen Sie das Informationsfeld **Automatische Bereitstellung** und wählen Sie dann **Aktivieren** aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpunkt- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld **Automatische Bereitstellung** für eingehende Daten jeden der Werte für die folgenden Optionen. Sie müssen diese im nächsten Schritt einfügen, wenn Sie die Bereitstellung konfigurieren. Microsoft Entra ID
 - a. SCIM-Endpunkt — Zum Beispiel
 - IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`

- Dualer Stack: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-5555555555/scim/v2`
- b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren.

5. Klicken Sie auf Schließen.
6. Beachten Sie, dass auf der Registerkarte Identitätsquelle jetzt die Bereitstellungsmethode auf SCIM eingestellt ist.

Step 4.3 >

Schritt 4.3: Konfigurieren Sie die automatische Bereitstellung in Microsoft Entra ID

Nachdem Sie Ihren RichRoe Testbenutzer eingerichtet und SCIM im IAM Identity Center aktiviert haben, können Sie mit der Konfiguration der SCIM-Synchronisierungseinstellungen unter fortfahren. Microsoft Entra ID

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann. AWS IAM Identity Center
2. Wählen Sie Provisioning aus und wählen Sie unter Verwalten erneut Provisioning aus.
3. Wählen Sie im Bereitstellungsmodus die Option Automatisch aus.
4. Fügen Sie unter Admin-Anmeldeinformationen in das Feld Mandanten-URL den URL-Wert für den SCIM-Endpunkt ein, den Sie zuvor kopiert haben. **Step 4.2** Fügen Sie im Feld Geheimer Token den Wert des Zugriffstokens ein.
5. Wählen Sie Test Connection (Verbindung testen) aus. Es sollte eine Meldung angezeigt werden, die darauf hinweist, dass die getesteten Anmeldeinformationen erfolgreich autorisiert wurden, um die Bereitstellung zu aktivieren.
6. Wählen Sie Speichern.
7. Wählen Sie unter Verwalten die Option Benutzer und Gruppen aus, und klicken Sie dann auf Hinzufügen user/group.

8. Wählen Sie auf der Seite „Aufgabe hinzufügen“ unter „Benutzer“ die Option „Keine ausgewählt“ aus.
9. Wählen Sie aus RichRoe, und klicken Sie dann auf Auswählen.
10. Wählen Sie auf der Seite Add Assignment (Zuweisung hinzufügen) Assign (Zuweisen) aus.
11. Wählen Sie Übersicht und dann Bereitstellung starten aus.

Step 4.4

Schritt 4.4: Stellen Sie sicher, dass die Synchronisierung stattgefunden hat

In diesem Abschnitt überprüfen Sie, ob Richards Benutzer erfolgreich bereitgestellt wurde und dass alle Attribute im IAM Identity Center angezeigt werden.

1. Wählen Sie in der [IAM Identity Center-Konsole Benutzer](#) aus.
2. Auf der Seite „Benutzer“ sollte Ihr RichRoe Benutzer angezeigt werden. Beachten Sie, dass in der Spalte Erstellt von der Wert auf SCIM gesetzt ist.
3. Wählen Sie RichRoe unter Profil aus Microsoft Entra ID, ob die folgenden Attribute kopiert wurden.
 - Vorname - **Richard**
 - Nachname - **Roe**
 - Abteilung - **Sales**
 - Titel - **Marketing Lead**
 - Nummer des Mitarbeiters - **12345**

Jetzt, da Richards Benutzer in IAM Identity Center erstellt wurde, können Sie ihn jedem beliebigen Berechtigungssatz zuweisen, sodass Sie kontrollieren können, welche Zugriffsebene er auf Ihre AWS Ressourcen hat. Sie könnten beispielsweise dem zuvor verwendeten **RegionalAdmin** Berechtigungssatz zuweisen, RichRoe um Nikki die Berechtigungen zur Verwaltung von Regionen zu gewähren (siehe **Step 2.3**), und dann testen, wie viel Zugriff er darauf hat. **Step 3.5**

 Herzlichen Glückwunsch!

Sie haben erfolgreich eine SAML-Verbindung zwischen Microsoft und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert, um alles synchron zu halten. Jetzt können Sie das Gelernte anwenden, um Ihre Produktionsumgebung reibungsloser einzurichten.

Schritt 5: ABAC konfigurieren - Optional

Nachdem Sie SAML und SCIM erfolgreich konfiguriert haben, können Sie optional die attributbasierte Zugriffskontrolle (ABAC) konfigurieren. ABAC ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert.

Mit können Sie eine der beiden folgenden Methoden verwendenMicrosoft Entra ID, um ABAC für die Verwendung mit IAM Identity Center zu konfigurieren.

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

Konfigurieren Sie Benutzerattribute Microsoft Entra ID für die Zugriffskontrolle im IAM Identity Center

Im folgenden Verfahren legen Sie fest, welche Attribute von IAM Identity Center zur Verwaltung des Zugriffs auf Ihre AWS Ressourcen verwendet werden Microsoft Entra ID sollen. Sobald sie definiert sind, werden diese Attribute über SAML-Assertions an IAM Identity Center Microsoft Entra ID gesendet. Anschließend müssen Sie [Erstellen Sie einen Berechtigungssatz](#) im IAM Identity Center den Zugriff auf Grundlage der Attribute verwalten, von denen Sie die Daten übergeben haben. Microsoft Entra ID

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die [Attribute für Zugriffskontrolle](#) Funktion aktivieren. Weitere Information dazu finden Sie unter [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#).

1. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie AWS IAM Identity Center dann.
2. Klicken Sie auf Single Sign-On.
3. Wählen Sie im Abschnitt Attribute und Ansprüche die Option Bearbeiten aus.
4. Gehen Sie auf der Seite „Attribute und Ansprüche“ wie folgt vor:

- a. Wählen Sie Neuen Anspruch hinzufügen aus
 - b. Geben Sie unter Name AccessControl:*AttributeName* ein.
AttributeName Ersetzen Sie es durch den Namen des Attributs, das Sie im IAM Identity Center erwarten. Beispiel, AccessControl:**Department**.
 - c. Geben Sie für Namespace **https://aws.amazon.com/SAML/Attributes** ein.
 - d. Wählen Sie unter Source (Quelle) die Option Attribute (Attribut) aus.
 - e. Verwenden Sie für das Quellattribut die Dropdownliste, um die Microsoft Entra ID Benutzerattribute auszuwählen. Beispiel, user.**department**.
5. Wiederholen Sie den vorherigen Schritt für jedes Attribut, das Sie in der SAML-Assertion an das IAM Identity Center senden müssen.
 6. Wählen Sie Speichern.

Configure ABAC using IAM Identity Center

Konfigurieren Sie ABAC mithilfe von IAM Identity Center

Bei dieser Methode verwenden Sie die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center, um ein Attribute Element zu übergeben, dessen Name Attribut auf gesetzt ist.
`https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Sie können dieses Element verwenden, um Attribute als Sitzungs-Tags in der SAML-Assertion zu übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie AWS STS [im IAM-Benutzerhandbuch unter Übergeben von Sitzungs-Tags](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das AttributeValue-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Tag-Schlüssel-Wert-Paar Department=billing zu übergeben:

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Weisen Sie den Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um Zugriff auf AWS-Konten nur zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

Note

Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Schritt 1: IAM Identity Center: Grant Microsoft Entra ID Benutzerzugriff auf Konten

1. Kehren Sie zur IAM Identity Center-Konsole zurück. Wählen Sie im IAM Identity Center-Navigationsbereich unter Multi-account Berechtigungen die Option. AWS-Konten
2. Auf der AWS-Konten Seite „Organisationsstruktur“ wird Ihr Organisationsstamm mit Ihren Konten darunter in der Hierarchie angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:
 - a. Für Schritt 1: Wählen Sie Benutzer und Gruppen aus, wählen Sie den Benutzer aus, der die Administratorfunktion ausführen soll. Klicken Sie anschließend auf Weiter.
 - b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Unterschritte führt, die zum Erstellen eines Berechtigungssatzes erforderlich sind.
 - i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:
 - Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
 - Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

Wählen Sie Weiter aus.
 - ii. Für Schritt 2: Geben Sie die Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter.

Mit den Standardeinstellungen wird ein Berechtigungssatz *AdministratorAccess* mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist.

- iii. Stellen Sie für Schritt 3: Prüfen und Erstellen sicher, dass der Berechtigungssatztyp die AWS verwaltete Richtlinie verwendet *AdministratorAccess*. Wählen Sie Erstellen aus. Auf der Seite „Berechtigungssätze“ wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diesen Tab jetzt in Ihrem Webbrowser schließen.
 - iv. Auf dem Browser-Tab Benutzer und Gruppen zuweisen befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.
 - v. Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *AdministratorAccess* Berechtigungssatz wird in der Liste angezeigt. Markieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter aus.
- c. Überprüfen Sie für Schritt 3: Prüfen und Absenden den ausgewählten Benutzer und den ausgewählten Berechtigungssatz und wählen Sie dann Senden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihre gerade konfiguriert AWS-Konto wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. Eine Benachrichtigung informiert Sie darüber, dass Ihre Berechtigungen erneut bereitgestellt AWS-Konto wurden und der aktualisierte Berechtigungssatz angewendet wurde. Wenn sich der Benutzer anmeldet, hat er die Möglichkeit, die Rolle auszuwählen. *AdministratorAccess*

Schritt 2: Microsoft Entra ID: Bestätigen Microsoft Entra ID Zugriff der Benutzer auf AWS Ressourcen

1. Kehren Sie zur Microsoft Entra ID Konsole zurück und navigieren Sie zu Ihrer IAM Identity SAML-based Sign-on Center-Anwendung.
2. Wählen Sie Benutzer und Gruppen und dann Benutzer oder Gruppen hinzufügen aus. Sie fügen den Benutzer, den Sie in diesem Tutorial in Schritt 4 erstellt haben, der Microsoft Entra ID Anwendung hinzu. Indem Sie den Benutzer hinzufügen, ermöglichen Sie ihm, sich anzumelden AWS. Suchen Sie nach dem Benutzer, den Sie in Schritt 4 erstellt haben. Wenn Sie diesen Schritt befolgt hätten, wäre dies der Fall **RichardRoe**.

- Eine Demo finden Sie unter Verbinden Sie [Ihre bestehende IAM Identity Center-Instanz mit Microsoft Entra ID](#)

Microsoft Entra ID Konfiguration für den Zugriff auf zusätzliche Regionen von IAM Identity Center — optional

Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und AWS-Konten über die zusätzlichen Regionen zu ermöglichen. Die folgenden Schritte führen Sie durch das Verfahren. Weitere Informationen zu diesem Thema, einschließlich der Voraussetzungen, finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

1. Rufen Sie die ACS-URLs für die zusätzlichen Regionen von der IAM Identity Center-Konsole ab, wie unter beschrieben [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#).
2. Navigieren Sie in der [Microsoft Entra Admin](#) Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann. AWS IAM Identity Center
3. Wählen Sie links 2 aus. Richten Sie Single Sign-On ein.
4. Wählen Sie auf der Seite SAML-Basiskonfiguration im Abschnitt Antwort-URL (Assertion Consumer Service URL) die Option Antwort-URL für die ACS-URL jeder weiteren Region hinzufügen aus. Sie können die ACS-URL der primären Region als Standardadresse beibehalten, sodass Benutzer immer wieder zur primären Region umgeleitet werden, wenn sie die Anwendung von dort aus starten. AWS IAM Identity Center Microsoft Entra ID
5. Wenn Sie mit dem Hinzufügen der ACS-URLs fertig sind, speichern Sie die AWS IAM Identity Center Anwendung.
6. Sie können in jeder weiteren Region eine Lesezeichen-App Microsoft Entra ID für das AWS Access Portal erstellen. Auf diese Weise können Ihre Benutzer in weiteren Regionen AWS auf das Zugangsportal zugreifen. Microsoft Entra ID Stellen Sie sicher, dass Sie Ihren Benutzern Berechtigungen für den Zugriff auf die Lesezeichen-Apps in Microsoft Entra ID gewähren. Weitere Informationen finden Sie in der [Microsoft Entra ID Dokumentation](#).
7. Stellen Sie sicher, dass Sie sich in jeder weiteren Region beim AWS Access Portal anmelden können. Navigieren Sie zu den URLs des [AWS Access-Portals](#) oder starten Sie die Lesezeichen-Apps von Microsoft Entra ID.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Fehlerbehebung mit Microsoft Entra ID finden Sie in den folgenden Abschnitten:

- [Probleme bei der Synchronisation mit Microsoft Entra ID und IAM Identity Center](#)
- [Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden](#)
- [Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden](#)
- [Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter](#)
- [Weitere Ressourcen](#)

Probleme bei der Synchronisation mit Microsoft Entra ID und IAM Identity Center

Wenn Sie Probleme mit Microsoft Entra ID Benutzern haben, die sich nicht mit IAM Identity Center synchronisieren, kann dies an einem Syntaxproblem liegen, das IAM Identity Center gemeldet hat, als ein neuer Benutzer zu IAM Identity Center hinzugefügt wird. Sie können dies bestätigen, indem Sie die Microsoft Entra ID Auditprotokolle auf fehlgeschlagene Ereignisse überprüfen, wie z. B. 'Export'. Der Statusgrund für dieses Ereignis lautet:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Sie können auch AWS CloudTrail nach dem fehlgeschlagenen Ereignis suchen. Sie können dies tun, indem Sie in der Event-History-Konsole nach dem folgenden Filter suchen: CloudTrail

```
"eventName": "CreateUser"
```

Der Fehler in der CloudTrail Veranstaltung lautet wie folgt:

```
"errorCode": "ValidationException",  
  "errorMessage": "Currently list attributes only allow single item"
```

Letztlich bedeutet diese Ausnahme, dass einer der übergebenen Werte mehr Werte als erwartet Microsoft Entra ID enthielt. Die Lösung besteht darin, die Attribute des Benutzers zu überprüfen

und sicherzustellen, dass Microsoft Entra ID, dass keines davon doppelte Werte enthält. Ein häufiges Beispiel für doppelte Werte ist das Vorhandensein mehrerer Werte für Kontaktnummern wie Handy, Arbeit und Fax. Obwohl es sich um separate Werte handelt, werden sie alle unter dem einzigen übergeordneten Attribut `PhoneNumbers` an IAM Identity Center übergeben.

Allgemeine Tipps zur SCIM-Fehlerbehebung finden Sie unter Problembehandlung. [???](#)

Microsoft Entra ID Synchronisierung des Gastkontos

Wenn Sie Ihre Microsoft Entra ID Gastbenutzer mit IAM Identity Center synchronisieren möchten, gehen Sie wie folgt vor.

Die E-Mail-Adresse von Gastbenutzern unterscheidet sich von der E-Mail-Adresse von Microsoft Entra ID Benutzern. Dieser Unterschied führt zu Problemen beim Versuch, Microsoft Entra ID Gastbenutzer mit IAM Identity Center zu synchronisieren. Sehen Sie sich zum Beispiel die folgende E-Mail-Adresse für einen Gastbenutzer an:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

IAM Identity Center erwartet nicht, dass die E-Mail-Adresse das `#EXT#@domain` Format enthält.

1. Melden Sie sich im [Microsoft Entra Admin Center](#) an und navigieren Sie zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann AWS IAM Identity Center
2. Navigieren Sie im linken Bereich zur Registerkarte Single Sign On.
3. Wählen Sie Bearbeiten aus. Diese Option wird neben Benutzerattribute und Ansprüche angezeigt.
4. Wählen Sie nach den erforderlichen Ansprüchen die Option Eindeutige Benutzerkennung (Namen-ID) aus.
5. Sie erstellen zwei Anspruchsbedingungen für Ihre Microsoft Entra ID Benutzer und Gastbenutzer:
 - a. Erstellen Sie für Microsoft Entra ID Benutzer einen Benutzertyp für Mitglieder, bei dem das Quellattribut auf festgelegt ist `user.userprincipalname`.
 - b. Erstellen Sie für Microsoft Entra ID Gastbenutzer einen Benutzertyp für externe Gäste, wobei das Quellattribut auf festgelegt ist `user.mail`.
 - c. Wählen Sie Speichern und versuchen Sie erneut, sich als Microsoft Entra ID Gastbenutzer anzumelden.

Weitere Ressourcen

- Allgemeine Tipps zur SCIM-Fehlerbehebung finden Sie unter [Problembehandlung bei IAM Identity Center-Problemen](#)
- Informationen zur Microsoft Entra ID Problembehandlung finden Sie in der [Microsoft Dokumentation](#).
- Weitere Informationen zum mehrfachen AWS-Konten Verbund finden Sie unter [Sichern AWS-Konten mit Azure Active Directory Federation](#).

Die folgenden Ressourcen können Ihnen bei der Arbeit mit folgenden Problemen helfen AWS:

- [AWS re:Post](#)- Hier finden Sie häufig gestellte Fragen und Links zu anderen Ressourcen, die Ihnen bei der Behebung von Problemen helfen.
- [AWS Support](#)- Holen Sie sich technischen Support

Konfigurieren Sie SAML und SCIM mit Okta und IAM Identity Center

Mithilfe des [SCIM 2.0-Protokolls \(System for Identity Management\)](#) können Sie Benutzer- und Gruppeninformationen automatisch Okta in IAM Cross-domain Identity Center bereitstellen oder synchronisieren. Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Um diese Verbindung zu konfigurieren Okta, verwenden Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Trägertoken, das automatisch von IAM Identity Center erstellt wird. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Okta zu den benannten Attributen in IAM Identity Center. Diese Zuordnung entspricht den erwarteten Benutzerattributen zwischen IAM Identity Center und Ihrem Konto. Okta

Okta unterstützt die folgenden Bereitstellungsfunktionen, wenn Sie über SCIM mit IAM Identity Center verbunden sind:

- Benutzer erstellen — Benutzer, die der IAM Identity Center-Anwendung in zugewiesen Okta sind, werden in IAM Identity Center bereitgestellt.
- Benutzerattribute aktualisieren — Attributänderungen für Benutzer, die der IAM Identity Center-Anwendung in zugewiesen sind, Okta werden in IAM Identity Center aktualisiert.

- Benutzer deaktivieren — Benutzer, denen die Zuweisung zur IAM Identity Center-Anwendung in aufgehoben wurde, Okta sind in IAM Identity Center deaktiviert.
- Gruppen-Push — Gruppen (und ihre Mitglieder) Okta werden mit IAM Identity Center synchronisiert.

 Note

Um den Verwaltungsaufwand Okta sowohl in IAM Identity Center als auch in IAM Identity Center zu minimieren, empfehlen wir, Gruppen zuzuweisen und zu pushen, anstatt einzelne Benutzer zu verwenden.

- Benutzer importieren — Benutzer können aus IAM Identity Center in importiert werden. Okta

Ziel

In diesem Tutorial werden Sie Schritt für Schritt die Einrichtung einer SAML-Verbindung mit Okta IAM Identity Center beschrieben. Später werden Sie Benutzer mithilfe von Okta SCIM synchronisieren. In diesem Szenario verwalten Sie alle Benutzer und Gruppen in Okta. Benutzer melden sich über das Okta Portal an. Um zu überprüfen, ob alles korrekt konfiguriert ist, melden Sie sich nach Abschluss der Konfigurationsschritte als Okta Benutzer an und verifizieren den Zugriff auf AWS Ressourcen.

Die folgenden Funktionen werden unterstützt, wenn Sie über SAML Okta eine Verbindung zum IAM Identity Center herstellen:

- IdP-initiated SAML-Anmeldung — Benutzer melden sich über das Okta Portal an und erhalten Zugriff auf das IAM Identity Center.
- SP-initiated SAML-Anmeldung — Benutzer greifen auf das Zugriffsportal AWS zu, das sie zur Anmeldung über das Portal weiterleitet. Okta

 Note

Sie können sich für ein Okta Konto ([kostenlose Testversion](#)) registrieren, auf dem die Okta's [IAM Identity Center-Anwendung](#) installiert ist. Bei kostenpflichtigen Okta Produkten müssen Sie möglicherweise bestätigen, dass Ihre Okta Lizenz das Lebenszyklusmanagement oder ähnliche Funktionen unterstützt, die die Bereitstellung ausgehender Daten ermöglichen. Diese Funktionen sind möglicherweise erforderlich, um SCIM von zu IAM Identity Center Okta zu konfigurieren.

Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter. [IAM Identity Center aktivieren](#)

Überlegungen

- Bevor Sie die SCIM-Bereitstellung zwischen Okta und IAM Identity Center konfigurieren, empfehlen wir Ihnen, dies zunächst zu überprüfen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#)
- Für jeden Okta Benutzer müssen die Werte Vorname, Nachname, Benutzername und Anzeigename angegeben werden.
- Jeder Okta Benutzer hat nur einen einzigen Wert pro Datenattribut, z. B. E-Mail-Adresse oder Telefonnummer. Alle Benutzer mit mehreren Werten können nicht synchronisiert werden. Wenn es Benutzer gibt, deren Attribute mehrere Werte enthalten, entfernen Sie die doppelten Attribute, bevor Sie versuchen, den Benutzer in IAM Identity Center bereitzustellen. Beispielsweise kann nur ein Telefonnummernattribut synchronisiert werden, da das Standard-Telefonnummernattribut „Geschäftstelefon“ ist. Verwenden Sie das Attribut „Geschäftstelefon“, um die Telefonnummer des Benutzers zu speichern, auch wenn es sich bei der Telefonnummer des Benutzers um ein Festnetz oder ein Mobiltelefon handelt.
- Bei Verwendung Okta mit IAM Identity Center wird IAM Identity Center in der Regel als Anwendung in konfiguriert. Okta Auf diese Weise können Sie mehrere Instanzen von IAM Identity Center als mehrere Anwendungen konfigurieren, die den Zugriff auf mehrere AWS Organizations innerhalb einer einzigen Instanz von unterstützen. Okta
- Berechtigungen und Rollenattribute werden nicht unterstützt und können nicht mit IAM Identity Center synchronisiert werden.
- Die Verwendung derselben Okta Gruppe sowohl für Zuweisungen als auch für Gruppen-Push wird derzeit nicht unterstützt. Um konsistente Gruppenmitgliedschaften zwischen Okta und IAM Identity Center aufrechtzuerhalten, erstellen Sie eine separate Gruppe und konfigurieren Sie sie so, dass Gruppen per Push an IAM Identity Center weitergeleitet werden.
- Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und über zusätzliche Regionen zu ermöglichen. AWS-Konten Weitere Informationen, einschließlich der Voraussetzungen, finden Sie unter. [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#) Okta-specific Die Schritte sind beschrieben in [OktaKonfiguration für den Zugriff auf zusätzliche Regionen](#)

Schritt 1: Okta: Besorgen Sie sich die SAML-Metadaten von Ihrem Okta Konto

1. Melden Sie sich bei anOkta admin dashboard, erweitern Sie Anwendungen und wählen Sie dann Anwendungen aus.
2. Wählen Sie auf der Seite Applications (Anwendungen) die Option Browse App Catalog (App-Katalog durchsuchen) aus.
3. Geben Sie in das Suchfeld die App ein AWS IAM Identity Center und wählen Sie sie aus, um die IAM Identity Center-App hinzuzufügen.
4. Wählen Sie den Tab Anmelden aus.
5. Wählen Sie unter SAML-Signaturzertifikate die Option Aktionen und dann IdP-Metadaten anzeigen aus. Ein neuer Browser-Tab wird geöffnet, der den Dokumentenbaum einer XML-Datei anzeigt. Wählen Sie das gesamte XML von `<md:EntityDescriptor>` bis aus `</md:EntityDescriptor>` und kopieren Sie es in eine Textdatei.
6. Speichern Sie die Textdatei unter `metadata.xml`.

Lassen Sie das Fenster Okta admin dashboard geöffnet, Sie werden diese Konsole in den späteren Schritten weiter verwenden.

Schritt 2: IAM Identity Center: Konfigurieren Okta als Identitätsquelle für IAM Identity Center

1. Öffnen Sie die [IAM Identity Center-Konsole](#) als Benutzer mit Administratorrechten.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Option Aktionen und dann Identitätsquelle ändern aus.
4. Wählen Sie unter Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.
5. Gehen Sie unter Externen Identitätsanbieter konfigurieren wie folgt vor:
 - a. Kopieren Sie unter Metadaten des Dienstanbieters die folgenden Elemente in eine Textdatei, um den Zugriff zu erleichtern:
 - URL des IAM Identity Center Assertion Consumer Service (ACS) — Sie haben die Wahl zwischen IPv4-only ACS-URLs mit zwei Stacks. Wenn Ihre IAM Identity Center-Instanz

in mehreren Regionen aktiviert ist, hat außerdem jede weitere Region ihre eigenen ACS-URLs IPv4-only und Dual-Stack-ACS-URLs. Weitere Informationen zu ACS-URLs finden Sie unter [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#)

- URL des IAM Identity Center-Ausstellers

Sie benötigen diese Werte später in diesem Tutorial.

- b. Wählen Sie unter Identitätsanbieter-Metadaten unter IdP-SAML-Metadaten die Option Datei auswählen und wählen Sie dann die `metadata.xml` Datei aus, die Sie im vorherigen Schritt erstellt haben.
 - c. Wählen Sie Weiter aus.
6. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
 7. Wählen Sie Identitätsquelle ändern aus.

Lassen Sie die AWS Konsole geöffnet, Sie werden diese Konsole im nächsten Schritt weiter verwenden.

8. Kehren Sie zur AWS IAM Identity Center App zurück Oka admin dashboard und wählen Sie die Registerkarte Anmelden aus. Wählen Sie dann Bearbeiten aus.
9. Geben Sie unter Erweiterte Sign-on Einstellungen Folgendes ein:
 - Geben Sie für ACS-URL die Werte ein, die Sie für die IAM Identity Center Assertion Consumer Service (ACS) -URL kopiert haben. Sie können die ACS-URL der primären Region als Standardadresse verwenden, sodass Benutzer in die primäre Region umgeleitet werden, wenn sie die Amazon Web Services Services-Anwendung von startenOka.
 - (Optional) Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, können Sie auch eine Lesezeichen-App Oka für das AWS Zugriffsportale in jeder weiteren Region erstellen. Auf diese Weise können Ihre Benutzer von aus auf das AWS Zugriffsportale in weiteren Regionen zugreifen. Oka Stellen Sie sicher, dass Sie Ihren Benutzern Berechtigungen für den Zugriff auf die Lesezeichen-Apps in Oka gewähren. Weitere Informationen finden Sie in der [OktaDokumentation](#). Wenn Sie planen, IAM Identity Center zu einem späteren Zeitpunkt in weitere Regionen zu replizieren, finden Sie [OktaKonfiguration für den Zugriff auf zusätzliche Regionen](#) unter Anleitung, wie Sie nach dieser ersten Einrichtung den Zugriff auf die zusätzlichen Regionen aktivieren können.
 - Geben Sie für Issuer URL den Wert ein, den Sie für IAM Identity Center Issuer URL kopiert haben

- Wählen Sie für das Format des Anwendungsbenutzernamens eine der Optionen aus dem Menü aus.

Stellen Sie sicher, dass der von Ihnen gewählte Wert für jeden Benutzer einzigartig ist. Wählen Sie für dieses Tutorial den Okta-Benutzernamen

10. Wählen Sie Speichern.

Sie sind jetzt bereit, Benutzer vom IAM Identity Center aus Okta bereitzustellen. Lassen Sie das Okta admin dashboard Fenster geöffnet und kehren Sie für den nächsten Schritt zur IAM Identity Center-Konsole zurück.

Schritt 3: IAM Identity Center und Okta: Bereitstellung Okta users

1. Suchen Sie in der IAM Identity Center-Konsole auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpunkt- und Zugriffstoken-Informationen angezeigt.
2. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten die einzelnen Werte für die folgenden Optionen:
 - a. SCIM-Endpunkt — Das Endpunktformat hängt von Ihrer Konfiguration ab:
 - IPv4: `https://scim.us-east-2.amazonaws.com//1111111111-2222-3333-4444-555555555555scim/v2`
 - Dual-stack `https://scim.us-east-2: 1111111111-2222-3333-4444-555555555555.api.aws//scim/v2`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte Okta später in diesem Tutorial eingeben, um die automatische Bereitstellung zu konfigurieren.

3. Klicken Sie auf Schließen.

4. Kehren Sie zur IAM Identity Center App zurück. Okta admin dashboard und navigieren Sie zur App.
5. Wählen Sie auf der Seite der IAM Identity Center-App den Tab Provisioning und wählen Sie dann in der linken Navigationsleiste unter Einstellungen die Option Integration aus.
6. Wählen Sie Bearbeiten und aktivieren Sie dann das Kontrollkästchen neben API-Integration aktivieren, um die automatische Bereitstellung zu aktivieren.
7. Verwenden Sie für die Konfiguration Okta die SCIM-Bereitstellungswerte AWS IAM Identity Center, die Sie zuvor in diesem Schritt kopiert haben:
 - a. Geben Sie im Feld Basis-URL den SCIM-Endpunkt ein.
 - b. Geben Sie im Feld API-Token den Wert für das Zugriffstoken ein.
8. Wählen Sie API-Anmeldeinformationen testen, um zu überprüfen, ob die eingegebenen Anmeldeinformationen gültig sind.

Die Nachricht AWS IAM Identity Center wurde erfolgreich verifiziert! zeigt an.

9. Wählen Sie Speichern. Sie werden in den Bereich Einstellungen verschoben, in dem Integration ausgewählt ist.
10. Wählen Sie unter Einstellungen die Option Zur App aus und aktivieren Sie dann das Kontrollkästchen Aktivieren für jede der Funktionen von Provisioning to App, die Sie aktivieren möchten. Wählen Sie für dieses Tutorial alle Optionen aus.
11. Wählen Sie Speichern.

Sie sind jetzt bereit, Ihre Benutzer Okta mit IAM Identity Center zu synchronisieren.

Schritt 4: Okta: Synchronisieren Sie Benutzer von Okta mit IAM Identity Center

Standardmäßig sind Ihrer Okta IAM Identity Center-App keine Gruppen oder Benutzer zugewiesen. Durch die Bereitstellung von Gruppen werden die Benutzer bereitgestellt, die Mitglieder der Gruppe sind. Gehen Sie wie folgt vor, um Gruppen und Benutzer mit AWS IAM Identity Center zu synchronisieren.

1. Wählen Sie auf der Seite der Okta IAM Identity Center-App den Tab Zuweisungen aus. Sie können der IAM Identity Center-App sowohl Personen als auch Gruppen zuweisen.
 - a. So weisen Sie Personen zu:

- Wählen Sie auf der Seite „Aufgaben“ die Option „Zuweisen“ und dann „Personen zuweisen“ aus.
- Wählen Sie die Okta Benutzer aus, die Zugriff auf die IAM Identity Center-App haben sollen. Wählen Sie „Zuweisen“, dann „Speichern und Zurück“ und anschließend „Fertig“.

Dadurch wird der Prozess der Bereitstellung der Benutzer für IAM Identity Center gestartet.

b. Um Gruppen zuzuweisen:

- Wählen Sie auf der Seite „Zuweisungen“ die Option „Zuweisen“ und anschließend „Gruppen zuweisen“.
- Wählen Sie die Okta Gruppen aus, für die Sie Zugriff auf die IAM Identity Center-App haben möchten. Wählen Sie „Zuweisen“, dann „Speichern und Zurück“ und anschließend „Fertig“.

Dadurch wird der Prozess der Bereitstellung der Benutzer in der Gruppe für IAM Identity Center gestartet.

 Note

Möglicherweise müssen Sie zusätzliche Attribute für die Gruppe angeben, wenn diese nicht in allen Benutzerdatensätzen vorhanden sind. Die für die Gruppe angegebenen Attribute haben Vorrang vor allen individuellen Attributwerten.

2. Wählen Sie die Registerkarte Push-Gruppen. Wählen Sie die Okta Gruppe aus, die Sie mit IAM Identity Center synchronisieren möchten. Wählen Sie Speichern.

Der Gruppenstatus ändert sich in Aktiv, nachdem die Gruppe und ihre Mitglieder per Push an IAM Identity Center weitergeleitet wurden.

3. Kehren Sie zur Registerkarte „Zuweisungen“ zurück.
4. Gehen Sie wie folgt vor, um einzelne Okta Benutzer zu IAM Identity Center hinzuzufügen:
 - a. Wählen Sie auf der Seite „Zuweisungen“ die Option „Zuweisen“ und dann „Personen zuweisen“.
 - b. Wählen Sie die Okta Benutzer aus, die Zugriff auf die IAM Identity Center-App haben sollen. Wählen Sie „Zuweisen“, dann „Speichern und Zurück“ und anschließend „Fertig“.

Damit wird der Prozess der Bereitstellung der einzelnen Benutzer für IAM Identity Center gestartet.

 Note

Sie können der AWS IAM Identity Center App auch Benutzer und Gruppen zuweisen, und zwar auf der Anwendungsseite von. Okta admin dashboard Wählen Sie dazu das Einstellungssymbol aus und wählen Sie dann Benutzern zuweisen oder Zu Gruppen zuweisen und geben Sie dann den Benutzer oder die Gruppe an.

5. Kehren Sie zur IAM Identity Center-Konsole zurück. Wählen Sie in der linken Navigationsleiste Benutzer aus. Sie sollten die Benutzerliste mit Ihren Okta Benutzern sehen.

 Herzlichen Glückwunsch!

Sie haben erfolgreich eine SAML-Verbindung zwischen Okta und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert. Sie können diese Benutzer jetzt Konten und Anwendungen in IAM Identity Center zuweisen. Für dieses Tutorial bestimmen wir im nächsten Schritt einen der Benutzer als IAM Identity Center-Administrator, indem wir ihm Administratorrechte für das Verwaltungskonto gewähren.

Übergabe von Attributen für die Zugriffskontrolle - Optional

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
```

```
</saml:AttributeValue>  
</saml:Attribute>  
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates `Attribute` Element hinzu.

Weisen Sie Zugriff zu AWS-Konten

Die folgenden Schritte sind nur erforderlich, um AWS-Konten nur Zugriff zu gewähren. Diese Schritte sind nicht erforderlich, um Zugriff auf AWS Anwendungen zu gewähren.

Note

Um diesen Schritt abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Schritt 1: IAM Identity Center: Grant Okta Benutzerzugriff auf Konten

1. Wählen Sie im Navigationsbereich von IAM Identity Center unter Multi-accountBerechtigungen die Option AWS-Konten.
2. Auf der AWS-KontenSeite „Organisationsstruktur“ wird Ihr Organisationsstamm mit Ihren Konten darunter in der Hierarchie angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:
 - a. Wählen Sie für Schritt 1: Benutzer und Gruppen auswählen den Benutzer aus, der die Administratorfunktion ausführen soll. Klicken Sie anschließend auf Weiter.
 - b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Teilschritte beim Erstellen eines Berechtigungssatzes führt.
 - i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:
 - Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.

- Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus `AdministratorAccess`.

Wählen Sie Weiter aus.

- ii. Für Schritt 2: Geben Sie die Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter aus.

Mit den Standardeinstellungen wird ein Berechtigungssatz `AdministratorAccess` mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist.

- iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet `AdministratorAccess`. Wählen Sie Erstellen aus. Auf der Seite Berechtigungssätze wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diese Registerkarte jetzt in Ihrem Webbrowser schließen.

Auf der Browser-Registerkarte „Benutzer und Gruppen zuweisen“ befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte `AdministratorAccess` Berechtigungssatz wird in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter.

- c. Überprüfen Sie für Schritt 3: Überprüfen und Absenden den ausgewählten Benutzer und den ausgewählten Berechtigungssatz und wählen Sie dann Absenden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihr AWS-Konto System gerade konfiguriert wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. In einer Benachrichtigung werden Sie darüber informiert, dass Ihr AWS-Konto Konto erneut bereitgestellt und der aktualisierte Berechtigungssatz angewendet wurde. Wenn sich der Benutzer anmeldet, hat er die Möglichkeit, die Rolle auszuwählen. `AdministratorAccess`

Schritt 2: Okta: Bestätigen Okta Benutzerzugriff auf AWS Ressourcen

1. Melden Sie sich mit einem Testkonto bei der anOkta dashboard.

2. Wählen Sie unter Meine Apps das AWS IAM Identity Center Symbol aus.
3. Sie sollten das AWS-Konto Symbol sehen. Erweitern Sie dieses Symbol, um die Liste zu sehen, auf AWS-Konten die der Benutzer zugreifen kann. In diesem Tutorial haben Sie nur mit einem einzigen Konto gearbeitet, sodass beim Erweitern des Symbols nur ein Konto angezeigt wird.
4. Wählen Sie das Konto aus, um die für den Benutzer verfügbaren Berechtigungssätze anzuzeigen. In diesem Tutorial haben Sie den AdministratorAccessBerechtigungssatz erstellt.
5. Neben dem Berechtigungssatz befinden sich Links für den Zugriffstyp, der für diesen Berechtigungssatz verfügbar ist. Bei der Erstellung des Berechtigungssatzes haben Sie sowohl den Zugriff auf den als auch den AWS-Managementkonsole programmatischen Zugriff angegeben. Wählen Sie Managementkonsole aus, um die zu öffnen. AWS-Managementkonsole
6. Der Benutzer ist bei angemeldet AWS-Managementkonsole.

Sie können auch das AWS Zugriffsportal verwenden. Dadurch werden Sie weitergeleitet, sich über das Okta Portal anzumelden, bevor Sie zum AWS Zugangsportal weitergeleitet werden. Dieser Pfad folgt dem SP-initiated SAML-Anmeldeablauf.

Okta Konfiguration für den Zugriff auf zusätzliche Regionen von IAM Identity Center — optional

Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und AWS-Konten über die zusätzlichen Regionen zu ermöglichen. Die folgenden Schritte führen Sie durch das Verfahren. Weitere Informationen zu diesem Thema, einschließlich der Voraussetzungen, finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

1. Rufen Sie die ACS-URLs für die zusätzlichen Regionen von der IAM Identity Center-Konsole ab, wie unter beschrieben [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#).
2. Wählen Sie im Navigationsbereich des Okta Admin-Dashboards Anwendungen und anschließend in der erweiterten Liste erneut Anwendungen aus.
3. Wählen Sie die AWS IAM Identity Center-Anwendung.
4. Wählen Sie die Registerkarte Sign On (Anmelden) aus.
5. Wählen Sie unter Erweiterte Sign-on Einstellungen und Andere anforderbare SSO-URLs die Option Weitere hinzufügen für die ACS-URL jeder weiteren Region aus und fügen Sie die ACS-URL in das Textfeld ein.

6. Wenn Sie mit dem Hinzufügen der ACS-URLs fertig sind, speichern Sie die AWS IAM Identity Center-Anwendung.
7. Sie können in jeder weiteren Region eine Lesezeichen-App Okta für das AWS Zugriffsportal erstellen. Auf diese Weise können Ihre Benutzer von aus auf das AWS Zugriffsportal in weiteren Regionen zugreifen. Stellen Sie sicher, dass Sie Ihren Benutzern Berechtigungen für den Zugriff auf die Lesezeichen-Apps in Okta gewähren. Weitere Informationen finden Sie in der [Okta-Dokumentation](#).
8. Stellen Sie sicher, dass Sie sich in jeder weiteren Region beim AWS Zugangsportal anmelden können. Navigieren Sie zu den [URLs des AWS Access-Portals](#) oder starten Sie die Lesezeichen-Apps von Okta.

Nächste Schritte

Nachdem Sie die Konfiguration Okta als Identitätsanbieter vorgenommen und Benutzer in IAM Identity Center bereitgestellt haben, können Sie:

- Zugriff gewähren auf AWS-Konten, siehe. [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#)
- Zugriff auf Cloud-Anwendungen gewähren, siehe [Weisen Sie den Benutzerzugriff auf Anwendungen in der IAM Identity Center-Konsole zu](#).
- Konfigurieren Sie Berechtigungen auf der Grundlage von Aufgabenfunktionen, siehe [Einen Berechtigungssatz erstellen](#).

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit Okta finden Sie in den folgenden Abschnitten:

- [Aus IAM Identity Center gelöschte Benutzer und Gruppen erneut bereitstellen](#)
- [Fehler bei der automatischen Bereitstellung in Okta](#)
- [Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden](#)
- [Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden](#)
- [Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter](#)

- [Weitere Ressourcen](#)

Aus IAM Identity Center gelöschte Benutzer und Gruppen erneut bereitstellen

- Wenn Sie versuchen, einen Benutzer oder eine Gruppe zu ändern, die einmal synchronisiert und dann aus IAM Identity Center gelöscht wurde, wird möglicherweise die folgende Fehlermeldung in der Okta Konsole angezeigt:
 - Der automatische Profil-Push des Benutzers *Jane Doe* zur App ist AWS IAM Identity Center fehlgeschlagen: Fehler beim Versuch, die Profilaktualisierung für zu pushen *jane_doe@example.com*: Für den Benutzer wurde kein Benutzer zurückgegeben *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Die verknüpfte Gruppe fehlt in AWS IAM Identity Center. Ändern Sie die verknüpfte Gruppe, um weiterhin Gruppenmitgliedschaften zu übertragen.
- Möglicherweise erhalten Sie auch die folgende Fehlermeldung in den Okta Systemprotokollen für synchronisierte und gelöschte IAM Identity Center-Benutzer oder -Gruppen:
 - Okta-Fehler: Eventfailed application.provision.user.push_profile: Für den Benutzer wurde kein Benutzer zurückgegeben *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Okta-Fehler: application.provision.group_push.mapping.update.or.delete.failed.with.error: Die verknüpfte Gruppe fehlt in. AWS IAM Identity Center Ändern Sie die verknüpfte Gruppe, um die Übertragung von Gruppenmitgliedschaften fortzusetzen.

Warning

Benutzer und Gruppen sollten Okta nicht aus dem IAM Identity Center gelöscht werden, wenn Sie das IAM Identity Center mit SCIM synchronisiert Okta haben.

Fehlerbehebung für gelöschte IAM Identity Center-Benutzer

Um dieses Problem mit gelöschten IAM Identity Center-Benutzern zu beheben, müssen die Benutzer von gelöscht werden. Okta Falls erforderlich, müssten diese Benutzer auch neu erstellt werden. Okta Wenn der Benutzer neu erstellt wird, wird er ebenfalls über SCIM erneut im IAM Identity Center bereitgestellt. [Weitere Informationen zum Löschen eines Benutzers finden Sie in der Dokumentation. Okta](#)

 Note

Wenn Sie einem Okta Benutzer den Zugriff auf IAM Identity Center entziehen müssen, sollten Sie ihn zuerst aus seinem Gruppen-Push und dann aus seiner Zuweisungsgruppe entfernen. Okta Dadurch wird sichergestellt, dass der Benutzer aus der ihm zugewiesenen Gruppenmitgliedschaft in IAM Identity Center entfernt wird. Weitere Informationen zur Fehlerbehebung bei Group Push finden Sie in der [OktaDokumentation](#).

Fehlerbehebung bei gelöschten IAM Identity Center-Gruppen

Um dieses Problem mit gelöschten IAM Identity Center-Gruppen zu beheben, muss die Gruppe aus Okta gelöscht werden. Falls erforderlich, müssten diese Gruppen auch in Okta mithilfe von Group Push neu erstellt werden. Wenn der Benutzer in Okta neu erstellt wird, wird er auch über SCIM erneut im IAM Identity Center bereitgestellt. [Weitere Informationen zum Löschen einer Gruppe finden Sie in der Okta-Dokumentation](#).

Fehler bei der automatischen Bereitstellung in Okta

Wenn Sie die folgende Fehlermeldung erhalten inOkta:

Die automatische Bereitstellung des Benutzers Jane Doe für die App ist AWS IAM Identity Center fehlgeschlagen: Der passende Benutzer wurde nicht gefunden

Weitere Informationen finden Sie in der [OktaDokumentation](#).

Weitere Ressourcen

- Allgemeine Tipps zur SCIM-Fehlerbehebung finden Sie unter [Problembehandlung bei IAM Identity Center-Problemen](#).

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit AWS helfen:

- [AWS re:Post](#)- Hier finden Sie häufig gestellte Fragen und Links zu anderen Ressourcen, die Ihnen bei der Behebung von Problemen helfen.
- [AWS Support](#)- Holen Sie sich technischen Support

Einrichtung der SCIM-Bereitstellung zwischen OneLogin und IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen aus dem OneLogin IAM Identity Center mithilfe des SCIM-Protokolls (System for Cross-Domain Identity Management) v2.0. Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Note

OneLogin unterstützt derzeit den SAML Multiple Assertion Consume Service (ACS) in der Anwendung nicht. URLs AWS IAM Identity Center Diese SAML-Funktion ist erforderlich, um die [Unterstützung mehrerer Regionen](#) in IAM Identity Center in vollem Umfang nutzen zu können. Wenn Sie planen, IAM Identity Center in weitere Regionen zu replizieren, beachten Sie, dass die Verwendung einer einzigen ACS-URL die Benutzererfahrung in diesen zusätzlichen Regionen beeinträchtigen kann. Ihre Hauptregion wird weiterhin normal funktionieren. Wir empfehlen, dass Sie mit Ihrem IdP-Anbieter zusammenarbeiten, um diese Funktion zu aktivieren. Weitere Informationen zur Benutzererfahrung in weiteren Regionen mit einer einzigen ACS-URL finden Sie unter [the section called “Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs”](#) und [the section called “AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu”](#).

Sie konfigurieren diese Verbindung in OneLogin, indem Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Trägertoken verwenden, das automatisch von IAM Identity Center erstellt wird. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute OneLogin zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. OneLogin

In den folgenden Schritten erfahren Sie, wie Sie mithilfe des SCIM-Protokolls die automatische Bereitstellung von Benutzern und Gruppen von OneLogin zu IAM Identity Center aktivieren.

Note

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu lesen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#)

Themen

- [Voraussetzungen](#)
- [Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center](#)
- [Schritt 2: Konfigurieren Sie die Bereitstellung in OneLogin](#)
- [\(Optional\) Schritt 3: Konfigurieren Sie Benutzerattribute OneLogin für die Zugriffskontrolle im IAM Identity Center](#)
- [\(Optional\) Übergabe von Attributen für die Zugriffskontrolle](#)
- [Fehlerbehebung](#)

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- Ein OneLogin Konto. Wenn Sie noch kein Konto haben, können Sie auf der [OneLoginWebsite](#) [möglicherweise ein kostenloses Test- oder Entwicklerkonto beantragen](#).
- Ein [IAM Identity Center-fähiges Konto \(kostenlos\)](#). Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
- Eine SAML-Verbindung von Ihrem OneLogin Konto zum IAM Identity Center. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On zwischen OneLogin und AWS](#) im AWS Partner Network-Blog.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung zu aktivieren.

Um die automatische Bereitstellung in IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.

4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpunkt — Zum Beispiel `https://scim.us-east-2.amazonaws.com/scim/v2/1111111111-2222-3333-4444-5555555555`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Sie haben jetzt die Bereitstellung in der IAM Identity Center-Konsole eingerichtet. Jetzt müssen Sie die verbleibenden Aufgaben mithilfe der OneLogin Admin-Konsole ausführen, wie im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren Sie die Bereitstellung in OneLogin

Verwenden Sie das folgende Verfahren in der OneLogin Admin-Konsole, um die Integration zwischen IAM Identity Center und der IAM Identity Center-App zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die AWS Single Sign-On-Anwendung bereits OneLogin für die SAML-Authentifizierung konfiguriert haben. Wenn Sie diese SAML-Verbindung noch nicht hergestellt haben, tun Sie dies, bevor Sie fortfahren, und kehren Sie dann hierher zurück, um den SCIM-Bereitstellungsprozess abzuschließen. Weitere Informationen zur Konfiguration von SAML mit OneLogin finden Sie unter [Aktivieren von Single Sign-On zwischen OneLogin und AWS](#) im Partner Network-Blog. AWS

So konfigurieren Sie die Bereitstellung in OneLogin

1. Melden Sie sich an OneLogin und navigieren Sie dann zu Anwendungen > Anwendungen.

2. Suchen Sie auf der Seite Anwendungen nach der Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen. Wählen Sie sie aus und wählen Sie dann im Navigationsbereich Konfiguration aus.
3. Im vorherigen Verfahren haben Sie den SCIM-Endpunkt in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Basis-URL ein. OneLogin Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Bearer-Token ein. OneLogin
4. Klicken Sie neben API-Verbindung auf Aktivieren und dann auf Speichern, um die Konfiguration abzuschließen.
5. Wählen Sie im Navigationsbereich Provisioning (Bereitstellung) aus.
6. Aktivieren Sie die Kontrollkästchen für Bereitstellung aktivieren, Benutzer erstellen, Benutzer löschen und Benutzer aktualisieren und wählen Sie dann Speichern aus.
7. Klicken Sie im Navigationsbereich auf Users (Benutzer).
8. Klicken Sie auf Weitere Aktionen und wählen Sie Logins synchronisieren aus. Sie sollten die Meldung Benutzer mit AWS Single Sign-On synchronisieren erhalten.
9. Klicken Sie erneut auf Weitere Aktionen und wählen Sie dann Berechtigungszuordnungen erneut anwenden aus. Sie sollten die Meldung „Zuordnungen werden erneut angewendet“ erhalten.
10. Zu diesem Zeitpunkt sollte der Bereitstellungsprozess beginnen. Um dies zu bestätigen, navigieren Sie zu Aktivität > Ereignisse und überwachen Sie den Fortschritt. Erfolgreiche Bereitstellungsereignisse sowie Fehler sollten im Event-Stream erscheinen.
11. Um zu überprüfen, ob Ihre Benutzer und Gruppen alle erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Ihre synchronisierten Benutzer von OneLogin werden auf der Seite Benutzer angezeigt. Sie können Ihre synchronisierten Gruppen auch auf der Gruppenseite einsehen.
12. Um Benutzeränderungen automatisch mit IAM Identity Center zu synchronisieren, navigieren Sie zur Seite Provisioning, suchen Sie den Abschnitt Administratorgenehmigung erforderlich, bevor diese Aktion ausgeführt wird, deaktivieren Sie die Optionen Benutzer erstellen, Benutzer löschen, Benutzer and/or aktualisieren und klicken Sie auf Speichern.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute OneLogin für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für die OneLogin Konfiguration von Attributen, die Sie in IAM Identity Center verwenden, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die Attribute,

die Sie definieren, OneLogin werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, die Sie übergeben haben. OneLogin

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die [Attribute für Zugriffskontrolle](#) Funktion aktivieren. Weitere Information dazu finden Sie unter [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#).

Um Benutzerattribute OneLogin für die Zugriffskontrolle im IAM Identity Center zu konfigurieren

1. Melden Sie sich an OneLogin und navigieren Sie dann zu Anwendungen > Anwendungen.
2. Suchen Sie auf der Seite Anwendungen nach der Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen. Wählen Sie sie aus und klicken Sie dann im Navigationsbereich auf Parameter.
3. Gehen Sie im Abschnitt Erforderliche Parameter für jedes Attribut, das Sie in IAM Identity Center verwenden möchten, wie folgt vor:
 - a. Wählen Sie +.
 - b. Geben Sie im Feld Feldname den Namen des Attributs ein `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, das Sie in IAM Identity Center erwarten, und ersetzen **AttributeName** Sie es durch. Beispiel, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
 - c. Aktivieren Sie unter Flags das Kontrollkästchen neben In SAML-Assertion einbeziehen und wählen Sie Speichern aus.
 - d. Verwenden Sie im Feld Wert die Dropdownliste, um die OneLogin Benutzerattribute auszuwählen. Zum Beispiel Abteilung.
4. Wählen Sie Speichern.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates `Attribute` Element hinzu.

Fehlerbehebung

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Einrichtung der automatischen Bereitstellung auftreten können. OneLogin

Gruppen werden nicht für IAM Identity Center bereitgestellt

Standardmäßig können Gruppen nicht vom IAM Identity Center aus OneLogin bereitgestellt werden. Stellen Sie sicher, dass Sie die Gruppenbereitstellung für Ihre IAM Identity Center-Anwendung in aktiviert haben. OneLogin Melden Sie sich dazu bei der OneLogin Admin-Konsole an und stellen Sie sicher, dass in den Eigenschaften der IAM Identity Center-Anwendung (IAM Identity Center-Anwendung > Parameter > Gruppen) die Option In die Benutzerverwaltung einbeziehen ausgewählt ist. [Weitere Informationen zum Erstellen von Gruppen in OneLogin, einschließlich der Synchronisation von OneLogin Rollen als Gruppen in SCIM, finden Sie auf der Website. OneLogin](#)

Es wird nichts vom OneLogin IAM Identity Center synchronisiert, obwohl alle Einstellungen korrekt sind

Zusätzlich zu dem obigen Hinweis zur Genehmigung durch den Administrator müssen Sie die Berechtigungszuordnungen erneut anwenden, damit viele Konfigurationsänderungen wirksam werden. Dies finden Sie unter Anwendungen > Anwendungen > IAM Identity Center-Anwendung > Weitere Aktionen. Details und Protokolle zu den meisten Aktionen OneLogin, einschließlich Synchronisierungsereignissen, finden Sie unter Aktivität > Ereignisse.

Ich habe eine Gruppe gelöscht oder deaktiviert OneLogin, aber sie wird immer noch in IAM Identity Center angezeigt

OneLogin unterstützt derzeit den SCIM DELETE-Vorgang für Gruppen nicht, was bedeutet, dass die Gruppe weiterhin in IAM Identity Center existiert. Sie müssen die Gruppe daher direkt aus IAM Identity Center entfernen, um sicherzustellen, dass alle entsprechenden Berechtigungen in IAM Identity Center für diese Gruppe entfernt werden.

Ich habe eine Gruppe in IAM Identity Center gelöscht, ohne sie vorher zu löschen, OneLogin und jetzt habe ich Synchronisierungsprobleme user/group

Um dieses Problem zu beheben, stellen Sie zunächst sicher, dass Sie keine redundanten Regeln oder Konfigurationen für die Gruppenbereitstellung eingerichtet haben. OneLogin Zum Beispiel eine Gruppe, die einer Anwendung direkt zugewiesen ist, zusammen mit einer Regel, die für dieselbe Gruppe veröffentlicht. Löschen Sie anschließend alle unerwünschten Gruppen in IAM Identity Center. Aktualisieren Sie abschließend die Berechtigungen (IAM Identity Center App > Provisioning > Berechtigungen) und wenden Sie dann die Berechtigungszuordnungen erneut an (IAM Identity Center App > Weitere Aktionen). OneLogin Um dieses Problem in future zu vermeiden, nehmen Sie zunächst die Änderung vor, um die Bereitstellung der Gruppe in zu beenden OneLogin, und löschen Sie dann die Gruppe aus IAM Identity Center.

Ping Identity Produkte mit IAM Identity Center verwenden

Die folgenden Ping Identity Produkte wurden mit IAM Identity Center getestet.

Themen

- [PingFederate](#)
- [PingOne](#)

PingFederate

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen aus dem PingFederate Produkt Ping Identity (im Folgenden „Ping“) in IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. Weitere Informationen finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Sie konfigurieren diese Verbindung PingFederate mithilfe Ihres IAM Identity Center SCIM-Endpoints und Ihres Zugriffstokens. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute PingFederate zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. PingFederate

Dieses Handbuch basiert auf PingFederate Version 10.2. Die Schritte für andere Versionen können variieren. Wenden Sie sich an Ping, um weitere Informationen zur Konfiguration der Bereitstellung im IAM Identity Center für andere Versionen von zu erhalten. PingFederate

In den folgenden Schritten erfahren Sie, wie Sie mithilfe des SCIM-Protokolls die automatische Bereitstellung von Benutzern und Gruppen von PingFederate zu IAM Identity Center aktivieren.

Note

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu lesen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#) Lesen Sie dann im nächsten Abschnitt weitere Überlegungen durch.

Themen

- [Voraussetzungen](#)
- [Überlegungen](#)
- [Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center](#)
- [Schritt 2: Konfigurieren Sie die Bereitstellung in PingFederate](#)
- [\(Optional\) Schritt 3: Konfigurieren Sie Benutzerattribute in PingFederate für die Zugriffskontrolle im IAM Identity Center](#)
- [\(Optional\) Übergabe von Attributen für die Zugriffskontrolle](#)
- [Fehlerbehebung](#)

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- Ein funktionierender PingFederate Server. Wenn Sie noch keinen PingFederate Server haben, können Sie auf der [Ping Identity-Website](#) möglicherweise ein kostenloses Test- oder Entwicklerkonto beantragen. Die Testversion umfasst Lizenzen und Software-Downloads sowie die zugehörige Dokumentation.
- Eine Kopie der auf Ihrem PingFederate Server installierten PingFederate IAM Identity Center Connector-Software. Weitere Informationen zum Erwerb dieser Software finden Sie auf der Website unter [IAM Identity Center Connector](#). Ping Identity

- [Ein IAM Identity Center-fähiges Konto \(kostenlos\)](#). Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
- Eine SAML-Verbindung von Ihrer PingFederate Instance zum IAM Identity Center. Anweisungen zur Konfiguration dieser Verbindung finden Sie in der PingFederate Dokumentation. Zusammenfassend lässt sich sagen, dass der empfohlene Weg darin besteht, den IAM Identity Center Connector zur Konfiguration von „Browser SSO“ zu verwenden und dabei die Metadaten-Funktionen „Herunterladen“ und „Importieren“ an beiden Enden zu verwenden, um SAML-Metadaten zwischen PingFederate und IAM Identity Center auszutauschen. PingFederate
- Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und von diesen Regionen aus zu ermöglichen. AWS-Konten Weitere Details finden Sie unter [the section called “Schritt 3 \(nur externe Identitätsanbieter\): Aktualisieren Sie das externe IdP-Setup”](#). Weitere Informationen finden Sie in der PingFederate Dokumentation.

Überlegungen

Im Folgenden finden Sie wichtige Überlegungen PingFederate, die sich darauf auswirken können, wie Sie die Bereitstellung mit IAM Identity Center implementieren.

- Wenn ein Attribut (z. B. eine Telefonnummer) von einem Benutzer im in konfigurierten Datenspeicher entfernt wird PingFederate, wird dieses Attribut nicht aus dem entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung bei der Implementierung von PingFederate's Provisionern. Wenn ein Attribut für einen Benutzer in einen anderen (nicht leeren) Wert geändert wird, wird diese Änderung mit IAM Identity Center synchronisiert.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung zu aktivieren.

Um die automatische Bereitstellung in IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity](#) Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM

Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.

4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpunkt — Zum Beispiel `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben über die PingFederate Verwaltungskonsole ausführen. Die Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren Sie die Bereitstellung in PingFederate

Verwenden Sie das folgende Verfahren in der PingFederate Verwaltungskonsole, um die Integration zwischen IAM Identity Center und dem IAM Identity Center Connector zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die IAM Identity Center Connector-Software bereits installiert haben. Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen zur [Voraussetzungen](#) Konfiguration der SCIM-Bereitstellung in diesem Verfahren und führen Sie es anschließend aus.

 Important

Wenn Ihr PingFederate Server noch nicht für ausgehende SCIM-Bereitstellung konfiguriert wurde, müssen Sie möglicherweise eine Änderung der Konfigurationsdatei vornehmen, um die Bereitstellung zu aktivieren. Weitere Informationen finden Sie in der Ping-

Dokumentation. Zusammenfassend müssen Sie die `pf.provisioner.mode` Einstellung in der `pingfederate-<version>/pingfederate/bin/run.properties` Datei auf einen anderen Wert als OFF (Standardeinstellung) ändern und den Server neu starten, falls er gerade läuft. Sie können beispielsweise die Option verwenden, `STANDALONE` wenn Sie derzeit keine Hochverfügbarkeitskonfiguration mit PingFederate haben.

So konfigurieren Sie die Bereitstellung in PingFederate

1. Melden Sie sich an der PingFederate Administrationskonsole an.
2. Wählen Sie oben auf der Seite Anwendungen aus und klicken Sie dann auf SP-Verbindungen.
3. Suchen Sie die Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen, und klicken Sie auf den Verbindungsnamen.
4. Wählen Sie in den dunklen Navigationsüberschriften oben auf der Seite den Verbindungstyp aus. Sie sollten sehen, dass Browser-SSO bereits aus Ihrer vorherigen SAML-Konfiguration ausgewählt wurde. Wenn nicht, müssen Sie zuerst diese Schritte ausführen, bevor Sie fortfahren können.
5. Aktivieren Sie das Kontrollkästchen Outbound Provisioning, wählen Sie IAM Identity Center Cloud Connector als Typ aus und klicken Sie auf Speichern. Wenn IAM Identity Center Cloud Connector nicht als Option angezeigt wird, stellen Sie sicher, dass Sie den IAM Identity Center Connector installiert und Ihren Server neu gestartet haben. PingFederate
6. Klicken Sie wiederholt auf Weiter, bis Sie zur Seite Outbound Provisioning gelangen, und klicken Sie dann auf die Schaltfläche Provisioning konfigurieren.
7. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-URL in der Konsole ein. PingFederate Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Zugriffstoken in der PingFederate Konsole ein. Klicken Sie auf Speichern.
8. Klicken Sie auf der Seite Kanalkonfiguration (Kanäle konfigurieren) auf Erstellen.
9. Geben Sie einen Kanalnamen für diesen neuen Bereitstellungskanal ein (z. **B.AWSIAMIdentityCenterchannel**) und klicken Sie auf Weiter.
10. Wählen Sie auf der Seite Quelle den Active Data Store aus, den Sie für Ihre Verbindung zum IAM Identity Center verwenden möchten, und klicken Sie auf Weiter.

 Note

Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Informationen zur Auswahl und Konfiguration einer Datenquelle finden Sie in der Ping Produktdokumentation unter `PingFederate`.

11. Vergewissern Sie sich auf der Seite mit den Quelleinstellungen, dass alle Werte für Ihre Installation korrekt sind, und klicken Sie dann auf Weiter.
12. Geben Sie auf der Seite Quellspeicherort die für Ihre Datenquelle geeigneten Einstellungen ein, und klicken Sie dann auf Weiter. Wenn Sie beispielsweise Active Directory als LDAP-Verzeichnis verwenden:
 - a. Geben Sie den Basis-DN Ihrer AD-Gesamtstruktur ein (z. **B.DC=myforest,DC=mydomain,DC=com**).
 - b. Geben Sie unter Benutzer > Gruppen-DN eine einzelne Gruppe an, die alle Benutzer enthält, die Sie für IAM Identity Center bereitstellen möchten. Wenn keine solche einzelne Gruppe existiert, erstellen Sie diese Gruppe in AD, kehren Sie zu dieser Einstellung zurück und geben Sie dann den entsprechenden DN ein.
 - c. Geben Sie an, ob Untergruppen (verschachtelte Suche) durchsucht werden sollen, und geben Sie alle erforderlichen LDAP-Filter an.
 - d. Geben Sie unter Gruppen > Gruppen-DN eine einzelne Gruppe an, die alle Gruppen enthält, die Sie für IAM Identity Center bereitstellen möchten. In vielen Fällen kann es sich dabei um denselben DN handeln, den Sie im Abschnitt Benutzer angegeben haben. Geben Sie nach Bedarf Werte für verschachtelte Suche und Filter ein.
13. Stellen Sie auf der Seite Attributzuordnung Folgendes sicher, und klicken Sie dann auf Weiter:
 - a. Das Feld `UserName` muss einem Attribut zugeordnet werden, das als E-Mail formatiert ist (`user@domain.com`). Es muss auch mit dem Wert übereinstimmen, den der Benutzer für die Anmeldung bei Ping verwenden wird. Dieser Wert wird wiederum während der Verbundauthentifizierung in den `nameId` SAML-Anspruch übernommen und für den Abgleich mit dem Benutzer in IAM Identity Center verwendet. Wenn Sie beispielsweise Active Directory verwenden, können Sie den `UserPrincipalName` als `UserName` angeben.
 - b. Andere Felder mit dem Suffix `*` müssen Attributen zugeordnet werden, die für Ihre Benutzer ungleich Null sind.

14. Setzen Sie auf der Seite Aktivierung und Zusammenfassung den Kanalstatus auf Aktiv, damit die Synchronisation sofort nach dem Speichern der Konfiguration gestartet wird.
15. Vergewissern Sie sich, dass alle Konfigurationswerte auf der Seite korrekt sind, und klicken Sie auf Fertig.
16. Klicken Sie auf der Seite „Kanäle verwalten“ auf Speichern.
17. An diesem Punkt beginnt die Bereitstellung. Um die Aktivität zu bestätigen, können Sie sich die Datei provisioner.log ansehen, die sich standardmäßig im pingfederate-`<version>/pingfederate/`logVerzeichnis auf Ihrem PingFederate Server befindet.
18. Um zu überprüfen, ob Benutzer und Gruppen erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center Console zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von PingFederate werden auf der Seite Benutzer angezeigt. Sie können synchronisierte Gruppen auch auf der Gruppenseite anzeigen.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute in PingFederate für die Zugriffskontrolle im IAM Identity Center

Dies ist ein optionales Verfahren für die PingFederate Konfiguration von Attributen, die Sie in IAM Identity Center verwenden, um den Zugriff auf Ihre Ressourcen zu verwalten. AWS Die Attribute, die Sie definieren, PingFederate werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, die Sie übergeben haben. PingFederate

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die [Attribute für Zugriffskontrolle](#) Funktion aktivieren. Weitere Information dazu finden Sie unter [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#).

Um Benutzerattribute PingFederate für die Zugriffskontrolle im IAM Identity Center zu konfigurieren

1. Melden Sie sich an der PingFederate Administrationskonsole an.
2. Wählen Sie oben auf der Seite Anwendungen aus und klicken Sie dann auf SP-Verbindungen.
3. Suchen Sie die Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen, und klicken Sie auf den Verbindungsnamen.
4. Wählen Sie in den dunklen Navigationsüberschriften oben auf der Seite die Option Browser-SSO aus. Klicken Sie anschließend auf Browser-SSO konfigurieren.
5. Wählen Sie auf der Seite Browser-SSO konfigurieren die Option Assertion Creation aus und klicken Sie dann auf Configure Assertion Creation.

6. Wählen Sie auf der Seite „Assertionserstellung konfigurieren“ die Option **Attributvertrag** aus.
7. Fügen Sie auf der Seite „Attributvertrag“ im Abschnitt „Vertrag verlängern“ ein neues Attribut hinzu, indem Sie die folgenden Schritte ausführen:
 - a. Geben Sie in das Textfeld den Namen des Attributs ein `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, das Sie in IAM Identity Center erwarten, und ersetzen **AttributeName** Sie es durch. Beispiel, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
 - b. Wählen Sie für Attributnamenformat die Option `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.
 - c. Wählen Sie „Hinzufügen“ und anschließend „Weiter“.
8. Wählen Sie auf der Seite „Zuordnung der Authentifizierungsquelle“ die mit Ihrer Anwendung konfigurierte Adapterinstanz aus.
9. Wählen Sie auf der Seite „Erfüllung des Attributvertrags“ die Quelle (Datenspeicher) und den Wert (Datenspeicherattribut) für den Attributvertrag aus `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.

 Note

Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Informationen zur Auswahl und Konfiguration einer Datenquelle finden Sie in der Ping Produktdokumentation unter [PingFederate](#).

10. Klicken Sie wiederholt auf Weiter, bis Sie zur Seite Aktivierung und Zusammenfassung gelangen, und klicken Sie dann auf Speichern.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit PingFederate finden Sie in den folgenden Abschnitten:

- [Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden](#)
- [Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden](#)
- [Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter](#)
- [Weitere Informationen zu finden Sie in der PingFederate Dokumentation](#)

Die folgenden Ressourcen können Ihnen bei der Problembhebung bei der Arbeit mit helfen AWS:

- [AWS re:Post](#)- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- [AWS Support](#)- Holen Sie sich technischen Support

PingOne

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzerinformationen aus dem PingOne Produkt Ping Identity (im Folgenden „Ping“) in IAM Identity Center. Bei dieser Bereitstellung wird das SCIM-Protokoll (System for Cross-Domain Identity Management) v2.0 verwendet. Sie konfigurieren diese Verbindung PingOne mithilfe Ihres IAM Identity Center SCIM-Endpoints und Ihres Zugriffstokens. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute PingOne zu den benannten

Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. PingOne

In den folgenden Schritten erfahren Sie, wie Sie mithilfe des SCIM-Protokolls die automatische Bereitstellung von Benutzern von PingOne bis zum IAM Identity Center aktivieren.

Note

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu lesen. [Überlegungen zur Verwendung der automatischen Bereitstellung](#) Lesen Sie dann im nächsten Abschnitt weitere Überlegungen durch.

Themen

- [Voraussetzungen](#)
- [Überlegungen](#)
- [Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center](#)
- [Schritt 2: Konfigurieren Sie die Bereitstellung in PingOne](#)
- [\(Optional\) Schritt 3: Konfigurieren Sie Benutzerattribute PingOne für die Zugriffskontrolle in IAM Identity Center](#)
- [\(Optional\) Übergabe von Attributen für die Zugriffskontrolle](#)
- [Fehlerbehebung](#)

Voraussetzungen

Bevor Sie beginnen können, benötigen Sie Folgendes:

- Ein PingOne Abonnement oder eine kostenlose Testversion mit föderierten Authentifizierungs- und Bereitstellungsfunktionen. Weitere Informationen darüber, wie Sie eine kostenlose Testversion erhalten, finden Sie auf der [Ping Identity](#) Website.
- [Ein IAM Identity Center-fähiges Konto \(kostenlos\)](#). Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
- Die PingOne IAM Identity Center-Anwendung wurde Ihrem PingOne Admin-Portal hinzugefügt. Sie können die PingOne IAM Identity Center-Anwendung aus dem PingOne Anwendungskatalog abrufen. Allgemeine Informationen finden [Sie unter Hinzufügen einer Anwendung aus dem Anwendungskatalog](#) auf der Ping Identity Website.

- Eine SAML-Verbindung von Ihrer PingOne Instance zum IAM Identity Center. Nachdem die PingOne IAM Identity Center-Anwendung zu Ihrem PingOne Admin-Portal hinzugefügt wurde, müssen Sie sie verwenden, um eine SAML-Verbindung von Ihrer PingOne Instance zum IAM Identity Center zu konfigurieren. Verwenden Sie die Funktion „Metadaten herunterladen“ und „Importieren“ an beiden Enden, um SAML-Metadaten zwischen PingOne und IAM Identity Center auszutauschen. Anweisungen zur Konfiguration dieser Verbindung finden Sie in der PingOne Dokumentation.
- Wenn Sie IAM Identity Center in weitere Regionen repliziert haben, müssen Sie Ihre Identity Provider-Konfiguration aktualisieren, um den Zugriff auf AWS verwaltete Anwendungen und AWS-Konten von diesen Regionen aus zu ermöglichen. Weitere Details finden Sie unter [the section called “Schritt 3 \(nur externe Identitätsanbieter\): Aktualisieren Sie das externe IdP-Setup”](#). Weitere Informationen finden Sie in der PingOne Dokumentation.

Überlegungen

Im Folgenden finden Sie wichtige Überlegungen PingOne, die sich darauf auswirken können, wie Sie die Bereitstellung mit IAM Identity Center implementieren.

- PingOne unterstützt die Bereitstellung von Gruppen über SCIM nicht. Wenden Sie sich an, Ping um die neuesten Informationen zur Gruppenunterstützung in SCIM für zu erhalten. PingOne
- Benutzer können auch PingOne nach der Deaktivierung der Bereitstellung im Admin-Portal weiterhin Provisioning erhalten. PingOne Wenn Sie die Bereitstellung sofort beenden müssen, löschen Sie das entsprechende SCIM-Bearer-Token und deaktivieren Sie es im IAM Identity Center. and/or [Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit](#)
- Wenn ein Attribut für einen Benutzer aus dem in konfigurierten Datenspeicher entfernt wird PingOne, wird dieses Attribut nicht aus dem entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung bei der Implementierung von PingOne's Provisionern. Wenn ein Attribut geändert wird, wird die Änderung mit IAM Identity Center synchronisiert.
- Im Folgenden finden Sie wichtige Hinweise zu Ihrer SAML-Konfiguration in: PingOne
 - IAM Identity Center unterstützt nur emailaddress als NameId Format. Das bedeutet, dass Sie für Ihre SAML_SUBJECT-Zuordnung in ein Benutzerattribut wählen müssen PingOne, das innerhalb Ihres Verzeichnisses eindeutig ist, einen Wert ungleich Null hat und das als email/UPN (z. B. user@domain.com) formatiert ist. PingOne E-Mail (Arbeit) ist ein sinnvoller Wert für Testkonfigurationen mit dem integrierten Verzeichnis. PingOne

- Benutzer PingOne mit einer E-Mail-Adresse, die ein +-Zeichen enthält, können sich möglicherweise nicht bei IAM Identity Center anmelden, was zu Fehlern wie 'SAML_215' oder 'Invalid input' führt. Um dieses Problem zu beheben PingOne, wählen Sie in unter Attributzuordnungen die Option Erweitert für die Zuordnung SAML_SUBJECT aus. Legen Sie dann im Drop-down-Menü das Name-ID-Format fest, das an SP: to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress gesendet werden soll.

Schritt 1: Aktivieren Sie die Bereitstellung im IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung zu aktivieren.

Um die automatische Bereitstellung in IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity](#) Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpoint und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpoint — Zum Beispiel `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpoint und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mithilfe der PingOne IAM Identity Center-Anwendung ausführen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren Sie die Bereitstellung in PingOne

Verwenden Sie das folgende Verfahren in der PingOne IAM Identity Center-Anwendung, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die PingOne IAM Identity Center-Anwendung bereits zu Ihrem Admin-Portal hinzugefügt haben. PingOne Falls Sie dies noch nicht getan haben, finden Sie weitere Informationen unter diesem Verfahren zur [Voraussetzungen](#) Konfiguration der SCIM-Bereitstellung und führen Sie es anschließend aus.

So konfigurieren Sie die Bereitstellung in PingOne

1. Öffnen Sie die PingOne IAM Identity Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben PingOne (Anwendungen > Meine Anwendungen). Siehe [Voraussetzungen](#).
2. Scrollen Sie zum Ende der Seite. Wählen Sie unter Benutzerbereitstellung den vollständigen Link aus, um zur Benutzerbereitstellungskonfiguration Ihrer Verbindung zu gelangen.
3. Wählen Sie auf der Seite mit den Anweisungen zur Bereitstellung die Option Weiter zum nächsten Schritt aus.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-URL in der PingOne IAM Identity Center-Anwendung ein. Außerdem haben Sie im vorherigen Verfahren den Wert des Zugriffstokens in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld ACCESS_TOKEN in der PingOne IAM Identity Center-Anwendung ein.
5. Wählen Sie für REMOVE_ACTION entweder Deaktiviert oder Gelöscht (weitere Informationen finden Sie im Beschreibungstext auf der Seite).
6. Wählen Sie auf der Seite „Attributzuordnung“ einen Wert aus, der für die SAML_SUBJECT (NameId) -Assertion verwendet werden soll. Folgen Sie dabei den Anweisungen weiter oben auf dieser Seite. [Überlegungen](#) Wählen Sie dann Weiter zum nächsten Schritt.
7. Nehmen Sie auf der Seite PingOneApp-Anpassung — IAM Identity Center die gewünschten Anpassungsänderungen vor (optional) und klicken Sie auf Weiter zum nächsten Schritt.

8. Wählen Sie auf der Seite Gruppenzugriff die Gruppen aus, die die Benutzer enthalten, die Sie für die Bereitstellung und das Single Sign-On bei IAM Identity Center aktivieren möchten. Wählen Sie Weiter zum nächsten Schritt.
9. Scrollen Sie zum Ende der Seite und wählen Sie Fertig stellen, um mit der Bereitstellung zu beginnen.
10. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von PingOne werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt Konten und Anwendungen in IAM Identity Center zugewiesen werden.

Denken Sie daran, dass die Bereitstellung von Gruppen oder Gruppenmitgliedschaften über SCIM PingOne nicht unterstützt wird. Kontaktieren Sie uns Ping für weitere Informationen.

(Optional) Schritt 3: Konfigurieren Sie Benutzerattribute PingOne für die Zugriffskontrolle in IAM Identity Center

Dies ist ein optionales Verfahren, PingOne wenn Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre AWS Ressourcen zu verwalten. Die von Ihnen definierten Attribute werden in PingOne einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie in IAM Identity Center einen Berechtigungssatz, um den Zugriff auf der Grundlage der Attribute zu verwalten, die Sie übergeben haben. PingOne

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die [Attribute für Zugriffskontrolle](#) Funktion aktivieren. Weitere Information dazu finden Sie unter [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#).

Um Benutzerattribute PingOne für die Zugriffskontrolle im IAM Identity Center zu konfigurieren

1. Öffnen Sie die PingOne IAM Identity Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben PingOne (Anwendungen > Meine Anwendungen).
2. Wählen Sie Bearbeiten und dann Weiter zum nächsten Schritt, bis Sie zur Seite „Attributzuordnungen“ gelangen.
3. Wählen Sie auf der Seite „Attributzuordnungen“ die Option Neues Attribut hinzufügen aus, und gehen Sie dann wie folgt vor. Sie müssen diese Schritte für jedes Attribut ausführen, das Sie zur Verwendung in IAM Identity Center für die Zugriffskontrolle hinzufügen möchten.

- a. Geben `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName` Sie im Feld Anwendungsattribut den Wert ein. *AttributeName* Ersetzen Sie es durch den Namen des Attributs, das Sie in IAM Identity Center erwarten. Beispiel, `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
 - b. Wählen Sie im Feld Identity Bridge-Attribut oder Literalwert Benutzerattribute aus Ihrem PingOne Verzeichnis aus. Zum Beispiel E-Mail (Arbeit).
4. Wählen Sie einige Male Weiter und dann Fertig stellen.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die [Attribute für Zugriffskontrolle](#) Funktion in IAM Identity Center verwenden, um ein Attribute Element zu übergeben, dessen Name Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie [AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben](#).

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates Attribute Element hinzu.

Fehlerbehebung

Informationen zur allgemeinen SCIM- und SAML-Problembehandlung mit PingOne finden Sie in den folgenden Abschnitten:

- [Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden](#)

- [Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden](#)
- [Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter](#)
- [Weitere Informationen zu finden Sie in der PingOne DokumentationPingOne.](#)

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit helfen AWS:

- [AWS re:Post](#)- Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, die Ihnen bei der Behebung von Problemen helfen.
- [AWS Support](#)- Holen Sie sich technischen Support

Benutzerzugriff mit dem Standard-IAM Identity Center-Verzeichnis konfigurieren

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert, sodass Sie keine Identitätsquelle auswählen müssen. Wenn Ihre Organisation einen anderen Identitätsanbieter wie Microsoft Active Directory, verwendet oder Okta erwägen Microsoft Entra ID, diese Identitätsquelle in IAM Identity Center zu integrieren, anstatt die Standardkonfiguration zu verwenden.

Ziel

In diesem Tutorial verwenden Sie das Standardverzeichnis als Identitätsquelle und eine IAM Identity Center-Organisationsinstanz, um einen Administratorbenutzer einzurichten und zu testen. Dieser Administratorbenutzer erstellt und verwaltet Benutzer und Gruppen und gewährt AWS Zugriff mit Berechtigungssätzen. In den nächsten Schritten erstellen Sie Folgendes:

- Ein administrativer Benutzer mit dem Namen *Nikki Wolf*
- Eine Gruppe mit dem Namen *Admin team*
- Ein Berechtigungssatz mit dem Namen *AdminAccess*

Um zu überprüfen, ob alles korrekt erstellt wurde, melden Sie sich an und legen das Passwort des Administratorbenutzers fest. Nach Abschluss dieses Tutorials können Sie den Administratorbenutzer verwenden, um weitere Benutzer in IAM Identity Center hinzuzufügen, zusätzliche Berechtigungssätze zu erstellen und den organisatorischen Zugriff auf Anwendungen einzurichten. Wenn Sie Benutzern Zugriff auf die Anwendung gewähren möchten, können

Sie alternativ [Schritt 1 dieses](#) Verfahrens ausführen und den Anwendungszugriff [Zugriff auf Anwendungen konfigurieren](#) konfigurieren.

Voraussetzungen

Die folgenden Voraussetzungen sind erforderlich, um dieses Tutorial abzuschließen:

- [IAM Identity Center aktivieren](#) und verfügen über eine [Organisationsinstanz von IAM Identity Center](#).
 - Wenn Sie eine [Kontoinstanz](#) von IAM Identity Center haben, können Sie Benutzer und Gruppen erstellen und ihnen Zugriff auf Anwendungen gewähren. Weitere Informationen finden Sie unter [Anwendungszugriff](#).
- Melden Sie sich bei der IAM Identity Center-Konsole an AWS-Managementkonsole und greifen Sie entweder wie folgt auf die IAM Identity Center-Konsole zu:
 - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie den AWS-Konto Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Bereits verwendet AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
 - Weitere Hilfe zur Anmeldung bei der finden Sie [AWS-Anmeldung im AWS-Managementkonsole Guide](#).
- Sie können die mehrstufige Authentifizierung für Ihre IAM Identity Center-Benutzer konfigurieren. Weitere Informationen finden Sie unter [MFA im IAM Identity Center konfigurieren](#).

Schritt 1: Einen Benutzer hinzufügen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich von IAM Identity Center die Option **Benutzer** und dann **Benutzer hinzufügen** aus.
3. Geben Sie auf der Seite „Benutzerdetails angeben“ die folgenden Informationen ein:
 - **Benutzername** — Geben Sie für dieses Tutorial Folgendes ein **nikkIW**.

Wählen Sie beim Erstellen von Benutzern Benutzernamen aus, die leicht zu merken sind. Ihre Benutzer müssen sich den Benutzernamen merken, um sich beim AWS Access-Portal anzumelden. Sie können ihn später nicht mehr ändern.

- **Passwort** — Wählen Sie Eine E-Mail mit Anweisungen zur Passwortkonfiguration an diesen Benutzer senden (empfohlen).

Diese Option sendet dem Benutzer eine von Amazon Web Services adressierte E-Mail mit dem Betreff Einladung zur Teilnahme am IAM Identity Center. Die E-Mail stammt von entweder `no-reply@signin.aws` oder `no-reply@login.awsapps.com`. Fügen Sie diese E-Mail-Adressen zu Ihrer Liste der zulässigen Absender hinzu.

- **E-Mail-Adresse** — Geben Sie eine E-Mail-Adresse für den Benutzer ein, an den Sie die E-Mail erhalten können. Geben Sie sie dann erneut ein, um sie zu bestätigen. Jeder Benutzer muss eine eindeutige E-Mail-Adresse haben.
 - **Vorname** — Geben Sie den Vornamen des Benutzers ein. Geben Sie für dieses Tutorial *Nikki* ein.
 - **Nachname** — Geben Sie den Nachnamen des Benutzers ein. Geben Sie für dieses Tutorial *Wolf* ein.
 - **Anzeigename** — Der Standardwert ist der Vor- und Nachname des Benutzers. Wenn Sie den Anzeigenamen ändern möchten, können Sie etwas anderes eingeben. Der Anzeigename ist im Anmeldeportal und in der Benutzerliste sichtbar.
 - **Füllen Sie bei Bedarf die optionalen Informationen aus.** Es wird in diesem Tutorial nicht verwendet und Sie können es später ändern.
4. Wählen Sie Weiter aus. Die Seite Benutzer zu Gruppen hinzufügen wird angezeigt. Wir werden eine Gruppe erstellen, der wir Administratorberechtigungen zuweisen können, anstatt sie direkt zu erteilen *Nikki*.

Wählen Sie Gruppe erstellen

Ein neuer Browser-Tab wird geöffnet, auf dem die Seite „Gruppe erstellen“ angezeigt wird.

- a. Geben Sie unter Gruppendetails im Feld Gruppenname einen Namen für die Gruppe ein. Wir empfehlen einen Gruppennamen, der die Rolle der Gruppe identifiziert. Geben Sie für dieses Tutorial *Admin team* ein.
 - b. Wählen Sie Gruppe erstellen
 - c. Schließen Sie den Browser-Tab „Gruppen“, um zum Browser-Tab „Benutzer hinzufügen“ zurückzukehren
5. Wählen Sie im Bereich Gruppen die Schaltfläche „Aktualisieren“. Die *Admin team* Gruppe wird in der Liste angezeigt.

Markieren Sie das Kontrollkästchen neben *Admin team*, und wählen Sie dann Weiter aus.

6. Bestätigen Sie auf der Seite „Benutzer überprüfen und hinzufügen“ Folgendes:

- Die Hauptinformationen werden so angezeigt, wie Sie es beabsichtigt haben
- Gruppen zeigt den Benutzer an, der der von Ihnen erstellten Gruppe hinzugefügt wurde

Wenn Sie Änderungen vornehmen möchten, wählen Sie Bearbeiten. Wenn alle Angaben korrekt sind, wählen Sie Benutzer hinzufügen.

Eine Benachrichtigung informiert Sie darüber, dass der Benutzer hinzugefügt wurde.

Als Nächstes fügen Sie Administratorberechtigungen für die *Admin team* Gruppe hinzu, damit diese *Nikki* auf Ressourcen zugreifen kann.

Schritt 2: Fügen Sie Administratorberechtigungen hinzu

Important

Folgen Sie diesen Schritten nur, wenn Sie eine [Organisationsinstanz von IAM Identity Center](#) aktiviert haben.

1. Wählen Sie im Navigationsbereich von IAM Identity Center unter Multi-account Berechtigungen die Option. AWS-Konten
2. Auf der AWS-Konten Seite „Organisationsstruktur“ wird Ihre Organisation mit Ihren Konten in der Hierarchie darunter angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:
 - a. Für Schritt 1: Wählen Sie Benutzer und Gruppen aus, wählen Sie die *Admin team* Gruppe aus, die Sie erstellt haben. Klicken Sie anschließend auf Weiter.
 - b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Unterschritte führt, die zum Erstellen eines Berechtigungssatzes erforderlich sind.
 - i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:

- Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
- Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

Wählen Sie Weiter aus.

- ii. Für Schritt 2: Geben Sie die Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter.

Mit den Standardeinstellungen wird ein Berechtigungssatz *AdministratorAccess* mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist. Sie können den Namen des Berechtigungssatzes ändern, indem Sie einen neuen Namen in das Feld für den Namen des Berechtigungssatzes eingeben.

- iii. Stellen Sie für Schritt 3: Prüfen und Erstellen sicher, dass der Typ des Berechtigungssatzes die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen aus. Auf der Seite „Berechtigungssätze“ wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diesen Tab jetzt in Ihrem Webbrowser schließen.

Auf dem Browser-Tab Benutzer und Gruppen zuweisen befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *AdministratorAccess* Berechtigungssatz wird in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter aus.

- c. Vergewissern Sie sich auf der Seite Schritt 3: Aufgaben überprüfen und einreichen, dass die *Admin team* Gruppe und der *AdministratorAccess* Berechtigungssatz ausgewählt sind, und wählen Sie dann Senden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihre konfiguriert AWS-Konto wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. Eine Benachrichtigung informiert Sie darüber, dass Ihre Berechtigungen erneut bereitgestellt AWS-Konto wurden und der aktualisierte Berechtigungssatz angewendet wurde.

 Herzlichen Glückwunsch!

Sie haben erfolgreich Ihren ersten Benutzer, Ihre erste Gruppe und Ihren ersten Berechtigungssatz eingerichtet.

Im nächsten Teil dieses Tutorials testen Sie den *Nikki 's* Zugriff, indem Sie sich mit ihren Administratoranmeldeinformationen beim AWS Access Portal anmelden und ihr Passwort festlegen. Melden Sie sich jetzt von der Konsole ab.

Schritt 3: Testen des Benutzerzugriffs

Da *Nikki Wolf* es sich nun um einen Benutzer in Ihrer Organisation handelt, kann er sich anmelden und auf die Ressourcen zugreifen, für die ihm gemäß seinem Berechtigungssatz Berechtigungen erteilt wurden. Um zu überprüfen, ob der Benutzer richtig konfiguriert ist, verwenden Sie im nächsten Schritt *Nikki 's* Anmeldeinformationen, um sich anzumelden und sein Passwort einzurichten. Als Sie den Benutzer *Nikki Wolf* in Schritt 1 hinzugefügt haben, haben Sie angegeben, dass Sie eine E-Mail mit Anweisungen zur Einrichtung des Passworts *Nikki* erhalten möchten. Es ist an der Zeit, diese E-Mail zu öffnen und Folgendes zu tun:

1. Wählen Sie in der E-Mail den Link *Einladung* annehmen, um die Einladung anzunehmen.

 Note

Die E-Mail enthält auch den *Nikki 's* Benutzernamen und die URL des AWS Zugangsportals, mit der sie sich bei der Organisation anmelden. Notieren Sie sich diese Informationen für die zukünftige Verwendung.

Sie werden zur Anmeldeseite für neue Benutzer weitergeleitet, auf der Sie *Nikki 's* ein Passwort festlegen und ihr MFA-Gerät [???](#) registrieren können.

2. Nachdem Sie **Nikki's** das Passwort festgelegt haben, werden Sie zur Anmeldeseite weitergeleitet. Geben Sie ein **nikkiw** und wählen Sie Weiter, geben Sie dann **Nikki's** das Passwort ein und wählen Sie Anmelden.
3. Das AWS Zugriffsportal wird geöffnet und zeigt die Organisation und die Anwendungen an, auf die Sie zugreifen können.

Wählen Sie die Organisation aus, um sie zu einer Liste von zu erweitern, und wählen Sie AWS-Konten dann das Konto aus, um die Rollen anzuzeigen, die Sie für den Zugriff auf Ressourcen im Konto verwenden können.

Jeder Berechtigungssatz hat zwei Verwaltungsmethoden, die Sie verwenden können, entweder Rollen - oder Zugriffsschlüssel.

- Rolle, zum Beispiel **AdministratorAccess** — Öffnet die AWS Console Home.
 - Zugriffsschlüssel — Stellt Anmeldeinformationen bereit, die Sie mit dem AWS CLI oder- und AWS SDK verwenden können. Enthält Informationen zur Verwendung von kurzfristigen Anmeldeinformationen, die automatisch aktualisiert werden, oder für kurzfristige Zugriffsschlüssel. Weitere Informationen finden Sie unter [Abrufen der IAM Identity Center-Benutzeranmeldedaten für AWS CLI oder AWS SDKs](#).
4. Wählen Sie den Link Rolle, um sich bei der anzumelden AWS Console Home.

Sie sind angemeldet und haben die AWS Console Home Seite aufgerufen. Erkunden Sie die Konsole und vergewissern Sie sich, dass Sie den erwarteten Zugriff haben.

Nächste Schritte

Nachdem Sie nun einen Administratorbenutzer in IAM Identity Center erstellt haben, können Sie:

- [Anwendungen zuweisen](#)
- [Andere Benutzer hinzufügen](#)
- [Ordnen Sie Benutzer Konten zu](#)
- [Konfigurieren Sie zusätzliche Berechtigungssätze](#)

Note

Sie können demselben Benutzer mehrere Berechtigungssätze zuweisen. Um der bewährten Methode zur Anwendung von Berechtigungen mit geringsten Rechten zu

folgen, erstellen Sie nach dem Erstellen Ihres Administratorbenutzers einen restriktiveren Berechtigungssatz und weisen Sie ihn demselben Benutzer zu. Auf diese Weise können Sie nur AWS-Konto mit den Berechtigungen zugreifen, die Sie benötigen, und nicht mit Administratorberechtigungen.

Nachdem Ihre Benutzer ihre [Einladung](#) zur Aktivierung ihres Kontos angenommen und sich beim AWS Access Portal angemeldet haben, werden im Portal nur noch Elemente für die AWS-Konten Rollen und Anwendungen angezeigt, denen sie zugewiesen sind.

Video-Tutorials

Als zusätzliche Ressource können Sie diese Video-Tutorials verwenden, um mehr über die Einrichtung externer Identitätsanbieter zu erfahren:

- [Migration zwischen externen Identitätsanbietern in AWS IAM Identity Center](#)
- [Föderieren Sie Ihre bestehende AWS IAM Identity Center Instanz mit Microsoft Entra ID](#)

Richten Sie Ihre Belegschaft im IAM Identity Center ein

IAM Identity Center ist die AWS Lösung, um die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Kiro und Amazon Quick und anderen AWS Ressourcen zu verbinden. Sie können Ihren bestehenden Identitätsanbieter verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt in IAM Identity Center erstellen und verwalten.

Verwenden Sie IAM bereits für den Zugriff auf? AWS-Konten

Sie müssen keine Änderungen an Ihren aktuellen AWS-Konto Workflows vornehmen, um IAM Identity Center für den Zugriff auf AWS verwaltete Anwendungen zu verwenden. Wenn Sie den [Verbund mit IAM](#) für den AWS-Konto Zugriff verwenden, können Ihre Benutzer weiterhin auf die gleiche AWS-Konten Weise zugreifen, wie sie es immer getan haben, und Sie können Ihre vorhandenen Workflows weiterhin verwenden, um diesen Zugriff zu verwalten.

Wählen Sie den Ansatz, der am besten zur Identitätsmanagementstrategie Ihres Unternehmens und zur vorhandenen Infrastruktur passt.

Themen

- [Benutzer, Gruppen und Bereitstellung im IAM Identity Center](#)
- [Verwaltung Ihrer Identitätsquelle](#)
- [Benutzer im Identity Center-Verzeichnis verwalten](#)

Benutzer, Gruppen und Bereitstellung im IAM Identity Center

Mit IAM Identity Center können Sie steuern, wer sich anmelden kann und auf welche Ressourcen sie zugreifen können. Für die Anmeldung muss ein Benutzer eingerichtet sein. Sie können den Zugriff dann nur Benutzern oder Gruppen zuweisen, denen die Zugriffsrechte zugewiesen wurden. Erfahren Sie mehr über Benutzer, Gruppen und Bereitstellung in IAM Identity Center.

Eindeutigkeit von Benutzernamen und E-Mail-Adresse

IAM Identity Center erfordert, dass jeder Benutzer einen eindeutigen Benutzernamen hat. Der Benutzername ist die primäre ID des Benutzers. Der Benutzername muss nicht mit der E-Mail-Adresse des Benutzers übereinstimmen. IAM Identity Center erfordert, dass alle Benutzernamen und E-Mail-Adressen Ihrer Benutzer ungleich Null und eindeutig sind.

Gruppen

Gruppen sind eine logische Kombination von Benutzern, die Sie definieren. Sie können Gruppen erstellen und Benutzer zu den Gruppen hinzufügen. IAM Identity Center unterstützt keine verschachtelten Gruppen (eine Gruppe innerhalb einer Gruppe). Gruppen sind nützlich, wenn Sie Zugriff auf Anwendungen zuweisen möchten AWS-Konten. Anstatt jeden Benutzer einzeln zuzuweisen, erteilen Sie einer Gruppe Berechtigungen. Wenn Sie später Benutzer zu einer Gruppe hinzufügen oder aus einer Gruppe entfernen, erhält oder verliert der Benutzer dynamisch den Zugriff auf Konten und Anwendungen, die Sie der Gruppe zugewiesen haben.

Bereitstellung für Benutzer und Gruppen

Bei der Bereitstellung werden Benutzer- und Gruppeninformationen für die Verwendung durch IAM Identity Center und AWS verwaltete Anwendungen oder vom Kunden verwaltete Anwendungen zur Verfügung gestellt. Sie können Benutzer und Gruppen direkt in IAM Identity Center erstellen oder Ihre Identitätsquelle mit IAM Identity Center verbinden. Mit IAM Identity Center können Sie Benutzern und Gruppen Zugriff auf verbundene Anwendungen zuweisen und AWS-Konten

Die Bereitstellung im IAM Identity Center variiert je nach der von Ihnen verwendeten Identitätsquelle. Weitere Informationen finden Sie unter [Verwaltung Ihrer Identitätsquelle](#).

Deprovisionierung für Benutzer und Gruppen

Beim Aufheben der Bereitstellung werden Benutzer- und Gruppeninformationen aus dem IAM Identity Center entfernt.

Wenn Sie Active Directory oder einen externen Identitätsanbieter mit IAM Identity Center verwenden, sollten Sie Benutzer und Gruppen aus diesen Identitätsquellen und nicht aus IAM Identity Center entfernen. Wenn Sie IAM Identity Center-Benutzer und -Gruppen löschen, werden sie nicht vollständig entfernt, wenn Ihre Identitätsquelle Active Directory oder ein externer Identitätsanbieter ist.

Wenn Sie die Bereitstellung von IAM Identity Center-Benutzern oder -Gruppen aufheben müssen, sollten Sie zunächst alle Zuweisungen von Berechtigungssätzen [oder Anwendungen an die Benutzer oder Gruppen](#) entfernen, für die Sie die Bereitstellung aufheben möchten. Andernfalls haben Sie in Ihrem IAM Identity Center nicht zugewiesene Berechtigungssätze und Anwendungszuweisungen.

Verwaltung Ihrer Identitätsquelle

Ihre Identitätsquelle in IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Nachdem Sie Ihre Identitätsquelle konfiguriert haben, können Sie nach Benutzern oder Gruppen suchen, um ihnen Single Sign-On-Zugriff auf Anwendungen oder AWS-Konten beides zu gewähren.

Sie können pro Organisation nur eine Identitätsquelle haben. AWS Organizations Sie können eine der folgenden Optionen als Identitätsquelle wählen:

- [Externer Identitätsanbieter](#) — Wählen Sie diese Option, wenn Sie Benutzer in einem externen Identitätsanbieter (IdP) wie Okta oder Microsoft Entra ID verwalten möchten.
- [Ihr AWS lokales oder verwaltetes Active Directory](#) — Wählen Sie diese Option, wenn Sie Ihre Active Directory (AD) Verbindung herstellen möchten.
- [Identity Center-Verzeichnis](#) — Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert, sofern Sie keine andere Identitätsquelle wählen. Mit dem Identity Center-Verzeichnis erstellen Sie Ihre Benutzer und Gruppen und weisen deren Zugriffsebene Ihren AWS-Konten Anwendungen zu.

Note

IAM Identity Center unterstützt SAMBA4 basiertes Simple AD nicht als Identitätsquelle.

Themen

- [Überlegungen zum Ändern Ihrer Identitätsquelle](#)
- [Ändern Sie Ihre Identitätsquelle](#)
- [Unterstützte Benutzer- und Gruppenattribute in IAM Identity Center](#)
- [Externe Identitätsanbieter](#)
- [Microsoft AD directory](#)

Überlegungen zum Ändern Ihrer Identitätsquelle

Obwohl Sie Ihre Identitätsquelle jederzeit ändern können, empfehlen wir Ihnen, zu berücksichtigen, wie sich diese Änderung auf Ihre aktuelle Bereitstellung auswirken könnte.

Wenn Sie bereits Benutzer und Gruppen in einer Identitätsquelle verwalten, werden durch den Wechsel zu einer anderen Identitätsquelle möglicherweise alle Benutzer- und Gruppenzuweisungen entfernt, die Sie im IAM Identity Center konfiguriert haben. In diesem Fall verlieren alle Benutzer, einschließlich des Administratorbenutzers in IAM Identity Center, den Single-Sign-On-Zugriff auf ihre AWS-Konten End-Anwendungen.

Bevor Sie die Identitätsquelle für IAM Identity Center ändern, sollten Sie die folgenden Überlegungen überprüfen, bevor Sie fortfahren. Wenn Sie mit der Änderung Ihrer Identitätsquelle fortfahren möchten, finden Sie [Ändern Sie Ihre Identitätsquelle](#) weitere Informationen unter.

Zwischen dem IAM Identity Center-Verzeichnis und Active Directory wechseln

Wenn Sie bereits Benutzer und Gruppen in Active Directory verwalten, empfehlen wir Ihnen, Ihr Verzeichnis zu verbinden, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Tun Sie dies, bevor Sie Benutzer und Gruppen im Standard-Identity Center-Verzeichnis erstellen und etwaige Zuweisungen vornehmen.

Important

Wenn Sie Ihren Identitätsquellentyp in IAM Identity Center zu oder von Active Directory ändern, beachten Sie, dass sich die Identity Store-ID ändert. Dies kann die folgenden Auswirkungen haben:

- Ihre Standard-URL für das AWS Zugangsportal wird sich ändern. Sie müssen Ihren Mitarbeitern die neue URL mitteilen und die Lesezeichen, die Zulassungslisten für Gatewalls oder Firewalls sowie die Konfigurationen aktualisieren, in denen auf diese URL verwiesen wird. Wir empfehlen Ihnen, diese Änderung in einem geplanten Wartungsfenster vorzunehmen, um die Beeinträchtigung Ihrer Benutzer so gering wie möglich zu halten.
- Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand im IAM Identity Center verwenden und die KMS-Schlüsselrichtlinie mit dem Verschlüsselungskontext konfiguriert haben, beachten Sie, dass sich der Verschlüsselungskontext für den Identitätsspeicher ändern wird. Im Identitätsspeicher-ARN „arn:aws:identitystore: :123456789012: -922763e9b3“ ist „d-922763e9b3“ beispielsweise die Identity Store-ID. identitystore/d Um Dienstunterbrechungen während dieser Umstellung zu vermeiden, ändern Sie vorübergehend Ihre KMS-Schlüsselrichtlinie, sodass ein Platzhaltermuster verwendet wird: „arn:aws:identitystore: :123456789012:identitystore/*“.

Wenn Sie bereits Benutzer und Gruppen im standardmäßigen Identity Center-Verzeichnis verwalten, sollten Sie Folgendes beachten:

- Zuweisungen entfernt und Benutzer und Gruppen gelöscht — Wenn Sie Ihre Identitätsquelle auf Active Directory ändern, werden Ihre Benutzer und Gruppen aus dem Identity Center-Verzeichnis gelöscht. Durch diese Änderung werden auch Ihre Zuweisungen entfernt. In diesem Fall müssen Sie nach dem Wechsel zu Active Directory Ihre Benutzer und Gruppen aus Active Directory in das Identity Center-Verzeichnis synchronisieren und dann ihre Zuweisungen erneut anwenden.

Wenn Sie Active Directory nicht verwenden möchten, müssen Sie Ihre Benutzer und Gruppen im Identity Center-Verzeichnis erstellen und dann Zuweisungen vornehmen.

- Zuweisungen werden nicht gelöscht, wenn Identitäten gelöscht werden — Wenn Identitäten im Identity Center-Verzeichnis gelöscht werden, werden die entsprechenden Zuweisungen auch im IAM Identity Center gelöscht. Wenn Identitäten in Active Directory gelöscht werden (entweder in Active Directory oder in den synchronisierten Identitäten), werden die entsprechenden Zuweisungen jedoch nicht gelöscht.
- Keine ausgehende Synchronisation für APIs — Wenn Sie Active Directory als Identitätsquelle verwenden, empfehlen wir, die APIs zum [Erstellen, Aktualisieren und Löschen](#) mit Vorsicht zu verwenden. IAM Identity Center unterstützt keine ausgehende Synchronisation, sodass Ihre Identitätsquelle nicht automatisch mit den Änderungen aktualisiert wird, die Sie mithilfe dieser APIs an Benutzern oder Gruppen vornehmen.
- Die URL des Access-Portals wird sich ändern — Wenn Sie Ihre Identitätsquelle zwischen IAM Identity Center und Active Directory ändern, ändert sich auch die URL für das AWS Zugriffsportal.
- Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store-APIs gelöscht oder deaktiviert werden, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).
- Multi-Region Support — Wenn Sie IAM Identity Center in weitere Regionen repliziert haben oder dies planen, müssen Sie einen externen Identitätsanbieter oder das Identity Center-Verzeichnis als Identitätsquelle verwenden. Multi-Region Unterstützung ist für Active Directory nicht verfügbar. Weitere Informationen einschließlich anderer Voraussetzungen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter [Microsoft AD directory](#).

Wechsel von IAM Identity Center zu einem externen IdP

Wenn Sie Ihre Identitätsquelle von IAM Identity Center zu einem externen Identitätsanbieter (IdP) ändern, beachten Sie Folgendes:

- Zuweisungen und Mitgliedschaften funktionieren mit korrekten Assertions — Ihre Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Assertions sendet (z. B. SAML-NameIDs). Diese Assertions müssen mit den Benutzernamen und Gruppen in IAM Identity Center übereinstimmen.
- Keine ausgehende Synchronisation — IAM Identity Center unterstützt keine ausgehende Synchronisation, sodass Ihr externer IdP nicht automatisch mit Änderungen an Benutzern und Gruppen aktualisiert wird, die Sie in IAM Identity Center vornehmen.
- SCIM-Bereitstellung — Wenn Sie die SCIM-Bereitstellung verwenden, werden Änderungen an Benutzern und Gruppen in Ihrem Identitätsanbieter erst in IAM Identity Center übernommen, nachdem Ihr Identitätsanbieter diese Änderungen an IAM Identity Center gesendet hat. Siehe [Überlegungen zur Verwendung der automatischen Bereitstellung](#).
- Rollback — Sie können Ihre Identitätsquelle jederzeit wieder auf IAM Identity Center umstellen. Siehe [Wechsel von einem externen IdP zu IAM Identity Center](#).
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt — Sobald Sie Ihre Identitätsquelle auf einen externen Identitätsanbieter ändern, bleiben aktive Benutzersitzungen für den Rest der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn beispielsweise die Sitzungsdauer im AWS Access Portal auf acht Stunden festgelegt ist und Sie die Identitätsquelle in der vierten Stunde geändert haben, bleiben aktive Benutzersitzungen für weitere vier Stunden bestehen. Informationen zum Widerrufen von Benutzersitzungen finden Sie unter [the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”](#).

Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store-APIs gelöscht oder deaktiviert werden, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Note

Sie können Benutzersitzungen nicht von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter [Externe Identitätsanbieter](#)

Wechsel von einem externen IdP zu IAM Identity Center

Wenn Sie Ihre Identitätsquelle von einem externen Identitätsanbieter (IdP) zu IAM Identity Center ändern, beachten Sie Folgendes:

- IAM Identity Center behält alle Ihre Zuweisungen bei.
- Passwort-Reset erzwingen — Benutzer, die Passwörter im IAM Identity Center hatten, können sich weiterhin mit ihren alten Passwörtern anmelden. Für Benutzer, die im externen IdP und nicht im IAM Identity Center waren, muss ein Administrator ein Zurücksetzen des Passworts erzwingen.
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt — Sobald Sie Ihre Identitätsquelle auf IAM Identity Center geändert haben, bleiben aktive Benutzersitzungen für die verbleibende Dauer der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn die AWS Access Portal-Sitzung beispielsweise acht Stunden dauert und Sie die Identitätsquelle in der vierten Stunde geändert haben, laufen aktive Benutzersitzungen weitere vier Stunden lang weiter. Informationen zum Widerrufen von Benutzersitzungen finden Sie unter [the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”](#).

Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store-APIs gelöscht oder deaktiviert werden, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Note

Sie können Benutzersitzungen nicht von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter [Benutzer im Identity Center-Verzeichnis verwalten](#)

Wechsel von einem externen IdP zu einem anderen externen IdP

Wenn Sie bereits einen externen IdP als Identitätsquelle für IAM Identity Center verwenden und zu einem anderen externen IdP wechseln, sollten Sie Folgendes beachten:

- Zuweisungen und Mitgliedschaften funktionieren mit korrekten Assertionen — IAM Identity Center behält alle Ihre Zuweisungen bei. Die Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Assertions sendet (z. B. SAML-NameIDs).

Diese Assertionen müssen mit den Benutzernamen im IAM Identity Center übereinstimmen, wenn sich Ihre Benutzer über den neuen externen IdP authentifizieren.

- SCIM-Bereitstellung — Wenn Sie SCIM für die Bereitstellung im IAM Identity Center verwenden, empfehlen wir Ihnen, die IdP-specific Informationen in diesem Handbuch und die vom IdP bereitgestellte Dokumentation zu lesen, um sicherzustellen, dass der neue Anbieter die Benutzer und Gruppen korrekt abgleicht, wenn SCIM aktiviert ist.
- Bestehende Benutzersitzungen werden nach Ablauf der Sitzungsdauer gesperrt — Sobald Sie Ihre Identitätsquelle auf einen anderen externen Identitätsanbieter ändern, bleiben aktive Benutzersitzungen für die verbleibende Dauer der in der Konsole konfigurierten maximalen Sitzungsdauer bestehen. Wenn die AWS Access Portal-Sitzung beispielsweise acht Stunden dauert und Sie die Identitätsquelle in der vierten Stunde geändert haben, bleiben aktive Benutzersitzungen für weitere vier Stunden bestehen. Informationen zum Widerrufen von Benutzersitzungen finden Sie unter [the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”](#).

Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store-APIs gelöscht oder deaktiviert werden, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

 Note

Sie können Benutzersitzungen nicht von der IAM Identity Center-Konsole aus widerrufen, nachdem Sie den Benutzer gelöscht haben.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter [Externe Identitätsanbieter](#)

Zwischen Active Directory und einem externen IdP wechseln

Wenn Sie Ihre Identitätsquelle von einem externen IdP zu Active Directory oder von Active Directory zu einem externen IdP ändern, beachten Sie Folgendes:

- Benutzer, Gruppen und Zuweisungen werden gelöscht — Alle Benutzer, Gruppen und Zuweisungen werden aus dem IAM Identity Center gelöscht. Weder im externen IdP noch in Active Directory sind Benutzer- oder Gruppeninformationen betroffen.
- Bereitstellung von Benutzern — Wenn Sie zu einem externen IdP wechseln, müssen Sie IAM Identity Center für die Bereitstellung Ihrer Benutzer konfigurieren. Alternativ müssen Sie die Benutzer und Gruppen für den externen IdP manuell bereitstellen, bevor Sie Zuweisungen konfigurieren können.
- Zuweisungen und Gruppen erstellen — Wenn Sie zu Active Directory wechseln, müssen Sie Zuweisungen mit den Benutzern und Gruppen erstellen, die sich in Ihrem Verzeichnis in Active Directory befinden.
- Wenn Benutzer in der IAM Identity Center-Konsole mithilfe von Identity Store-APIs gelöscht oder deaktiviert werden, können Benutzer mit aktiven Sitzungen weiterhin auf integrierte Anwendungen und Konten zugreifen. Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).
- Multi-Region Support — Wenn Sie IAM Identity Center in weitere Regionen repliziert haben oder dies planen, müssen Sie einen externen Identitätsanbieter oder das Identity Center-Verzeichnis als Identitätsquelle verwenden. Multi-Region Unterstützung ist für Active Directory nicht verfügbar. Weitere Informationen einschließlich anderer Voraussetzungen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter [Microsoft AD directory](#).

Ändern Sie Ihre Identitätsquelle

Das folgende Verfahren beschreibt, wie Sie von einem von IAM Identity Center bereitgestellten Verzeichnis (dem standardmäßigen Identity Center-Verzeichnis) zu Active Directory oder einem externen Identitätsanbieter wechseln oder umgekehrt. Bevor Sie fortfahren, überprüfen Sie die Informationen unter [Überlegungen zum Ändern Ihrer Identitätsquelle](#). Um dieses Verfahren abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

 Warning

Abhängig von Ihrer aktuellen Bereitstellung entfernt diese Änderung alle Benutzer- und Gruppenzuweisungen, die Sie in IAM Identity Center konfiguriert haben. Durch diese Änderung werden auch die IAM-Rollen mit Berechtigungssätzen aus Ihren entfernt. AWS-Konten Daher müssen Sie möglicherweise Ihre Ressourcenrichtlinien aktualisieren und sollten sicherstellen, dass Ihr Zugriff auf AWS KMS Schlüssel und Amazon EKS-Cluster dadurch nicht beeinträchtigt wird. Weitere Informationen hierzu finden Sie unter [Verweisen auf Berechtigungssätze in Ressourcenrichtlinien, Amazon EKS-Cluster-Konfigurationszuordnungen und AWS KMS Schlüsselrichtlinien](#).

In diesem Fall verlieren alle Benutzer und Gruppen, einschließlich des Administratorbenutzers in IAM Identity Center, den Single-Sign-On-Zugriff auf ihre AWS-Konten Anwendungen.

Um Ihre Identitätsquelle zu ändern

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ den Tab „Identitätsquelle“. Wählen Sie Aktionen und dann Identitätsquelle ändern aus.
4. Wählen Sie unter Identitätsquelle auswählen die Quelle aus, zu der Sie wechseln möchten, und klicken Sie dann auf Weiter.

Wenn Sie zu Active Directory wechseln, wählen Sie das verfügbare Verzeichnis aus dem Menü auf der nächsten Seite aus.

 Important

Wenn Sie Ihre Identitätsquelle zu oder von Active Directory ändern, werden Benutzer und Gruppen aus dem Identity Center-Verzeichnis gelöscht. Durch diese Änderung werden auch alle Zuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben.

 Note

Wenn Sie IAM Identity Center in weitere Regionen repliziert haben und Ihre Identitätsquelle auf Active Directory ändern möchten, müssen Sie zuerst alle zusätzlichen Regionen entfernen. Multi-Region Unterstützung ist nicht für Instanzen verfügbar, die Active Directory als Identitätsquelle verwenden. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Wenn Sie zu einem externen Identitätsanbieter wechseln, empfehlen wir Ihnen, die Schritte unter zu befolgen [Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her](#).

5. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
6. Wählen Sie Identitätsquelle ändern aus. Wenn Sie Ihre Identitätsquelle in Active Directory ändern, fahren Sie mit dem nächsten Schritt fort.
7. Wenn Sie Ihre Identitätsquelle auf Active Directory ändern, gelangen Sie zur Seite „Einstellungen“. Führen Sie auf der Seite „Einstellungen“ eine der folgenden Aktionen aus:
 - Wählen Sie „Geführte Einrichtung starten“. Informationen zum Abschließen des geführten Einrichtungsvorgangs finden Sie unter [Geführte Einrichtung](#).
 - Wählen Sie im Abschnitt „Identitätsquelle“ die Option „Aktionen“ und dann „Synchronisierung verwalten“ aus, um Ihren Synchronisierungsbereich, die Liste der zu synchronisierenden Benutzer und Gruppen, zu konfigurieren.

Unterstützte Benutzer- und Gruppenattribute in IAM Identity Center

Dieses Handbuch enthält eine Referenz zur Unterstützung von SCIM-Attributen im IAM Identity Center. Es listet auf, welche Benutzer- und Gruppenattribute aus der SCIM-Spezifikation im IAM Identity Center-Identitätsspeicher unterstützt werden, und identifiziert bestimmte Attribute und Unterattribute, die nicht unterstützt werden.

Attribute sind Informationen, die Ihnen helfen, einzelne Benutzer- oder Gruppenobjekte wie `wiename`, `email` oder zu definieren und zu identifizieren. `members` IAM Identity Center unterstützt die am häufigsten verwendeten Attribute sowohl durch manuelle Eingabe als auch durch automatische SCIM-Bereitstellung.

- [Informationen zur SCIM-Spezifikation \(System for Cross-Domain Identity Management\) finden Sie unter /rfc7642. <https://tools.ietf.org/html>](#)
- Informationen zur manuellen und automatischen Bereitstellung finden Sie unter. [Bereitstellung, wenn Benutzer von einem externen IdP kommen](#)
- Informationen zur Attributzuweisung finden Sie unter [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#).

Da IAM Identity Center SCIM für Anwendungsfälle der automatischen Bereitstellung unterstützt, unterstützt das Identity Center-Verzeichnis mit einigen Ausnahmen dieselben Benutzer- und Gruppenattribute, die in der SCIM-Spezifikation aufgeführt sind. In den folgenden Abschnitten wird beschrieben, welche Attribute von IAM Identity Center nicht unterstützt werden.

Benutzerobjekte werden nicht unterstützt

Alle Attribute aus dem SCIM-Benutzerschema (<https://tools.ietf.org/html/rfc7643#section-8.3>) werden im IAM Identity Center-Identitätsspeicher unterstützt, mit Ausnahme der folgenden:

- password
- ims
- photos
- entitlements
- x509Certificates

Alle Unterattribute für Benutzer werden unterstützt, mit Ausnahme der folgenden:

- 'display' Unterattribut eines beliebigen Attributs mit mehreren Werten (z. B. oder) emails
phoneNumbers
- 'version' Unterattribut eines Attributs 'meta'

Gruppenobjekte werden nicht unterstützt

Alle Attribute aus dem SCIM-Gruppenschema (<https://tools.ietf.org/html/rfc7643#section-8.4>) werden unterstützt.

Alle Unterattribute für Gruppen werden unterstützt, mit Ausnahme der folgenden:

- 'display' Unterattribut eines beliebigen Attributs mit mehreren Werten (z. B. Mitglieder).

Externe Identitätsanbieter

Mit IAM Identity Center können Sie Ihre bestehenden Mitarbeiteridentitäten von externen Identitätsanbietern (IdPs) über die Protokolle Security Assertion Markup Language (SAML) 2.0 und System for Cross-Domain Identity Management (SCIM) verbinden. Auf diese Weise können sich Ihre Benutzer mit ihren Unternehmensanmeldedaten beim AWS Access Portal anmelden. Sie können dann zu den ihnen zugewiesenen Konten, Rollen und Anwendungen navigieren, die auf einem externen Server gehostet IdPs werden.

Sie können beispielsweise einen externen IdP wie Okta oder Microsoft Entra ID mit dem IAM Identity Center verbinden. Ihre Benutzer können sich dann mit ihren vorhandenen AWS Zugangsdaten Okta oder Microsoft Entra ID Anmeldedaten beim Zugriffsportal anmelden. Um zu kontrollieren, was Ihre Benutzer nach der Anmeldung tun können, können Sie ihnen zentral Zugriffsberechtigungen für alle Konten und Anwendungen in Ihrer AWS Organisation zuweisen. Darüber hinaus können sich Entwickler einfach mit ihren vorhandenen Anmeldeinformationen bei AWS Command Line Interface (AWS CLI) anmelden und von der automatischen kurzfristigen Generierung und Rotation von Anmeldeinformationen profitieren.

Wenn Sie ein selbstverwaltetes Verzeichnis in Active Directory oder einem anderen verwenden AWS Managed Microsoft AD, finden Sie weitere Informationen unter [Microsoft AD directory](#)

Note

Das SAML-Protokoll bietet keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Daher müssen Sie IAM Identity Center auf diese Benutzer und Gruppen aufmerksam machen, indem Sie sie in IAM Identity Center bereitstellen.

Bereitstellung, wenn Benutzer von einem externen IdP kommen

Wenn Sie einen externen IdP verwenden, müssen Sie alle entsprechenden Benutzer und Gruppen in IAM Identity Center bereitstellen, bevor Sie Zuweisungen zu AWS-Konten unseren Anwendungen vornehmen können. Dazu können Sie [Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit](#) für Ihre Benutzer und Gruppen konfigurieren oder verwenden. [Manuelles Provisioning](#) Unabhängig davon, wie Sie Benutzer bereitstellen, leitet IAM Identity Center die AWS-Managementkonsole Befehlszeilenschnittstelle und die

Anwendungsauthentifizierung an Ihren externen IdP weiter. IAM Identity Center gewährt dann Zugriff auf diese Ressourcen auf der Grundlage der Richtlinien, die Sie in IAM Identity Center erstellen. Weitere Informationen zur Bereitstellung finden Sie unter. [Bereitstellung für Benutzer und Gruppen](#)

Themen

- [Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her](#)
- [Wie ändere ich die Metadaten eines externen Identitätsanbieters in IAM Identity Center](#)
- [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#)
- [SCIM-Profil und SAML 2.0-Implementierung](#)

Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her

Für die unterstützten externen IdPs Geräte gelten unterschiedliche Voraussetzungen, Überlegungen und Bereitstellungsverfahren. Für mehrere IdPs sind Anleitungen mit schrittweisen Anleitungen verfügbar:

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping-Identität](#)

Weitere Informationen zu den Überlegungen für externe Geräte IdPs , die IAM Identity Center unterstützt, finden Sie unter [Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern](#).

Das folgende Verfahren bietet einen allgemeinen Überblick über das Verfahren, das bei allen externen Identitätsanbietern verwendet wird.

So stellen Sie eine Verbindung zu einem externen Identitätsanbieter her

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.

3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle und dann Aktionen > Identitätsquelle ändern aus.
4. Wählen Sie unter Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.
5. Gehen Sie unter Externen Identitätsanbieter konfigurieren wie folgt vor:
 - a. Wählen Sie unter Metadaten des Dienstanbieters die Option Metadatendatei herunterladen aus, um die Metadatendatei herunterzuladen und auf Ihrem System zu speichern. Die SAML-Metadatendatei von IAM Identity Center wird von Ihrem externen Identitätsanbieter benötigt.

 Note

Die SAML-Metadatendatei, die Sie herunterladen, enthält IPv4-only sowohl URLs als auch ACS-URLs (Dual-Stack Assertion Consumer Service). Wenn Ihr IAM Identity Center in weitere Regionen repliziert wird, enthält die Metadatendatei außerdem ACS-URLs für jede weitere Region. Wenn Ihr externer IdP ein Limit für die Anzahl der ACS-URLs hat, müssen Sie die unnötigen ACS-URLs entfernen. Wenn Ihre Organisation beispielsweise Dual-Stack-Endgeräte vollständig eingeführt hat und keine mehr verwendet, können Sie IPv4-only letztere entfernen. Ein alternativer Ansatz besteht darin, nicht die Metadatendatei zu verwenden, sondern die ACS-URLs zu kopieren und in den externen IdP einzufügen.

- b. Wählen Sie unter Metadaten des Identitätsanbieters die Option Datei auswählen aus und suchen Sie die Metadatendatei, die Sie von Ihrem externen Identitätsanbieter heruntergeladen haben. Laden Sie dann die Datei hoch. Diese Metadatendatei enthält das erforderliche öffentliche x509-Zertifikat, das verwendet wird, um Nachrichten zu vertrauen, die vom IdP gesendet werden.
 - c. Wählen Sie Weiter aus.

 Important

Wenn Sie Ihre Quelle zu oder von Active Directory ändern, werden alle vorhandenen Benutzer- und Gruppenzuweisungen entfernt. Sie müssen die Zuweisungen manuell erneut anwenden, nachdem Sie Ihre Quelle erfolgreich geändert haben.

6. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
7. Wählen Sie Identitätsquelle ändern aus. In einer Statusmeldung werden Sie darüber informiert, dass Sie die Identitätsquelle erfolgreich geändert haben.

Wie ändere ich die Metadaten eines externen Identitätsanbieters in IAM Identity Center

Sie können die Metadaten Ihres externen Identitätsanbieters ändern, die Sie zuvor an das IAM Identity Center übermittelt haben. Diese Änderungen wirken sich auf die Fähigkeit Ihrer Benutzer aus, sich über IAM Identity Center anzumelden und auf AWS Ressourcen zuzugreifen. Im folgenden Verfahren wird beschrieben, wie Sie die Metadaten Ihres externen IdP aktualisieren, die im IAM Identity Center gespeichert sind. Um dieses Verfahren abzuschließen, benötigen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Um die Metadaten eines externen Identitätsanbieters zu ändern

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle aus. Wählen Sie Aktionen und dann Authentifizierung verwalten.
4. Wählen Sie im Abschnitt Metadaten des Identitätsanbieters die Option IdP-Metadaten bearbeiten aus. Auf dieser Seite können Sie die Änderungen an der IdP-Anmelde-URL und/oder der IdP-Aussteller-URL für Ihren externen IdP vornehmen. Wählen Sie Änderungen speichern, wenn Sie alle erforderlichen Änderungen vorgenommen haben.

Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern

IAM Identity Center implementiert die folgenden standardbasierten Protokolle für den Identitätsverbund:

- SAML 2.0 für die Benutzerauthentifizierung
- SCIM für die Bereitstellung

Von jedem Identitätsanbieter (IdP), der diese Standardprotokolle implementiert, wird erwartet, dass er erfolgreich mit IAM Identity Center zusammenarbeitet, wobei die folgenden besonderen Überlegungen zu beachten sind:

- SAML

- IAM Identity Center erfordert ein SAML-NameID-Format für die E-Mail-Adresse (d. h.).
`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- [Der Wert des Felds NameID in Assertionen muss eine RFC 2822 \(https://tools.ietf.org/html/rfc2822\) -Adressspezifikationskonforme \(„“\) Zeichenfolge sein \(#section -3.4.1\).](https://tools.ietf.org/html/rfc2822)
[name@domain.com https://tools.ietf.org/html/rfc2822](https://tools.ietf.org/html/rfc2822)
- Der **Subject NameID** Wert der SAML-Assertion muss exakt mit dem Benutzernamen eines Benutzers übereinstimmen, der in IAM Identity Center bereitgestellt wurde. Sign-in schlägt fehl, wenn IAM Identity Center den NameID nicht mit einem Benutzernamen abgleichen kann, auch wenn der externe IdP den Benutzer erfolgreich authentifiziert hat.
- Die Metadatendatei darf nicht mehr als 75000 Zeichen enthalten.
- Die Metadaten müssen eine EntityID und ein X509-Zertifikat enthalten und Teil der SingleSignOnService Anmelde-URL sein.
- Ein Verschlüsselungsschlüssel wird nicht unterstützt.
- IAM Identity Center unterstützt nicht das Signieren von SAML-Authentifizierungsanforderungen, die es an externe Empfänger sendet. IdPs
- Der IdP muss mehrere Assertion Consumer Service (ACS) -URLs unterstützen, wenn Sie planen, IAM Identity Center in weitere Regionen zu replizieren und die Vorteile eines IAM Identity Center mit mehreren Regionen voll auszuschöpfen. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#). Die Verwendung einer einzigen ACS-URL kann sich auf die Benutzererfahrung in weiteren Regionen auswirken. Ihre Hauptregion wird weiterhin normal funktionieren. Weitere Informationen zur Benutzererfahrung in weiteren Regionen mit einer einzigen ACS-URL finden Sie unter [the section called “Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs”](#) und [the section called “AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu”](#).

- SCIM

- [Die SCIM-Implementierung von IAM Identity Center basiert auf den SCIM-RFCs 7642 \(https://tools.ietf.org/html/rfc7642\), 7643 \(\) und 7644 \(https://tools.ietf.org/html/rfc7643https://tools.ietf.org/html/rfc7644\)](https://tools.ietf.org/html/rfc7642) sowie den Interoperabilitätsanforderungen, die im Entwurf des [FastFed Basic SCIM Profile 1.0 vom März 2020 \(#rfc .section.4\)](#) dargelegt sind. <https://>

openid.net/specs/fastfed-scim-1_0-02.html Alle Unterschiede zwischen diesen Dokumenten und der aktuellen Implementierung in IAM Identity Center werden im Abschnitt [Unterstützte API-Operationen](#) des IAM Identity Center SCIM Implementation Developer Guide beschrieben.

IdPs die nicht den oben genannten Standards und Überlegungen entsprechen, werden nicht unterstützt. Bitte wenden Sie sich an Ihren IdP, wenn Sie Fragen oder Erläuterungen zur Konformität seiner Produkte mit diesen Standards und Überlegungen haben.

Wenn Sie Probleme haben, Ihren IdP mit dem IAM Identity Center zu verbinden, empfehlen wir Ihnen, Folgendes zu überprüfen:

- AWS CloudTrail protokolliert, indem nach dem Namen des Ereignisses gefiltert wird ExternalIdPDirectoryLogin
- IdP-specific protokolliert and/or Debug-Protokolle
- [Problembehandlung bei IAM Identity Center-Problemen](#)

Note

Einige IdPs, wie die in der [Tutorials zu Identitätsquellen im IAM Identity Center](#), bieten eine vereinfachte Konfigurationserfahrung für IAM Identity Center in Form einer „Anwendung“ oder eines „Connectors“, die speziell für IAM Identity Center entwickelt wurden. Wenn Ihr IdP diese Option anbietet, empfehlen wir Ihnen, sie zu verwenden. Achten Sie darauf, den Artikel auszuwählen, der speziell für IAM Identity Center entwickelt wurde. Andere Elemente, die als „AWS“, „AWS Federation“ oder ähnliche generische "AWS" Namen bezeichnet werden, verwenden möglicherweise and/or Endpunkte mit anderen Verbundansätzen und funktionieren möglicherweise nicht wie erwartet mit IAM Identity Center.

SCIM-Profil und SAML 2.0-Implementierung

Sowohl SCIM als auch SAML sind wichtige Überlegungen bei der Konfiguration von IAM Identity Center.

SAML 2.0-Implementierung

IAM Identity Center unterstützt den Identitätsverbund mit [SAML \(Security Assertion Markup Language\) 2.0](#). Dadurch kann IAM Identity Center Identitäten von externen Identitätsanbietern

authentifizieren (). IdPs SAML 2.0 ist ein offener Standard, der für den sicheren Austausch von SAML-Assertionen verwendet wird. SAML 2.0 überträgt Informationen über einen Benutzer zwischen einer SAML-Behörde (als Identitätsanbieter oder IdP bezeichnet) und einem SAML-Verbraucher (als Service Provider oder SP bezeichnet). Der IAM Identity Center-Dienst verwendet diese Informationen, um föderiertes Single Sign-On bereitzustellen. Single Sign-On ermöglicht Benutzern den Zugriff auf AWS-Konten und die Konfiguration von Anwendungen auf der Grundlage ihrer vorhandenen Identity Provider-Anmeldeinformationen.

IAM Identity Center erweitert Ihren IAM Identity Center-Shop oder einen externen Identitätsanbieter um SAML-IdP-Funktionen. AWS Managed Microsoft AD Benutzer können sich dann per Single Sign-On bei Diensten anmelden, die SAML unterstützen, einschließlich Anwendungen AWS-Managementkonsole und Drittanbieteranwendungen wie, und. Microsoft 365 Concur Salesforce

Das SAML-Protokoll bietet jedoch keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Daher müssen Sie IAM Identity Center auf diese Benutzer und Gruppen aufmerksam machen, indem Sie sie in IAM Identity Center bereitstellen.

SCIM-Profil

IAM Identity Center bietet Unterstützung für den Standard System for Cross-domain Identity Management (SCIM) v2.0. SCIM synchronisiert Ihre IAM Identity Center-Identitäten mit den Identitäten Ihres IdP. Dies beinhaltet jegliche Bereitstellung, Aktualisierung und Deprovisionierung von Benutzern zwischen Ihrem IdP und IAM Identity Center.

Weitere Informationen zur Implementierung von SCIM finden Sie unter [Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit](#) Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im [IAM Identity Center SCIM Implementation Developer Guide](#).

Themen

- [Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit](#)
- [Wechseln Sie die SAML 2.0-Zertifikate](#)

Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen von Ihrem Identity Provider (IdP) in IAM Identity Center mithilfe des System for Cross-domain Identity Management (SCIM) v2.0-Protokolls. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Identity Provider (IdP) -Benutzerattribute zu den

benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und Ihrem IdP überein. Sie konfigurieren diese Verbindung in Ihrem IdP mithilfe Ihres SCIM-Endpunkts für IAM Identity Center und eines Bearer-Tokens, das Sie in IAM Identity Center erstellen.

Themen

- [Überlegungen zur Verwendung der automatischen Bereitstellung](#)
- [IdentityStore API-Zugriff mit SCIM-Bereitstellung](#)
- [Wie überwacht man den Ablauf des Zugriffstokens](#)
- [Generieren Sie ein Zugriffstoken](#)
- [Aktivieren Sie die automatische Bereitstellung](#)
- [Löschen Sie ein Zugriffstoken](#)
- [Deaktivieren Sie die automatische Bereitstellung](#)
- [Ein Zugriffstoken rotieren](#)
- [Automatisch bereitgestellte Ressourcen prüfen und abgleichen](#)
- [Manuelles Provisioning](#)

Überlegungen zur Verwendung der automatischen Bereitstellung

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die folgenden wichtigen Überlegungen zur Funktionsweise von SCIM mit IAM Identity Center zu lesen. Weitere Überlegungen zur Bereitstellung finden Sie in den für Ihren IdP [Tutorials zu Identitätsquellen im IAM Identity Center](#) geltenden Bestimmungen.

- Wenn Sie eine primäre E-Mail-Adresse bereitstellen, muss dieser Attributwert für jeden Benutzer eindeutig sein. In einigen IdPs Fällen ist die primäre E-Mail-Adresse möglicherweise keine echte E-Mail-Adresse. Beispielsweise könnte es sich um einen Universal Principal Name (UPN) handeln, der nur wie eine E-Mail aussieht. Diese IdPs können eine sekundäre oder „andere“ E-Mail-Adresse haben, die die tatsächliche E-Mail-Adresse des Benutzers enthält. Sie müssen SCIM in Ihrem IdP so konfigurieren, dass die eindeutige E-Mail-Adresse ungleich NULL dem primären E-Mail-Adressattribut von IAM Identity Center zugeordnet wird. Und Sie müssen die eindeutige Anmelde-ID des Benutzers, die nicht NULL ist, dem Benutzernamenattribut von IAM Identity Center zuordnen. Prüfen Sie, ob Ihr IdP einen einzigen Wert hat, der sowohl die Anmelde-ID als auch den E-Mail-Namen des Benutzers ist. Wenn ja, können Sie dieses IdP-Feld sowohl der primären IAM Identity Center-E-Mail-Adresse als auch dem IAM Identity Center-Benutzernamen zuordnen.

- Damit die SCIM-Synchronisierung funktioniert, müssen für jeden Benutzer die Werte Vorname, Nachname, Benutzername und Anzeigename angegeben werden. Wenn einer dieser Werte bei einem Benutzer fehlt, wird diesem Benutzer keine Provisionierung zugewiesen.
- Wenn Sie Anwendungen von Drittanbietern verwenden müssen, müssen Sie zunächst das Betreffattribut für ausgehende SAML dem Benutzernamenattribut zuordnen. Wenn die Drittanbieteranwendung eine routbare E-Mail-Adresse benötigt, müssen Sie Ihrem IdP das E-Mail-Attribut zur Verfügung stellen.
- Stellen Sie für SCIM-provisioned Benutzer sicher, dass das Attribut, das Ihr IdP als SAML sendet, dasselbe Attribut Subject NameID ist, das Sie dem Benutzernamen in Ihrer SCIM-Konfiguration zuordnen. Wenn sie sich unterscheiden, schlägt die Anmeldung fehl.
- Die SCIM-Bereitstellungs- und Aktualisierungsintervalle werden von Ihrem Identitätsanbieter gesteuert. Änderungen an Benutzern und Gruppen in Ihrem Identity Provider werden erst in IAM Identity Center übernommen, nachdem Ihr Identity Provider diese Änderungen an IAM Identity Center gesendet hat. Einzelheiten zur Häufigkeit von Benutzer- und Gruppenaktualisierungen erhalten Sie bei Ihrem Identitätsanbieter.
- Derzeit werden mehrwertige Attribute (wie mehrere E-Mails oder Telefonnummern für einen bestimmten Benutzer) nicht mit SCIM bereitgestellt. Versuche, mehrwertige Attribute mit SCIM mit IAM Identity Center zu synchronisieren, schlagen fehl. Um Fehler zu vermeiden, stellen Sie sicher, dass für jedes Attribut nur ein einziger Wert übergeben wird. Wenn Sie Benutzer mit mehrwertigen Attributen haben, entfernen oder ändern Sie die doppelten Attributzuordnungen in SCIM bei Ihrem IdP für die Verbindung zum IAM Identity Center.
- Stellen Sie sicher, dass die `externalId` SCIM-Zuordnung bei Ihrem IdP einem Wert entspricht, der eindeutig und immer vorhanden ist und sich für Ihre Benutzer am wenigsten ändert. Beispielsweise kann Ihr IdP eine garantierte `objectId` oder eine andere Kennung bereitstellen, auf die sich Änderungen an Benutzerattributen wie Name und E-Mail nicht auswirken. Wenn ja, können Sie diesen Wert dem `externalId` SCIM-Feld zuordnen. Dadurch wird sichergestellt, dass Ihre Benutzer keine AWS Berechtigungen, Zuweisungen oder Berechtigungen verlieren, wenn Sie ihren Namen oder ihre E-Mail-Adresse ändern müssen.
- Benutzer, denen noch keine Anwendung zugewiesen wurde oder denen AWS-Konto keine Bereitstellung für IAM Identity Center möglich ist. Um Benutzer und Gruppen zu synchronisieren, stellen Sie sicher, dass sie der Anwendung oder einem anderen Setup zugewiesen sind, das die Verbindung Ihres IdP zum IAM Identity Center darstellt.
- Das Verhalten bei der Deprovisionierung von Benutzern wird vom Identitätsanbieter verwaltet und kann je nach Implementierung variieren. Einzelheiten zur Deprovisionierung von Benutzern erhalten Sie bei Ihrem Identitätsanbieter.

- Nachdem Sie die automatische Bereitstellung mit SCIM für Ihren IdP eingerichtet haben, können Sie in der IAM Identity Center-Konsole keine Benutzer mehr hinzufügen oder bearbeiten. Wenn Sie einen Benutzer hinzufügen oder ändern müssen, müssen Sie dies von Ihrem externen IdP oder Ihrer Identitätsquelle aus tun.

Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im [IAM Identity Center SCIM Implementation Developer Guide](#).

IdentityStore API-Zugriff mit SCIM-Bereitstellung

Wenn Sie die SCIM-Bereitstellung von einem externen IdP aus konfigurieren, bleiben die Identity Store-APIs zugänglich, die das Mutieren von Benutzern und Gruppenmitgliedschaften ermöglichen. Prinzipale im Verwaltungskonto und im delegierten Administratorkonto können sie aufrufen.

Es gibt triftige Gründe, diese APIs zusammen mit SCIM zu verwenden. Beispielsweise unterstützen einige Apps IdPs die Bereitstellung von SCIM-Gruppen Google Workspace nicht und erfordern, dass Sie [Gruppen manuell über die Identity Store-APIs erstellen und verwalten](#). Andere Anwendungsfälle umfassen die schnelle Deaktivierung von Benutzern und die Vorabbereitstellung von Gruppen vor der IdP-Synchronisierung.

Important

Wenn Ihre Organisation keinen direkten API-Zugriff benötigt, beachten Sie, dass die Verwendung mutierender Identity Store-APIs in einem SCIM-provisioned Verzeichnis dazu führen kann, dass das Verzeichnis in IAM Identity Center von Ihrem externen IdP abweicht. Die SCIM-Synchronisierung wird mit Deltas vom Quell-IdP IdP. Das bedeutet, dass über die API vorgenommene Änderungen möglicherweise nicht durch nachfolgende SCIM-Synchronisierungen korrigiert werden. Dies kann zu folgenden Ergebnissen führen:

- Benutzer- oder Gruppenmitgliedschaften in IAM Identity Center, die nicht zu Ihrem externen IdP passen, was die Erwartung widerspricht, dass der IdP die einzige Quelle der Wahrheit ist.
- Unbeabsichtigte Rechteerweiterung, wenn ein Principal sich selbst oder andere zu Gruppen hinzufügt, die Zugriff auf unsere Anwendungen gewähren. AWS-Konten
- Audit- und Compliance-Lücken, da die am externen IdP durchgeführten Berechtigungsprüfungen möglicherweise nicht den tatsächlichen Status des Zugriffs in widerspiegeln. AWS

Wenn Sie API-based Mutationen verhindern möchten, fügen Sie dem delegierten Administratorkonto eine Service Control Policy (SCP) hinzu. Beachten Sie, dass SCPs nicht für das Verwaltungskonto selbst gelten.

Das folgende Beispiel für SCP verweigert alle mutierenden Identity Store-Aktionen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIdentityStoreMutations",
      "Effect": "Deny",
      "Action": [
        "identitystore:Create*",
        "identitystore:Update*",
        "identitystore:Delete*"
      ],
      "Resource": "*"
    }
  ]
}
```

Wie überwacht man den Ablauf des Zugriffstokens

SCIM-Zugriffstoken werden mit einer Gültigkeit von einem Jahr generiert. Wenn Ihr SCIM-Zugriffstoken so eingestellt ist, dass es in 90 Tagen oder weniger abläuft, AWS sendet es Ihnen in der IAM Identity Center-Konsole und über das AWS Health Dashboard Erinnerungen, damit Sie das Token wechseln können. Indem Sie das SCIM-Zugriffstoken rotieren, bevor es abläuft, stellen Sie kontinuierlich die automatische Bereitstellung von Benutzer- und Gruppeninformationen sicher. Wenn das SCIM-Zugriffstoken abläuft, wird die Synchronisation von Benutzer- und Gruppeninformationen von Ihrem Identitätsanbieter mit dem IAM Identity Center beendet, sodass bei der automatischen Bereitstellung keine Aktualisierungen mehr vorgenommen oder Informationen erstellt und gelöscht werden können. Eine Unterbrechung der automatischen Bereitstellung kann zu erhöhten Sicherheitsrisiken führen und den Zugriff auf Ihre Dienste beeinträchtigen.

Die Erinnerungen der Identity Center-Konsole bleiben bestehen, bis Sie das SCIM-Zugriffstoken rotieren und alle ungenutzten oder abgelaufenen Zugriffstoken löschen. Die AWS Health Dashboard-Ereignisse werden wöchentlich zwischen 90 und 60 Tagen, zweimal pro Woche zwischen 60 und 30 Tagen, dreimal pro Woche zwischen 30 und 15 Tagen und täglich zwischen 15 Tagen, bis die SCIM-Zugriffstoken ablaufen, erneuert.

Generieren Sie ein Zugriffstoken

Gehen Sie wie folgt vor, um ein neues Zugriffstoken in der IAM Identity Center-Konsole zu generieren.

Note

Für dieses Verfahren müssen Sie zuvor die automatische Bereitstellung aktiviert haben. Weitere Informationen finden Sie unter [Aktivieren Sie die automatische Bereitstellung](#).

Um ein neues Zugriffstoken zu generieren

1. Wählen Sie in der [IAM Identity Center-Konsole](#) im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung unter Zugriffstoken die Option Token generieren aus.
4. Kopieren Sie im Dialogfeld Neues Zugriffstoken generieren das neue Zugriffstoken und speichern Sie es an einem sicheren Ort.
5. Klicken Sie auf Schließen.

Aktivieren Sie die automatische Bereitstellung

Gehen Sie wie folgt vor, um die automatische Bereitstellung von Benutzern und Gruppen von Ihrem IdP an das IAM Identity Center mithilfe des SCIM-Protokolls zu aktivieren.

Note

Bevor Sie mit diesem Verfahren beginnen, empfehlen wir Ihnen, zunächst die Überlegungen zur Bereitstellung zu überprüfen, die für Ihren IdP gelten. Weitere Informationen finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#) Für Ihren IdP.

Um die automatische Bereitstellung im IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die [IAM Identity Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.

3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten den SCIM-Endpunkt und das Zugriffstoken. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
 - a. SCIM-Endpunkt — zum Beispiel `amazonaws.com//https://scim.us-east-21111111111-2222-3333-4444-555555555555scim/v2`
 - b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.

 Warning

Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken abrufen können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren. Sie werden diese Werte eingeben, um die automatische Bereitstellung in Ihrem IdP später in diesem Tutorial zu konfigurieren.

5. Klicken Sie auf Schließen.

Nachdem Sie dieses Verfahren abgeschlossen haben, müssen Sie die automatische Bereitstellung in Ihrem IdP konfigurieren. Weitere Informationen finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#) Für Ihren IdP.

Löschen Sie ein Zugriffstoken

Gehen Sie wie folgt vor, um ein vorhandenes Zugriffstoken in der IAM Identity Center-Konsole zu löschen.

Um ein vorhandenes Zugriffstoken zu löschen

1. Wählen Sie in der [IAM Identity Center-Konsole](#) im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung unter Zugriffstoken das Zugriffstoken aus, das Sie löschen möchten, und wählen Sie dann Löschen aus.

4. Überprüfen Sie im Dialogfeld Zugriffstoken löschen die Informationen, geben Sie DELETE ein, und wählen Sie dann Zugriffstoken löschen aus.

Deaktivieren Sie die automatische Bereitstellung

Gehen Sie wie folgt vor, um die automatische Bereitstellung in der IAM Identity Center-Konsole zu deaktivieren.

Important

Sie müssen das Zugriffstoken löschen, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter [Löschen Sie ein Zugriffstoken](#).

Um die automatische Bereitstellung in der IAM Identity Center-Konsole zu deaktivieren

1. Wählen Sie in der [IAM Identity Center-Konsole](#) im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung die Option Deaktivieren aus.
4. Überprüfen Sie im Dialogfeld Automatische Bereitstellung deaktivieren die Informationen, geben Sie DISABLE ein, und wählen Sie dann Automatische Bereitstellung deaktivieren aus.

Ein Zugriffstoken rotieren

Ein IAM Identity Center-Verzeichnis unterstützt bis zu zwei Zugriffstoken gleichzeitig. Um vor jeder Rotation ein zusätzliches Zugriffstoken zu generieren, löschen Sie alle abgelaufenen oder ungenutzten Zugriffstoken.

Wenn Ihr SCIM-Zugriffstoken bald abläuft, können Sie das folgende Verfahren verwenden, um ein vorhandenes Zugriffstoken in der IAM Identity Center-Konsole rotieren zu lassen.

Um ein Zugriffstoken zu rotieren

1. Wählen Sie in der [IAM Identity Center-Konsole](#) im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.

3. Notieren Sie sich auf der Seite Automatische Bereitstellung unter Zugriffstoken die Token-ID des Tokens, das Sie rotieren möchten.
4. Folgen Sie den Schritten unter [Generieren Sie ein Zugriffstoken](#), um ein neues Token zu erstellen. Wenn Sie bereits die maximale Anzahl von SCIM-Zugriffstoken erstellt haben, müssen Sie zunächst eines der vorhandenen Token löschen.
5. Rufen Sie die Website Ihres Identitätsanbieters auf und konfigurieren Sie das neue Zugriffstoken für die SCIM-Bereitstellung. Testen Sie dann die Konnektivität zum IAM Identity Center mithilfe des neuen SCIM-Zugriffstokens. Sobald Sie bestätigt haben, dass die Bereitstellung mit dem neuen Token erfolgreich funktioniert, fahren Sie mit dem nächsten Schritt in diesem Verfahren fort.
6. Folgen Sie den Schritten unter [Löschen Sie ein Zugriffstoken](#), um das alte Zugriffstoken zu löschen, das Sie zuvor notiert haben. Sie können das Erstellungsdatum des Tokens auch als Hinweis dafür verwenden, welches Token entfernt werden soll.

Automatisch bereitgestellte Ressourcen prüfen und abgleichen

Mit SCIM können Sie automatisch Benutzer, Gruppen und Gruppenmitgliedschaften aus Ihrer Identitätsquelle für IAM Identity Center bereitstellen. Dieses Handbuch hilft Ihnen dabei, diese Ressourcen zu überprüfen und abzugleichen, um eine korrekte Synchronisation zu gewährleisten.

Warum sollten Sie Ihre Ressourcen prüfen?

Regelmäßige Prüfungen tragen dazu bei, dass Ihre Zugriffskontrollen korrekt bleiben und Ihr Identity Provider (IdP) ordnungsgemäß mit IAM Identity Center synchronisiert bleibt. Dies ist besonders wichtig für die Einhaltung von Sicherheitsbestimmungen und das Zugriffsmanagement.

Ressourcen, die Sie prüfen können:

- Benutzer
- Gruppen
- Gruppenmitgliedschaften

Sie können AWS Identity [Store-APIs](#) oder [CLI-Befehle](#) verwenden, um die Prüfung und den Abgleich durchzuführen. In den folgenden Beispielen AWS CLI werden Befehle verwendet. API-Alternativen finden Sie in den [entsprechenden Vorgängen](#) in der Identity Store-API-Referenz.

Wie prüft man Ressourcen

Im Folgenden finden Sie Beispiele dafür, wie Sie diese Ressourcen mithilfe von AWS CLI Befehlen prüfen können.

Stellen Sie vor Beginn sicher, dass Sie über Folgendes verfügen:

- Administratorzugriff auf IAM Identity Center.
- AWS CLI installiert und konfiguriert. Weitere Informationen finden Sie im [Benutzerhandbuch für die AWS Befehlszeilenschnittstelle](#).
- Erforderliche IAM-Berechtigungen für Identity Store-Befehle.

Schritt 1: Aktuelle Ressourcen auflisten

Sie können Ihre aktuellen Ressourcen mit dem anzeigen AWS CLI.

Note

Wenn Sie den verwenden AWS CLI, erfolgt die Seitennummerierung automatisch, sofern Sie nichts anderes angeben `--no-paginate`. Wenn Sie die API direkt aufrufen (z. B. mit einem SDK oder einem benutzerdefinierten Skript), behandeln Sie das `NextToken` in der Antwort. Dadurch wird sichergestellt, dass Sie alle Ergebnisse auf mehreren Seiten abrufen.

Example für Benutzer

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example für Gruppen

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example für Gruppenmitgliedschaften

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

```
--identity-store-id IDENTITY_STORE_ID
--group-id GROUP_ID
```

Schritt 2: Mit Ihrer Identitätsquelle vergleichen

Vergleichen Sie die aufgelisteten Ressourcen mit Ihrer Identitätsquelle, um etwaige Unstimmigkeiten zu ermitteln, z. B.:

- Fehlende Ressourcen, die in IAM Identity Center bereitgestellt werden sollten.
- Zusätzliche Ressourcen, die aus IAM Identity Center entfernt werden sollten.

Example für Benutzer

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Example für Gruppen

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example für Gruppenmitgliedschaften

```
# Add missing members
```

```
aws identitystore create-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID \  
  --member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --membership-id MEMBERSHIP_ID
```

Überlegungen

- Befehle unterliegen [Dienstkontingenten und API-Drosselung](#).
- Wenn Sie beim Abgleich viele Unterschiede feststellen, nehmen Sie kleine, schrittweise Änderungen am AWS Identity Store vor. Auf diese Weise können Sie Fehler vermeiden, die mehrere Benutzer betreffen.
- Die SCIM-Synchronisierung kann Ihre manuellen Änderungen außer Kraft setzen. Überprüfe deine IdP-Einstellungen, um dieses Verhalten zu verstehen.

Manuelles Provisioning

Einige bieten IdPs keine Unterstützung für System for Cross-domain Identity Management (SCIM) oder haben eine inkompatible SCIM-Implementierung. In diesen Fällen können Sie Benutzer manuell über die IAM Identity Center-Konsole bereitstellen. Wenn Sie Benutzer zu IAM Identity Center hinzufügen, stellen Sie sicher, dass der Benutzername mit dem Benutzernamen identisch ist, den Sie in Ihrem IdP haben. Sie müssen mindestens eine eindeutige E-Mail-Adresse und einen eindeutigen Benutzernamen haben. Weitere Informationen finden Sie unter [Eindeutigkeit von Benutzernamen und E-Mail-Adresse](#).

Außerdem müssen Sie alle Gruppen manuell in IAM Identity Center verwalten. Dazu erstellen Sie die Gruppen und fügen sie mithilfe der IAM Identity Center-Konsole hinzu. Diese Gruppen müssen nicht mit dem übereinstimmen, was in Ihrem IdP vorhanden ist. Weitere Informationen finden Sie unter [Gruppen](#).

Wechseln Sie die SAML 2.0-Zertifikate

IAM Identity Center verwendet Zertifikate, um eine SAML-Vertrauensstellung zwischen IAM Identity Center und Ihrem externen Identitätsanbieter (IdP) einzurichten. Wenn Sie einen externen IdP in IAM Identity Center hinzufügen, müssen Sie außerdem mindestens ein öffentliches SAML X.509 2.0-

Zertifikat vom externen IdP beziehen. Dieses Zertifikat wird normalerweise automatisch während des IdP-SAML-Metadatenaustauschs während der Vertrauenserstellung installiert.

Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere IdP-Zertifikate durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein IdP-Zertifikat ersetzen, wenn sich das Ablaufdatum des Zertifikats nähert. Der Vorgang, bei dem ein älteres Zertifikat durch ein neueres ersetzt wird, wird als Zertifikatsrotation bezeichnet.

Themen

- [Ein SAML 2.0-Zertifikat rotieren](#)
- [Indikatoren für den Ablaufstatus des Zertifikats](#)

Ein SAML 2.0-Zertifikat rotieren

Möglicherweise müssen Sie Zertifikate regelmäßig importieren, um ungültige oder abgelaufene Zertifikate, die von Ihrem Identitätsanbieter ausgestellt wurden, rotieren zu lassen. Dies trägt dazu bei, Unterbrechungen oder Ausfallzeiten bei der Authentifizierung zu vermeiden. Alle importierten Zertifikate sind automatisch aktiv. Zertifikate sollten erst gelöscht werden, nachdem sichergestellt wurde, dass sie nicht mehr mit dem zugehörigen Identitätsanbieter verwendet werden.

Sie sollten auch berücksichtigen, dass einige Zertifikate IdPs möglicherweise nicht mehrere Zertifikate unterstützen. In diesem Fall IdPs kann die Rotation von Zertifikaten mit diesen Zertifikaten eine vorübergehende Unterbrechung des Dienstes für Ihre Benutzer bedeuten. Der Dienst wird wiederhergestellt, wenn das Vertrauen zu diesem IdP erfolgreich wiederhergestellt wurde. Planen Sie diesen Vorgang möglichst außerhalb der Spitzenzeiten sorgfältig.

Note

Aus Sicherheitsgründen sollten Sie bei Anzeichen einer Beeinträchtigung oder falschen Handhabung eines vorhandenen SAML-Zertifikats das Zertifikat sofort entfernen und rotieren lassen.

Die Rotation eines IAM Identity Center-Zertifikats ist ein mehrstufiger Prozess, der Folgendes umfasst:

- Ein neues Zertifikat vom IdP erhalten
- Das neue Zertifikat wird in das IAM Identity Center importiert

- Aktivierung des neuen Zertifikats im IdP
- Löschen des älteren Zertifikats

Verwenden Sie alle der folgenden Verfahren, um den Zertifikatsrotationsprozess abzuschließen und gleichzeitig Ausfallzeiten bei der Authentifizierung zu vermeiden.

Schritt 1: Besorgen Sie sich ein neues Zertifikat vom IdP

Gehen Sie zur IdP-Website und laden Sie ihr SAML 2.0-Zertifikat herunter. Stellen Sie sicher, dass die Zertifikatsdatei im PEM-codierten Format heruntergeladen wurde. Bei den meisten Anbietern können Sie mehrere SAML 2.0-Zertifikate im IdP erstellen. Es ist wahrscheinlich, dass diese als deaktiviert oder inaktiv markiert werden.

Schritt 2: Importieren Sie das neue Zertifikat in IAM Identity Center

Gehen Sie wie folgt vor, um das neue Zertifikat mithilfe der IAM Identity Center-Konsole zu importieren.

1. Wählen Sie in der [IAM Identity Center-Konsole](#) Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Authentifizierung verwalten“.
3. Wählen Sie auf der Seite SAML 2.0-Zertifikate verwalten die Option Zertifikat importieren aus.
4. Wählen Sie im Dialogfeld SAML 2.0-Zertifikat importieren die Option Datei auswählen aus, navigieren Sie zu Ihrer Zertifikatsdatei, wählen Sie sie aus und wählen Sie dann Zertifikat importieren aus.

Ab diesem Zeitpunkt vertraut IAM Identity Center allen eingehenden SAML-Nachrichten, die von beiden importierten Zertifikaten signiert wurden.

Schritt 3: Aktivieren Sie das neue Zertifikat im IdP

Gehen Sie zurück zur IdP-Website und markieren Sie das neue Zertifikat, das Sie zuvor erstellt haben, als primär oder aktiv. Zu diesem Zeitpunkt sollten alle vom IdP signierten SAML-Nachrichten das neue Zertifikat verwenden.

Schritt 4: Löschen Sie das alte Zertifikat

Gehen Sie wie folgt vor, um den Zertifikatsrotationsprozess für Ihren IdP abzuschließen. Es muss immer mindestens ein gültiges Zertifikat aufgeführt sein, das nicht entfernt werden kann.

 Note

Stellen Sie sicher, dass Ihr Identitätsanbieter keine SAML-Antworten mehr mit diesem Zertifikat signiert, bevor Sie es löschen.

1. Wählen Sie auf der Seite SAML 2.0-Zertifikate verwalten das Zertifikat aus, das Sie löschen möchten. Wählen Sie Löschen aus.
2. Geben Sie im Dialogfeld SAML 2.0-Zertifikat löschen **DELETE** zur Bestätigung den Text ein, und wählen Sie dann Löschen aus.
3. Kehren Sie zur Website des IdP zurück und führen Sie die erforderlichen Schritte aus, um das ältere inaktive Zertifikat zu entfernen.

Indikatoren für den Ablaufstatus des Zertifikats

Auf der Seite SAML 2.0-Zertifikate verwalten werden in der Spalte Läuft ab neben jedem Zertifikat in der Liste farbige Statusanzeigesymbole angezeigt. Im Folgenden werden die Kriterien beschrieben, anhand derer IAM Identity Center bestimmt, welches Symbol für jedes Zertifikat angezeigt wird.

- Rot — Zeigt an, dass ein Zertifikat abgelaufen ist.
- Gelb — Zeigt an, dass ein Zertifikat in 90 Tagen oder weniger abläuft.
- Grün — Zeigt an, dass ein Zertifikat gültig ist und noch mindestens 90 Tage gültig bleibt.

Um den aktuellen Status eines Zertifikats zu überprüfen

1. Wählen Sie in der [IAM Identity Center-Konsole](#) Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Authentifizierung verwalten“.
3. Überprüfen Sie auf der Seite SAML 2.0-Authentifizierung verwalten unter SAML 2.0-Zertifikate verwalten den Status der Zertifikate in der Liste, wie in der Spalte Läuft ab am angegeben.

Microsoft AD directory

Mit AWS IAM Identity Center können Sie ein selbstveraltetes Verzeichnis in Active Directory (AD) oder ein Verzeichnis mithilfe von AWS Managed Microsoft AD von AWS Directory Service. Dieses Microsoft AD-Verzeichnis definiert den Identitätspool, aus dem Administratoren abrufen können,

wenn sie die IAM Identity Center-Konsole verwenden, um Single Sign-On-Zugriff zuzuweisen. Nachdem Sie Ihr Unternehmensverzeichnis mit dem IAM Identity Center verbunden haben, können Sie Ihren AD-Benutzern oder -Gruppen Zugriff AWS-Konten auf Anwendungen oder beides gewähren.

AWS Directory Service hilft Ihnen bei der Einrichtung und Ausführung eines eigenständigen AWS Managed Microsoft AD Verzeichnisses, das in der AWS Cloud gehostet wird. Sie können es auch verwenden Directory Service , um Ihre AWS Ressourcen mit einem vorhandenen selbstverwalteten AD zu verbinden. Um die Konfiguration AWS Directory Service für die Verwendung mit Ihrem selbstverwalteten AD durchzuführen, müssen Sie zunächst Vertrauensbeziehungen einrichten, um die Authentifizierung auf die Cloud auszudehnen.

IAM Identity Center verwendet die von bereitgestellte Verbindung Directory Service , um die Passthrough-Authentifizierung für die AD-Quellinstanz durchzuführen. Wenn Sie IAM Identity Center AWS Managed Microsoft AD als Identitätsquelle verwenden, kann es mit Benutzern aus AWS Managed Microsoft AD oder von jeder Domain zusammenarbeiten, die über einen AD-Trust verbunden ist. Wenn Sie Ihre Benutzer in vier oder mehr Domänen suchen möchten, müssen Benutzer die DOMAIN\user Syntax als ihren Benutzernamen verwenden, wenn sie sich bei IAM Identity Center anmelden.

Hinweise

- Stellen Sie als Voraussetzung sicher, dass sich Ihr AD Connector oder Ihr Verzeichnis AWS Managed Microsoft AD in in in Ihrem AWS Organizations Verwaltungskonto Directory Service befindet.
- IAM Identity Center unterstützt SAMBA 4-basiertes Simple AD nicht als verbundenes Verzeichnis.
- IAM Identity Center kann Foreign Security Principals (FSPs) nicht synchronisieren. Wenn eine Gruppe Mitglieder aus einer vertrauenswürdigen Domäne als FSPs AWS Managed Microsoft AD enthält, werden diese Mitglieder nicht synchronisiert.

Eine Demonstration der Verwendung von Active Directory als Identitätsquelle für IAM Identity Center finden Sie im folgenden Video: YouTube

[Verwenden von Active Directory als Identitätsquelle für AWS IAM Identity Center | Amazon Web Services](#)

Überlegungen zur Verwendung von Active Directory

Wenn Sie Active Directory als Identitätsquelle verwenden möchten, muss Ihre Konfiguration die folgenden Voraussetzungen erfüllen:

- Wenn Sie IAM Identity Center verwenden AWS Managed Microsoft AD, müssen Sie es dort aktivieren AWS-Region , wo Ihr AWS Managed Microsoft AD Verzeichnis eingerichtet ist. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der IAM Identity Center konfiguriert ist. Beachten Sie außerdem, dass das AWS Zugriffsportal dieselbe Zugriffs-URL wie Ihr Verzeichnis verwendet.
- Verwenden Sie ein Active Directory, das sich im Verwaltungskonto befindet:

Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis eingerichtet haben AWS Directory Service, und es muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können jeweils nur ein AD Connector Connector-Verzeichnis oder ein Verzeichnis verbinden. AWS Managed Microsoft AD Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie unter:

- [Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#)
- [Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect](#)
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

Wenn Sie planen, den delegierten IAM Identity Center-Administrator zu aktivieren und Active Directory als Ihre IAM Identity Center-Identitätsquelle zu verwenden, können Sie einen vorhandenen AD Connector oder ein Verzeichnis verwenden, das im AWS Managed Microsoft AD Verzeichnis eingerichtet ist und sich im AWS delegierten Administratorkonto befindet.

Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle in Active Directory oder von Active Directory in eine andere Quelle zu ändern, muss sich das Verzeichnis in dem delegierten IAM Identity Center-Administrator-Mitgliedskonto befinden (diesem gehören), falls eines existiert; andernfalls muss es sich im Verwaltungskonto befinden.

Connect Active Directory und geben Sie einen Benutzer an

Wenn Sie Active Directory bereits verwenden, helfen Ihnen die folgenden Themen bei der Vorbereitung der Verbindung Ihres Verzeichnisses mit IAM Identity Center.

Sie können ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center verbinden.

 Note

IAM Identity Center unterstützt SAMBA4-based Simple AD nicht als Identitätsquelle.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unter [Microsoft AD directory](#).
2. Führen Sie die Schritte unter [Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#) aus.
3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter [Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center](#).

Self-managed Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unter [Microsoft AD directory](#).
2. Führen Sie die Schritte unter [Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect](#) aus.
3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter [Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center](#).

Externer IdP

1. Lesen Sie die Anleitung unter [Externe Identitätsanbieter](#).
2. Führen Sie die Schritte unter [Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her](#) aus.
3. Konfigurieren Sie Ihren IdP so, dass er Benutzer für das IAM Identity Center bereitstellt.

 Note

Bevor Sie die automatische, gruppenbasierte Bereitstellung all Ihrer Mitarbeiteridentitäten von Ihrem IdP in IAM Identity Center einrichten, empfehlen wir Ihnen, den einen Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center zu synchronisieren.

Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center

Nachdem Sie Ihr Active Directory mit dem IAM Identity Center verbunden haben, können Sie einen Benutzer angeben, dem Sie Administratorrechte gewähren möchten, und diesen Benutzer dann aus Ihrem Verzeichnis mit IAM Identity Center synchronisieren.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, klicken Sie auf „Aktionen“ und anschließend auf „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Gehen Sie unter Hinzugefügte Benutzer und Gruppen wie folgt vor:
 - a. Vergewissern Sie sich, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, angegeben ist.
 - b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.
 - c. Wählen Sie Absenden aus.
7. Auf der Seite „Synchronisation verwalten“ wird der von Ihnen angegebene Benutzer in der Liste „Synchronisierte Benutzer“ angezeigt.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf der Seite Benutzer kann es einige Zeit dauern, bis der von Ihnen angegebene Benutzer in der Liste erscheint. Wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

Zu diesem Zeitpunkt hat Ihr Benutzer keinen Zugriff auf das Verwaltungskonto. Sie richten den Administratorzugriff auf dieses Konto ein, indem Sie einen Administratorberechtigungssatz erstellen und den Benutzer diesem Berechtigungssatz zuweisen. Weitere Informationen finden Sie unter [Erstellen Sie einen Berechtigungssatz](#).

Bereitstellung, wenn Benutzer aus Active Directory kommen

IAM Identity Center verwendet die von der bereitgestellte Verbindung, Directory Service um Benutzer-, Gruppen- und Mitgliedschaftsinformationen aus Ihrem Quellverzeichnis in Active Directory mit dem IAM Identity Center-Identitätsspeicher zu synchronisieren. Es werden keine Kennwortinformationen mit IAM Identity Center synchronisiert, da die Benutzerauthentifizierung direkt aus dem Quellverzeichnis in Active Directory erfolgt. Diese Identitätsdaten werden von Anwendungen verwendet, um anwendungsinterne Such-, Autorisierungs- und Kollaborationsszenarien zu ermöglichen, ohne LDAP-Aktivitäten zurück an das Quellverzeichnis in Active Directory zu übergeben.

Weitere Informationen zur Bereitstellung finden Sie unter [Bereitstellung für Benutzer und Gruppen](#)

Themen

- [Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#)
- [Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect](#)
- [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#)
- [IAM Identity Center, konfigurierbare AD-Synchronisierung](#)

Connect ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center

Gehen Sie wie folgt vor, um ein Verzeichnis, das von verwaltet wird AWS Managed Microsoft AD , mit dem IAM Identity Center AWS Directory Service zu verbinden.

Um eine Verbindung herzustellen AWS Managed Microsoft AD zum IAM Identity Center

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

 Note

Stellen Sie sicher, dass die IAM Identity Center-Konsole eine der Regionen verwendet, in denen sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Identitätsquelle ändern“.
4. Wählen Sie unter Identitätsquelle auswählen die Option Active Directory und dann Weiter aus.
5. Wählen Sie unter Active Directory verbinden ein Verzeichnis in AWS Managed Microsoft AD aus der Liste aus, und klicken Sie dann auf Weiter.
6. Überprüfen Sie unter Änderung bestätigen die Informationen, geben Sie ACCEPT ein, wenn Sie bereit sind, und wählen Sie dann Identitätsquelle ändern aus.

 Important

Um einen Benutzer in Active Directory als Administratorbenutzer in IAM Identity Center anzugeben, müssen Sie zuerst den Benutzer, dem Sie Administratorrechte aus Active Directory gewähren möchten, mit IAM Identity Center synchronisieren. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter [Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center](#).

Ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center Connect

Benutzer in Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) können auch über Single Sign-On auf Anwendungen im AWS-Konten Zugriffsportal zugreifen. AWS Um den Single Sign-On-Zugriff für diese Benutzer zu konfigurieren, können Sie einen der folgenden Schritte ausführen:

- Eine bidirektionale Vertrauensstellung einrichten — Wenn wechselseitige Vertrauensstellungen zwischen AWS Managed Microsoft AD und einem selbstverwalteten Verzeichnis in AD eingerichtet werden, können sich Benutzer in Ihrem selbstverwalteten Verzeichnis in AD mit ihren Unternehmensanmeldeinformationen bei verschiedenen AWS Diensten und Geschäftsanwendungen anmelden. One-way Vertrauensstellungen funktionieren nicht mit IAM Identity Center.

AWS IAM Identity Center erfordert eine bidirektionale Vertrauensstellung, damit Benutzer- und Gruppeninformationen aus Ihrer Domain gelesen und Benutzer- und Gruppenmetadaten synchronisiert werden können. IAM Identity Center verwendet diese Metadaten, wenn es Zugriff auf Berechtigungssätze oder Anwendungen zuweist. Benutzer- und Gruppenmetadaten werden auch von Anwendungen für die Zusammenarbeit verwendet, z. B. wenn Sie ein Dashboard mit einem anderen Benutzer oder einer anderen Gruppe teilen. Das Vertrauen von Directory Service Microsoft Active Directory zu Ihrer Domain ermöglicht es IAM Identity Center, Ihrer Domain bei der Authentifizierung zu vertrauen. Das Vertrauen in die entgegengesetzte Richtung gewährt AWS Berechtigungen zum Lesen von Benutzer- und Gruppenmetadaten.

Weitere Informationen zum Einrichten einer bidirektionalen Vertrauensstellung finden Sie unter [Wann sollte eine Vertrauensstellung eingerichtet werden?](#) im AWS Directory Service Administratorhandbuch.

 Note

Um AWS Anwendungen wie IAM Identity Center zum Lesen von Directory Service Verzeichnisbenutzern aus vertrauenswürdigen Domänen verwenden zu können, benötigen die Directory Service Konten Berechtigungen für das AccountControl Benutzerattribut der vertrauenswürdigen Benutzer. Ohne Leseberechtigungen für dieses Attribut können AWS Anwendungen nicht feststellen, ob das Konto aktiviert oder deaktiviert ist. Lesezugriff auf dieses Attribut wird standardmäßig gewährt, wenn eine Vertrauensstellung erstellt wird. Wenn Sie den Zugriff auf dieses Attribut verweigern (nicht empfohlen), verhindern Sie, dass Anwendungen wie Identity Center vertrauenswürdige Benutzer lesen können. Die Lösung besteht darin, den Lesezugriff auf das `userAccountControl` Attribut der AWS Dienstkonten unter der AWS reservierten Organisationseinheit (mit dem Präfix `AWS_`) ausdrücklich zuzulassen.

- Erstellen Sie einen AD-Connector — AD Connector ist ein Verzeichnis-Gateway, das Verzeichnisanfragen an Ihr selbstverwaltetes AD umleiten kann, ohne Informationen in der Cloud zwischenspeichern. Weitere Informationen finden Sie unter [Connect einem Verzeichnis herstellen](#) im AWS Directory Service Administratorhandbuch. Bei der Verwendung von AD Connector sollten Sie Folgendes beachten:
- Wenn Sie IAM Identity Center mit einem AD Connector Connector-Verzeichnis verbinden, müssen alle future Benutzerpasswörter von AD aus zurückgesetzt werden. Das bedeutet, dass Benutzer ihre Passwörter nicht über das AWS Zugriffsportal zurücksetzen können.

- Wenn Sie AD Connector verwenden, um Ihren Active Directory-Domänendienst mit IAM Identity Center zu verbinden, hat IAM Identity Center nur Zugriff auf die Benutzer und Gruppen der einzelnen Domäne, an die AD Connector angehängt ist. Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie Directory Service Microsoft Active Directory.

 Note

IAM Identity Center funktioniert nicht mit SAMBA4-based Simple AD AD-Verzeichnissen.

Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter

Attributzuordnungen werden verwendet, um Attributtypen, die in IAM Identity Center vorhanden sind, ähnlichen Attributen in Ihrer externen Identitätsquelle zuzuordnen, z. B., und. Google Workspace Microsoft Active Directory (AD) Okta IAM Identity Center ruft Benutzerattribute aus Ihrer Identitätsquelle ab und ordnet sie den IAM Identity Center-Benutzerattributen zu.

Wenn Ihr IAM Identity Center so synchronisiert ist, dass es einen externen Identitätsanbieter (IdP) wie Google Workspace Okta, oder Ping als Identitätsquelle verwendet, müssen Sie Ihre Attribute in Ihrem IdP zuordnen.

IAM Identity Center füllt eine Reihe von Attributen für Sie auf der Registerkarte Attributzuordnungen auf der Konfigurationsseite automatisch aus. IAM Identity Center verwendet diese Benutzerattribute, um SAML-Assertionen (als SAML-Attribute) aufzufüllen, die an die Anwendung gesendet werden. Diese Benutzerattribute werden wiederum aus Ihrer Identitätsquelle abgerufen. Jede Anwendung bestimmt die Liste der SAML 2.0-Attribute, die sie für ein erfolgreiches Single Sign-On benötigt. Weitere Informationen finden Sie unter [Ordnen Sie Attribute in Ihrer Anwendung den IAM Identity Center-Attributen zu](#).

IAM Identity Center verwaltet auch eine Reihe von Attributen für Sie im Abschnitt Attributzuordnungen auf Ihrer Active Directory-Konfigurationsseite, wenn Sie Active Directory als Identitätsquelle verwenden. Weitere Informationen finden Sie unter [Zuordnung von Benutzerattributen zwischen IAM Identity Center und Microsoft AD directory](#).

Unterstützte externe Identitätsanbieter-Attribute

In der folgenden Tabelle sind alle unterstützten Attribute des externen Identitätsanbieters (IdP) aufgeführt. Sie können Attributen zugeordnet werden, die Sie bei der Konfiguration [Attribute für Zugriffskontrolle](#) in IAM Identity Center verwenden können. Wenn Sie SAML-Assertionen verwenden, können Sie alle Attribute verwenden, die Ihr IdP unterstützt.

Unterstützte Attribute in Ihrem IdP

```
${path:userName}
```

```
${path:name.familyName}
```

```
${path:name.givenName}
```

```
${path:displayName}
```

```
${path:nickName}
```

```
${path:emails[primary eq true].value}
```

```
${path:addresses[type eq "work"].streetAddress}
```

```
${path:addresses[type eq "work"].locality}
```

```
${path:addresses[type eq "work"].region}
```

```
${path:addresses[type eq "work"].postalCode}
```

```
${path:addresses[type eq "work"].country}
```

```
${path:addresses[type eq "work"].formatted}
```

```
${path:phoneNumbers[type eq "work"].value}
```

```
${path:userType}
```

```
${path:title}
```

```
${path:locale}
```

Unterstützte Attribute in Ihrem IdP

```
${path:timezone}
```

```
${path:enterprise.employeeNumber}
```

```
${path:enterprise.costCenter}
```

```
${path:enterprise.organization}
```

```
${path:enterprise.division}
```

```
${path:enterprise.department}
```

```
${path:enterprise.manager.value}
```

Standardzuordnungen zwischen IAM Identity Center und Microsoft AD

In der folgenden Tabelle sind die Standardzuordnungen für Benutzerattribute in IAM Identity Center zu den Benutzerattributen in Ihrem Verzeichnis aufgeführt. Microsoft AD IAM Identity Center unterstützt nur die Liste der Attribute in der Spalte Benutzerattribut in IAM Identity Center.

Benutzerattribut im IAM Identity Center	Ordnet diesem Attribut in Ihrem Active Directory zu
displayname	\${displayname}
emails[?primary].value *	\${mail}
externalid	\${objectguid}
name.givenname	\${givenname}
name.familyname	\${sn}
name.middlename	\${initials}
sid	\${objectsid}
username	\${userprincipalname}

* Das E-Mail-Attribut in IAM Identity Center muss innerhalb des Verzeichnisses eindeutig sein.

Gruppenattribut in IAM Identity Center	Ordnet diesem Attribut in Ihrem Active Directory zu
externalid	\${objectguid}
description	\${description}
displayname	\${samaccountname}@{associateddomain}

Überlegungen

- Wenn Sie bei der Aktivierung der konfigurierbaren AD-Synchronisierung keine Zuweisungen für Ihre Benutzer und Gruppen in IAM Identity Center haben, werden die Standardzuordnungen in den vorherigen Tabellen verwendet. Informationen zum Anpassen dieser Zuordnungen finden Sie unter. [Konfigurieren Sie Attributzuordnungen für Ihre Synchronisierung](#)
- Bestimmte IAM Identity Center-Attribute können nicht geändert werden, da sie unveränderlich sind und standardmäßig bestimmten Microsoft AD-Verzeichnisattributen zugeordnet sind.

Beispielsweise ist „Benutzername“ ein obligatorisches Attribut in IAM Identity Center. Wenn Sie „username“ einem AD-Verzeichnisattribut mit einem leeren Wert zuordnen, betrachtet IAM Identity Center den windowsUpn Wert als Standardwert für „username“. Wenn Sie die Attributzuordnung für „Benutzername“ gegenüber Ihrer aktuellen Zuordnung ändern möchten, stellen Sie sicher, dass IAM Identity Center-Datenflüsse, die von „Benutzername“ abhängig sind, weiterhin wie erwartet funktionieren, bevor Sie die Änderung vornehmen.

Unterstützt Microsoft AD Attribute für IAM Identity Center

In der folgenden Tabelle sind alle Microsoft AD Verzeichnisattribute aufgeführt, die unterstützt werden und Benutzerattributen in IAM Identity Center zugeordnet werden können.

Unterstützte Attribute in Ihrem Microsoft AD-Verzeichnis
\${samaccountname}

Unterstützte Attribute in Ihrem Microsoft AD-Verzeichnis

`${description}`

`${objectguid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

Überlegungen

- Sie können eine beliebige Kombination unterstützter Microsoft AD Verzeichnisattribute angeben, um sie einem einzelnen veränderbaren Attribut in IAM Identity Center zuzuordnen.

Unterstützte IAM Identity Center-Attribute für Microsoft AD

In der folgenden Tabelle sind alle IAM Identity Center-Attribute aufgeführt, die unterstützt werden und Benutzerattributen in Ihrem Verzeichnis zugeordnet werden können. Microsoft AD Nachdem Sie Ihre Anwendungsattributzuordnungen eingerichtet haben, können Sie dieselben IAM Identity Center-Attribute verwenden, um sie den tatsächlichen Attributen zuzuordnen, die von dieser Anwendung verwendet werden.

Unterstützte Attribute in IAM Identity Center für Active Directory

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

Zuordnung von Benutzerattributen zwischen IAM Identity Center und Microsoft AD directory

Mithilfe des folgenden Verfahrens können Sie angeben, wie Ihre Benutzerattribute in IAM Identity Center den entsprechenden Attributen in Ihrem Microsoft AD Verzeichnis zugeordnet werden sollen.

So ordnen Sie Attribute in IAM Identity Center Attributen in Ihrem Verzeichnis zu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Attribute für die Zugriffskontrolle“ und dann „Attribute verwalten“.
4. Suchen Sie auf der Seite „Attribut für Zugriffskontrolle verwalten“ in IAM Identity Center nach dem Attribut, das Sie zuordnen möchten, und geben Sie dann einen Wert in das Textfeld ein. Beispielsweise möchten Sie möglicherweise das IAM Identity Center-Benutzerattribut **email** dem Microsoft AD-Verzeichnisattribut zuordnen **\${mail}**.
5. Wählen Sie Änderungen speichern aus.

IAM Identity Center, konfigurierbare AD-Synchronisierung

Mit der konfigurierbaren Active Directory-Synchronisierung (AD) von IAM Identity Center können Sie die Identitäten in Microsoft Active Directory, die automatisch mit IAM Identity Center synchronisiert werden, explizit konfigurieren und den Synchronisierungsprozess steuern.

- Mit dieser Synchronisierungsmethode können Sie Folgendes tun:
 - Kontrollieren Sie Datengrenzen, indem Sie explizit die Benutzer und Gruppen in Microsoft Active Directory definieren, die automatisch mit IAM Identity Center synchronisiert werden. Sie können [Benutzer und Gruppen hinzufügen](#) oder [Benutzer und Gruppen entfernen](#), um den Umfang der Synchronisierung jederzeit zu ändern.
 - Weisen Sie synchronisierten Benutzern und Gruppen Single [Sign-On-Zugriff auf AWS-Konten](#) oder [Zugriff auf Anwendungen zu](#). Bei den Anwendungen kann AWS es sich um verwaltete Anwendungen oder um vom Kunden verwaltete Anwendungen handeln.
 - Steuern Sie den Synchronisierungsvorgang, indem Sie die [Synchronisierung bei Bedarf pausieren und wieder aufnehmen](#). Auf diese Weise können Sie die Auslastung der Produktionssysteme regulieren.

Voraussetzungen und Überlegungen

Bevor Sie die konfigurierbare AD-Synchronisierung verwenden, sollten Sie die folgenden Voraussetzungen und Überlegungen beachten:

- Angeben der zu synchronisierenden Benutzer und Gruppen in Active Directory

Bevor Sie IAM Identity Center verwenden können, um neuen Benutzern und Gruppen Zugriff auf verwaltete oder vom Kunden AWS verwaltete Anwendungen zuzuweisen, müssen Sie die Benutzer und Gruppen in Active Directory angeben, die synchronisiert werden sollen, und sie dann mit IAM Identity Center synchronisieren. AWS-Konten

- Konfigurierbare AD-Synchronisierung — IAM Identity Center durchsucht Ihren Domain-Controller nicht direkt nach Benutzern und Gruppen. Stattdessen müssen Sie zunächst die Liste der Benutzer und Gruppen angeben, die synchronisiert werden sollen. Sie können diese Liste, auch Synchronisierungsbereich genannt, auf eine der folgenden Arten konfigurieren, je nachdem, ob Sie Benutzer und Gruppen haben, die bereits mit IAM Identity Center synchronisiert sind, oder ob Sie neue Benutzer und Gruppen haben, die Sie mithilfe der konfigurierbaren AD-Synchronisierung zum ersten Mal synchronisieren.

- **Bestehende Benutzer und Gruppen:** Wenn Sie Benutzer und Gruppen haben, die bereits mit IAM Identity Center synchronisiert sind, ist der Synchronisierungsbereich in der konfigurierbaren AD-Synchronisierung bereits mit einer Liste dieser Benutzer und Gruppen gefüllt. Um neue Benutzer oder Gruppen zuzuweisen, müssen Sie sie ausdrücklich zum Synchronisierungsbereich hinzufügen. Weitere Informationen finden Sie unter [Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu](#).
- **Neue Benutzer und Gruppen:** Wenn Sie neuen Benutzern und Gruppen Zugriff auf und auf Anwendungen zuweisen möchten, müssen Sie in der konfigurierbaren AD-Synchronisierung angeben, welche Benutzer und Gruppen dem Synchronisierungsbereich hinzugefügt werden sollen, bevor Sie IAM Identity Center für die Zuweisung verwenden können. AWS-Konten Weitere Informationen finden Sie unter [Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu](#).

- Zuweisungen zu verschachtelten Gruppen in Active Directory vornehmen

Gruppen, die Mitglieder anderer Gruppen sind, werden als verschachtelte Gruppen (oder untergeordnete Gruppen) bezeichnet.

- **Konfigurierbare AD-Synchronisierung** — Die Verwendung der konfigurierbaren AD-Synchronisierung, um Zuweisungen zu einer Gruppe in Active Directory vorzunehmen, die verschachtelte Gruppen enthält, kann die Anzahl der Benutzer erhöhen, die Zugriff auf AWS-Konten oder auf Anwendungen haben. In diesem Fall gilt die Zuweisung für alle Benutzer, auch für Benutzer in verschachtelten Gruppen. Wenn Sie beispielsweise Gruppe A Zugriff zuweisen und Gruppe B Mitglied von Gruppe A ist, erben Mitglieder von Gruppe B diesen Zugriff ebenfalls.
- **Aktualisierung automatisierter Workflows**

Wenn Sie automatisierte Workflows verwenden, die die IAM Identity Center-API-Aktionen für den Identitätsspeicher und die IAM Identity Center-Zuweisungs-API-Aktionen verwenden, um neuen Benutzern und Gruppen Zugriff auf Konten und Anwendungen zuzuweisen und sie mit IAM Identity Center zu synchronisieren, müssen Sie diese Workflows bis zum 15. April 2022 anpassen, sodass sie mit konfigurierbarer AD-Synchronisierung wie erwartet funktionieren. Die konfigurierbare AD-Synchronisierung ändert die Reihenfolge, in der Benutzer- und Gruppenzuweisungen und -bereitstellungen erfolgen, und die Art und Weise, wie Abfragen ausgeführt werden.

- **Konfigurierbare AD-Synchronisierung** — Die Bereitstellung erfolgt zuerst und nicht automatisch. Stattdessen müssen Sie zuerst Benutzer und Gruppen explizit zum Identitätsspeicher hinzufügen, indem Sie sie Ihrem Synchronisierungsbereich hinzufügen. Informationen

zu den empfohlenen Schritten zur Automatisierung Ihrer Synchronisierungskonfiguration für die konfigurierbare AD-Synchronisierung finden Sie unter [Automatisieren Sie Ihre Synchronisierungskonfiguration für eine konfigurierbare AD-Synchronisierung](#).

Themen

- [So funktioniert die konfigurierbare AD-Synchronisierung](#)
- [Konfigurieren Sie Attributzuordnungen für Ihre Synchronisierung](#)
- [First-time Einrichtung der Synchronisierung zwischen Active Directory und IAM Identity Center](#)
- [Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu](#)
- [Entfernen Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich](#)
- [Unterbrechen Sie die Synchronisierung und setzen Sie sie fort](#)
- [Automatisieren Sie Ihre Synchronisierungskonfiguration für eine konfigurierbare AD-Synchronisierung](#)

So funktioniert die konfigurierbare AD-Synchronisierung

IAM Identity Center aktualisiert die AD-based Identitätsdaten im Identitätsspeicher mithilfe des folgenden Verfahrens. Weitere Informationen zu den Voraussetzungen finden Sie unter [Voraussetzungen und Überlegungen](#)

Erstellung

Nachdem Sie Ihr selbstverwaltetes Verzeichnis in Active Directory oder Ihr von Directory Service IAM Identity Center verwaltetes AWS Managed Microsoft AD Verzeichnis verbunden haben, können Sie die Active Directory-Benutzer und -Gruppen, die Sie mit dem IAM Identity Center-Identitätsspeicher synchronisieren möchten, explizit konfigurieren. Die von Ihnen ausgewählten Identitäten werden etwa alle drei Stunden mit dem IAM Identity Center-Identitätsspeicher synchronisiert. Je nach Größe Ihres Verzeichnisses kann der Synchronisierungsvorgang länger dauern.

Gruppen, die Mitglieder anderer Gruppen sind (sogenannte verschachtelte Gruppen oder untergeordnete Gruppen), werden ebenfalls in den Identitätsspeicher geschrieben.

Sie können neuen Benutzern oder Gruppen erst Zugriff zuweisen, nachdem sie mit dem IAM Identity Center-Identitätsspeicher synchronisiert wurden.

Aktualisierung

Die Identitätsdaten im IAM Identity Center-Identitätsspeicher bleiben aktuell, da regelmäßig Daten aus dem Quellverzeichnis in Active Directory gelesen werden. IAM Identity Center synchronisiert standardmäßig stündlich Daten aus Ihrem Active Directory in einem Synchronisierungszyklus. Je nach Größe Ihres Active Directory kann es 30 Minuten bis 2 Stunden dauern, bis die Daten mit IAM Identity Center synchronisiert sind.

Benutzer- und Gruppenobjekte, die sich im Synchronisierungsbereich befinden, und ihre Mitgliedschaften werden in IAM Identity Center erstellt oder aktualisiert, sodass sie den entsprechenden Objekten im Quellverzeichnis in Active Directory zugeordnet werden. Bei Benutzerattributen wird nur die Teilmenge der Attribute, die im Abschnitt Attribute für die Zugriffskontrolle der IAM Identity Center-Konsole aufgeführt sind, in IAM Identity Center aktualisiert. Es kann einen Synchronisierungszyklus dauern, bis alle Attributaktualisierungen, die Sie in Active Directory vornehmen, in IAM Identity Center übernommen werden.

Sie können auch die Teilmenge der Benutzer und Gruppen aktualisieren, die Sie mit dem IAM Identity Center-Identitätsspeicher synchronisieren. Sie können wählen, ob Sie dieser Teilmenge neue Benutzer oder Gruppen hinzufügen oder sie entfernen möchten. Alle Identitäten, die Sie hinzufügen, werden bei der nächsten geplanten Synchronisierung synchronisiert. Identitäten, die Sie aus der Teilmenge entfernen, werden nicht mehr im IAM Identity Center-Identitätsspeicher aktualisiert. Jeder Benutzer, der länger als 28 Tage nicht synchronisiert wurde, wird im IAM Identity Center-Identitätsspeicher deaktiviert. Die entsprechenden Benutzerobjekte werden während des nächsten Synchronisierungszyklus automatisch im IAM Identity Center-Identitätsspeicher deaktiviert, sofern sie nicht Teil einer anderen Gruppe sind, die immer noch Teil des Synchronisierungsbereichs ist.

Löschung

Benutzer und Gruppen werden aus dem IAM Identity Center-Identitätsspeicher gelöscht, wenn die entsprechenden Benutzer- oder Gruppenobjekte aus dem Quellverzeichnis in Active Directory gelöscht werden. Alternativ können Sie Benutzerobjekte mithilfe der IAM Identity Center-Konsole explizit aus dem IAM Identity Center-Identitätsspeicher löschen. Wenn Sie die IAM Identity Center-Konsole verwenden, müssen Sie die Benutzer auch aus dem Synchronisierungsbereich entfernen, um sicherzustellen, dass sie beim nächsten Synchronisierungszyklus nicht erneut mit IAM Identity Center synchronisiert werden.

Sie können die Synchronisation auch jederzeit unterbrechen und neu starten. Wenn Sie die Synchronisation für mehr als 28 Tage unterbrechen, werden alle Ihre Benutzer deaktiviert.

Konfigurieren Sie Attributzuordnungen für Ihre Synchronisierung

Weitere Informationen zu verfügbaren Attributen finden Sie unter [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#)

So konfigurieren Sie Attributzuordnungen in IAM Identity Center zu Ihrem Verzeichnis

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“.
4. Wählen Sie unter Synchronisierung verwalten die Option Attributzuordnung anzeigen aus.
5. Konfigurieren Sie unter Active Directory-Benutzerattribute die IAM Identity Center-Identitätsspeicherattribute und die Active Directory-Benutzerattribute. Beispielsweise möchten Sie möglicherweise das IAM Identity Center-Identitätsspeicherattribut email dem Active Directory-Benutzerverzeichnisattribut zuordnen. `${objectguid}`

Note

Unter Gruppenattribute können die IAM Identity Center-Identitätsspeicherattribute und die Active Directory-Gruppenattribute nicht geändert werden.

6. Wählen Sie Änderungen speichern aus. Dadurch kehren Sie zur Seite „Sync verwalten“ zurück.

First-time Einrichtung der Synchronisierung zwischen Active Directory und IAM Identity Center

Gehen Sie wie folgt vor, wenn Sie Ihre Benutzer und Gruppen zum ersten Mal aus Active Directory mit dem IAM Identity Center synchronisieren. Alternativ können Sie den unter beschriebenen Schritten folgen, [Ändern Sie Ihre Identitätsquelle](#) um Ihre Identitätsquelle von IAM Identity Center auf Active Directory zu ändern.

Geführte Einrichtung

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

 Note

Stellen Sie sicher, dass die IAM Identity Center-Konsole eines der Verzeichnisse verwendet, AWS-Regionen in dem sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Einstellungen aus.
3. Wählen Sie oben auf der Seite in der Benachrichtigung die Option Geführte Installation starten aus.
4. Überprüfen Sie in Schritt 1 — optional: Attributzuordnungen konfigurieren die standardmäßigen Benutzer- und Gruppenattributzuordnungen. Wenn keine Änderungen erforderlich sind, wählen Sie Weiter. Wenn Änderungen erforderlich sind, nehmen Sie die Änderungen vor und wählen Sie dann Änderungen speichern.
5. Wählen Sie in Schritt 2 — optional: Synchronisierungsbereich konfigurieren die Registerkarte Benutzer aus. Geben Sie dann den genauen Benutzernamen des Benutzers ein, den Sie zu Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen. Wählen Sie als Nächstes die Registerkarte Gruppen. Geben Sie den genauen Gruppennamen der Gruppe ein, die Sie zu Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen. Wählen Sie anschließend Weiter. Wenn Sie später Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzufügen möchten, nehmen Sie keine Änderungen vor und wählen Sie Weiter.
6. Bestätigen Sie in Schritt 3: Konfiguration überprüfen und speichern Sie Ihre Attributzuordnungen in Schritt 1: Attributzuordnungen und Ihre Benutzer und Gruppen in Schritt 2: Synchronisierungsbereich. Wählen Sie Save configuration (Konfiguration speichern) aus. Dadurch gelangen Sie zur Seite „Sync verwalten“.

Fügen Sie Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzu

 Note

Wenn Sie Gruppen zu Ihrem Synchronisierungsbereich hinzufügen, synchronisieren Sie Gruppen direkt aus der vertrauenswürdigen lokalen Domäne und nicht aus Gruppen in der AWS Managed Microsoft AD Domäne. Gruppen, die direkt von der vertrauenswürdigen Domain aus synchronisiert wurden, enthalten tatsächliche Benutzerobjekte, auf die IAM Identity Center zugreifen und die erfolgreich synchronisiert werden können.

Gehen Sie wie folgt vor, um Ihre Active Directory-Benutzer und -Gruppen zu IAM Identity Center hinzuzufügen.

So fügen Sie Benutzer hinzu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Überprüfen Sie unter Hinzugefügte Benutzer und Gruppen den Benutzer, den Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer). Wenn der von Ihnen angegebene Benutzer nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

Um Gruppen hinzuzufügen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ den Tab Gruppen und dann Benutzer und Gruppen hinzufügen aus.
5. Wählen Sie die Registerkarte Groups (Gruppen). Geben Sie unter Gruppe den genauen Gruppennamen ein und wählen Sie Hinzufügen aus.
6. Überprüfen Sie unter Hinzugefügte Benutzer und Gruppen die Gruppe, die Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.

8. Wählen Sie im Navigationsbereich die Option Groups (Gruppen). Wenn die von Ihnen angegebene Gruppe nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol, um die Gruppenliste zu aktualisieren.

Entfernen Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich

Weitere Informationen darüber, was passiert, wenn Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich entfernen, finden Sie unter [So funktioniert die konfigurierbare AD-Synchronisierung](#).

Um Benutzer zu entfernen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie die Registerkarte Users.
5. Aktivieren Sie unter Benutzer im Synchronisierungsbereich das Kontrollkästchen neben dem Benutzer, den Sie löschen möchten. Um alle Benutzer zu löschen, aktivieren Sie das Kontrollkästchen neben Benutzername.
6. Wählen Sie Remove (Entfernen) aus.

Um Gruppen zu entfernen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Aktivieren Sie unter Gruppen im Synchronisierungsbereich das Kontrollkästchen neben dem Benutzer, den Sie löschen möchten. Um alle Gruppen zu löschen, aktivieren Sie das Kontrollkästchen neben Gruppenname.
6. Wählen Sie Remove (Entfernen) aus.

Unterbrechen Sie die Synchronisierung und setzen Sie sie fort

Wenn Sie Ihre Synchronisierung unterbrechen, werden alle future Synchronisierungszyklen angehalten und verhindert, dass Änderungen, die Sie an Benutzern und Gruppen in Active Directory vornehmen, in IAM Identity Center widergespiegelt werden. Nachdem Sie die Synchronisierung wieder aufgenommen haben, übernimmt der Synchronisierungszyklus diese Änderungen ab der nächsten geplanten Synchronisierung.

Um die Synchronisierung anzuhalten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ den Tab „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie unter „Synchronisierung verwalten“ die Option „Synchronisierung unterbrechen“ aus.

Um die Synchronisierung fortzusetzen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ den Tab „Identitätsquelle“, dann „Aktionen“ und anschließend „Synchronisation verwalten“ aus.
4. Wählen Sie unter Synchronisierung verwalten die Option Synchronisierung fortsetzen aus.

 Note

Wenn Sie „Synchronisierung unterbrechen“ statt „Synchronisierung fortsetzen“ sehen, wurde die Synchronisierung von Active Directory mit IAM Identity Center bereits wieder aufgenommen.

Automatisieren Sie Ihre Synchronisierungskonfiguration für eine konfigurierbare AD-Synchronisierung

Um sicherzustellen, dass Ihr automatisierter Workflow mit konfigurierbarer AD-Synchronisierung wie erwartet funktioniert, empfehlen wir Ihnen, die folgenden Schritte durchzuführen, um Ihre Synchronisierungskonfiguration zu automatisieren.

Um Ihre Synchronisierungskonfiguration für die konfigurierbare AD-Synchronisierung zu automatisieren

1. Erstellen Sie in Active Directory eine übergeordnete Synchronisierungsgruppe, die alle Benutzer und Gruppen enthält, die Sie mit IAM Identity Center synchronisieren möchten. Sie können der Gruppe IAMIdentityCenterAllUsersAndGroupsbeispielsweise einen Namen geben.
2. Fügen Sie in IAM Identity Center die übergeordnete Synchronisierungsgruppe zu Ihrer konfigurierbaren Synchronisierungsliste hinzu. IAM Identity Center synchronisiert alle Benutzer, Gruppen, Untergruppen und Mitglieder aller Gruppen, die in der übergeordneten Synchronisierungsgruppe enthalten sind.
3. Verwenden Sie die von Microsoft bereitgestellten API-Aktionen für die Active Directory-Benutzer- und Gruppenverwaltung, um Benutzer und Gruppen zur übergeordneten Synchronisierungsgruppe hinzuzufügen oder daraus zu entfernen.

Benutzer im Identity Center-Verzeichnis verwalten

IAM Identity Center bietet die folgenden Funktionen für Ihre Benutzer und Gruppen:

- Erstellen Sie Ihre Benutzer und Gruppen.
- Fügen Sie Ihre Benutzer den Gruppen als Mitglieder hinzu.
- Weisen Sie den Gruppen die gewünschte Zugriffsebene für Ihre Anwendungen AWS-Konten zu.

AWS Unterstützt die unter Identity [Center-Aktionen aufgeführten API-Operationen zur Verwaltung von Benutzern und Gruppen im IAM Identity Center](#) Store.

Bereitstellung, wenn sich Benutzer im IAM Identity Center befinden

Wenn Sie Benutzer und Gruppen direkt in IAM Identity Center erstellen, erfolgt die Bereitstellung automatisch. Diese Identitäten sind sofort für die Zuweisung von Aufgaben und für Anwendungen verfügbar. Weitere Informationen finden Sie unter [Bereitstellung für Benutzer und Gruppen](#).

Ändern Sie Ihre Identitätsquelle

Wenn Sie Benutzer lieber in verwalten möchten AWS Managed Microsoft AD, können Sie die Verwendung Ihres Identity Center-Verzeichnisses jederzeit beenden und stattdessen IAM Identity Center mit Ihrem Verzeichnis in Microsoft AD verbinden, indem Sie Directory Service Weitere

Informationen finden Sie unter Überlegungen zu [Zwischen dem IAM Identity Center-Verzeichnis und Active Directory wechseln](#).

Wenn Sie es vorziehen, Benutzer in einem externen Identitätsanbieter (IdP) zu verwalten, können Sie IAM Identity Center mit Ihrem IdP verbinden und die automatische Bereitstellung aktivieren. Weitere Informationen finden Sie unter Überlegungen zu. [Wechsel von IAM Identity Center zu einem externen IdP](#)

Themen

- [Fügen Sie Benutzer zu Ihrem Identity Center-Verzeichnis hinzu](#)
- [Fügen Sie Gruppen zu Ihrem Identity Center-Verzeichnis hinzu](#)
- [Fügen Sie Benutzer zu Gruppen hinzu](#)
- [Löschen Sie Gruppen in IAM Identity Center](#)
- [Benutzer in IAM Identity Center löschen](#)
- [Benutzer aus Gruppen entfernen](#)
- [Benutzereigenschaften des Identity Center-Verzeichnisses bearbeiten](#)

Fügen Sie Benutzer zu Ihrem Identity Center-Verzeichnis hinzu

Benutzer und Gruppen, die Sie in Ihrem Identity Center-Verzeichnis erstellen, sind nur in IAM Identity Center verfügbar. Gehen Sie wie folgt vor, um Benutzer zu Ihrem Identity Center-Verzeichnis hinzuzufügen. Alternativ können Sie den AWS API-Vorgang aufrufen [CreateUser](#), um Benutzer hinzuzufügen.

Console

So fügen Sie einen Benutzer hinzu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie Benutzer hinzufügen und geben Sie die folgenden erforderlichen Informationen ein:
 - a. Benutzername — Dieser Benutzername ist für die Anmeldung am AWS Access Portal erforderlich und kann später nicht geändert werden. Es muss zwischen 1 und 100 Zeichen lang sein.

- b. **Passwort** — Sie können entweder eine E-Mail mit den Anweisungen zur Einrichtung des Passworts senden (dies ist die Standardoption) oder ein Einmalpasswort generieren. Wenn Sie einen Administratorbenutzer erstellen und sich dafür entscheiden, eine E-Mail zu senden, stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie zugreifen können.
- i. Eine E-Mail mit Anweisungen zur Passworteinrichtung an diesen Benutzer senden — Diese Option sendet dem Benutzer automatisch eine von Amazon Web Services adressierte E-Mail mit der Betreffzeile Einladung zum Beitritt AWS IAM Identity Center. In der E-Mail wird der Benutzer im Namen Ihres Unternehmens aufgefordert, auf das Zugriffsportal für das IAM Identity Center AWS zuzugreifen, und es wird ein Passwort registriert. Die E-Mail-Einladung läuft in sieben Tagen ab. In diesem Fall können Sie die E-Mail erneut senden, indem Sie „Passwort zurücksetzen“ und dann „E-Mail an den Benutzer senden“ mit Anweisungen zum Zurücksetzen des Passworts auswählen. Bevor der Benutzer die Einladung annimmt, wird der Link E-Mail-Bestätigung senden angezeigt, mit dem die E-Mail-Adresse bestätigt werden soll. Dieser Schritt ist jedoch optional und verschwindet, nachdem der Benutzer die Einladung angenommen und ein Passwort registriert hat.

 Note

In bestimmten Regionen sendet IAM Identity Center E-Mails an Benutzer, die Amazon Simple Email Service von einer anderen AWS-Region Region aus verwenden. Informationen darüber, wie E-Mails gesendet werden, finden Sie unter [Cross-Region E-Mails mit Amazon SES](#).

Alle vom IAM Identity Center-Dienst gesendeten E-Mails stammen entweder von der Adresse `no-reply@signin.aws.com` oder `no-reply@login.awsapps.com`. Wir empfehlen Ihnen, Ihr E-Mail-System so zu konfigurieren, dass es E-Mails von diesen Absender-E-Mail-Adressen akzeptiert und sie nicht als Junk oder Spam behandelt.

- ii. Generieren Sie ein Einmalkennwort, das Sie mit diesem Benutzer teilen können — Mit dieser Option erhalten Sie die URL und das Passwort des AWS Zugriffsportals, die Sie dem Benutzer manuell von Ihrer E-Mail-Adresse aus senden können. Der Benutzer muss seine E-Mail-Adresse verifizieren. Sie können den Vorgang einleiten, indem Sie auf Link zur E-Mail-Bestätigung senden klicken. Der Link zur E-Mail-Bestätigung läuft in sieben Tagen ab. In diesem Fall können Sie den Link zur E-

Mail-Bestätigung erneut senden, indem Sie Passwort zurücksetzen und dann Einmalpasswort generieren und das Passwort mit dem Benutzer teilen wählen.

- c. E-Mail-Adresse — Die E-Mail-Adresse muss eindeutig sein.
- d. E-Mail-Adresse bestätigen
- e. Vorname — Sie müssen hier einen Namen eingeben, damit die automatische Bereitstellung funktioniert. Weitere Informationen finden Sie unter [Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit](#).
- f. Nachname — Sie müssen hier einen Namen eingeben, damit die automatische Bereitstellung funktioniert.
- g. Anzeigename

 Note

(Optional) Falls zutreffend, können Sie Werte für zusätzliche Attribute wie die unveränderliche Microsoft 365-ID des Benutzers angeben, um dem Benutzer Single Sign-On-Zugriff auf bestimmte Geschäftsanwendungen zu ermöglichen.

- 4. Wählen Sie Weiter aus.
- 5. Wählen Sie gegebenenfalls eine oder mehrere Gruppen aus, zu denen Sie den Benutzer hinzufügen möchten, und klicken Sie auf Weiter.
- 6. Überprüfen Sie die Informationen, die Sie für Schritt 1: Benutzerdetails angeben und Schritt 2: Benutzer zu Gruppen hinzufügen — optional angegeben haben. Wählen Sie in einem der beiden Schritte die Option Bearbeiten aus, um Änderungen vorzunehmen. Nachdem Sie bestätigt haben, dass die richtigen Informationen für beide Schritte angegeben wurden, wählen Sie Benutzer hinzufügen.

AWS CLI

So fügen Sie einen Benutzer hinzu

Der folgende `create-user` Befehl erstellt einen neuen Benutzer in Ihrem Identity Center-Verzeichnis.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --password "Password123!"
```

```
--display-name "John Doe" \  
--emails "Type=work,Value=johndoe@example.com"
```

Ausgabe:

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

 Note

Wenn Sie Benutzer mit dem `create-user` CLI-Befehl oder der [CreateUserAPI](#)-Operation erstellen, haben die Benutzer keine Passwörter. Sie können die Einstellungen in IAM Identity Center aktualisieren, um diesen Benutzern nach ihrem ersten Anmeldeversuch eine Bestätigungs-E-Mail zu senden, damit sie ein Passwort einrichten können. Wenn Sie diese Einstellung nicht aktivieren, müssen Sie ein Einmalkennwort generieren und es mit dem Benutzer teilen. Weitere Informationen finden Sie unter [Senden Sie Benutzern, die mit API oder CLI erstellt wurden, ein Einmalpasswort per E-Mail](#).

Fügen Sie Gruppen zu Ihrem Identity Center-Verzeichnis hinzu

Gehen Sie wie folgt vor, um Gruppen zu Ihrem Identity Center-Verzeichnis hinzuzufügen. Alternativ können Sie den AWS API-Vorgang aufrufen [CreateGroup](#), um Gruppen hinzuzufügen.

Console

So fügen Sie eine Gruppe hinzu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Klicken Sie auf Groups (Gruppen).
3. Wählen Sie Create group (Gruppe erstellen) aus.
4. Geben Sie einen Gruppennamen und eine Beschreibung ein — optional. Die Beschreibung sollte Angaben darüber enthalten, welche Berechtigungen der Gruppe zugewiesen wurden oder werden. Suchen Sie unter Benutzer zur Gruppe hinzufügen — optional

nach den Benutzern, die Sie als Mitglieder hinzufügen möchten. Aktivieren Sie dann das Kontrollkästchen neben jedem von ihnen.

5. Wählen Sie **Create group** (Gruppe erstellen) aus.

AWS CLI

So fügen Sie eine Gruppe hinzu

Der folgende `create-group` Befehl erstellt eine neue Gruppe in Ihrem Identity Center-Verzeichnis.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Ausgabe:

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Nachdem Sie diese Gruppe zu Ihrem Identity Center-Verzeichnis hinzugefügt haben, können Sie der Gruppe Single Sign-On-Zugriff zuweisen. Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).

Fügen Sie Benutzer zu Gruppen hinzu

Gehen Sie wie folgt vor, um Benutzer als Mitglieder einer Gruppe hinzuzufügen, die Sie zuvor in Ihrem Identity Center-Verzeichnis erstellt haben. Alternativ können Sie den AWS API-Vorgang aufrufen [CreateGroupMembership](#), um einen Benutzer als Mitglied einer Gruppe hinzuzufügen.

Console

So fügen Sie einen Benutzer einer Gruppe als Mitglied hinzu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Klicken Sie auf **Groups** (Gruppen).

3. Wählen Sie den Gruppennamen, den Sie aktualisieren möchten.
4. Wählen Sie auf der Seite mit den Gruppendetails unter Benutzer in dieser Gruppe die Option Benutzer zur Gruppe hinzufügen aus.
5. Suchen Sie auf der Seite Benutzer zur Gruppe hinzufügen unter Andere Benutzer nach den Benutzern, die Sie als Mitglieder hinzufügen möchten. Aktivieren Sie dann das Kontrollkästchen neben jedem von ihnen.
6. Wählen Sie Add Users (Benutzer hinzufügen).

AWS CLI

So fügen Sie einen Benutzer einer Gruppe als Mitglied hinzu

Mit dem folgenden `create-group-membership` Befehl wird einer Gruppe in Ihrem Identity Center-Verzeichnis ein Benutzer hinzugefügt.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Ausgabe:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

Löschen Sie Gruppen in IAM Identity Center

Wenn Sie eine Gruppe in Ihrem IAM Identity Center-Verzeichnis löschen, werden dadurch der Zugriff auf AWS-Konten und die Anwendungen für alle Benutzer, die Mitglieder dieser Gruppe sind, entfernt. Nachdem eine Gruppe gelöscht wurde, kann sie nicht mehr rückgängig gemacht werden. Gehen Sie wie folgt vor, um eine Gruppe in Ihrem Identity Center-Verzeichnis zu löschen.

Important

Die Anweisungen auf dieser Seite gelten für [AWS IAM Identity Center](#). Sie gelten nicht für [AWS Identity and Access Management](#)(IAM). IAM Identity Center-Benutzer, -Gruppen

und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Löschen von Gruppen in IAM finden Sie unter [Löschen einer IAM-Benutzergruppe im Benutzerhandbuch](#).AWS Identity and Access Management

Console

So löschen Sie eine Gruppe

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Klicken Sie auf Groups (Gruppen).
3. Es gibt zwei Möglichkeiten, eine Gruppe zu löschen:
 - Auf der Seite Gruppen können Sie mehrere Gruppen zum Löschen auswählen. Wählen Sie den Gruppennamen aus, den Sie löschen möchten, und wählen Sie Gruppe löschen.
 - Wählen Sie den Gruppennamen, den Sie löschen möchten. Wählen Sie auf der Seite mit den Gruppendetails die Option Gruppe löschen aus.
4. Möglicherweise werden Sie aufgefordert, Ihre Absicht zu bestätigen, die Gruppe zu löschen.
 - Wenn Sie mehrere Gruppen gleichzeitig löschen, bestätigen Sie Ihre Absicht, indem Sie **Delete** im Dialogfeld Gruppe löschen etwas eingeben.
 - Wenn Sie eine einzelne Gruppe löschen, die Benutzer enthält, bestätigen Sie Ihre Absicht, indem Sie den Namen der Gruppe, die Sie löschen möchten, in das Dialogfeld Gruppe löschen eingeben.
5. Wählen Sie Delete group (Gruppe löschen) aus. Wenn Sie mehrere Gruppen zum Löschen ausgewählt haben, wählen Sie „# Gruppen löschen“.

AWS CLI

So löschen Sie eine Gruppe

Der folgende `delete-group` Befehl löscht die angegebene Gruppe aus Ihrem Identity Center-Verzeichnis.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-name mygroup
```



```
--group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Benutzer in IAM Identity Center löschen

Wenn Sie einen Benutzer in Ihrem IAM Identity Center-Verzeichnis löschen, wird ihm dadurch der Zugriff auf AWS-Konten und die Anwendungen entzogen. Nachdem Sie einen Benutzer gelöscht haben, können Sie diese Aktion nicht rückgängig machen. Gehen Sie wie folgt vor, um einen Benutzer in Ihrem Identity Center-Verzeichnis zu löschen.

Note

Wenn Sie den Benutzerzugriff deaktivieren oder einen Benutzer in IAM Identity Center löschen, wird dieser Benutzer sofort daran gehindert, sich beim AWS Zugriffsportal anzumelden, und er kann keine neuen Anmeldesitzungen erstellen. Weitere Informationen finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Important

Die Anweisungen auf dieser Seite gelten für [AWS IAM Identity Center](#). Sie gelten nicht für [AWS Identity and Access Management \(IAM\)](#). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Löschen von Benutzern in IAM finden Sie unter [Löschen eines IAM-Benutzers im Benutzerhandbuch](#). AWS Identity and Access Management

Console

So löschen Sie einen Benutzer

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Users (Benutzer) aus.
3. Es gibt zwei Möglichkeiten, einen Benutzer zu löschen:
 - Auf der Seite Benutzer können Sie mehrere Benutzer zum Löschen auswählen. Wählen Sie den Benutzernamen aus, den Sie löschen möchten, und wählen Sie Benutzer löschen.

- Wählen Sie den Benutzernamen, den Sie löschen möchten. Wählen Sie auf der Seite mit den Benutzerdetails die Option Benutzer löschen aus.
4. Wenn Sie mehrere Benutzer gleichzeitig löschen, bestätigen Sie Ihre Absicht, indem Sie etwas **Delete** in das Dialogfeld „Benutzer löschen“ eingeben.
 5. Wählen Sie Benutzer löschen. Wenn Sie mehrere Benutzer zum Löschen ausgewählt haben, wählen Sie Anzahl Benutzer löschen.

AWS CLI

So löschen Sie einen Benutzer

Der folgende `delete-user` Befehl löscht einen Benutzer aus Ihrem Identity Center-Verzeichnis.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Benutzer aus Gruppen entfernen

Gehen Sie wie folgt vor, um Mitglieder aus einer Gruppe zu entfernen. Alternativ können Sie den AWS API-Vorgang aufrufen [DeleteGroupMembership](#), um einen Benutzer aus einer Gruppe zu entfernen.

Console

So entfernen Sie einen Benutzer aus einer Gruppe

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Klicken Sie auf Groups (Gruppen).
3. Wählen Sie die Gruppe aus, die Sie aktualisieren möchten.
4. Wählen Sie auf der Seite mit den Gruppendetails unter Benutzer in dieser Gruppe die Benutzer aus, die Sie entfernen möchten.
5. Wählen Sie Benutzer aus Gruppe entfernen aus.
6. Wählen Sie im Dialogfeld Benutzer entfernen die Option Benutzer aus Gruppe entfernen aus, um zu überprüfen, ob Sie den Benutzern den Zugriff auf das Konto und die Anwendungen, die der Gruppe zugewiesen sind, entziehen möchten.

AWS CLI

So entfernen Sie einen Benutzer aus einer Gruppe

Mit dem folgenden `delete-group-membership` Befehl wird eine Mitgliedschaft aus einer Gruppe entfernt.

```
aws identitystore delete-group-membership
  --identity-store-id d-1234567890 \
  --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Benutzereigenschaften des Identity Center-Verzeichnisses bearbeiten

Gehen Sie wie folgt vor, um die Eigenschaften eines Benutzers in Ihrem Identity Center-Verzeichnis zu bearbeiten. Alternativ können Sie den AWS API-Vorgang aufrufen, [UpdateUser](#) um die Benutzereigenschaften zu aktualisieren.

Console

Um Benutzereigenschaften im IAM Identity Center zu bearbeiten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.
4. Wählen Sie auf der Benutzerprofilseite neben Profildetails die Option Bearbeiten aus.
5. Aktualisieren Sie auf der Seite Profildetails bearbeiten die Eigenschaften nach Bedarf. Dann wählen Sie Save changes (Änderungen speichern) aus.

Note

(Optional) Sie können zusätzliche Attribute wie die Mitarbeiternummer und die unveränderliche Office 365-ID ändern, um die Identität des Benutzers in IAM Identity Center bestimmten Geschäftsanwendungen zuzuordnen, die Benutzer verwenden müssen.

 Note

Das E-Mail-Adressattribut ist ein bearbeitbares Feld, und der von Ihnen angegebene Wert muss eindeutig sein.

AWS CLI

Um Benutzereigenschaften im IAM Identity Center zu bearbeiten

Der folgende `update-user` Befehl aktualisiert den Spitznamen des Benutzers.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Richten Sie den Zugriff Ihrer Mitarbeiter auf AWS Ressourcen

Richten Sie ein, wie sich Ihre Mitarbeiter über das IAM Identity Center authentifizieren und auf AWS Ressourcen zugreifen. In diesem Abschnitt werden die folgenden Komponenten behandelt, die den Zugriff von Workforce-Benutzern auf Ihre AWS Umgebung regeln:

- **Authentifizierungssitzungen** — Erfahren Sie, wie IAM Identity Center verschiedene Arten von Benutzersitzungen verwaltet — von interaktiven Portalsitzungen bis hin zu Anwendungssitzungen im Hintergrund — und wie diese miteinander interagieren.
- **Verwaltung des Benutzerzugriffs** — Konfigurieren Sie die Sitzungsdauer, deaktivieren Sie Benutzerkonten und implementieren Sie unternehmensweite Zugriffssperren, um Sicherheit und Compliance zu gewährleisten.
- **Passwortverwaltung** — Legen Sie für Benutzer, die im Identity Center-Verzeichnis erstellt wurden, die Kennwortanforderungen fest, kümmern Sie sich um die Einrichtung der Benutzeranmeldeinformationen und verwalten Sie das Zurücksetzen von Kennwörtern für Benutzer.
- **Multi-factor Authentifizierung** — Erhöhen Sie die Sicherheit von Benutzern, die im Identity Center-Verzeichnis erstellt wurden, mit MFA, indem Sie Authentifikator-Apps, Sicherheitsschlüssel oder integrierte Authentifikatoren verwenden, um Benutzeranmeldungen zu schützen.

Themen

- [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#)
- [Konfigurieren Sie die Sitzungsdauer im IAM Identity Center](#)
- [Deaktivieren Sie den Benutzerzugriff auf AWS-Konten und Anwendungen im IAM Identity Center](#)
- [Verweigern Sie den Benutzerzugriff mit Service Control-Richtlinien](#)
- [Verwaltung des Zugriffs für Benutzer im Identity Center-Verzeichnis](#)

Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center

Wenn sich ein Benutzer beim [AWS Access Portal anmeldet](#), erstellt IAM Identity Center eine Authentifizierungssitzung, die die verifizierte Identität des Benutzers darstellt.

Nach der Authentifizierung kann der Benutzer ohne zusätzliche Anmeldungen auf alle ihm zugewiesenen AWS-Konten, [AWS verwalteten Anwendungen](#) und vom [Kunden verwalteten Anwendungen](#) zugreifen, zu deren Verwendung ihm die Administratorrechte erteilt haben.

Arten von Authentifizierungssitzungen

Interaktive Benutzersitzungen

Nachdem sich ein Benutzer beim AWS Zugriffsportal angemeldet hat, erstellt IAM Identity Center eine interaktive Benutzersitzung. Diese Sitzung stellt den authentifizierten Status des Benutzers in IAM Identity Center dar und dient als Grundlage für die Erstellung anderer Sitzungstypen. Interaktive Benutzersitzungen können für die in IAM Identity Center konfigurierte Dauer dauern, die bis zu 90 Tage betragen kann.

Interaktive Benutzersitzungen sind der primäre Authentifizierungsmechanismus. Sie enden, wenn sich der Benutzer abmeldet oder wenn ein Administrator seine Sitzung beendet. Die Dauer dieser Sitzungen sollte sorgfältig auf der Grundlage der Sicherheitsanforderungen Ihres Unternehmens konfiguriert werden.

Informationen zur Konfiguration der Dauer interaktiver Benutzersitzungen finden Sie unter [the section called “Konfigurieren Sie die Sitzungsdauer”](#).

Anwendungssitzungen

Anwendungssitzungen sind die authentifizierten Verbindungen zwischen Benutzern und AWS verwalteten Anwendungen (wie Kiro oder Amazon Quick), die IAM Identity Center per Single Sign-On herstellt.

Standardmäßig haben Anwendungssitzungen eine Lebensdauer von einer Stunde, aber sie werden automatisch aktualisiert, solange die zugrunde liegende interaktive Benutzersitzung gültig bleibt. Dieser Aktualisierungsmechanismus bietet Benutzern ein nahtloses Erlebnis und gewährleistet gleichzeitig die Sicherheitskontrollen. Wenn eine interaktive Benutzersitzung entweder durch Benutzerabmeldung oder Administratoraktion beendet wird, werden die Anwendungssitzungen beim nächsten Aktualisierungsversuch beendet, in der Regel innerhalb von 30 Minuten.

Wenn Sie den [Account Access Manager](#) für den Zugriff auf verwenden AWS-Konten, ist das zugehörige Benutzerportal als AWS Kontozugriffsanwendung im AWS Zugriffsportal verfügbar. Die Sitzung der AWS Kontozugriffsanwendung wird vom IAM Identity Center als Anwendungssitzung verwaltet.

Benutzersitzungen im Hintergrund

Benutzer-Hintergrundsitzungen sind Sitzungen mit längerer Dauer, die für Anwendungen konzipiert sind, bei denen Prozesse stunden- oder tagelang ohne Unterbrechung ausgeführt werden müssen. Derzeit gilt dieser Sitzungstyp hauptsächlich für [Amazon SageMaker Studio](#), wo Datenwissenschaftler möglicherweise Trainingsaufgaben für maschinelles Lernen ausführen, deren Abschluss viele Stunden in Anspruch nimmt.

Informationen zur Konfiguration der Dauer von Benutzersitzungen im Hintergrund finden Sie unter [Benutzersitzungen im Hintergrund](#).

Kiro-Sitzungen

Sie können Kiro-Sitzungen verlängern, sodass Entwickler, die Kiro in IDEs verwenden, die Authentifizierung bis zu 90 Tage lang aufrechterhalten können. Diese Funktion reduziert Anmeldeunterbrechungen, während Sie am Code arbeiten.

Diese Sitzungen sind unabhängig von anderen Sitzungstypen und wirken sich nicht auf interaktive Benutzersitzungen oder andere AWS verwaltete Anwendungen aus. Je nachdem, wann Sie IAM Identity Center aktiviert haben, ist diese Funktion möglicherweise standardmäßig aktiviert.

Informationen zur Konfiguration erweiterter Kiro-Sitzungen finden Sie unter [???](#)

IAM-Rollensitzungen

Auf Berechtigungssätzen basierende IAM-Rollensitzungen

IAM Identity Center erstellt einen anderen Sitzungstyp, wenn Benutzer auf das oder zugreifen. AWS-Managementkonsole AWS CLI In diesen Fällen verwendet IAM Identity Center die Anmeldesitzung, um eine IAM-Sitzung abzurufen, indem es eine IAM-Rolle annimmt, die im Berechtigungssatz des Benutzers angegeben ist.

Vom Account Access Manager erstellte IAM-Rollensitzungen

Wenn Sie den Kontozugriffsmanager für den Zugriff auf verwenden AWS-Konten, übernimmt der Kontozugriffsmanager die zugewiesenen IAM-Rollen und initiiert somit IAM-Rollensitzungen.

Important

Im Gegensatz zu Anwendungssitzungen werden IAM-Rollensitzungen unabhängig voneinander ausgeführt, sobald sie eingerichtet sind. Sie bleiben für die im Berechtigungssatz (oder in der IAM-Rolle, wenn Sie den Account Access Manager verwenden) konfigurierte

Dauer bestehen, die unabhängig vom Status der ursprünglichen Anmeldesitzung bis zu 12 Stunden betragen kann. Dieses Verhalten stellt sicher, dass lang andauernde CLI-Operationen oder Konsolensitzungen nicht unerwartet beendet werden.

Möglichkeiten zum Beenden von Benutzersitzungen im IAM Identity Center

User-initiated

Wenn sich ein Benutzer vom AWS Access Portal abmeldet, endet die Anmeldesitzung, sodass der Benutzer nicht auf neue Ressourcen zugreifen kann.

Bestehende Anwendungssitzungen werden jedoch nicht sofort beendet. Stattdessen werden sie innerhalb von etwa 30 Minuten beendet, wenn sie ihre nächste Aktualisierung versuchen und feststellen, dass die Anmeldesitzung nicht mehr gültig ist. Bestehende IAM-Rollensitzungen laufen weiter, bis sie je nach Konfiguration des Berechtigungssatzes (oder der IAM-Rollenkonfiguration bei Verwendung des Account Access Managers) ablaufen. Dies kann bis zu 12 Stunden später sein.

Administrator-initiated

Jeder in Ihrer Organisation mit IAM Identity Center-Administratorberechtigungen, in der Regel IT-Administratoren oder Sicherheitsteams, kann die Sitzung eines Benutzers [beenden](#). Diese Aktion funktioniert genauso, als ob sich Benutzer selbst abmelden würden, sodass Administratoren von Benutzern verlangen können, dass sie sich bei Bedarf erneut anmelden. Diese Funktion ist nützlich, wenn sich Sicherheitsrichtlinien ändern oder wenn verdächtige Aktivitäten erkannt werden.

Wenn ein IAM Identity Center-Administrator einen Benutzer [löscht](#) oder den Zugriff eines Benutzers [deaktiviert](#), verliert der Benutzer den Zugriff auf das AWS Zugriffsportale und kann sich nicht erneut anmelden, um eine neue Anwendungs- oder IAM-Rollensitzung zu starten. Der Benutzer verliert innerhalb von 30 Minuten den Zugriff auf bestehende Anwendungssitzungen. Alle vorhandenen IAM-Rollensitzungen werden auf der Grundlage der Sitzungsdauer fortgesetzt, die im IAM Identity Center-Berechtigungssatz konfiguriert ist (oder in der IAM-Rolle, wenn der Account Access Manager verwendet wird). Die maximale Sitzungsdauer kann 12 Stunden betragen.

Was passiert mit dem Benutzerzugriff, wenn Sie eine Sitzung beenden

Diese Referenz enthält detaillierte Informationen darüber, wie sich IAM Identity Center-Sitzungen verhalten, wenn administrative Maßnahmen ergriffen werden. Die Tabellen in diesem Abschnitt zeigen die Dauer und die Auswirkungen von Benutzerverwaltungsaktionen und

Berechtigungsänderungen auf den Zugriff auf das AWS Access Portal, Anwendungen und AWS-Konto Sitzungen.

Benutzerverwaltung

In dieser Tabelle wird zusammengefasst, wie sich Änderungen an der Benutzerverwaltung auf den Zugriff auf AWS Ressourcen, Anwendungssitzungen und AWS Kontositzungen auswirken.

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
Der Zugriff des Benutzers ist deaktiviert	Mit sofortiger Wirkung	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die für den Berechtigungsatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).
Benutzer wurde gelöscht	Mit sofortiger Wirkung	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
				für den Berechtigungsatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).
Benutzersitzung wurde widerrufen	Der Benutzer muss sich erneut anmelden, um wieder Zugriff zu erhalten	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die für den Berechtigungsatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
Der Benutzer meldet sich ab	Der Benutzer muss sich erneut anmelden, um wieder Zugriff zu erhalten	Mit sofortiger Wirkung	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle ab, die für den Berechtigungssatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).

Gruppenmitgliedschaft

In dieser Tabelle wird zusammengefasst, wie sich Änderungen an Benutzerberechtigungen und Gruppenmitgliedschaften auf den Zugriff auf AWS Ressourcen, Anwendungssitzungen und Kontositzungen auswirken. AWS

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
Dem Benutzer wurde die Anwendung oder der AWS-Konto Zugriff entzogen	Nein — Benutzer können weiterhin auf IAM Identity Center zugreifen	Ab sofort wirksam	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die für den Berechtig ungssatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).
Der Benutzer wurde aus der Gruppe entfernt, der eine Anwendung zugewiesen war, oder AWS-Konto	Nein — Der Benutzer kann weiterhin auf IAM Identity Center zugreifen	Ab sofort wirksam	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die für den Berechtig ungssatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account

Action	Der Benutzer verliert den Zugriff auf das IAM Identity Center	Der Benutzer kann keine neuen Anwendungssitzungen erstellen	Der Benutzer kann nicht auf bestehende Anwendungssitzungen zugreifen	Der Benutzer verliert den Zugriff auf bestehende AWS-Konto Sitzungen
				Access Manager verwendet wird).
Die Anwendung oder der AWS-Konto Zugriff wurde aus der Gruppe entfernt	Nein — Der Benutzer kann weiterhin auf IAM Identity Center zugreifen	Ab sofort wirksam	Innerhalb von 30 Minuten	Innerhalb von 12 Stunden oder weniger. Die Dauer hängt von der Ablaufdauer der IAM-Rolle nsitzung ab, die für den Berechtig ungssatz konfiguriert ist (oder von der IAM-Rolle, wenn der Account Access Manager verwendet wird).

Note

Das AWS Zugriffsportal und die aktualisierten Benutzerberechtigungen AWS CLI werden sofort angezeigt, nachdem Sie einen Benutzer zu dieser Gruppe hinzugefügt oder daraus entfernt haben. Wenn Sie einen externen Identitätsanbieter verwenden, werden die Änderungen wirksam, nachdem Ihr Anbieter das Update mit dem IAM Identity Center synchronisiert hat.

Verstehen von Zeitunterschieden

- **Ab sofort gültig** — IAM Identity Center bewertet Änderungen der Gruppenmitgliedschaft und der Berechtigungen in Echtzeit. Wenn ein Benutzer das nächste Mal versucht, eine neue Sitzung zu erstellen, wird die Änderung durchgesetzt.
- **Innerhalb von 30 Minuten** — Bestehende Anwendungssitzungen enden beim nächsten Aktualisierungsversuch, in der Regel innerhalb von 30 Minuten.
- **Innerhalb von 12 Stunden oder weniger** — IAM-Rollensitzungen laufen unabhängig voneinander ab und enden erst, wenn ihre konfigurierte Dauer abgelaufen ist.

Einmaliges Abmelden

IAM Identity Center unterstützt kein SAML Single Logout (ein Protokoll, das Benutzer automatisch von allen verbundenen Anwendungen abmeldet, wenn sie sich von einer abmelden), initiiert von einem Identitätsanbieter, der als Ihre Identitätsquelle fungiert. [???](#) Darüber hinaus sendet es kein SAML Single Logout an [SAML 2.0-Anwendungen, die IAM Identity Center als](#) Identitätsanbieter verwenden.

Bewährte Methoden für das Sitzungsmanagement

Effektives Sitzungsmanagement erfordert eine durchdachte Konfiguration und Überwachung. Unternehmen sollten die Sitzungsdauer entsprechend ihren Sicherheitsanforderungen konfigurieren und in der Regel kürzere Sitzungsdauern für sensible Anwendungen und Umgebungen verwenden.

Die Implementierung von Prozessen zur Beendigung von Sitzungen, wenn Benutzer die Rolle wechseln oder das Unternehmen verlassen, ist für die Einhaltung der Sicherheitsgrenzen unerlässlich. Die regelmäßige Überprüfung der aktiven Sitzungen sollte in die Sicherheitsüberwachungspraktiken integriert werden, um anomales Verhalten zu erkennen, das auf Sicherheitsprobleme hinweisen könnte, wie z. B. ungewöhnliche Zugriffsmuster, unerwartete Anmeldezeiten oder -orte oder Zugriffe auf Ressourcen außerhalb der normalen Aufgaben.

Konfigurieren Sie die Sitzungsdauer im IAM Identity Center

Sie können die Sitzungsdauer für die Benutzer Ihrer Belegschaft konfigurieren, wenn sie die AWS-Zugangsportal und Anwendungen verwenden, die mit IAM Identity Center funktionieren, einschließlich Kiro. IAM Identity Center bietet die folgenden Sitzungstypen: interaktive Benutzersitzungen, Benutzer-Hintergrundsitzungen und erweiterte Sitzungen für Kiro.

Themen

- [Interaktive Benutzersitzungen](#)
- [Benutzersitzungen im Hintergrund](#)
- [Erweiterte Sitzungen für Kiro](#)
- [Aktive Sitzungen für Ihre Workforce-Benutzer anzeigen und beenden](#)
- [Überlegungen zur Sitzungsdauer bei der Verwendung von Identitätsquellen: AWS CLI und AWS SDKs](#)

Interaktive Benutzersitzungen

Interaktive Benutzersitzungen sind Sitzungen, die mit der Anmeldung eines Benutzers beim AWS Zugriffsportal oder dem Zugriff auf [AWS verwaltete Anwendungen](#) verknüpft sind. Die Sitzungsdauer der Authentifizierung bei den AWS-Zugangsportal und Anwendungen ist die maximale Zeitdauer, für die ein Benutzer angemeldet werden kann, ohne sich erneut zu authentifizieren. Wenn Sie eine aktive AWS Access-Portalsitzung beenden, werden damit auch alle Sitzungen für diese verwalteten Anwendungen beendet.

Die Standardsitzungsdauer für interaktive Benutzersitzungen beträgt 8 Stunden. Sie können eine andere Dauer angeben, von mindestens 15 Minuten bis maximal 90 Tagen. Benutzerdefinierte Werte für die Dauer müssen in Minuten eingegeben werden und zwischen 15 Minuten und 129.600 Minuten (90 Tage) liegen. Weitere Informationen finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Überlegungen dazu, wie sich IAM Identity Center-Identitätsquellen auf die Dauer interaktiver Benutzersitzungen auswirken könnten, finden Sie unter [the section called “Überlegungen zu Identitätsquellen, AWS CLI und AWS SDKs”](#)

So konfigurieren Sie die Dauer einer interaktiven Benutzersitzung

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Authentifizierung“.
4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.

5. Wählen Sie im Dialogfeld Sitzungsdauer konfigurieren unter Interaktive Benutzersitzungen die maximale Sitzungsdauer für Ihre Benutzer aus, indem Sie auf den Dropdown-Pfeil klicken. Wählen Sie die Dauer der Sitzung aus, und klicken Sie dann auf Speichern.

 Note

Änderungen der Sitzungsdauer gelten nur für neue Sitzungen. Aktuelle Sitzungen behalten ihre ursprüngliche Dauer bei.

6. Sie kehren zur Registerkarte Authentifizierung zurück. Eine grüne Benachrichtigung über der Registerkarte weist darauf hin, dass die Sitzungseinstellungen erfolgreich aktualisiert wurden.

Benutzersitzungen im Hintergrund

Benutzersitzungen im Hintergrund ermöglichen es einem Benutzer, einen Job mit langer Laufzeit in einer AWS verwalteten Anwendung wie [Amazon SageMaker Studio zu initiieren](#), ohne dass dieser Benutzer angemeldet bleiben muss, während der Job ausgeführt wird. Der Job wird sofort ausgeführt und nutzt die [Funktion zur Weitergabe](#) vertrauenswürdiger Identitäten von IAM Identity Center, um sicherzustellen, dass die Benutzerberechtigungen beibehalten werden, während der Job im Hintergrund ausgeführt wird. Der Job kann auch dann weiter ausgeführt werden, wenn der Benutzer seinen Computer ausschaltet, seine IAM Identity Center-Anmeldesitzung abläuft oder der Benutzer sich vom Access Portal abmeldet. AWS Diese Funktion ermöglicht es Datenwissenschaftlern, Machine-Learning-Ingenieuren und anderen, Workflows für Analysen und maschinelles Lernen zu starten, die im Hintergrund ohne aktive Benutzerbeteiligung ausgeführt werden.

Benutzersitzungen im Hintergrund sind für unterstützte AWS verwaltete Anwendungen wie Amazon SageMaker Studio standardmäßig aktiviert. Um diese Funktion nutzen zu können, müssen Sie jedoch die Verbreitung vertrauenswürdiger Identitäten in Amazon SageMaker Studio aktivieren, wenn Sie eine Domain erstellen oder aktualisieren. Weitere Informationen finden Sie unter [Aktivieren Sie die Verbreitung vertrauenswürdiger Identitäten in Ihrer Amazon SageMaker AI-Domain](#).

Die Standardsitzungsdauer für Benutzersitzungen im Hintergrund beträgt 7 Tage. Sie können eine andere Dauer angeben, von mindestens 15 Minuten bis maximal 90 Tagen. Benutzerdefinierte Werte für die Dauer müssen in Minuten eingegeben werden und zwischen 15 Minuten und 129.600 Minuten (90 Tage) liegen.

Beachten Sie bei Benutzersitzungen im Hintergrund die folgenden Überlegungen:

- Eine Benutzer-Hintergrundsitzung kann nur erstellt werden, wenn ein Benutzer manuell einen Job in Amazon SageMaker Studio initiiert. Diese Funktion wird für automatisierte, geplante Workflows nicht unterstützt.
- Eine Liste der AWS Regionen, die Benutzersitzungen im Hintergrund unterstützen, finden Sie unter [Unterstützte AWS Regionen](#).
- Sie können Benutzersitzungen im Hintergrund in einsehen CloudTrail. Weitere Informationen finden Sie unter [Identifizieren der Hintergrundsitzungsdetails von Benutzern](#).
- Sie können auch aktive Sitzungen für einen Benutzer in Ihrer Organisation beenden. Weitere Informationen finden Sie unter [Beenden aktiver Sitzungen für Ihre Mitarbeiter](#).

So konfigurieren Sie die Dauer einer Benutzersitzung im Hintergrund

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Authentifizierung“.
4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.
5. Wenn im Dialogfeld Sitzungsdauer konfigurieren das Kontrollkästchen Benutzersitzungen im Hintergrund aktivieren nicht bereits aktiviert ist, wählen Sie es aus. Deaktivieren Sie das Kontrollkästchen, um Benutzersitzungen im Hintergrund zu deaktivieren.

 Note

Aktuelle Sitzungen sind nicht betroffen, wenn Sie Benutzersitzungen im Hintergrund deaktivieren.

6. Wählen Sie unter Benutzer-Hintergrundsitzungen die maximale Sitzungsdauer aus, indem Sie auf den Dropdown-Pfeil klicken. Wählen Sie die Dauer der Sitzung aus, und klicken Sie dann auf Speichern.

 Note

Änderungen der Sitzungsdauer gelten nur für neue Sitzungen. Aktuelle Sitzungen behalten ihre ursprüngliche Dauer bei.

7. Sie kehren zur Registerkarte **Authentifizierung** zurück. Eine grüne Benachrichtigung über der Registerkarte weist darauf hin, dass die Sitzungseinstellungen erfolgreich aktualisiert wurden.

 Note

Eine vom Kunden verwaltete Anwendung kann keine Benutzersitzung im Hintergrund erstellen.

Erweiterte Sitzungen für Kiro

Wenn Ihre Entwickler Kiro als Teil einer integrierten Entwicklungsumgebung (IDE) verwenden, können Sie die Sitzungsdauer für Kiro auf 90 Tage festlegen. Je nachdem, wann Sie IAM Identity Center aktiviert haben, ist die erweiterte Sitzungsdauer für Kiro möglicherweise standardmäßig aktiviert. Diese erweiterte Sitzung hat keinen Einfluss auf die Sitzungsdauer des AWS Access Portals oder anderer AWS verwalteter Anwendungen.

Überlegungen dazu, wie sich IAM Identity Center-Identitätsquellen auf die verlängerte Sitzungsdauer auswirken könnten, finden Sie unter [the section called “Überlegungen zu Identitätsquellen, AWS CLI und AWS SDKs”](#).

 Note

Kiro ist über Konsolen zugänglich, AWS-Regionen die auf kommerziell eingestellt sind und standardmäßig aktiviert sind. Wenn sich Ihre IAM Identity Center-Instanz in einer Region befindet, in der Kiro derzeit nicht zugänglich ist, wird die Standardeinstellung durch die Aktivierung der verlängerten Sitzungsdauer von 90 Tagen nicht außer Kraft gesetzt. Das bedeutet, dass Ihre Sitzungsdauer unverändert bleibt, unabhängig davon, ob Sie die verlängerte Sitzungsdauer um 90 Tage aktivieren oder nicht. Weitere Informationen finden Sie unter [Unterstützte AWS Regionen für Kiro](#).

Um eine Sitzung für Kiro zu verlängern

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie **Einstellungen** aus.
3. Wählen Sie auf der Seite **„Einstellungen“** den Tab **„Authentifizierung“**.

4. Wählen Sie unter Authentifizierung neben Sitzungsdauer die Option Konfigurieren aus. Das Dialogfeld Sitzungsdauer konfigurieren wird angezeigt.
5. Markieren Sie im Dialogfeld Sitzungsdauer konfigurieren das Kontrollkästchen Erweiterte Sitzungen für Kiro aktivieren. Deaktivieren Sie das Kontrollkästchen, um erweiterte Sitzungssitzungen für Kiro zu deaktivieren.
6. Wählen Sie Speichern, um zur Einstellungsseite zurückzukehren.

Aktive Sitzungen für Ihre Workforce-Benutzer anzeigen und beenden

Als IAM Identity Center-Administrator können Sie die Liste der aktiven Sitzungen Ihrer Workforce-Benutzer einsehen und bei Bedarf eine oder mehrere Sitzungen für einen Benutzer beenden. Beispielsweise müssen Sie möglicherweise die Sitzungen eines Benutzers beenden, wenn:

- Der Benutzer benötigt die Sitzungen nicht mehr.
- Der Benutzer sollte seinen aktuellen Authentifizierungsstatus nicht beibehalten. Dies kann passieren, wenn sie das Unternehmen verlassen oder sich ihre Berechtigungen ändern.

Sie können diese Sitzungen mithilfe der IAM Identity Center-Konsole anzeigen und beenden. Ihre Benutzer können ihre eigenen Sitzungen auch über das AWS Zugriffsportal anzeigen und beenden. Informationen darüber, wie Ihre Mitarbeiter ihre Sitzungen ohne Unterstützung eines Administrators einsehen und beenden können, finden Sie unter [Ihre aktive Sitzung anzeigen und beenden](#).

Note

Durch das Beenden einer aktiven Sitzung für einen IAM Identity Center-Benutzer werden keine aktiven IAM-Rollensitzungen im AWS-Managementkonsole oder beendet. AWS CLI Weitere Informationen finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Um eine aktive Sitzung für einen Workforce-Benutzer zu beenden (IAM Identity Center-Konsole)

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie auf der Seite Benutzer den Benutzernamen des Benutzers aus, dessen Sitzungen Sie verwalten möchten. Dadurch gelangen Sie zu einer Seite mit den Benutzerinformationen.

4. Wählen Sie auf der Benutzerseite den Tab **Aktive Sitzungen**. Die Zahl in Klammern neben **Aktive Sitzungen** gibt die Anzahl der aktiven Sitzungen für diesen Benutzer an.
5. Suchen Sie nach Benutzersitzungen im Hintergrund (optional)

Um anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen zu suchen, wählen Sie in der Liste **Sitzungstyp** die Option **Benutzerhintergrundsitzungen** aus und geben Sie dann die Job-ARN in das Suchfeld ein.

 Note

Sie können nur aktive Sitzungen beenden, die geladen sind. Wenn ein Benutzer viele Sitzungen hat, wählen Sie **Weitere aktive Sitzungen laden**, um weitere Sitzungen anzuzeigen.

6. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann Sitzungen **beenden** aus.
7. Ein Dialogfeld wird angezeigt, das bestätigt, dass Sie aktive Sitzungen für diesen Benutzer beenden. Überprüfen Sie die Informationen. Wenn Sie den Vorgang fortsetzen möchten, geben Sie Folgendes ein **confirm**, und wählen Sie dann Sitzungen **beenden** aus.
8. Sie kehren zur Seite des Benutzers zurück. Eine grüne Benachrichtigung wird angezeigt, um darauf hinzuweisen, dass die ausgewählten Sitzungen erfolgreich beendet wurden.

Überlegungen zur Sitzungsdauer bei der Verwendung von Identitätsquellen: AWS CLI und AWS SDKs

Im Folgenden finden Sie Überlegungen zur Konfiguration der Sitzungsdauer, wenn Sie Microsoft Active Directory (AD) oder einen externen Identitätsanbieter (IdP) als Identitätsquelle oder die AWS Command Line Interface AWS Software Development Kits (SDKs) oder andere AWS Entwicklungstools für den programmgesteuerten Zugriff auf AWS Dienste verwenden.

Microsoft Active Directory, interaktive Benutzersitzungen und erweiterte Sitzungen für Kiro

Wenn Sie Microsoft Active Directory (AD) als Identitätsquelle verwenden und die Sitzungsdauer für interaktive Benutzersitzungen oder erweiterte Sitzungen für Kiro konfigurieren, sollten Sie die folgenden Überlegungen berücksichtigen.

 Note

Diese Überlegungen gelten nicht für Benutzersitzungen im Hintergrund.

Unabhängig davon, ob Sie AD Connector verwenden AWS Managed Microsoft AD oder in AWS Directory Service diesem konfiguriert ist, kann die in Microsoft AD definierte maximale Gültigkeitsdauer für Kerberos-Tickets für Benutzer beeinflussen, wie lange interaktive Benutzersitzungen und erweiterte Sitzungen für Kiro gültig sind. Weitere Informationen zu dieser Einstellung finden Sie [auf der Microsoft-Website unter](#) Maximale Gültigkeitsdauer für Benutzertickets.

- **AWS Managed Microsoft AD:** Wenn Sie Configure AWS Managed Microsoft AD in verwenden AWS Directory Service, ist die maximale Gültigkeitsdauer für Benutzer-Kerberos-Tickets auf 10 Stunden festgelegt. Daher ist die Dauer interaktiver Benutzersitzungen auf 10 Stunden festgelegt, je nachdem, welcher Wert in der IAM Identity Center-Einstellung liegt, je nachdem, welcher Wert kürzer ist. Wenn Sie beispielsweise die Dauer interaktiver Benutzersitzungen auf 12 Stunden festlegen, müssen sich Ihre Benutzer nach 10 Stunden erneut im AWS Access Portal authentifizieren. Das gleiche 10-Stunden-Limit gilt für längere Sitzungen für Kiro.
- **AD Connector:** Wenn Sie AD Connector verwenden, der in konfiguriert ist AWS Directory Service, wird die maximale Gültigkeitsdauer für Benutzer-Kerberos-Tickets in Microsoft AD hinter dem AD Connector definiert. Der Standardwert ist 10 Stunden und hat den gleichen Effekt auf interaktive Benutzersitzungen und erweiterte Sitzungen wie für. AWS Managed Microsoft AD Obwohl dieses Limit in Microsoft AD konfigurierbar sein kann, empfehlen wir, dass Sie mit Ihrem IT-Administrator zusammenarbeiten, um die Risiken abzuwägen, insbesondere, weil sich diese Einstellung auf die Sitzungsdauer für andere Microsoft AD-Clientanwendungen auswirken kann.

Externe Identitätsanbieter, interaktive Benutzersitzungen und erweiterte Sitzungen für Kiro

Wenn Sie einen externen Identitätsanbieter (IdP) verwenden und die Sitzungsdauer für interaktive Benutzersitzungen oder erweiterte Sitzungen für Kiro konfigurieren, sollten Sie die folgenden Überlegungen berücksichtigen.

 Note

Diese Überlegungen gelten nicht für Benutzersitzungen im Hintergrund.

IAM Identity Center verwendet `SessionNotOnOrAfter` Attribute aus SAML-Assertionen, um zu ermitteln, wie lange die Sitzung gültig sein kann.

- Wenn keine SAML-Assertion übergeben `SessionNotOnOrAfter` wird, wird die Dauer einer AWS Access Portal-Sitzung (benutzerinteraktiv) und einer erweiterten Sitzung nicht von der Dauer Ihrer externen IdP-Sitzung beeinflusst. Wenn Ihre IdP-Sitzung beispielsweise 24 Stunden dauert und Sie im IAM Identity Center eine Sitzungsdauer von 18 Stunden festlegen, müssen sich Ihre Benutzer nach 18 Stunden erneut im Access Portal authentifizieren. AWS Ebenso müssen sich Ihre Kiro-Benutzer nach 90 Tagen erneut authentifizieren, wenn Sie eine verlängerte 90-tägige Sitzung für Kiro einrichten.
- Wenn eine SAML-Assertion übergeben `SessionNotOnOrAfter` wird, wird der Wert für die Sitzungsdauer auf den kürzeren Wert aus der Sitzung oder der erweiterten Sitzung im AWS Access Portal (interaktiv) und der Dauer Ihrer SAML-IdP-Sitzung gesetzt. Wenn Sie im IAM Identity Center eine Sitzungsdauer von 72 Stunden festlegen und Ihr IdP eine Sitzungsdauer von 18 Stunden hat, haben Ihre Benutzer für die in Ihrem IdP definierten 18 Stunden Zugriff auf AWS Ressourcen. Ebenso müssen sich Ihre Kiro-Benutzer nach 18 Stunden erneut in Kiro authentifizieren, wenn Sie eine verlängerte 90-tägige Sitzung für Kiro einrichten.
- Wenn die Sitzungsdauer Ihres IdP länger ist als die im IAM Identity Center festgelegte, können Ihre Benutzer eine neue IAM Identity Center-Sitzung starten, ohne ihre Anmeldeinformationen erneut eingeben zu müssen, basierend auf ihrer immer noch gültigen Anmeldesitzung mit Ihrem IdP.

AWS CLI und SDK-Sitzungen

Wenn Sie die AWS CLI, AWS SDKs oder andere AWS Entwicklungstools verwenden, um programmgesteuert auf AWS Dienste zuzugreifen, müssen die folgenden Voraussetzungen erfüllt sein, um die Sitzungsdauer für das AWS Access Portal und die AWS verwalteten Anwendungen festzulegen.

- Sie müssen die Sitzungsdauer des AWS Access Portals [in der IAM Identity Center-Konsole](#) konfigurieren.
- Sie müssen ein Profil für Single-Sign-On-Einstellungen in Ihrer gemeinsam genutzten AWS Konfigurationsdatei definieren. Dieses Profil wird verwendet, um eine Verbindung zum AWS

Access-Portal herzustellen. Wir empfehlen, die Konfiguration des SSO-Token-Anbieters zu verwenden. Mit dieser Konfiguration kann Ihr AWS SDK oder Tool automatisch aktualisierte Authentifizierungstoken abrufen. Weitere Informationen finden Sie unter Konfiguration des [SSO-Token-Anbieters](#) im AWS SDK- und Tools-Referenzhandbuch.

- Benutzer müssen eine Version des AWS CLI oder eines SDK ausführen, das die Sitzungsverwaltung unterstützt.

Mindestversionen von AWS CLI die das Sitzungsmanagement unterstützen

Im Folgenden sind die Mindestversionen von aufgeführt AWS CLI , die die Sitzungsverwaltung unterstützen.

- AWS CLI V2 2.9 oder höher
- AWS CLI V1 1.27.10 oder höher

 Note

Wenn Ihre Benutzer den verwenden und Sie Ihren Berechtigungssatz kurz vor Ablauf der AWS CLI IAM Identity Center-Sitzung aktualisieren und die Sitzungsdauer auf 20 Stunden festgelegt ist, während die Dauer des Berechtigungssatzes auf 12 Stunden festgelegt ist, läuft die AWS CLI Sitzung maximal 20 Stunden plus 12 Stunden für insgesamt 32 Stunden. Weitere Informationen zur IAM Identity Center CLI finden Sie unter [AWS CLI Befehlsreferenz](#).

Mindestversionen von SDKs, die das IAM Identity Center-Sitzungsmanagement unterstützen

Im Folgenden sind die Mindestversionen der SDKs aufgeführt, die die IAM Identity Center-Sitzungsverwaltung unterstützen.

SDK	Mindestversion
Python	1.26.10
PHP	3,245,0
Ruby	AWS-SDK-Kern 3.167.0
Java V2	AWS SDK für Java v2 (2.18.13)

SDK	Mindestversion
Gehe zu V2	Gesamtes SDK: Release-2022-11-11 und spezifische Go-Module: .13.0, .18.0 credentials/v1 config/v1
IST V2	2,1253,0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Deaktivieren Sie den Benutzerzugriff auf AWS-Konten und Anwendungen im IAM Identity Center

Wenn Sie den Benutzerzugriff in Ihrem IAM Identity Center-Verzeichnis deaktivieren, können Sie deren Benutzerdetails nicht bearbeiten, ihr Passwort nicht zurücksetzen, den Benutzer einer Gruppe hinzufügen oder seine Gruppenmitgliedschaft nicht einsehen. Die Deaktivierung des Benutzerzugriffs verhindert, dass sie sich beim AWS Zugriffsportal anmelden, und sie haben keinen Zugriff mehr auf ihre zugewiesenen Anwendungen AWS-Konten . Verwenden Sie die Option Benutzerzugriff deaktivieren, um den Zugriff vorübergehend zu entfernen, wenn Sie den Zugriff möglicherweise später wiederherstellen müssen.

Gehen Sie wie folgt vor, um den Benutzerzugriff in Ihrem Identity Center-Verzeichnis mithilfe der IAM Identity Center-Konsole zu deaktivieren.

Note

Wenn Sie den Benutzerzugriff deaktivieren oder einen Benutzer in IAM Identity Center löschen, wird dieser Benutzer sofort daran gehindert, sich beim AWS Zugriffsportal anzumelden, und er kann keine neuen Anmeldesitzungen erstellen. Weitere Informationen finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#).

Um den Benutzerzugriff in IAM Identity Center zu deaktivieren

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

Important

Die Anweisungen auf dieser Seite gelten für [AWS IAM Identity Center](#). Sie gelten nicht für [AWS Identity and Access Management](#) (IAM). IAM Identity Center-Benutzer, Gruppen und Benutzeranmeldeinformationen unterscheiden sich von IAM-Benutzern, Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Deaktivieren von Benutzern in IAM finden Sie im Benutzerhandbuch unter IAM-Benutzer [verwalten](#). AWS Identity and Access Management

2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie den Benutzernamen des Benutzers aus, dessen Zugriff Sie deaktivieren möchten.
4. Wählen Sie unter dem Benutzernamen des Benutzers, dessen Zugriff Sie deaktivieren möchten, im Abschnitt Allgemeine Informationen die Option Benutzerzugriff deaktivieren aus.
5. Wählen Sie im Dialogfeld „Benutzerzugriff deaktivieren“ die Option Benutzerzugriff deaktivieren.

Verweigern Sie den Benutzerzugriff mit Service Control-Richtlinien

Um sofort den Zugriff auf autorisierte API-Aufrufe zu verweigern, wenn der Zugriff eines IAM Identity Center-Benutzers deaktiviert oder der Benutzer gelöscht wird, können Sie:

1. [Fügen Sie](#) die [Inline-Richtlinie](#) der dem Benutzer zugewiesenen Berechtigungssätze (oder die IAM-Rollenrichtlinie bei Verwendung des [Account Access Managers](#)) hinzu oder aktualisieren Sie sie, indem Sie einen expliziten Deny Effekt für alle Aktionen auf allen Ressourcen hinzufügen.
2. Geben Sie den `identitystore:user_id` Bedingungsschlüssel `aws:user_id` oder an.

Alternativ können Sie eine [Service Control Policy verwenden](#), um dem Benutzer den Zugriff auf alle Mitgliedskonten in Ihrer Organisation zu verweigern.

Example Beispiel: SCP, um den Zugriff zu verweigern

Diese Ablehnungsrichtlinie blockiert alle AWS Aktionen für einen bestimmten Benutzer, unabhängig von anderen Berechtigungen, die ihm möglicherweise an anderer Stelle gewährt wurden. Diese Richtlinie hat Vorrang vor allen Allow Richtlinien.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

}

Verwaltung des Zugriffs für Benutzer im Identity Center-Verzeichnis

Erfahren Sie, wie Sie Passwörter und die Multifaktor-Authentifizierung (MFA) für Benutzer im IAM Identity Center-Verzeichnis verwalten. Diese Sicherheitsfunktionen tragen zum Schutz von Benutzerkonten bei.

Note

Diese Funktionen gelten nicht für Active Directory-Benutzer oder Benutzer von externen Identitätsanbietern.

Administratoren können sowohl Passwörter als auch MFA über die IAM Identity Center-Konsole verwalten. Diese Sicherheitsfunktionen funktionieren nur mit dem integrierten Identity Center-Verzeichnis.

Verwaltung von Kennwörtern

Die Passwortverwaltung umfasst die folgenden Funktionen:

- Setzen Sie Passwörter mit Anweisungen per E-Mail zurück
- Generieren Sie Einmalpasswörter
- Konfigurieren Sie die automatische E-Mail-Überprüfung für API-created Benutzer

AWS setzt feste Sicherheitsanforderungen durch, einschließlich Komplexitätsregeln und Einschränkungen bei der Wiederverwendung von Passwörtern.

MFA

MFA ist standardmäßig aktiviert und unterstützt bis zu acht Geräte pro Benutzer.

Zu den unterstützten Gerätetypen gehören:

- Authentifikator-Apps
- Sicherheitsschlüssel

- Built-in biometrische Authentifikatoren

Administratoren können MFA-Geräte für Benutzer registrieren und verwalten.

Themen

- [Benutzerpasswörter einrichten](#)
- [MFA für Identity Center-Verzeichnisbenutzer](#)

Benutzerpasswörter einrichten

Für Benutzer, die im Identity Center-Verzeichnis erstellt wurden, können Administratoren Passwortrichtlinien verwalten, Benutzer ohne Anfangspasswörter behandeln und Passwörter bei Bedarf zurücksetzen. Diese Funktionen zur Passwortverwaltung gelten nur für Benutzer im integrierten Identity Center-Verzeichnis. Wenn Sie Active Directory oder einen externen Identitätsanbieter verwenden, müssen Sie die Passwörter in diesen Systemen verwalten.

Optionen zur Passwortverwaltung

- **Passwortanforderungen** — Sicherheitsanforderungen, die Benutzer beim Festlegen oder Ändern von Passwörtern erfüllen müssen. Dazu gehören Komplexitätsregeln und Einschränkungen bei der Wiederverwendung.
- **One-time Passwort-Setup** — Konfigurieren Sie die E-Mail-Verifizierung für Benutzer, die über die API oder CLI erstellt wurden und keine ersten Passwörter haben. Sie können auch temporäre Passwörter für den sofortigen Zugriff generieren.
- **Kennwortrücksetzungen** — Setzen Sie Passwörter für Benutzer zurück, die gesperrt sind oder neue Anmeldeinformationen benötigen. Sie können Anweisungen zum Zurücksetzen per E-Mail senden oder Einmalpasswörter generieren.

Themen

- [Kennwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center](#)
- [Senden Sie Benutzern, die mit API oder CLI erstellt wurden, ein Einmalpasswort per E-Mail](#)
- [Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück](#)

Kennwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center

Note

Diese Anforderungen gelten nur für Benutzer, die im Identity Center-Verzeichnis erstellt wurden. Wenn Sie eine andere Identitätsquelle als IAM Identity Center für die Authentifizierung konfiguriert haben, z. B. [Active Directory](#) einen [externen Identitätsanbieter](#), werden die Passwortrichtlinien für Ihre Benutzer in diesen Systemen definiert und durchgesetzt, nicht in IAM Identity Center. Wenn es sich um Ihre Identitätsquelle handelt AWS Managed Microsoft AD, finden Sie weitere Informationen unter [Passwortrichtlinien verwalten. AWS Managed Microsoft AD](#)

Wenn Sie IAM Identity Center als Identitätsquelle verwenden, müssen Benutzer die folgenden Kennwortanforderungen erfüllen, um ihr Passwort festzulegen oder zu ändern:

- Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.
- Passwörter müssen zwischen 8 und 64 Zeichen lang sein.
- Passwörter müssen mindestens ein Zeichen aus jeder der folgenden vier Kategorien enthalten:
 - Kleinbuchstaben (a – z)
 - Großbuchstaben (A–Z)
 - Zahlen (0 – 9)
 - Non-alphanumeric Zeichen (~! @#\$%^&* _-+=` \ () { } [] ; ' "<> , . ? /)
- Die letzten drei Passwörter können nicht wiederverwendet werden.
- Passwörter, die aufgrund eines von Dritten durchgesickerten Datensatzes öffentlich bekannt sind, können nicht verwendet werden.

Senden Sie Benutzern, die mit API oder CLI erstellt wurden, ein Einmalpasswort per E-Mail

Wenn Sie Benutzer mit der [CreateUser](#) API-Operation oder dem `create-user` CLI-Befehl erstellen, haben die Benutzer keine Passwörter. Sie können die Einstellungen in IAM Identity Center aktualisieren, um diesen Benutzern nach ihrem ersten Anmeldeversuch eine Bestätigungs-E-Mail zu senden, sofern Sie bei der Erstellung eine E-Mail-Adresse für den Benutzer angegeben haben. Nach Erhalt der Bestätigungs-E-Mail muss der Benutzer ein Passwort für die Anmeldung festlegen.

Wenn Sie diese Einstellung nicht aktivieren, müssen Sie ein Einmalkennwort [generieren](#) und es an Benutzer weitergeben, die Sie mit dem CreateUser API- oder create-user CLI-Befehl erstellen.

Um eine E-Mail zur Bestätigung der E-Mail-Adresse an Benutzer zu senden, die mit dem CreateUser API- oder **CLI-Befehl „Create-User“**

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Authentifizierung“.
4. Wählen Sie im Abschnitt Standardauthentifizierung die Option Konfigurieren aus.
5. Aktivieren Sie im Dialogfeld Standardauthentifizierung konfigurieren das Kontrollkästchen E-Mail-OTP senden. Wählen Sie dann Save (Speichern) aus. Der Status wird von Deaktiviert auf Aktiviert aktualisiert.

Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück

Dieses Verfahren richtet sich an Administratoren, die das Passwort für einen Benutzer im IAM Identity Center-Verzeichnis zurücksetzen müssen. Sie verwenden die IAM Identity Center-Konsole, um Passwörter zurückzusetzen.

Überlegungen zu Identitätsanbietern und Benutzertypen

- Microsoft Active Directory oder externer Anbieter — Wenn Sie IAM Identity Center mit Microsoft Active Directory oder einem externen Anbieter verbinden, müssen Benutzerkennwörter innerhalb von Active Directory oder vom externen Anbieter zurückgesetzt werden. Das bedeutet, dass die Passwörter für diese Benutzer nicht von der IAM Identity Center-Konsole aus zurückgesetzt werden können.
- Benutzer im IAM Identity Center-Verzeichnis — Wenn Sie ein IAM Identity Center-Benutzer sind, können Sie Ihr eigenes IAM Identity Center-Passwort zurücksetzen, siehe. [Zurücksetzen Ihres AWS Passwort für den Zugriff auf das Portal](#)

So setzen Sie ein Passwort für einen IAM Identity Center-Endbenutzer zurück

Important

Die Anweisungen auf dieser Seite gelten für [AWS IAM Identity Center](#). Sie gelten nicht für [AWS Identity and Access Management \(IAM\)](#). IAM Identity Center-Benutzer, Gruppen und

Benutzeranmeldeinformationen unterscheiden sich von IAM-Benutzern, Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Ändern von Passwörtern für IAM-Benutzer finden Sie im Benutzerhandbuch unter [Verwalten von Passwörtern für IAM-Benutzer](#). AWS Identity and Access Management

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie den Benutzernamen des Benutzers aus, dessen Passwort Sie zurücksetzen möchten.
4. Wählen Sie auf der Seite mit den Benutzerdetails die Option Passwort zurücksetzen aus.
5. Wählen Sie im Dialogfeld „Passwort zurücksetzen“ eine der folgenden Optionen und wählen Sie dann „Passwort zurücksetzen“ aus:
 - a. Eine E-Mail mit Anweisungen zum Zurücksetzen des Passworts an den Benutzer senden — Diese Option sendet dem Benutzer automatisch eine E-Mail-Adresse von Amazon Web Services, die ihm erklärt, wie er sein Passwort zurücksetzen kann.

 Warning

Stellen Sie aus Sicherheitsgründen sicher, dass die E-Mail-Adresse für diesen Benutzer korrekt ist, bevor Sie diese Option auswählen. Wenn diese E-Mail zum Zurücksetzen des Passworts an eine falsche oder falsch konfigurierte E-Mail-Adresse gesendet wird, könnte ein böswilliger Empfänger sie verwenden, um sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

- b. Generieren Sie ein Einmalkennwort und teilen Sie das Passwort mit dem Benutzer — Mit dieser Option erhalten Sie die Passwortdetails, die Sie manuell von Ihrer E-Mail-Adresse aus an den Benutzer senden können.

MFA für Identity Center-Verzeichnisbenutzer

 Important

MFA in IAM Identity Center wird derzeit nicht für [externe Identitätsanbieter](#) unterstützt.

IAM Identity Center ist vorkonfiguriert und die Multi-Faktor-Authentifizierung (MFA) ist standardmäßig aktiviert, sodass sich alle Benutzer zusätzlich zu ihrem Benutzernamen und Passwort mit MFA anmelden müssen. Dadurch wird sichergestellt, dass sich Benutzer mithilfe der folgenden zwei Faktoren beim AWS Access Portal anmelden müssen:

- Ihr Benutzername und Passwort. Dies ist der erste Faktor und ist etwas, das die Benutzer wissen.
- Entweder ein Code, ein Sicherheitsschlüssel oder Biometrie. Dies ist der zweite Faktor und ist etwas, das Benutzer besitzen (besitzen) oder sind (biometrisch). Der zweite Faktor kann entweder ein von ihrem Mobilgerät generierter Authentifizierungscode, ein mit ihrem Computer verbundener Sicherheitsschlüssel oder ein biometrischer Scan des Benutzers sein.

Zusammen sorgen diese verschiedenen Faktoren für mehr Sicherheit, indem sie unbefugten Zugriff auf Ihre AWS Ressourcen verhindern, es sei denn, eine gültige MFA-Anfrage wurde erfolgreich abgeschlossen.

Jeder Benutzer kann bis zu zwei virtuelle Authentifikator-Apps registrieren, bei denen es sich um Einmalpasswortauthentifizierungsanwendungen handelt, die auf Ihrem Mobilgerät oder Tablet installiert sind, sowie sechs FIDO-Authentifikatoren, die integrierte Authentifikatoren und Sicherheitsschlüssel enthalten, für insgesamt acht MFA-Geräte. Weitere Informationen zu [Verfügbare MFA-Typen für IAM Identity Center](#).

Themen

- [Verfügbare MFA-Typen für IAM Identity Center](#)
- [MFA im IAM Identity Center konfigurieren](#)
- [Registrieren Sie ein MFA-Gerät für Benutzer](#)
- [Umbenennen und Löschen von MFA-Geräten in IAM Identity Center](#)

Verfügbare MFA-Typen für IAM Identity Center

Die Multi-Faktor-Authentifizierung (MFA) ist ein einfacher und effektiver Mechanismus, um die Sicherheit Ihrer Benutzer zu erhöhen. Der erste Faktor eines Benutzers — sein Passwort — ist ein Geheimnis, das er sich merkt, auch Wissensfaktor genannt. Andere Faktoren können Besitzfaktoren (etwas, das Sie besitzen, wie etwa ein Sicherheitsschlüssel) oder Inhärenzfaktoren (etwas, das Sie sind, wie etwa ein biometrischer Scan) sein. Wir empfehlen dringend, MFA zu konfigurieren, um Ihrem Konto eine zusätzliche Sicherheitsebene hinzuzufügen.

IAM Identity Center MFA unterstützt die folgenden Gerätetypen. Alle MFA-Typen werden sowohl für den browserbasierten Konsolenzugriff als auch für die Verwendung der AWS CLI Version v2 mit IAM Identity Center unterstützt.

- [FIDO2 Authentifikatoren](#), einschließlich integrierter Authentifikatoren und Sicherheitsschlüssel
- [Apps für virtuelle Authentifikatoren](#)
- Ihre eigene [RADIUS MFA](#) Implementierung ist verbunden durch AWS Managed Microsoft AD

Ein Benutzer kann bis zu acht MFA-Geräte, darunter bis zu zwei virtuelle Authentifikator-Apps und sechs FIDO-Authentifikatoren, auf einem registrieren lassen. AWS-Konto Sie können die MFA-Einstellungen auch so konfigurieren, dass MFA immer dann erforderlich ist, wenn versucht wird, sich von einem neuen Gerät oder Browser aus anzumelden, oder wenn sie sich von einer unbekannten IP-Adresse aus anmelden. Weitere Informationen zur Konfiguration der MFA-Einstellungen für Ihre Benutzer finden Sie unter [Wählen Sie MFA-Typen für die Benutzerauthentifizierung](#) und [MFA-Gerätedurchsetzung konfigurieren](#).

FIDO2 Authentifikatoren

[FIDO2](#) ist ein Standard, der Kryptografie mit öffentlichen Schlüsseln beinhaltet CTAP2 [WebAuthn](#) und darauf basiert. FIDO-Anmeldeinformationen sind Phishing-resistent, da sie nur für die Website gelten, auf der die Anmeldeinformationen erstellt wurden, z. B. AWS

AWS unterstützt die beiden gängigsten Formfaktoren für FIDO-Authentifikatoren: integrierte Authentifikatoren und Sicherheitsschlüssel. Im Folgenden finden Sie weitere Informationen zu den gängigsten Arten von FIDO-Authentifikatoren.

Themen

- [Integrierte Authentifikatoren](#)
- [Sicherheitsschlüssel](#)
- [Passwort-Manager, Passkey-Anbieter und andere FIDO-Authentifikatoren](#)

Integrierte Authentifikatoren

Viele moderne Computer und Mobiltelefone verfügen über integrierte Authentifikatoren, z. B. TouchID auf einem Macbook oder eine Windows Hello-kompatible Kamera. Wenn Ihr Gerät über einen integrierten FIDO-kompatiblen Authentifikator verfügt, können Sie Ihren Fingerabdruck, Ihr Gesicht oder Ihre Geräte-PIN als zweiten Faktor verwenden.

Sicherheitsschlüssel

Sicherheitsschlüssel sind FIDO-kompatible externe Hardware-Authentifikatoren, die Sie erwerben und über USB, BLE oder NFC mit Ihrem Gerät verbinden können. Wenn Sie zur Eingabe von MFA aufgefordert werden, führen Sie einfach eine Geste mit dem Sensor der Taste aus. Zu den Sicherheitsschlüsseln gehören beispielsweise Feitian-Schlüssel, YubiKeys und mit den gängigsten Sicherheitsschlüsseln werden gerätegebundene FIDO-Anmeldeinformationen erstellt. [Eine Liste aller FIDO-zertifizierten Sicherheitsschlüssel finden Sie unter FIDO-zertifizierte Produkte.](#)

Passwort-Manager, Passkey-Anbieter und andere FIDO-Authentifikatoren

Zahlreiche Drittanbieter unterstützen die FIDO-Authentifizierung in mobilen Anwendungen, z. B. in Passwort-Managern, Smartcards mit FIDO-Modus und anderen Formfaktoren. Diese FIDO-kompatiblen Geräte können mit IAM Identity Center verwendet werden. Wir empfehlen jedoch, dass Sie einen FIDO-Authentifikator selbst testen, bevor Sie diese Option für MFA aktivieren.

Note

Einige FIDO-Authentifikatoren können auffindbare FIDO-Anmeldeinformationen, sogenannte Hauptschlüssel, erstellen. Hauptschlüssel können an das Gerät gebunden sein, das sie erstellt, oder sie können synchronisiert und in einer Cloud gesichert werden. Sie können beispielsweise einen Hauptschlüssel mit der Apple Touch ID auf einem unterstützten Macbook registrieren und sich dann von einem Windows-Laptop aus mithilfe von Google Chrome mit Ihrem Hauptschlüssel in iCloud bei einer Website anmelden, indem Sie bei der Anmeldung den Anweisungen auf dem Bildschirm folgen. Weitere Informationen darüber, welche Geräte synchronisierbare Hauptschlüssel und die aktuelle Passkey-Interoperabilität zwischen Betriebssystemen und Browsern Support, finden Sie unter [Geräteunterstützung](#) auf passkeys.dev, einer Ressource, die vom FIDO Alliance And World Wide Web Consortium (W3C) verwaltet wird.

Apps für virtuelle Authentifikatoren

Bei Authenticator-Apps handelt es sich im Wesentlichen um Authentifikatoren von Drittanbietern, die auf Einmalkennwörtern (OTP) basieren. Sie können eine auf Ihrem Mobilgerät oder Tablet installierte Authentifizierungsanwendung als autorisiertes MFA-Gerät verwenden. Die Authentifizierungs-App eines Drittanbieters muss mit RFC 6238 konform sein. Dabei handelt es sich um einen standardbasierten Algorithmus für zeitgesteuerte Einmalpasswörter (TOTP), der sechsstellige Authentifizierungs-codes erzeugen kann.

Wenn Benutzer zur Eingabe von MFA aufgefordert werden, müssen sie einen gültigen Code aus ihrer Authenticator-App in das angezeigte Eingabefeld eingeben. Jedes MFA-Gerät, das einem Benutzer zugeordnet ist, muss eindeutig sein. Für jeden Benutzer können zwei Authentifizierungs-Apps registriert werden.

Getestete Authenticator-Apps

Jede TOTP-konforme Anwendung funktioniert mit IAM Identity Center MFA. In der folgenden Tabelle sind bekannte Authentifikator-Apps von Drittanbietern aufgeführt, aus denen Sie wählen können.

Betriebssystem	Getestete Authentifizierungs-App
Android	Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator
iOS	Authy , Duo Mobile , Microsoft Authenticator , Google Authenticator

RADIUS MFA

Der [Remote Authentication Dial-In User Service \(RADIUS\)](#) ist ein branchenübliches Client-Server-Protokoll, das Authentifizierung, Autorisierung und Kontoverwaltung ermöglicht, sodass Benutzer eine Verbindung zu Netzwerkdiensten herstellen können. Directory Service beinhaltet einen RADIUS-Client, der eine Verbindung zu dem RADIUS-Server herstellt, auf dem Sie Ihre MFA-Lösung implementiert haben. Weitere Informationen finden Sie unter [Aktivieren der Multi-Faktor-Authentifizierung für](#). AWS Managed Microsoft AD

Sie können entweder RADIUS MFA oder MFA in IAM Identity Center für Benutzeranmeldungen am Benutzerportal verwenden, aber nicht beide. MFA in IAM Identity Center ist eine Alternative zu RADIUS MFA in Fällen, in denen Sie eine AWS native Zwei-Faktor-Authentifizierung für den Zugriff auf das Portal wünschen.

Wenn Sie MFA in IAM Identity Center aktivieren, benötigen Ihre Benutzer ein MFA-Gerät, um sich beim Access Portal anzumelden. AWS Wenn Sie zuvor RADIUS MFA verwendet haben, überschreibt die Aktivierung von MFA in IAM Identity Center RADIUS MFA für Benutzer, die sich beim Access Portal anmelden. AWS RADIUS MFA stellt Benutzer jedoch weiterhin vor Herausforderungen, wenn sie sich bei allen anderen Anwendungen anmelden, die damit arbeiten Directory Service, z. B. Amazon RDS for SQL Server.

Wenn Ihr MFA auf der IAM Identity Center-Konsole deaktiviert ist und Sie RADIUS MFA mit konfiguriert haben Directory Service, regelt AWS RADIUS MFA die Anmeldung am Access Portal. Das bedeutet, dass IAM Identity Center auf die RADIUS-MFA-Konfiguration zurückgreift, wenn MFA deaktiviert ist.

MFA im IAM Identity Center konfigurieren

Sie können Multi-Faktor-Authentifizierungsfunktionen (MFA) in IAM Identity Center konfigurieren, wenn Ihre Identitätsquelle mit dem Identitätsspeicher oder AD Connector von IAM Identity Center konfiguriert ist. AWS Managed Microsoft AD MFA in IAM Identity Center wird derzeit nicht für [externe Identitätsanbieter](#) unterstützt.

Im Folgenden finden Sie allgemeine MFA-Empfehlungen, die von Ihren IAM Identity Center-Einstellungen und Unternehmenspräferenzen abhängen.

- Benutzern wird empfohlen, mehrere Backup-Authentifikatoren für alle aktivierten MFA-Typen zu registrieren. Diese Vorgehensweise kann verhindern, dass der Zugriff verloren geht, falls ein MFA-Gerät defekt oder falsch platziert ist.
- Wählen Sie nicht die Option Per E-Mail zugesandtes Einmalpasswort verlangen, wenn sich Ihre Benutzer beim AWS Zugriffsportal anmelden müssen, um auf ihre E-Mails zuzugreifen. Beispielsweise könnten Ihre Benutzer das AWS Access Portal verwendenMicrosoft 365, um ihre E-Mails zu lesen. In diesem Fall können Benutzer den Bestätigungscode nicht abrufen und sich auch nicht beim AWS Access Portal anmelden. Weitere Informationen finden Sie unter [MFA-Gerätedurchsetzung konfigurieren](#).
- Wenn Sie bereits RADIUS MFA verwenden, mit dem Sie konfiguriert haben Directory Service, müssen Sie MFA nicht in IAM Identity Center aktivieren. MFA in IAM Identity Center ist eine Alternative zu RADIUS MFA für Microsoft Active Directory Benutzer von IAM Identity Center. Weitere Informationen finden Sie unter [RADIUS MFA](#).
- Das folgende YouTube Video bietet einen Überblick über MFA und IAM Identity Center:

[IAM Identity Center: Standardwerte für die Multi-Faktor-Authentifizierung für neue Instanzen](#)

Themen

- [Benutzer zur MFA auffordern](#)
- [Wählen Sie MFA-Typen für die Benutzerauthentifizierung](#)
- [MFA-Gerätedurchsetzung konfigurieren](#)
- [Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren](#)

Benutzer zur MFA auffordern

Mithilfe der folgenden Schritte können Sie festlegen, wie oft Workforce-Benutzer bei jedem Versuch, sich am Access Portal anzumelden, zur Multi-Faktor-Authentifizierung (MFA) aufgefordert werden. AWS Bevor Sie beginnen, empfehlen wir Ihnen, das zu verstehen. [Verfügbare MFA-Typen für IAM Identity Center](#)

Important

Die Anweisungen in diesem Abschnitt gelten für [AWS IAM Identity Center](#). Sie gelten nicht für [AWS Identity and Access Management](#) (IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zur Deaktivierung von MFA für IAM-Benutzer finden Sie im Benutzerhandbuch unter [Deaktivierung von MFA-Geräten](#). AWS Identity and Access Management

Note

Wenn Sie einen externen IdP verwenden, ist der Bereich Multi-Faktor-Authentifizierung nicht verfügbar. Ihr externer IdP verwaltet die MFA-Einstellungen, anstatt sie von IAM Identity Center verwaltet zu werden.

So konfigurieren Sie MFA

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Benutzer zur MFA auffordern je nach Sicherheitsstufe, die Ihr Unternehmen benötigt, einen der folgenden Authentifizierungsmodi aus:
 - Jedes Mal, wenn sie sich anmelden (immer aktiv)

In diesem Modus (Standardeinstellung) verlangt IAM Identity Center, dass Benutzer mit einem registrierten MFA-Gerät bei jeder Anmeldung dazu aufgefordert werden. Dies ist die

sicherste Einstellung und stellt sicher, dass Ihre Organisations- oder Compliance-Richtlinien durchgesetzt werden, indem vorgeschrieben wird, dass MFA bei jeder Anmeldung am AWS Access Portal verwendet wird. PCI DSS empfiehlt beispielsweise nachdrücklich, bei jeder Anmeldung MFA zu verwenden, um auf Anwendungen zuzugreifen, die Zahlungsvorgänge mit hohem Risiko unterstützen.

- Nur wenn sich ihr Anmeldekontext ändert (kontextsensitiv)

In diesem Modus bietet IAM Identity Center Benutzern die Möglichkeit, ihrem Gerät bei der Anmeldung zu vertrauen. Nachdem ein Benutzer angegeben hat, dass er einem Gerät vertrauen möchte, fordert IAM Identity Center den Benutzer einmal zur Eingabe von MFA auf und analysiert den Anmeldekontext (wie Gerät, Browser und Standort) für die nachfolgenden Anmeldungen des Benutzers. Bei nachfolgenden Anmeldungen ermittelt IAM Identity Center, ob sich der Benutzer mit einem zuvor vertrauenswürdigen Kontext anmeldet. Wenn sich der Anmeldekontext des Benutzers ändert, fordert IAM Identity Center den Benutzer zusätzlich zu seiner E-Mail-Adresse und seinen Kennwortanmeldeinformationen zur Eingabe von MFA auf.

Dieser Modus bietet Benutzern, die sich häufig von ihrem Arbeitsplatz aus anmelden, eine einfache Bedienung, ist jedoch weniger sicher als die Always-On-Option. Benutzer werden nur dann zur Eingabe von MFA aufgefordert, wenn sich ihr Anmeldekontext ändert.

- Niemals (deaktiviert)

In diesem Modus melden sich alle Benutzer nur mit ihrem Standardbenutzernamen und Passwort an. Die Auswahl dieser Option deaktiviert IAM Identity Center MFA und wird nicht empfohlen.

MFA ist zwar für Ihr Identity Center-Verzeichnis für Benutzer deaktiviert, aber Sie können MFA-Geräte nicht in ihren Benutzerdetails verwalten, und Identity Center-Verzeichnisbenutzer können MFA-Geräte nicht über das AWS Zugriffsportal verwalten.

Note

Wenn Sie RADIUS MFA bereits mit verwenden und es weiterhin als Standard-MFA-Typ verwenden möchten Directory Service, können Sie den Authentifizierungsmodus deaktiviert lassen, um die MFA-Funktionen in IAM Identity Center zu umgehen. Wenn Sie vom deaktivierten Modus in den kontextsensitiven oder Always-On-Modus wechseln, werden die vorhandenen RADIUS-MFA-Einstellungen außer Kraft gesetzt. Weitere Informationen finden Sie unter [RADIUS MFA](#).

6. Wählen Sie Änderungen speichern aus.

Verwandte Themen

- [Wählen Sie MFA-Typen für die Benutzerauthentifizierung](#)
- [MFA-Gerätedurchsetzung konfigurieren](#)
- [Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren](#)

Wählen Sie MFA-Typen für die Benutzerauthentifizierung

Gehen Sie wie folgt vor, um die Gerätetypen auszuwählen, mit denen sich Ihre Benutzer authentifizieren können, wenn sie im Access Portal zur Multi-Faktor-Authentifizierung (MFA) aufgefordert werden. AWS

So konfigurieren Sie MFA-Typen für Ihre Benutzer

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Benutzer können sich mit diesen MFA-Typen authentifizieren je nach Ihren Geschäftsanforderungen einen der folgenden MFA-Typen aus. Weitere Informationen finden Sie unter [Verfügbare MFA-Typen für IAM Identity Center](#).
 - Sicherheitsschlüssel und integrierte Authentifikatoren
 - Authenticator-Apps
6. Wählen Sie Änderungen speichern aus.

MFA-Gerätedurchsetzung konfigurieren

Gehen Sie wie folgt vor, um zu ermitteln, ob Ihre Benutzer bei der Anmeldung am AWS Access Portal über ein registriertes MFA-Gerät verfügen müssen.

Weitere Informationen zu MFA in IAM finden Sie unter [AWS Multi-Faktor-Authentifizierung](#) in IAM.

So konfigurieren Sie die MFA-Gerätedurchsetzung für Ihre Benutzer

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Falls ein Benutzer noch kein registriertes MFA-Gerät besitzt, je nach Ihren Geschäftsanforderungen eine der folgenden Optionen aus:

- Fordere sie auf, bei der Anmeldung ein MFA-Gerät zu registrieren

Dies ist die Standardeinstellung, wenn Sie MFA für IAM Identity Center zum ersten Mal konfigurieren. Verwenden Sie diese Option, wenn Sie festlegen möchten, dass Benutzer, die noch kein registriertes MFA-Gerät haben, ein Gerät bei der Anmeldung nach erfolgreicher Passwortauthentifizierung selbst registrieren müssen. Auf diese Weise können Sie die AWS Umgebungen Ihres Unternehmens mit MFA schützen, ohne Authentifizierungsgeräte einzeln registrieren und an Ihre Benutzer verteilen zu müssen. Während der Selbstregistrierung können Ihre Benutzer jedes Gerät aus den verfügbaren [Verfügbare MFA-Typen für IAM Identity Center](#) Geräten registrieren, die Sie zuvor aktiviert haben. Nach Abschluss der Registrierung haben Benutzer die Möglichkeit, ihrem neu registrierten MFA-Gerät einen benutzerfreundlichen Namen zu geben. Danach leitet IAM Identity Center den Benutzer zu seinem ursprünglichen Ziel weiter. Wenn das Gerät des Benutzers verloren geht oder gestohlen wird, können Sie dieses Gerät einfach aus seinem Konto entfernen. IAM Identity Center fordert ihn dann auf, ein neues Gerät bei der nächsten Anmeldung selbst zu registrieren.

- Fordere sie auf, ein Einmalpasswort einzugeben, das per E-Mail gesendet wurde, um sich anzumelden

Verwenden Sie diese Option, wenn Sie Benutzern Bestätigungs_codes per E-Mail zusenden möchten. Da E-Mails nicht an ein bestimmtes Gerät gebunden sind, erfüllt diese Option nicht die Anforderungen für die branchenübliche Multi-Faktor-Authentifizierung. Sie verbessert jedoch die Sicherheit gegenüber der alleinigen Verwendung eines Kennworts. Eine E-Mail-Bestätigung wird nur angefordert, wenn ein Benutzer kein MFA-Gerät registriert hat. Wenn die kontextsensitive Authentifizierungsmethode aktiviert wurde, hat der Benutzer die Möglichkeit, das Gerät, auf dem er die E-Mail erhält, als vertrauenswürdig zu markieren. Danach müssen

sie bei future Anmeldungen von dieser Kombination aus Gerät, Browser und IP-Adresse keinen E-Mail-Code mehr verifizieren.

 Note

Wenn Sie Active Directory als Ihre IAM Identity Center-fähige Identitätsquelle verwenden, basiert die E-Mail-Adresse immer auf dem Active Directory-Attribut. `email`. Durch benutzerdefinierte Active Directory-Attributzuordnungen wird dieses Verhalten nicht außer Kraft gesetzt.

- Blockieren Sie ihre Anmeldung

Verwenden Sie die Option „Ihre Anmeldung blockieren“, wenn Sie die Verwendung von MFA durch alle Benutzer erzwingen möchten, bevor sie sich anmelden können. AWS

 Important

Wenn Ihre Authentifizierungsmethode auf Kontextsensitiv eingestellt ist, kann ein Benutzer auf der Anmeldeseite das Kontrollkästchen Dies ist ein vertrauenswürdiges Gerät aktivieren. In diesem Fall wird dieser Benutzer nicht zur Eingabe von MFA aufgefordert, auch wenn Sie die Einstellung Anmeldung blockieren aktiviert haben. Wenn Sie möchten, dass diese Benutzer dazu aufgefordert werden, ändern Sie Ihre Authentifizierungsmethode auf Immer aktiviert.

- Erlauben Sie ihnen, sich anzumelden

Verwenden Sie diese Option, um anzugeben, dass keine MFA-Geräte erforderlich sind, damit sich Ihre Benutzer beim AWS Access Portal anmelden können. Benutzer, die sich für die Registrierung von MFA-Geräten entschieden haben, werden weiterhin zur Eingabe von MFA aufgefordert.

6. Wählen Sie Änderungen speichern aus.

Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren

IAM Identity Center-Administratoren können Benutzern ermöglichen, ihre eigenen MFA-Geräte selbst zu registrieren.

Um Benutzern die Registrierung ihrer eigenen MFA-Geräte zu ermöglichen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung aus.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Wer kann MFA-Geräte verwalten die Option Benutzer können ihre eigenen MFA-Geräte hinzufügen und verwalten aus.
6. Wählen Sie Änderungen speichern aus.

 Note

Nachdem Sie die Selbstregistrierung für Ihre Benutzer eingerichtet haben, möchten Sie ihnen möglicherweise einen Link zum Verfahren senden. [Registrieren Sie Ihr Gerät für MFA](#) Dieses Thema enthält Anweisungen zum Einrichten ihrer eigenen MFA-Geräte.

Registrieren Sie ein MFA-Gerät für Benutzer

IAM Identity Center-Administratoren können in der IAM Identity Center-Konsole ein neues MFA-Gerät für den Zugriff durch einen bestimmten Benutzer einrichten. Administratoren müssen physischen Zugriff auf das MFA-Gerät des Benutzers haben, um es registrieren zu können. Wenn Sie beispielsweise MFA für einen Benutzer konfigurieren, der ein MFA-Gerät verwendet, das auf einem Smartphone ausgeführt wird, benötigen Sie physischen Zugriff auf das Smartphone, um den Registrierungsprozess abzuschließen. Alternativ können Sie Benutzern ermöglichen, ihre eigenen MFA-Geräte zu konfigurieren und zu verwalten. Weitere Informationen finden Sie unter [Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren](#).

Um ein MFA-Gerät zu registrieren

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie einen Benutzer in der Liste aus. Markieren Sie für diesen Schritt nicht das Kontrollkästchen neben dem Benutzer.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte und dann MFA-Gerät registrieren aus.

4. Wählen Sie auf der Seite MFA-Gerät registrieren einen der folgenden MFA-Gerätetypen aus und folgen Sie den Anweisungen:

- Authenticator-App

1. Auf der Seite Authentifikator-App einrichten zeigt IAM Identity Center Konfigurationsinformationen für das neue MFA-Gerät an, einschließlich einer QR-Code-Grafik. Die Grafik ist eine Darstellung des geheimen Schlüssels, der für die manuelle Eingabe auf Geräten verfügbar ist, die QR-Codes nicht unterstützen.
2. Gehen Sie mit dem physischen MFA-Gerät wie folgt vor:
 - a. Öffnen Sie eine kompatible MFA-Authenticator-App. Eine Liste der getesteten Apps, die Sie mit MFA-Geräten verwenden können, finden Sie unter [Apps für virtuelle Authentifikatoren](#). Wenn die MFA-App mehrere Konten (mehrere MFA-Geräte) unterstützt, wählen Sie die Option zum Erstellen eines neuen Kontos (ein neues MFA-Gerät).
 - b. Stellen Sie fest, ob die MFA-App QR-Codes unterstützt, und führen Sie dann auf der Seite Authenticator-App einrichten einen der folgenden Schritte aus:
 - i. Wählen Sie Show QR code (QR-Code anzeigen) und verwenden Sie anschließend die App, um den QR-Code zu scannen. Sie können beispielsweise das Kamerasymbol oder eine ähnliche Option wie Scan code (Code scannen) auswählen. Verwenden Sie anschließend die Kamera des Geräts, um den Code zu scannen.
 - ii. Wählen Sie Geheimen Schlüssel anzeigen und geben Sie dann diesen geheimen Schlüssel in Ihre MFA-App ein.

 Important

Wenn Sie ein MFA-Gerät für IAM Identity Center konfigurieren, empfehlen wir Ihnen, eine Kopie des QR-Codes oder geheimen Schlüssels an einem sicheren Ort aufzubewahren. Dies kann hilfreich sein, wenn der zugewiesene Benutzer das Telefon verliert oder die MFA-Authenticator-App neu installieren muss. Wenn eines dieser Dinge eintritt, können Sie die App schnell neu konfigurieren, um dieselbe MFA-Konfiguration zu verwenden. Dadurch entfällt die Notwendigkeit, ein neues MFA-Gerät in IAM Identity Center für den Benutzer zu erstellen.

3. Geben Sie auf der Seite Authenticator-App einrichten unter Authenticator-Code das Einmalpasswort ein, das derzeit auf dem physischen MFA-Gerät angezeigt wird.

 Important

Senden Sie die Anforderung direkt nach der Erzeugung der Codes. Wenn Sie den Code generieren und dann zu lange warten, um die Anfrage einzureichen, wurde das MFA-Gerät erfolgreich mit dem Benutzer verknüpft. Das MFA-Gerät ist jedoch nicht synchron. Dies liegt daran, weil die zeitgesteuerten Einmalpasswörter (TOTP) nach einer kurzen Zeit ungültig werden. In diesem Fall können Sie das Gerät neu synchronisieren.

4. Klicken Sie auf Assign MFA (MFA zuordnen). Das MFA-Gerät kann jetzt mit der Generierung von Einmalkennwörtern beginnen und ist jetzt für die Verwendung mit AWS bereit.

- Sicherheitsschlüssel

1. Folgen Sie auf der Seite Sicherheitsschlüssel Ihres Benutzers registrieren den Anweisungen Ihres Browsers oder Ihrer Plattform.

 Note

Die Benutzererfahrung ist je nach Betriebssystem und Browser unterschiedlich. Folgen Sie daher bitte den Anweisungen Ihres Browsers oder Ihrer Plattform. Nachdem das Gerät Ihres Benutzers erfolgreich registriert wurde, haben Sie die Möglichkeit, dem neu registrierten Gerät Ihres Benutzers einen benutzerfreundlichen Anzeigenamen zuzuweisen. Wenn Sie dies ändern möchten, wählen Sie Umbenennen, geben Sie den neuen Namen ein und wählen Sie dann Speichern. Wenn Sie die Option aktiviert haben, dass Benutzer ihre eigenen Geräte verwalten können, wird dem Benutzer dieser benutzerfreundliche Name im AWS Zugriffsportal angezeigt.

Umbenennen und Löschen von MFA-Geräten in IAM Identity Center

IAM Identity Center-Administratoren können die folgenden Verfahren verwenden, um das MFA-Gerät eines Benutzers umzubenennen oder zu löschen.

Um ein MFA-Gerät umzubenennen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie den Benutzer in der Liste aus. Markieren Sie für diesen Schritt nicht das Kontrollkästchen neben dem Benutzer.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte, wählen Sie das Gerät aus und klicken Sie dann auf Umbenennen.
4. Wenn Sie dazu aufgefordert werden, geben Sie den neuen Namen ein und wählen Sie dann Umbenennen.

So löschen Sie ein MFA-Gerät

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie den Benutzer in der Liste aus.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte, wählen Sie das Gerät aus und klicken Sie dann auf Löschen.
4. Geben Sie zur Bestätigung DELETE ein und wählen Sie dann Löschen.

Zugriff auf Anwendungen konfigurieren

Mit können Sie steuern AWS IAM Identity Center, wer Single Sign-On auf Ihre Anwendungen zugreifen kann. Benutzer erhalten nahtlosen Zugriff auf diese Anwendungen, nachdem sie sich mit ihren Verzeichnisanmeldeinformationen angemeldet haben.

IAM Identity Center kommuniziert sicher mit diesen Anwendungen über eine vertrauenswürdige Beziehung zwischen IAM Identity Center und dem Dienstanbieter der Anwendung. Diese Vertrauensstellung kann je nach Anwendungstyp auf unterschiedliche Weise hergestellt werden.

IAM Identity Center unterstützt zwei Anwendungstypen: [AWS verwaltete Anwendungen](#) und vom [Kunden verwaltete Anwendungen](#). AWS verwaltete Anwendungen werden direkt von den jeweiligen Anwendungskonsolen aus oder über die Anwendungs-APIs konfiguriert. Vom Kunden verwaltete Anwendungen müssen der IAM Identity Center-Konsole hinzugefügt und mit den entsprechenden Metadaten sowohl für IAM Identity Center als auch für den Dienstanbieter konfiguriert werden.

Nachdem Sie Anwendungen für die Verwendung mit IAM Identity Center konfiguriert haben, können Sie verwalten, welche Benutzer oder Gruppen auf die Anwendungen zugreifen. Standardmäßig sind Anwendungen keine Benutzer zugewiesen.

Sie können Ihren Mitarbeitern auch Zugriff auf das Formular gewähren, das AWS-Managementkonsole AWS-Konto in Ihrer Organisation spezifisch ist. Weitere Informationen finden Sie unter [Konfigurieren Sie den Zugriff auf AWS-Konten](#).

Themen

- [AWS verwaltete Anwendungen](#)
- [Vom Kunden verwaltete Anwendungen](#)
- [Überblick über die Verbreitung vertrauenswürdiger Identitäten](#)
- [Richten Sie Ihre eigene OAuth 2.0-Anwendung ein](#)
- [IAM Identity Center-Zertifikate rotieren](#)
- [Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut](#)
- [Weisen Sie den Benutzerzugriff auf Anwendungen in der IAM Identity Center-Konsole zu](#)
- [Entfernen Sie den Benutzerzugriff auf SAML 2.0-Anwendungen](#)
- [Ordnen Sie Attribute in Ihrer Anwendung den IAM Identity Center-Attributen zu](#)

AWS verwaltete Anwendungen

AWS IAM Identity Center optimiert und vereinfacht die Aufgabe, die Benutzer Ihrer Belegschaft mit AWS verwalteten Anwendungen wie Kiro und Amazon Quick zu verbinden. Mit IAM Identity Center können Sie Ihren bestehenden Identitätsanbieter einmal verbinden und Benutzer und Gruppen aus Ihrem Verzeichnis synchronisieren oder Ihre Benutzer direkt in IAM Identity Center erstellen und verwalten. Da IAM Identity Center einen Verbund bietet, entfällt die Notwendigkeit, einen Verbund oder die Benutzer- und Gruppensynchronisierung für jede Anwendung einzurichten, und reduziert Ihren Verwaltungsaufwand. Außerdem erhalten Sie eine gemeinsame [Ansicht der Benutzer- und Gruppenzuweisungen](#).

Eine Tabelle der AWS Anwendungen, die mit IAM Identity Center funktionieren, finden Sie unter [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#).

Steuerung des Zugriffs auf AWS verwaltete Anwendungen

Der Zugriff auf AWS verwaltete Anwendungen wird auf zwei Arten gesteuert:

- Erster Zugriff auf die Anwendung

IAM Identity Center verwaltet dies durch Zuweisungen an die Anwendung. Standardmäßig sind Zuweisungen für AWS verwaltete Anwendungen erforderlich. Wenn Sie ein Anwendungsadministrator sind, können Sie wählen, ob Zuweisungen für eine Anwendung erforderlich sind.

Falls Zuweisungen erforderlich sind, können nur Benutzer AWS-Zugangsportal, die der Anwendung direkt oder über eine Gruppenzuweisung zugewiesen sind, die Anwendungskachel sehen, wenn sich Benutzer bei der anmelden.

Wenn Zuweisungen nicht erforderlich sind, können Sie allen IAM Identity Center-Benutzern den Zugriff auf die Anwendung ermöglichen. In diesem Fall verwaltet die Anwendung den Zugriff auf Ressourcen und die Anwendungskachel ist für alle Benutzer sichtbar, die die AWS-Zugangsportal besuchen.

Important

Wenn Sie ein IAM Identity Center-Administrator sind, können Sie die IAM Identity Center-Konsole verwenden, um Zuweisungen zu AWS verwalteten Anwendungen zu entfernen. Bevor Sie Zuweisungen entfernen, empfehlen wir Ihnen, sich mit

dem Anwendungsadministrator abzustimmen. Sie sollten sich auch mit dem Anwendungsadministrator abstimmen, wenn Sie die Einstellung ändern möchten, die bestimmt, ob Zuweisungen erforderlich sind, oder Anwendungszuweisungen automatisieren möchten.

- Zugriff auf Anwendungsressourcen

Die Anwendung verwaltet dies durch unabhängige Ressourcenzuweisungen, die sie kontrolliert.

AWS verwaltete Anwendungen bieten eine administrative Benutzeroberfläche, mit der Sie den Zugriff auf Anwendungsressourcen verwalten können. Beispielsweise können Schnelladministratoren Benutzern auf der Grundlage ihrer Gruppenmitgliedschaft den Zugriff auf Dashboards zuweisen. Die meisten AWS verwalteten Anwendungen bieten auch AWS-Managementkonsole eine Oberfläche, mit der Sie der Anwendung Benutzer zuweisen können. Die Konsolenumgebung für diese Anwendungen könnte beide Funktionen integrieren, um Funktionen zur Benutzerzuweisung mit der Möglichkeit zu kombinieren, den Zugriff auf Anwendungsressourcen zu verwalten.

Weitergabe von Identitätsinformationen

Überlegungen zum Teilen von Identitätsinformationen in AWS-Konten

IAM Identity Center unterstützt die am häufigsten verwendeten Attribute in allen Anwendungen. Zu diesen Attributen gehören Vor- und Nachname, Telefonnummer, E-Mail-Adresse, Adresse und bevorzugte Sprache. Überlegen Sie sorgfältig, welche Anwendungen und welche Konten diese personenbezogenen Daten verwenden können.

Sie können den Zugriff auf diese Informationen auf eine der folgenden Arten kontrollieren:

- Sie können wählen, ob Sie den Zugriff nur für das AWS Organizations Verwaltungskonto oder für alle Konten in aktivieren möchten AWS Organizations.
- Alternativ können Sie Service Control Policies (SCPs) verwenden, um zu steuern, welche Anwendungen auf die Informationen in welchen Konten zugreifen können. AWS Organizations

Wenn Sie beispielsweise den Zugriff nur im AWS Organizations Verwaltungskonto aktivieren, haben Anwendungen in Mitgliedskonten keinen Zugriff auf die Informationen. Wenn Sie den Zugriff jedoch für alle Konten aktivieren, können Sie SCPs verwenden, um allen Anwendungen den Zugriff zu verbieten, mit Ausnahme der Anwendungen, die Sie zulassen möchten.

Richtlinien zur Dienstkontrolle sind eine Funktion von. AWS Organizations Anweisungen zum Anhängen eines SCP finden Sie im Benutzerhandbuch unter [Anhängen und Trennen von Service Control-Richtlinien](#). AWS Organizations

Konfiguration von IAM Identity Center für die gemeinsame Nutzung von Identitätsinformationen

IAM Identity Center bietet einen Identitätsspeicher, der Benutzer- und Gruppenattribute mit Ausnahme der Anmeldeinformationen enthält. Sie können eine der folgenden Methoden verwenden, um die Benutzer und Gruppen in Ihrem IAM Identity Center-Identitätsspeicher auf dem neuesten Stand zu halten:

- Verwenden Sie den IAM Identity Center-Identitätsspeicher als Ihre Hauptidentitätsquelle. Wenn Sie diese Methode wählen, verwalten Sie Ihre Benutzer, ihre Anmeldeinformationen und Gruppen in der IAM Identity Center-Konsole oder AWS Command Line Interface (AWS CLI). Weitere Informationen finden Sie unter [Benutzer im Identity Center-Verzeichnis verwalten](#).
- Richten Sie die Bereitstellung (Synchronisation) von Benutzern und Gruppen aus einer der folgenden Identitätsquellen für Ihren IAM Identity Center-Identitätsspeicher ein:
 - Active Directory — Weitere Informationen finden Sie unter [Microsoft AD directory](#)
 - Externer Identitätsanbieter — Weitere Informationen finden Sie unter [Externe Identitätsanbieter](#).

Wenn Sie sich für diese Bereitstellungsmethode entscheiden, verwalten Sie Ihre Benutzer und Gruppen weiterhin von Ihrer Identitätsquelle aus, und diese Änderungen werden mit dem IAM Identity Center-Identitätsspeicher synchronisiert.

Für welche Identitätsquelle Sie sich auch entscheiden, IAM Identity Center kann die Benutzer- und Gruppeninformationen mit verwalteten Anwendungen teilen. AWS Auf diese Weise können Sie eine Identitätsquelle einmal mit IAM Identity Center verbinden und dann Identitätsinformationen mit mehreren Anwendungen in der teilen. AWS Cloud Dadurch entfällt die Notwendigkeit, für jede Anwendung unabhängig voneinander den Verbund und die Identitätsbereitstellung einzurichten. Diese Freigabefunktion macht es auch einfach, Ihren Benutzern Zugriff auf viele Anwendungen in verschiedenen AWS-Konten Bereichen zu gewähren.

Einschränkung der Verwendung von AWS verwaltete Anwendungen

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es als Identitätsquelle für AWS verwaltete Anwendungen auf allen Konten in Ihrem AWS Organizations Konto verfügbar. Um

Anwendungen einzuschränken, müssen Sie Service Control Policies (SCPs) implementieren. SCPs sind eine Funktion, mit der Sie AWS Organizations die maximale Anzahl von Berechtigungen, die Identitäten (Benutzer und Rollen) in Ihrer Organisation haben können, zentral steuern können. Sie können SCPs verwenden, um den Zugriff auf die Benutzer- und Gruppeninformationen des IAM Identity Center zu blockieren und zu verhindern, dass die Anwendung gestartet wird, außer in bestimmten Konten. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien \(SCPs\)](#) im AWS Organizations -Benutzerhandbuch.

Das folgende SCP-Beispiel blockiert den Zugriff auf die Benutzer- und Gruppeninformationen des IAM Identity Center und verhindert, dass die Anwendung gestartet wird, außer in den angegebenen Konten (111111111111 und 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können

Mit IAM Identity Center können Sie Ihre bestehende Identitätsquelle verbinden oder Benutzer einmal erstellen. Auf diese Weise können Anwendungsadministratoren den Zugriff auf die folgenden AWS verwalteten Anwendungen ohne separaten Verbund oder Benutzer- und Gruppensynchronisierung verwalten.

AWS verwaltete Anwendungen, die in IAM Identity Center integriert sind

Alle AWS verwalteten Anwendungen in der folgenden Tabelle lassen sich in [Organisationsinstanzen von IAM Identity Center integrieren](#). Die Tabelle enthält auch Informationen zu den folgenden Punkten für eine unterstützte AWS verwaltete Anwendung:

- Ob die Anwendung auch in Kontoinstanzen von IAM Identity Center integriert ist
- Ob die Anwendung die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center ermöglichen kann
- Ob die Anwendung IAM Identity Center unterstützt, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist
- Ob die Anwendung die Bereitstellung in weiteren Regionen von IAM Identity Center unterstützt

Note

Anwendungen, die die Bereitstellung in weiteren Regionen von IAM Identity Center unterstützen, unterstützen auch IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Jede hier aufgeführte AWS verwaltete Anwendung unterstützt die Bereitstellung in der Hauptregion. Weitere Informationen finden Sie unter [the section called “Bereitstellung und Verwaltung AWS verwalteter Anwendungen auf mehreren AWS-Regionen”](#).

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist	Unterstützt die Bereitstellung in weiteren Regionen von IAM Identity Center
Amazon Athena SQL	Ja	Ja	Ja	Ja
Amazonas CodeCatalyst	Ja	Nein	Ja	Nein

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist	Unterstützt die Bereitstellung in weiteren Regionen von IAM Identity Center
Amazonas DataZone	Ja	Ja	Ja	Nein
Funktionen von Amazon EKS	Ja	Ja	Ja	Nein
Amazon EMR in EC2	Ja	Ja	Ja	Ja
Amazon EMR in EKS	Ja	Ja	Ja	Ja
Amazon EMR Serverless	Ja	Ja	Ja	Ja
Amazon EMR Studio	Ja	Ja	Ja	Ja
Amazon Kendra	Nein	Nein	Ja	Nein
Amazon Managed Grafana	Nein	Nein	Ja	Nein
Amazon Monitron	Nein	Nein	Ja	Nein
OpenSearch Amazon-Dienst	Ja	Ja	Ja	Nein
OpenSearch Amazon-Dienst Serverless Service	Ja	Ja	Ja	Nein
Amazon Q Business	Ja	Ja	Ja	Nein
Amazon Quick	Ja	Ja	Ja	Nein
Amazon Redshift	Ja ²	Ja	Ja	Ja

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdigere Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist	Unterstützt die Bereitstellung in weiteren Regionen von IAM Identity Center
Amazon S3 Access Grants	Ja	Ja	Ja	Ja
Amazon SageMaker Studio	Nein	Ja	Ja	Nein
Amazon SageMaker Unified Studio	Ja	Ja	Ja	Ja
Amazon WorkMail	Ja	Ja	Ja	Nein
Amazonas WorkSpaces	Ja	Nein	Ja	Nein
Amazon WorkSpaces Secure Browser	Nein	Nein	Ja	Nein
AWS Kontozugriff (Kontozugriffsmanager)	Nein	Ja	Ja	Nr. ³
AWS App Studio	Ja	Nein	Nein	Nein
AWS Deadline Cloud	Ja	Nein	Ja	Ja
AWS DevOps Agent	Ja	Ja	Ja	Ja
AWS Glue	Ja	Ja	Ja	Ja
AWS IoT Events	Nein	Nein	Nein	Nein
AWS IoT SiteWise	Nein	Nein	Nein	Nein
AWS Lake Formation	Ja	Ja	Ja	Ja

AWS verwaltete Anwendung	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center	Unterstützt IAM Identity Center, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist	Unterstützt die Bereitstellung in weiteren Regionen von IAM Identity Center
AWS re:Post Private	Ja	Nein	Ja	Nein
AWS Supply Chain	Ja	Nein	Ja	Nein
AWS Sicherheitsagent	Ja	Ja	Ja	Nein
AWS Systems Manager	Nein	Nein	Ja	Ja — Fleet Manager Remote Desktop
AWS Transfer Family Web-Apps	Ja	Ja	Ja	Ja
AWS Transformation	Ja	Nein	Ja	Nein
AWS Verified Access	Nein	Nein	Ja	Nein
Kiro	Ja ¹	Ja	Ja	Nein
Multi-party Genehmigung	Nein	Ja	Ja	Nein
OpenSearch user interface (Dashboards)	Ja	Ja	Ja	Nein

¹ Für Kiro werden Kontoinstanzen von IAM Identity Center unterstützt, es sei denn, Ihre Benutzer benötigen Zugriff auf alle Kiro-Funktionen auf Websites. AWS Weitere Informationen finden Sie unter Kiro [einrichten](#) im Kiro-Benutzerhandbuch.

² Für Amazon Redshift werden Kontoinstanzen von IAM Identity Center unterstützt, mit Ausnahme von Anwendungen wie Query Editor v2, für die Berechtigungssätze erforderlich sind, die von Kontoinstanzen nicht unterstützt werden.

³ Sie aktivieren den Account Access Manager in der Hauptregion von IAM Identity Center, wodurch die AWS Kontozugriffsanwendung dort verfügbar ist. Sie können die Account Access Manager-Instance in weitere Regionen von IAM Identity Center replizieren, um die AWS Kontozugriffsanwendung in diesen zusätzlichen Regionen verfügbar zu machen.

 Note

Einige AWS Dienste wie Connect Customer AWS Client VPN sind in dieser Tabelle nicht aufgeführt, obwohl Sie sie mit IAM Identity Center verwenden können. Das liegt daran, dass sie ausschließlich mithilfe von SAML in IAM Identity Center integriert werden und daher als vom [Kunden verwaltete Anwendungen eingestuft werden](#).

Schnellstart: IAM Identity Center zum Testen einrichten AWS verwaltete Anwendungen

Wenn Ihr Administrator Ihnen noch keinen Zugriff auf IAM Identity Center gewährt hat, können Sie die Schritte in diesem Thema verwenden, um IAM Identity Center zum Testen AWS verwalteter Anwendungen einzurichten. Sie erfahren, wie Sie IAM Identity Center aktivieren, einen Benutzer direkt im IAM Identity Center erstellen und diesen Benutzer einer verwalteten Anwendung zuweisen.

AWS

Dieses Thema enthält Schnellstartschritte zur Aktivierung von IAM Identity Center auf eine der folgenden Arten:

- Mit AWS Organizations — Wenn Sie diese Option wählen, wird eine Organisationsinstanz von IAM Identity Center erstellt.
- Nur für Sie AWS-Konto — Wenn Sie diese Option wählen, wird eine Kontoinstanz von IAM Identity Center erstellt.

Informationen zu diesen Instanztypen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Voraussetzungen

Bevor Sie IAM Identity Center aktivieren, überprüfen Sie Folgendes:

- Sie haben eine AWS-Konto — Falls Sie noch keine haben AWS-Konto, finden Sie weitere Informationen unter [Erste Schritte mit einer AWS-Konto](#) im Referenzhandbuch zur AWS Kontoverwaltung.
- Die AWS verwaltete Anwendung funktioniert mit IAM Identity Center — Überprüfen Sie die Liste von, [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#) um sicherzustellen, dass die AWS verwaltete Anwendung, die Sie testen möchten, mit IAM Identity Center funktioniert.
- Sie haben regionale Überlegungen gelesen — Stellen Sie sicher, dass die AWS verwaltete Anwendung, die Sie testen möchten, in dem Land unterstützt wird, in AWS-Region dem Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie in der Dokumentation zur AWS verwalteten Anwendung.

Note

Sie müssen Ihre AWS verwaltete Anwendung in derselben Region bereitstellen, in der Sie IAM Identity Center aktivieren möchten.

Einrichtung einer Organisationsinstanz von IAM Identity Center zum Testen AWS verwaltete Anwendungen

Note

In diesem Thema wird beschrieben, wie IAM Identity Center mit AWS Organizations aktiviert wird. Dies ist die empfohlene Methode zur Aktivierung von IAM Identity Center.

Bestätigen Sie Ihre Berechtigungen

Um IAM Identity Center mit zu aktivieren AWS Organizations, müssen Sie sich mit einer der folgenden Optionen bei der AWS Management Console anmelden:

- Ein Benutzer mit Administratorrechten in dem Bereich, mit AWS-Konto dem IAM Identity Center aktiviert werden soll. AWS Organizations

- Der Root-Benutzer (nicht empfohlen, es sei denn, es gibt keine anderen administrativen Benutzer).

 Important

Der Root-Benutzer hat Zugriff auf alle AWS Dienste und Ressourcen im Konto. Verwenden Sie aus Sicherheitsgründen nicht die Root-Anmeldeinformationen Ihres Kontos für den Zugriff auf AWS Ressourcen, es sei denn, Sie haben keine anderen Anmeldeinformationen. Diese Anmeldeinformationen bieten uneingeschränkten Zugriff auf Konten und können nur schwer widerrufen werden.

Schritt 1. Aktivieren Sie IAM Identity Center mit AWS Organizations

1. Gehen Sie wie folgt vor, um sich bei der AWS-Managementkonsole anzumelden.
 - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Wird bereits AWS mit einem Standalone-Gerät verwendet AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
2. Wählen Sie auf der Startseite der AWS Management Console den IAM Identity Center-Dienst aus oder navigieren Sie zur [IAM Identity Center-Konsole](#).
3. Wählen Sie Aktivieren und aktivieren Sie IAM Identity Center mit AWS Organizations Wenn Sie dies tun, erstellen Sie eine [Organisationsinstanz](#) von IAM Identity Center.

Schritt 2. Erstellen Sie einen Administratorbenutzer in IAM Identity Center

Dieses Verfahren beschreibt, wie Sie einen Benutzer direkt im integrierten Identity Center-Verzeichnis erstellen. Dieses Verzeichnis ist mit keinem anderen Verzeichnis verbunden, das Ihr Administrator zur Verwaltung von Workforce-Benutzern verwenden könnte. Nachdem Sie den Benutzer in IAM Identity Center erstellt haben, geben Sie neue Anmeldeinformationen für diesen Benutzer an. Wenn Sie sich als dieser Benutzer anmelden, um Ihre AWS verwaltete Anwendung zu testen, melden Sie sich mit den neuen Anmeldeinformationen an, nicht mit den vorhandenen Anmeldeinformationen, die Sie für den Zugriff auf Unternehmensressourcen verwenden.

 Note

Wir empfehlen, dass Sie diese Methode nur zu Testzwecken verwenden, um Benutzer zu erstellen.

1. Wählen Sie im Navigationsbereich der IAM Identity Center-Konsole **Benutzer** und dann **Benutzer hinzufügen** aus.
2. Folgen Sie den Anweisungen in der Konsole, um den Benutzer hinzuzufügen. Lassen Sie die Option **E-Mail an diesen Benutzer senden mit Anweisungen zur Passwortkonfiguration** aktiviert und stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie Zugriff haben.
3. Wählen Sie im Navigationsbereich **AWS-Konten**, aktivieren Sie das Kontrollkästchen neben Ihrem Konto und wählen Sie **Benutzer oder Gruppen zuweisen** aus.
4. Wählen Sie die Registerkarte **Benutzer**, aktivieren Sie das Kontrollkästchen neben dem Benutzer, den Sie gerade hinzugefügt haben, und wählen Sie **Weiter**.
5. Wählen Sie **„Berechtigungssatz erstellen“** und folgen Sie den Anweisungen in der Konsole, um den **AdministratorAccess** vordefinierten Berechtigungssatz zu erstellen.
6. Wenn Sie fertig sind, wird der neue Berechtigungssatz in der Liste angezeigt. Schließen Sie die Registerkarte **„Berechtigungssätze“** in Ihrem Browserfenster, kehren Sie zur Registerkarte **„Benutzer und Gruppen zuweisen“** zurück und wählen Sie das Aktualisierungssymbol neben **„Berechtigungssatz erstellen“**.
7. Auf dem Browser-Tab **Benutzer und Gruppen zuweisen** wird der neue Berechtigungssatz in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen neben dem Namen des Berechtigungssatzes, wählen Sie **Weiter** und dann **Absenden** aus.
8. Melden Sie sich bei der -Konsole ab.

Schritt 3. Melden Sie sich bei AWS als administrativer Benutzer auf das Portal zugreifen

Das AWS Zugriffsportal ist ein Webportal, das dem Benutzer, den Sie erstellt haben, Zugriff auf die AWS Managementkonsole gewährt. Bevor Sie sich beim AWS Zugriffsportal anmelden können, müssen Sie die Einladung zum IAM Identity Center annehmen und Ihre Benutzeranmeldeinformationen aktivieren.

1. Suchen Sie in Ihrer E-Mail nach der Betreffzeile **Einladung zum Beitritt zu AWS IAM Identity Center**.

2. Wählen Sie Einladung annehmen und folgen Sie den Anweisungen auf der Anmeldeseite, um ein neues Passwort festzulegen, sich anzumelden und ein MFA-Gerät für Ihren Benutzer zu registrieren.
3. Nachdem Sie Ihr MFA-Gerät registriert haben, wird das AWS Zugangsportal geöffnet.
4. Wählen Sie im AWS Zugangsportal Ihre aus AWS-Konto und wählen Sie AdministratorAccess. Sie werden zur AWS Management Console weitergeleitet.

Schritt 4. Konfigurieren Sie die AWS verwaltete Anwendung zur Verwendung von IAM Identity Center

1. Während Sie bei der AWS Management Console angemeldet sind, öffnen Sie die Konsole für die AWS verwaltete Anwendung, die Sie verwenden möchten.
2. Folgen Sie den Anweisungen in der Konsole, um die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center zu konfigurieren. Während dieses Vorgangs können Sie den Benutzer, den Sie erstellt haben, der Anwendung zuweisen.

Einrichtung einer Kontoinstanz von IAM Identity Center zum Testen AWS verwaltete Anwendungen

Note

Eine Kontoinstanz von IAM Identity Center beschränkt Ihre Bereitstellung auf eine einzige AWS-Konto. Sie müssen diese Instanz genauso aktivieren AWS-Region wie die AWS Anwendung, die Sie testen möchten.

Bestätigen Sie Ihre App

Alle AWS verwalteten Anwendungen, die mit IAM Identity Center funktionieren, können mit Organisationsinstanzen von IAM Identity Center verwendet werden. Allerdings können nur einige dieser Anwendungen mit Kontoinstanzen von IAM Identity Center verwendet werden. Überprüfen Sie die Liste von. [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#)

Schritt 1. Aktivieren einer Konto-Instance von IAM Identity Center

1. Gehen Sie wie folgt vor, um sich bei der AWS-Managementkonsole anzumelden.

- Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Wird bereits AWS mit einem Standalone-Gerät verwendet AWS-Konto (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
2. Wählen Sie auf der Startseite der AWS Management Console den IAM Identity Center-Dienst aus oder navigieren Sie zur [IAM Identity Center-Konsole](#).
 3. Wählen Sie Enable (Aktivieren) aus.
 4. Wählen Sie auf der AWS Organizations Seite IAM Identity Center aktivieren mit die Option Eine Kontoinstanz von IAM Identity Center aktivieren aus.
 5. Überprüfen Sie auf der Seite „Kontoinstanz von IAM Identity Center aktivieren“ die Informationen und fügen Sie optional Tags hinzu, die Sie dieser Kontoinstanz zuordnen möchten. Wählen Sie dann Aktivieren.

Schritt 2. Erstellen Sie einen Benutzer im IAM Identity Center

Dieses Verfahren beschreibt, wie Sie einen Benutzer direkt im integrierten Identity Center-Verzeichnis erstellen. Dieses Verzeichnis ist mit keinem anderen Verzeichnis verbunden, das Ihr Administrator zur Verwaltung von Workforce-Benutzern verwenden könnte. Nachdem Sie den Benutzer in IAM Identity Center erstellt haben, geben Sie neue Anmeldeinformationen für diesen Benutzer an. Wenn Sie sich als dieser Benutzer anmelden, um Ihre AWS verwaltete Anwendung zu testen, melden Sie sich mit den neuen Anmeldeinformationen an. Mit den neuen Anmeldeinformationen können Sie nicht auf andere Unternehmensressourcen zugreifen.

Note

Wir empfehlen, dass Sie diese Methode verwenden, um Benutzer nur zu Testzwecken zu erstellen.

1. Wählen Sie im Navigationsbereich der IAM Identity Center-Konsole Benutzer und dann Benutzer hinzufügen aus.

2. Folgen Sie den Anweisungen in der Konsole, um den Benutzer hinzuzufügen. Lassen Sie die Option E-Mail an diesen Benutzer senden mit Anweisungen zur Passwortkonfiguration aktiviert und stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie Zugriff haben.
3. Melden Sie sich bei der -Konsole ab.

Schritt 3. Loggen Sie sich ein bei AWS greifen Sie als IAM Identity Center-Benutzer auf das Portal zu

Das AWS Zugriffsportal ist ein Webportal, das dem Benutzer, den Sie erstellt haben, Zugriff auf die AWS Managementkonsole gewährt. Bevor Sie sich beim AWS Zugriffsportal anmelden können, müssen Sie die Einladung zum IAM Identity Center annehmen und Ihre Benutzeranmeldeinformationen aktivieren.

1. Suchen Sie in Ihrer E-Mail nach der Betreffzeile Einladung zum Beitritt zu AWS IAM Identity Center.
2. Wählen Sie Einladung annehmen und folgen Sie den Anweisungen auf der Anmeldeseite, um ein neues Passwort festzulegen, sich anzumelden und ein MFA-Gerät für Ihren Benutzer zu registrieren.
3. Nachdem Sie Ihr MFA-Gerät registriert haben, wird das AWS Zugangsportal geöffnet. Wenn Ihnen Anwendungen zur Verfügung stehen, finden Sie sie auf der Registerkarte Anwendungen.

 Note

AWS Anwendungen, die Kontoinstanzen unterstützen, ermöglichen es Benutzern, sich bei Anwendungen anzumelden, ohne dass zusätzliche Berechtigungen erforderlich sind. Daher bleibt die Registerkarte „Konten“ leer.

Schritt 4. Konfigurieren Sie das AWS verwaltete Anwendung zur Verwendung von IAM Identity Center

1. Während Sie bei der AWS Management Console angemeldet sind, öffnen Sie die Konsole für die AWS verwaltete Anwendung, die Sie verwenden möchten.
2. Folgen Sie den Anweisungen in der Konsole, um die AWS verwaltete Anwendung für die Verwendung von IAM Identity Center zu konfigurieren. Während dieses Vorgangs können Sie den Benutzer, den Sie erstellt haben, der Anwendung zuweisen.

Details zu einem anzeigen und ändern AWS verwaltete Anwendung

Nachdem Sie eine AWS verwaltete Anwendung mithilfe der Konsole oder der APIs für die Anwendung mit IAM Identity Center verbunden haben, wird die Anwendung bei IAM Identity Center registriert. Nachdem eine Anwendung bei IAM Identity Center registriert wurde, können Sie Details zur Anwendung in der IAM Identity Center-Konsole anzeigen und ändern.

Zu den Informationen über die Anwendung gehören, ob Benutzer- und Gruppenzuweisungen erforderlich sind, und falls zutreffend, zugewiesene Benutzer und Gruppen sowie vertrauenswürdige Anwendungen für die Identitätsverbreitung. Hinweise zur Weitergabe vertrauenswürdiger Identitäten finden Sie unter [Überblick über die Verbreitung vertrauenswürdiger Identitäten](#).

So können Sie Informationen über eine anzeigen und ändern AWS verwaltete Anwendung in der IAM Identity Center-Konsole

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „AWS Verwaltet“.
4. Wählen Sie den Link für die verwaltete Anwendung, die Sie öffnen und anzeigen möchten.
5. Wenn Sie Informationen zu einer AWS verwalteten Anwendung ändern möchten, wählen Sie Aktion und dann Details bearbeiten aus.
6. Sie können den Anzeigenamen, die Beschreibung sowie die Methode für die Benutzer- und Gruppenzuweisung ändern.
 - a. Um den Anzeigenamen zu ändern, geben Sie den gewünschten Namen in das Feld Anzeigename ein und wählen Sie Änderungen speichern.
 - b. Um die Beschreibung zu ändern, geben Sie die gewünschte Beschreibung in das Feld Beschreibung ein und wählen Sie Änderungen speichern.
 - c. Um die Methode für die Benutzer- und Gruppenzuweisung zu ändern, nehmen Sie die gewünschte Änderung vor und wählen Sie Änderungen speichern. Weitere Informationen finden Sie unter [the section called “Benutzer, Gruppen und Bereitstellung”](#).

Deaktivierung einer AWS verwaltete Anwendung

Um zu verhindern, dass sich Benutzer bei einer AWS verwalteten Anwendung authentifizieren, können Sie die Anwendung in der IAM Identity Center-Konsole deaktivieren.

Um eine zu deaktivieren AWS verwaltete Anwendung

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie auf der Seite Anwendungen unter AWS Verwaltete Anwendungen die Anwendung aus, die Sie deaktivieren möchten.
4. Wählen Sie bei ausgewählter Anwendung die Option Aktionen und anschließend Deaktivieren aus.
5. Wählen Sie im Dialogfeld „Anwendung deaktivieren“ die Option „Deaktivieren“.
6. In der Liste der AWS verwalteten Anwendungen wird der Anwendungsstatus als Inaktiv angezeigt.

Note

Wenn eine AWS verwaltete Anwendung deaktiviert ist, können Sie die Fähigkeit der Benutzer wiederherstellen, sich bei der Anwendung zu authentifizieren, indem Sie Aktionen und dann Aktivieren auswählen.

Aktivieren von Konsolensitzungen mit verbesserter Identität

Eine Sitzung mit erweiterter Identität für die Konsole verbessert die Konsolensitzung eines Benutzers AWS, indem sie zusätzlichen Benutzerkontext bereitstellt, um die Benutzererfahrung zu personalisieren. Diese Funktion wird derzeit für Amazon Q Developer Pro-Benutzer von [Amazon Q auf AWS Apps und Websites unterstützt](#).

Sie können Konsolensitzungen mit erweiterter Identität aktivieren, ohne Änderungen an bestehenden Zugriffsmustern oder dem Verbund mit der AWS Konsole vorzunehmen. Wenn sich Ihre Benutzer mit IAM bei der AWS Konsole anmelden (z. B. wenn sie sich als IAM-Benutzer oder über Verbundzugriff mit IAM anmelden), können sie diese Methoden weiterhin verwenden. Wenn sich Ihre Benutzer beim AWS Zugriffsportal anmelden, können sie weiterhin ihre IAM Identity Center-Benutzeranmeldedaten verwenden.

Themen

- [Voraussetzungen und Überlegungen](#)
- [Wie aktiviere ich Konsolensitzungen mit erweiterter Identität](#)

- [So funktionieren Konsolensitzungen mit erweiterter Identität](#)

Voraussetzungen und Überlegungen

Bevor Sie Konsolensitzungen mit erweiterter Identität aktivieren, sollten Sie die folgenden Voraussetzungen und Überlegungen beachten:

- Wenn Ihre Benutzer über ein Amazon Q Developer Pro-Abonnement über AWS Apps und Websites auf Amazon Q zugreifen, müssen Sie Konsolensitzungen mit erweiterter Identität aktivieren.

Note

Amazon Q Developer-Benutzer können ohne identitätserweiterte Sitzungen auf Amazon Q zugreifen, sie haben jedoch keinen Zugriff auf ihre Amazon Q Developer Pro-Abonnements.

- Identity-enhanced Konsolensitzungen erfordern eine [Organisationsinstanz](#) von IAM Identity Center.
- Die Integration mit Amazon Q wird nicht unterstützt, wenn Sie IAM Identity Center in einem Opt-In aktivieren. AWS-Region
- Um Konsolensitzungen mit erweiterter Identität zu aktivieren, benötigen Sie die folgenden Berechtigungen:
 - `sso:CreateApplication`
 - `sso:GetSharedSsoConfiguration`
 - `sso:ListApplications`
 - `sso:PutApplicationAssignmentConfiguration`
 - `sso:PutApplicationAuthenticationMethod`
 - `sso:PutApplicationGrant`
 - `sso:PutApplicationAccessScope`
 - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
 - `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Damit Ihre Benutzer Konsolensitzungen mit erweiterter Identität verwenden können, müssen Sie ihnen die entsprechenden `sts:setContext` Berechtigungen in einer identitätsbasierten

Richtlinie gewähren. Weitere Informationen finden Sie unter [Benutzern Berechtigungen zur Nutzung identitätsverstärkter Konsolensitzungen gewähren](#).

Wie aktiviere ich Konsolensitzungen mit erweiterter Identität

Sie können Konsolensitzungen mit erweiterter Identität in der Amazon Q-Konsole oder in der IAM Identity Center-Konsole aktivieren.

Aktivieren Sie Konsolensitzungen mit erweiterter Identität in der Amazon Q-Konsole

Bevor Sie Konsolensitzungen mit erweiterter Identität aktivieren, müssen Sie über eine Organisationsinstanz von IAM Identity Center verfügen, an die eine Identitätsquelle angeschlossen ist. Wenn Sie IAM Identity Center bereits konfiguriert haben, fahren Sie mit Schritt 3 fort.

1. Öffnen Sie die IAM-Identity-Center-Konsole. Wählen Sie **Aktivieren** und erstellen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
2. Verbinden Sie Ihre Identitätsquelle mit IAM Identity Center und stellen Sie Benutzern IAM Identity Center zur Verfügung. Sie können Ihre bestehende Identitätsquelle mit IAM Identity Center verbinden oder das Identity Center-Verzeichnis verwenden, falls Sie nicht bereits eine andere Identitätsquelle verwenden. Weitere Informationen finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#).
3. Nachdem Sie die Einrichtung von IAM Identity Center abgeschlossen haben, öffnen Sie die Amazon Q-Konsole und folgen Sie den Schritten unter [Abonnements](#) im Amazon Q Developer User Guide. Stellen Sie sicher, dass Konsolensitzungen mit erweiterter Identität aktiviert sind.

Note

Wenn Sie nicht über ausreichende Berechtigungen verfügen, um identitätserweiterte Konsolensitzungen zu aktivieren, müssen Sie möglicherweise einen IAM Identity Center-Administrator bitten, diese Aufgabe in der IAM Identity Center-Konsole für Sie auszuführen. Weitere Informationen finden Sie im nächsten Verfahren .

Aktivieren Sie Konsolensitzungen mit erweiterter Identität in der IAM Identity Center-Konsole

Wenn Sie ein IAM Identity Center-Administrator sind, werden Sie möglicherweise von einem anderen Administrator aufgefordert, identitätserweiterte Konsolensitzungen in der IAM Identity Center-Konsole zu aktivieren.

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter Sitzungen mit erweiterter Identität aktivieren die Option Aktivieren aus.
4. Wählen Sie in der zweiten Nachricht die Option Aktivieren aus.
5. Nachdem Sie die Aktivierung von Konsolensitzungen mit erweiterter Identität abgeschlossen haben, wird oben auf der Seite „Einstellungen“ eine Bestätigungsmeldung angezeigt.
6. Im Abschnitt Details lautet der Status für Identity-enhanced Sitzungen Aktiviert.

So funktionieren Konsolensitzungen mit erweiterter Identität

IAM Identity Center erweitert die aktuelle Konsolensitzung eines Benutzers um die ID des aktiven IAM Identity Center-Benutzers und die IAM Identity Center-Sitzungs-ID.

Identity-enhanced Konsolensitzungen enthalten die folgenden drei Werte:

- Benutzer-ID des Identitätsspeichers ([Identitätsspeicher: UserId](#)) — Dieser Wert wird verwendet, um einen Benutzer in der Identitätsquelle, der mit IAM Identity Center verbunden ist, eindeutig zu identifizieren.
- Identitätsspeicher-Verzeichnis ARN ([Identitätsspeicher: IdentityStoreArn](#)) — Dieser Wert ist der ARN des Identitätsspeichers, der mit IAM Identity Center verbunden ist und für den Sie nach Attributen suchen können. `identitystore:UserId`
- IAM Identity Center-Sitzungs-ID — Dieser Wert gibt an, ob die IAM Identity Center-Sitzung des Benutzers noch gültig ist.

Die Werte sind dieselben, werden jedoch auf unterschiedliche Weise ermittelt und zu unterschiedlichen Zeitpunkten des Vorgangs hinzugefügt, je nachdem, wie sich der Benutzer anmeldet:

- IAM Identity Center (AWS Zugriffsportal): In diesem Fall werden die Benutzer-ID und die ARN-Werte für den Identitätsspeicher des Benutzers bereits in der aktiven IAM Identity Center-Sitzung

bereitgestellt. IAM Identity Center verbessert die aktuelle Sitzung, indem nur die Sitzungs-ID hinzugefügt wird.

- **Andere Anmeldemethoden:** Wenn sich der Benutzer AWS als IAM-Benutzer, mit einer IAM-Rolle oder als Verbundbenutzer mit IAM anmeldet, wird keiner dieser Werte bereitgestellt. IAM Identity Center erweitert die aktuelle Sitzung, indem es die Benutzer-ID des Identitätsspeichers, den ARN des Identitätsspeicher-Verzeichnisses und die Sitzungs-ID hinzufügt.

Vom Kunden verwaltete Anwendungen

IAM Identity Center fungiert als zentraler Identitätsdienst für Ihre Mitarbeiter und Gruppen. Wenn Sie bereits einen Identitätsanbieter (IdP) verwenden, kann IAM Identity Center in Ihren IdP integriert werden, sodass Sie Ihre Benutzer und Gruppen in IAM Identity Center bereitstellen und Ihren IdP für die Authentifizierung verwenden können. Mit einer einzigen Verbindung repräsentiert IAM Identity Center Ihren IdP vor mehreren AWS-Services und ermöglicht es Ihren OAuth 2.0-Anwendungen, im Namen Ihrer Benutzer Zugriff auf Daten in diesen Diensten anzufordern. Sie können IAM Identity Center auch verwenden, um Ihren Benutzern Zugriff auf SAML 2.0-Anwendungen zuzuweisen.

<https://wiki.oasis-open.org/security> Dazu gehören AWS Dienste wie Connect Customer und AWS Client VPN, die ausschließlich mithilfe von SAML in IAM Identity Center integriert werden und daher als vom Kunden verwaltete Anwendungen eingestuft werden.

- Wenn Ihre Anwendung JSON Web Tokens (JWTs) unterstützt, können Sie die Funktion zur Weitergabe vertrauenswürdiger Identitäten von IAM Identity Center verwenden, damit Ihre Anwendung im Namen Ihrer Benutzer Zugriff AWS-Services auf Daten anfordern kann. Trusted Identity Propagation basiert auf dem OAuth 2.0 Authorization Framework und beinhaltet eine Option für Anwendungen, Identitätstoken, die von einem externen OAuth 2.0-Autorisierungsserver stammen, gegen Token auszutauschen, die vom IAM Identity Center ausgestellt und von erkannt wurden. AWS-Services Weitere Informationen finden Sie unter [Anwendungsfälle für vertrauenswürdige Identitätsverbreitung](#).
- Wenn Ihre Anwendung SAML 2.0 unterstützt, können Sie sie mit einer [Organisationsinstanz von IAM Identity Center verbinden](#). Sie können IAM Identity Center verwenden, um Ihrer SAML 2.0-Anwendung Zugriff zuzuweisen.

Note

Wenn Sie vom Kunden verwaltete Anwendungen in eine IAM Identity Center-Instanz integrieren, die einen vom [Kunden verwalteten KMS-Schlüssel verwendet](#), überprüfen Sie,

ob die Anwendung die IAM Identity Center Service-APIs aufruft. Ist dies der Fall, finden Sie in der [grundlegenden KMS-Schlüsselrichtlinie](#) die erforderlichen Berechtigungen.

Themen

- [Single-Sign-On-Zugriff auf SAML 2.0- und OAuth 2.0-Anwendungen](#)
- [Einrichtung von kundenverwalteten SAML 2.0-Anwendungen](#)
- [Aktivieren AWS Kontozugriff für vom Kunden verwaltete Anwendungen](#)

Single-Sign-On-Zugriff auf SAML 2.0- und OAuth 2.0-Anwendungen

Mit IAM Identity Center können Sie Ihren Benutzern Single-Sign-On-Zugriff auf SAML 2.0- oder OAuth 2.0-Anwendungen gewähren. Die folgenden Themen bieten einen allgemeinen Überblick über SAML 2.0 und OAuth 2.0.

Themen

- [SAML 2.0](#)
- [OAuth 2.0](#)

SAML 2.0

SAML 2.0 ist ein Industriestandard, der für den sicheren Austausch von SAML-Assertionen verwendet wird, die Informationen über einen Benutzer zwischen einer SAML-Behörde (als Identitätsanbieter oder IdP bezeichnet) und einem SAML 2.0-Verbraucher (Service Provider oder SP genannt) weitergeben. IAM Identity Center verwendet diese Informationen, um Benutzern, die zur Verwendung von Anwendungen im Zugriffsportal autorisiert sind, den Verbundzugriff über Single Sign-On bereitzustellen. AWS

Note

IAM Identity Center unterstützt nicht die Validierung von Signaturen eingehender SAML-Authentifizierungsanfragen von SAML-Anwendungen.

OAuth 2.0

OAuth 2.0 ist ein Protokoll, mit dem Anwendungen sicher auf Benutzerdaten zugreifen und diese gemeinsam nutzen können, ohne Passwörter weitergeben zu müssen. Diese Funktion bietet Benutzern eine sichere und standardisierte Möglichkeit, Anwendungen den Zugriff auf ihre Ressourcen zu ermöglichen. Der Zugriff wird durch verschiedene OAuth 2.0-Zuschüsse erleichtert.

Mit IAM Identity Center können Anwendungen, die auf öffentlichen Clients ausgeführt werden, temporäre Anmeldeinformationen für den Zugriff AWS-Konten und die Dienste programmgesteuert im Namen ihrer Benutzer abrufen. Öffentliche Clients sind in der Regel Desktops, Laptops oder andere mobile Geräte, die zur lokalen Ausführung von Anwendungen verwendet werden. Beispiele für AWS Anwendungen, die auf öffentlichen Clients ausgeführt werden AWS Toolkit, sind die AWS Command Line Interface (AWS CLI) und die AWS Software Development Kits (SDKs). Damit diese Anwendungen Anmeldeinformationen abrufen können, unterstützt IAM Identity Center Teile der folgenden OAuth 2.0-Flows:

- Autorisierungscode-Erteilung mit Proof Key for Code Exchange (PKCE) ([RFC 6749 und RFC 7636](#)) <https://www.rfc-editor.org/rfc/rfc7636>
- Geräteautorisierung (RFC 8628) <https://datatracker.ietf.org/doc/html/rfc8628>

Note

Diese Gewährungstypen können nur verwendet werden, wenn sie AWS-Services diese Funktion unterstützen. Diese Dienste unterstützen diesen Zuschusstyp möglicherweise überhaupt nicht AWS-Regionen. Beachten Sie die Dokumentation der AWS-Services für regionale Unterschiede relevanten Informationen.

OpenID Connect (OIDC) ist ein Authentifizierungsprotokoll, das auf dem OAuth 2.0 Framework basiert. OIDC spezifiziert, wie OAuth 2.0 für die Authentifizierung verwendet wird. Über die OIDC-Dienst-APIs von [IAM Identity Center registriert eine Anwendung einen OAuth 2.0-Client und verwendet einen dieser Flows](#), um ein Zugriffstoken abzurufen, das Berechtigungen für durch IAM Identity Center geschützte APIs gewährt. Eine Anwendung legt [Zugriffsbereiche fest, um den vorgesehenen API-Benutzer zu](#) deklarieren. Nachdem Sie als IAM Identity Center-Administrator Ihre Identitätsquelle konfiguriert haben, müssen die Endbenutzer Ihrer Anwendung einen Anmeldevorgang abschließen, sofern sie dies nicht bereits getan haben. Ihre Endbenutzer müssen dann ihre Zustimmung geben, damit die Anwendung API-Aufrufe tätigen kann. Diese API-

Aufrufe werden mithilfe der Benutzerberechtigungen getätigt. Als Antwort gibt IAM Identity Center einen Zugriffstoken an die Anwendung zurück, der die Zugriffsbereiche enthält, denen die Benutzer zugestimmt haben.

Mithilfe eines OAuth 2.0-Grant-Flows

OAuth 2.0-Grant-Flows sind nur über AWS verwaltete Anwendungen verfügbar, die die Flows unterstützen. Um einen OAuth 2.0-Flow verwenden zu können, müssen Ihre IAM Identity Center-Instanz und alle unterstützten AWS verwalteten Anwendungen, die Sie verwenden, in einer einzigen Instanz bereitgestellt werden. AWS-Region Informationen zur regionalen Verfügbarkeit der AWS verwalteten Anwendungen und der IAM Identity Center-Instanz, die Sie verwenden möchten, finden Sie in der jeweiligen AWS-Service Dokumentation.

Um eine Anwendung zu verwenden, die einen OAuth 2.0-Flow verwendet, muss der Endbenutzer die URL eingeben, über die die Anwendung eine Verbindung herstellt, und sich bei Ihrer IAM Identity Center-Instanz registrieren. Je nach Anwendung müssen Sie als Administrator Ihren Benutzern die AWS Zugriffsportals-URL oder die Aussteller-URL Ihrer IAM Identity Center-Instanz zur Verfügung stellen. Sie finden diese beiden Einstellungen auf der Einstellungsseite der [IAM Identity Center-Konsole](#). Weitere Informationen zur Konfiguration einer Client-Anwendung finden Sie in der Dokumentation zu dieser Anwendung.

Wie der Endbenutzer sich bei einer Anwendung anmeldet und seine Zustimmung erteilt, hängt davon ab, ob die Anwendung [Erteilung des Autorisierungs-codes mit PKCE](#) oder verwendet [Autorisierung des Geräts](#).

Erteilung des Autorisierungs-codes mit PKCE

Dieser Ablauf wird von Anwendungen verwendet, die auf einem Gerät ausgeführt werden, das über einen Browser verfügt.

1. Es wird ein Browserfenster geöffnet.
2. Wenn sich der Benutzer nicht authentifiziert hat, leitet ihn der Browser zur vollständigen Benutzerauthentifizierung weiter.
3. Nach der Authentifizierung wird dem Benutzer ein Zustimmungsbildschirm angezeigt, auf dem die folgenden Informationen angezeigt werden:
 - Der Name der Anwendung
 - Die Zugriffsbereiche, zu deren Nutzung die Anwendung um Zustimmung bittet
4. Der Benutzer kann den Einwilligungsprozess abbrechen oder er kann seine Zustimmung geben und die Anwendung setzt den Zugriff auf der Grundlage der Berechtigungen des Benutzers fort.

Autorisierung des Geräts

Dieser Ablauf kann von Anwendungen verwendet werden, die auf einem Gerät mit oder ohne Browser ausgeführt werden. Wenn die Anwendung den Flow initiiert, präsentiert die Anwendung eine URL und einen Benutzercode, die der Benutzer später im Flow überprüfen muss. Der Benutzercode ist erforderlich, da die Anwendung, die den Flow initiiert, möglicherweise auf einem anderen Gerät ausgeführt wird als dem Gerät, auf dem der Benutzer seine Zustimmung erteilt. Der Code stellt sicher, dass der Benutzer dem Flow zustimmt, den er auf dem anderen Gerät initiiert hat.

Note

Wenn Ihre Kunden ihn verwendend `device.sso.region.amazonaws.com`, müssen Sie Ihren Autorisierungsablauf aktualisieren, um Proof Key for Code Exchange (PKCE) verwenden zu können. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter [Konfiguration der IAM Identity Center-Authentifizierung mit AWS CLI](#) dem.

1. Wenn der Flow von einem Gerät mit einem Browser aus gestartet wird, wird ein Browserfenster geöffnet. Wenn der Flow von einem Gerät ohne Browser aus gestartet wird, muss der Benutzer einen Browser auf einem anderen Gerät öffnen und zu der URL wechseln, die von der Anwendung angezeigt wurde.
2. In beiden Fällen leitet der Browser den Benutzer zur vollständigen Benutzerauthentifizierung weiter, wenn er sich nicht authentifiziert hat.
3. Nach der Authentifizierung wird dem Benutzer ein Zustimmungsbildschirm angezeigt, auf dem die folgenden Informationen angezeigt werden:
 - Der Name der Anwendung
 - Die Zugriffsbereiche, zu deren Nutzung die Anwendung um Zustimmung bittet
 - Der Benutzercode, den die Anwendung dem Benutzer präsentiert hat
4. Der Benutzer kann den Einwilligungsprozess abbrechen oder er kann seine Zustimmung geben und die Anwendung setzt den Zugriff auf der Grundlage der Berechtigungen des Benutzers fort.

Zugriffsbereiche

Ein Bereich definiert den Zugriff für einen Dienst, auf den über einen OAuth 2.0-Flow zugegriffen werden kann. Bereiche sind eine Möglichkeit für den Dienst, der auch als Ressourcenserver

bezeichnet wird, Berechtigungen zu gruppieren, die sich auf Aktionen und die Dienstressourcen beziehen, und sie spezifizieren die groben Operationen, die OAuth 2.0-Clients anfordern können. Wenn sich ein OAuth 2.0-Client beim [IAM Identity Center OIDC-Dienst registriert, gibt der Client die Bereiche an, um die beabsichtigten Aktionen zu deklarieren](#), für die der Benutzer seine Zustimmung geben muss.

OAuth 2.0-Clients verwenden scope Werte, wie sie in [Abschnitt 3.3 von OAuth 2.0 \(RFC 6749\)](#) definiert sind, um anzugeben, welche Berechtigungen für ein Zugriffstoken angefordert werden. Clients können maximal 25 Bereiche angeben, wenn sie ein Zugriffstoken anfordern. Wenn ein Benutzer während des Ablaufs „Autorisierungscode mit PKCE“ oder „Geräteautorisierung“ seine Zustimmung erteilt, kodiert IAM Identity Center die Bereiche in das zurückgegebene Zugriffstoken.

AWS fügt IAM Identity Center Bereiche für unterstützte Bereiche hinzu. AWS-Services In der folgenden Tabelle sind die Bereiche aufgeführt, die der OIDC-Dienst von IAM Identity Center unterstützt, wenn Sie einen öffentlichen Client registrieren.

Zugriffsbereiche, die vom IAM Identity Center OIDC-Dienst bei der Registrierung eines öffentlichen Clients unterstützt werden

Scope	Description	Dienste, die unterstützt werden von
<code>sso:account:access</code>	Greifen Sie auf von IAM Identity Center verwaltete Konten und Berechtigungssätze zu.	IAM Identity Center
<code>codewhisperer:analysis</code>	Ermöglichen Sie den Zugriff auf die Kiro-Codeanalyse.	AWS Builder ID und IAM Identity Center
<code>codewhisperer:completions</code>	Ermöglichen Sie den Zugriff auf die Inline-Code-Vorschläge von Kiro.	AWS Builder ID und IAM Identity Center
<code>codewhisperer:conversations</code>	Aktiviere den Zugriff auf den Kiro-Chat.	AWS Builder ID und IAM Identity Center
<code>codewhisperer:taskassist</code>	Ermöglichen Sie den Zugriff auf Kiro Agent für die Softwareentwicklung.	AWS Builder ID und IAM Identity Center

Scope	Description	Dienste, die unterstützt werden von
<code>codewhisperer:transformations</code>	Ermöglichen Sie den Zugriff auf Kiro Agent für die Codetransformation.	AWS Builder ID und IAM Identity Center
<code>codecatalyst:read_write</code>	Lesen und schreiben Sie in Ihre CodeCatalyst Amazon-Ressourcen, sodass Sie auf alle Ihre vorhandenen Ressourcen zugreifen können.	AWS Builder ID und IAM Identity Center
<code>verified_access:application:connect</code>	Aktiviere AWS Verified Access	AWS Verified Access
<code>redshift:connect</code>	Stellen Sie eine Verbindung zu Amazon Redshift her	Amazon Redshift
<code>datazone:domain:access</code>	Greifen Sie auf Ihre DataZone Domain-Ausführungsrolle zu	Amazon DataZone
<code>nosqlworkbench:datamodeladviser</code>	Datenmodelle erstellen und lesen	NoSQL Workbench
<code>transform:read_write</code>	Aktivieren Sie den Zugriff auf AWS Transform Agent für die Codetransformation	AWS Transformation

Einrichtung von kundenverwalteten SAML 2.0-Anwendungen

Wenn Sie vom Kunden verwaltete Anwendungen verwenden, die [SAML 2.0 unterstützen](#), können Sie Ihren IdP über SAML 2.0 mit IAM Identity Center verbinden und IAM Identity Center verwenden, um den Benutzerzugriff auf diese Anwendungen zu verwalten. Sie können in der IAM Identity Center-Konsole eine SAML 2.0-Anwendung aus einem Katalog häufig verwendeter Anwendungen auswählen oder Ihre eigene SAML 2.0-Anwendung einrichten.

 Note

Wenn Sie über vom Kunden verwaltete Anwendungen verfügen, die OAuth 2.0 unterstützen, und Ihre Benutzer Zugriff auf diese Anwendungen benötigen AWS-Services, können Sie Trusted Identity Propagation verwenden. Bei der Weitergabe vertrauenswürdiger Identitäten kann sich ein Benutzer bei einer Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Datenzugriff weitergeben. AWS-Services

Themen

- [Richten Sie eine Anwendung aus dem IAM Identity Center-Anwendungskatalog ein](#)
- [Richten Sie Ihre eigene SAML 2.0-Anwendung ein](#)

Richten Sie eine Anwendung aus dem IAM Identity Center-Anwendungskatalog ein

Sie können den Anwendungskatalog in der IAM Identity Center-Konsole verwenden, um viele häufig verwendete SAML 2.0-Anwendungen hinzuzufügen, die mit IAM Identity Center funktionieren.

Beispiele hierfür sind Salesforce, Box und Microsoft 365.

Die meisten Anwendungen enthalten detaillierte Informationen darüber, wie das Vertrauen zwischen IAM Identity Center und dem Dienstanbieter der Anwendung eingerichtet wird. Diese Informationen sind auf der Konfigurationsseite für die Anwendung verfügbar, nachdem Sie die Anwendung im Katalog ausgewählt haben. Nachdem Sie die Anwendung konfiguriert haben, können Sie Benutzern oder Gruppen im IAM Identity Center nach Bedarf Zugriff zuweisen.

Gehen Sie wie folgt vor, um eine SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer Anwendung einzurichten.

Bevor Sie mit diesem Verfahren beginnen, ist es hilfreich, über die Metadaten-Austauschdatei des Dienstanbieters zu verfügen, damit Sie die Vertrauensstellung effizienter einrichten können. Wenn Sie nicht über diese Datei verfügen, können Sie dieses Verfahren trotzdem verwenden, um die Vertrauensstellung manuell zu konfigurieren.

So fügen Sie eine Anwendung aus dem Anwendungskatalog hinzu und konfigurieren sie

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte Vom Kunden verwaltet aus.

4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Voreinstellung die Option Ich möchte eine Anwendung aus dem Katalog auswählen aus.
6. Beginnen Sie unter Anwendungskatalog mit der Eingabe des Namens der Anwendung, die Sie hinzufügen möchten, in das Suchfeld.
7. Wählen Sie den Namen der Anwendung aus der Liste aus, wenn er in den Suchergebnissen erscheint, und klicken Sie dann auf Weiter.
8. Auf der Seite „Anwendung konfigurieren“ sind die Felder Anzeigename und Beschreibung vorab mit relevanten Details für die Anwendung ausgefüllt. Sie können diese Informationen bearbeiten.
9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:
 - a. Wählen Sie unter IAM Identity Center SAML-Metadatendatei die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.
 - b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Zertifikat herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

 Note

Sie benötigen diese Dateien später, wenn Sie die Anwendung von der Website des Dienstanbieters aus einrichten. Befolgen Sie die Anweisungen des Anbieters.

10. (Optional) Unter Anwendungseigenschaften können Sie die URL für den Anwendungsstart, den Relaystatus und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter [Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut](#).
11. Führen Sie unter Anwendungsmetadaten eine der folgenden Aktionen aus:
 - a. Wenn Sie eine Metadatendatei haben, wählen Sie Anwendungs-SAML-Metadatendatei hochladen aus. Wählen Sie dann Datei auswählen, um die Metadatendatei zu suchen, und wählen Sie sie aus.
 - b. Wenn Sie keine Metadatendatei haben, wählen Sie Manuell geben Sie Ihre Metadatenwerte ein und geben Sie dann die ACS-URL der Anwendung und die SAML-Zielgruppenwerte der Anwendung ein.
12. Wählen Sie Absenden aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Richten Sie Ihre eigene SAML 2.0-Anwendung ein

Sie können Ihre eigenen Anwendungen einrichten, die einen Identitätsverbund mithilfe von SAML 2.0 ermöglichen, und sie zum IAM Identity Center hinzufügen. Die meisten Schritte zum Einrichten Ihrer eigenen SAML 2.0-Anwendungen entsprechen dem Einrichten einer SAML 2.0-Anwendung aus dem Anwendungskatalog in der IAM Identity Center-Konsole. Sie müssen jedoch auch zusätzliche SAML-Attributzuordnungen für Ihre eigenen SAML 2.0-Anwendungen bereitstellen. Diese Zuordnungen ermöglichen es IAM Identity Center, die SAML 2.0-Assertion für Ihre Anwendung korrekt auszufüllen. Sie können diese zusätzliche SAML-Attributzuordnung bereitstellen, wenn Sie die Anwendung zum ersten Mal einrichten. Sie können SAML 2.0-Attributzuordnungen auch auf der Seite mit den Anwendungsdetails in der IAM Identity Center-Konsole bereitstellen.

Gehen Sie wie folgt vor, um eine SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer SAML 2.0-Anwendung einzurichten. Bevor Sie damit beginnen, stellen Sie sicher, dass Sie die Zertifikatsdatei sowie die Austauschdatei mit den Metadaten des Service-Anbieters haben, damit Sie die Einrichtung der Vertrauensstellung abschließen können.

So richten Sie Ihre eigene SAML 2.0-Anwendung ein

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte Vom Kunden verwaltet aus.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Einrichtungspräferenz die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
6. Wählen Sie unter Anwendungstyp die Option SAML 2.0 aus.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Anwendung konfigurieren unter Anwendung konfigurieren einen Anzeigenamen für die Anwendung ein, z. B. **MyApp**. Geben Sie dann eine Beschreibung ein.
9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:
 - a. Wählen Sie unter IAM Identity Center SAML-Metadatendatei die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.
 - b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

 Note

Sie benötigen diese Dateien später, wenn Sie die benutzerdefinierte Anwendung über die Website des Service-Anbieters einrichten.

10. (Optional) Unter **Anwendungseigenschaften** können Sie auch die URL für den Anwendungsstart, den Relaystatus und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter [Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut](#).
11. Wählen Sie unter **Anwendungsmetadaten** die Option **Manuell Ihre Metadatenwerte eingeben** aus. Geben Sie dann die ACS-URL der Anwendung und die SAML-Zielgruppenwerte der Anwendung an.
12. Wählen Sie **Absenden** aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Aktivieren AWS Kontozugriff für vom Kunden verwaltete Anwendungen

[Sie können den AWS Kontozugriff für vom Kunden verwaltete Anwendungen in IAM Identity Center aktivieren, indem Sie einen vertrauenswürdigen Token-Aussteller konfigurieren.](#) Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token im Namen authentifizierter Benutzer ausgibt. IAM Identity Center tauscht diese Token gegen Anmeldeinformationen aus, die es Ihrer Anwendung ermöglichen, programmgesteuert auf AWS Konten und Rollen zuzugreifen, die diesen Benutzern zugewiesen sind. Vertrauenswürdige Token-Aussteller können auch für den Zugriff auf verwaltete Anwendungen verwendet werden. AWS Weitere Informationen finden Sie unter [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#).

 Note

Sie können diese Funktion nur für [Organisationsinstanzen](#) von IAM Identity Center aktivieren. Nur Administratoren von Verwaltungskonten oder delegierte Administratoren können den `sso:account:access` Bereich für eine vom Kunden verwaltete Anwendung aktivieren. Wenn Sie ein Anwendungsentwickler in einem Mitgliedskonto sind, wenden Sie sich an Ihren IAM Identity Center-Administrator, um diesen Bereich für Ihre Anwendung zu aktivieren.

Funktionsweise

Nachdem ein Administrator den `sso:account:access` Bereich für eine vom Kunden verwaltete Anwendung aktiviert hat, läuft der folgende Workflow ab:

1. Ein Benutzer meldet sich über Ihren externen Identitätsanbieter (IdP) bei Ihrer Anwendung an.
2. Ihre Anwendung erhält ein signiertes JWT-Token vom IdP.
3. Ihre Anwendung tauscht dieses Token gegen ein IAM Identity Center-Token aus, indem sie die `CreateTokenWithIAM` API mit dem `JWT-Bearer-Grant-Typ` () aufruft. `urn:ietf:params:oauth:grant-type:jwt-bearer` Für diesen Aufruf ist eine Authentifizierung mit Signature Version 4 (Sigv4) erforderlich. Weitere Informationen finden Sie [CreateTokenWithIAM](#) in der IAM Identity Center OIDC API-Referenz.
4. Ihre Anwendung verwendet das IAM Identity Center-Token, um [Portal-API-Operationen](#) (`ListAccounts`, `GetRoleCredentials`) aufzurufen `ListAccountRoles`, um Konten und Rollen zu ermitteln, die dem Benutzer zugewiesen sind, und um temporäre AWS Anmeldeinformationen in seinem Namen abzurufen.
5. Der Benutzer greift über Ihre Anwendung auf AWS Ressourcen zu, ohne dass zusätzliche Anmeldeschritte erforderlich sind.

Wenn Sie bei der Einrichtung Ihrer Anwendung die Erteilung von Aktualisierungstoken aktiviert haben, wird zusammen mit dem Zugriffstoken `CreateTokenWithIAM` auch ein Aktualisierungstoken zurückgegeben. Ihre Anwendung kann dieses Aktualisierungstoken verwenden, um neue Zugriffstoken zu erhalten, ohne den vollständigen Austausch des JWT Bearer-Tokens wiederholen zu müssen. Um ein Zugriffstoken zu aktualisieren, rufen Sie `CreateTokenWithIAM` mit dem `refresh_token` Grant-Typ auf.

Voraussetzungen

Bevor Sie den Kontozugriff für eine vom Kunden verwaltete Anwendung aktivieren, benötigen Sie:

- Eine vom [Kunden verwaltete Anwendung](#), die in IAM Identity Center konfiguriert ist und JSON Web Tokens (JWTs) unterstützt. Die Anwendung muss über eine Backend-Serverkomponente verfügen, die Anmeldeinformationen sicher speichern kann. Browser-based Anwendungen wie Single Page Applications (SPAs) und andere öffentliche Clients werden für diese Funktion nicht unterstützt.
- Ein [vertrauenswürdiger Token-Aussteller](#), der Ihrer Anwendung beigelegt ist.

- Zugriff auf das AWS Organizations Verwaltungskonto oder das delegierte Administratorkonto für IAM Identity Center. Anwendungsentwickler in Mitgliedskonten können diesen Bereich nicht direkt aktivieren.

Kontozugriff aktivieren

Um den Bereich **sso:account:access** für eine vom Kunden verwaltete Anwendung zu aktivieren

1. Melden Sie sich AWS-Managementkonsole mit dem Verwaltungskonto Ihrer Organisation oder dem delegierten Administratorkonto an.
2. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
3. Wählen Sie im Navigationsbereich Applications (Anwendungen).
4. Wählen Sie die Registerkarte Vom Kunden verwaltet aus.
5. Wählen Sie den Namen der Anwendung, die Sie konfigurieren möchten.
6. Aktivieren Sie im Bereich AWS Kontozugriff die Option AWS Kontozugriff aktivieren.

Nachdem Sie den Kontozugriff aktiviert haben, kann die Anwendung programmgesteuert Identity Portal-API-Operationen aufrufen, um Konten und Rollen aufzulisten und temporäre AWS Anmeldeinformationen für Rollen abzurufen, auf die ein authentifizierter Benutzer zugreifen darf.

Important

Wenn Sie den **sso:account:access** Bereich für eine Anwendung aktivieren, kann diese Anwendung über deren Berechtigungssatzzuweisungen auf alle Konten und Rollen zugreifen, die für einen authentifizierten Benutzer verfügbar sind. Sie können die Anwendung nicht auf bestimmte Konten oder Rollen beschränken. Stellen Sie sicher, dass Sie diese Zugriffsebene verstehen, bevor Sie diese Funktion aktivieren.

Programmgesteuerter Zugriff

Sie können die `PutApplicationAccessScope` API verwenden, um den **sso:account:access** Geltungsbereich für eine vom Kunden verwaltete Anwendung programmgesteuert zu aktivieren. Sie müssen die API über das Verwaltungskonto oder das delegierte Administratorkonto Ihrer Organisation aufrufen.

AWS CLI

```
aws sso-admin put-application-access-scope \  
  --application-arn  
  arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef \  
  --scope "sso:account:access"
```

API-Anfrage:

```
{  
  "ApplicationArn":  
  "arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef",  
  "Scope": "sso:account:access"  
}
```

Um den Kontozugriff zu deaktivieren, verwenden Sie die `DeleteApplicationAccessScope` API mit demselben Anwendungs-ARN und Bereichswert.

Weitere Informationen finden Sie unter [PutApplicationAccessScope](#) und [DeleteApplicationAccessScope](#) in der IAM Identity Center API-Referenz.

Bewährte Methoden für die Gewährleistung der Sicherheit

- Der `sso:account:access` Geltungsbereich gewährt der Anwendung Zugriff auf alle Konten und Rollen, die dem authentifizierten Benutzer zur Verfügung stehen. Sie können den Zugriff nicht auf bestimmte Konten oder Rollen einschränken. Aktivieren Sie diesen Bereich nur für Anwendungen, die diesen Zugriffsebene erfordern.
- Bewahren Sie die Zugriffs- und Aktualisierungstoken für IAM Identity Center auf Ihrem Backend-Server auf. Setzen Sie sie niemals clientseitigem Code aus.
- Protokollieren Sie keine Token oder Anmeldeinformationen in Anwendungsprotokollen, Fehlermeldungen oder Debugging-Ausgaben.
- Übergeben Sie keine Token in URL-Abfrageparametern. Verwenden Sie den `x-amz-sso-bearer-token` Header für Zugriffstoken.
- Wird verwendet [AWS CloudTrail](#), um API-Aufrufe Ihrer Anwendungen zu überwachen.

Ähnliche Informationen

- [Vom Kunden verwaltete Anwendungen](#)
- [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#)

- [AWS API-Referenz für das Zugangsportal](#)

Überblick über die Verbreitung vertrauenswürdiger Identitäten

Die Weitergabe vertrauenswürdiger Identitäten ist eine Funktion von IAM Identity Center, die es Administratoren ermöglicht, Berechtigungen auf der Grundlage von Benutzerattributen wie Gruppenzuordnungen AWS-Services zu gewähren. Bei der Weitergabe vertrauenswürdiger Identitäten wird einer IAM-Rolle ein Identitätskontext hinzugefügt, um den Benutzer zu identifizieren, der Zugriff AWS auf Ressourcen anfordert. Dieser Kontext wird an andere weitergegeben. AWS-Services

Der Identitätskontext umfasst Informationen, AWS-Services anhand derer Autorisierungsentscheidungen getroffen werden, wenn sie Zugriffsanfragen erhalten. Zu diesen Informationen gehören Metadaten, die den Anforderer (z. B. einen IAM Identity Center-Benutzer), die AWS-Service Person, für die der Zugriff angefordert wird (z. B. Amazon Redshift), und den Umfang des Zugriffs (z. B. schreibgeschützter Zugriff) identifizieren. Der Empfänger AWS-Service verwendet diesen Kontext und alle dem Benutzer zugewiesenen Berechtigungen, um den Zugriff auf seine Ressourcen zu autorisieren.

Vorteile der Verbreitung vertrauenswürdiger Identitäten

Die Verbreitung vertrauenswürdiger Identitäten ermöglicht es den Administratoren von AWS-Services, mithilfe der Unternehmensidentitäten Ihrer Mitarbeiter Berechtigungen für Ressourcen wie Daten zu erteilen. Darüber hinaus können sie anhand von Serviceprotokollen oder AWS CloudTrail überprüfen, wer auf welche Daten zugegriffen hat. Wenn Sie ein IAM Identity Center-Administrator sind, werden Sie möglicherweise von anderen AWS-Service Administratoren aufgefordert, die Weitergabe vertrauenswürdiger Identitäten zu aktivieren.

Aktivierung der Verbreitung vertrauenswürdiger Identitäten

Das Verfahren zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten umfasst die folgenden zwei Schritte:

1. Aktivieren Sie IAM Identity Center und verbinden Sie Ihre bestehende Identitätsquelle mit IAM Identity Center — Sie verwalten die Identitäten Ihrer Mitarbeiter weiterhin in Ihrer vorhandenen Identitätsquelle. Wenn Sie sie mit IAM Identity Center verbinden, entsteht ein Verweis auf Ihre Belegschaft, den alle AWS-Services in Ihrem Anwendungsfall gemeinsam nutzen können. Es ist auch für Dateneigentümer verfügbar, um es in zukünftigen Anwendungsfällen zu verwenden.

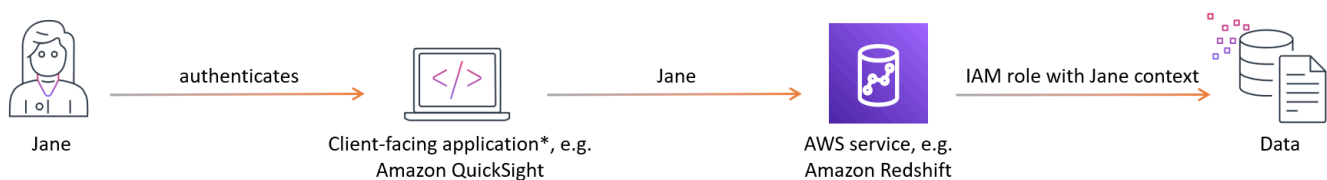
2. Verbinden Sie das AWS-Services in Ihrem Anwendungsfall mit IAM Identity Center — AWS-Service Im Anwendungsfall „Vertrauenswürdige Identitätsverbreitung“ folgt der Administrator der jeweiligen Dienste den Anweisungen in der jeweiligen Servicedokumentation, um den Dienst mit IAM Identity Center zu verbinden.

Note

Wenn es sich bei Ihrem Anwendungsfall um eine Drittanbieter - oder Kundenanwendung handelt, aktivieren Sie die Verbreitung vertrauenswürdiger Identitäten, indem Sie eine Vertrauensbeziehung zwischen dem Identitätsanbieter, der die Anwendungsbenutzer authentifiziert, und IAM Identity Center konfigurieren. Auf diese Weise kann Ihre Anwendung den zuvor beschriebenen Ablauf der Weitergabe vertrauenswürdiger Identitäten nutzen. Weitere Informationen finden Sie unter [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#).

So funktioniert die Propagierung vertrauenswürdiger Identitäten

Das folgende Diagramm zeigt den allgemeinen Workflow für die Verbreitung vertrauenswürdiger Identitäten:



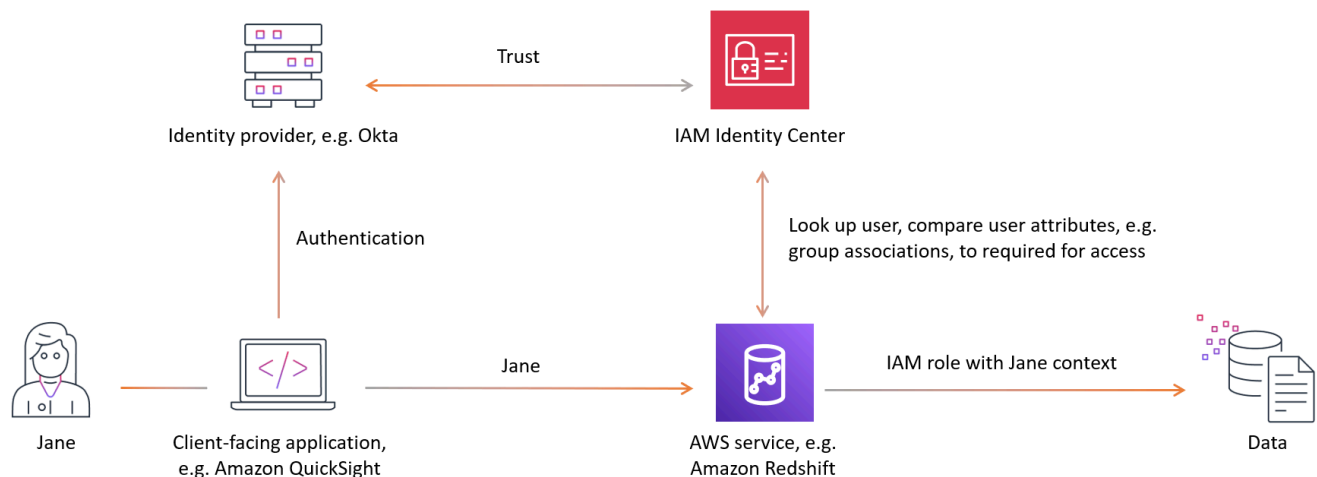
1. Benutzer authentifizieren sich mit einer clientseitigen Anwendung, z. B. Quick.
2. Die clientseitige Anwendung fordert den Zugriff zur Verwendung und zur Abfrage von Daten AWS-Service an und enthält Informationen über den Benutzer.

Note

Einige Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten beinhalten Tools, die AWS-Services mithilfe von Servicetreibern interagieren. Ob dies auf Ihren Anwendungsfall zutrifft, erfahren Sie in der Anleitung zum [Anwendungsfall](#).

3. Das AWS-Service überprüft die Benutzeridentität mit IAM Identity Center und vergleicht die Benutzerattribute, wie z. B. ihre Gruppenzuordnungen, mit denen, die für den Zugriff erforderlich sind. Der AWS-Service autorisiert den Zugriff, solange der Benutzer oder seine Gruppe über die erforderlichen Berechtigungen verfügt.
4. AWS-Services kann die Benutzererkennung in AWS CloudTrail und in ihren Serviceprotokollen protokollieren. Einzelheiten finden Sie in der Servicedokumentation.

Die folgende Abbildung bietet einen Überblick über die zuvor beschriebenen Schritte im Workflow zur Verbreitung vertrauenswürdiger Identitäten:



Themen

- [Voraussetzungen und Überlegungen](#)
- [Anwendungsfälle für vertrauenswürdige Identitätsverbreitung](#)
- [Autorisierungsdienste](#)

Voraussetzungen und Überlegungen

Bevor Sie die Verbreitung vertrauenswürdiger Identitäten einrichten, sollten Sie sich mit den folgenden Voraussetzungen und Überlegungen vertraut machen.

Themen

- [Voraussetzungen](#)
- [Überlegungen](#)
- [Überlegungen zu vom Kunden verwalteten Anwendungen](#)

Voraussetzungen

Um die Propagierung vertrauenswürdiger Identitäten zu verwenden, stellen Sie sicher, dass Ihre Umgebung die folgenden Voraussetzungen erfüllt:

- IAM Identity Center aktivieren und bereitstellen
 - Um die Verbreitung vertrauenswürdiger Identitäten zu verwenden, müssen Sie IAM Identity Center an derselben AWS-Region Stelle aktivieren, an der die AWS Anwendungen und Dienste aktiviert sind, auf die Ihre Benutzer zugreifen werden. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).
 - Die IAM Identity Center Organization-Instanz wird empfohlen — Wir empfehlen Ihnen, eine [Organisationsinstanz](#) von IAM Identity Center zu verwenden, die Sie im Verwaltungskonto von aktivieren. AWS Organizations Sie können die Verwaltung einer Organisationsinstanz [von IAM Identity Center an ein Mitgliedskonto](#) delegieren. Wenn Sie eine [Kontoinstanz](#) von IAM Identity Center auswählen, muss sich alles AWS-Services , worauf Benutzer mithilfe der vertrauenswürdigen Identitätsverbreitung zugreifen sollen, an derselben AWS-Konto Stelle befinden, an der Sie IAM Identity Center aktivieren. Weitere Informationen finden Sie unter [Konto-Instances von IAM Identity Center](#).
 - Verbinden Sie Ihren vorhandenen Identitätsanbieter mit IAM Identity Center und stellen Sie Ihre Benutzer und Gruppen im IAM Identity Center bereit. Weitere Informationen finden Sie unter [Tutorials zu Identitätsquellen im IAM Identity Center](#).
- Verbinden Sie die AWS verwalteten Anwendungen und Dienste in Ihrem Anwendungsfall für vertrauenswürdige Identitätsverbreitung mit IAM Identity Center. Um die Verbreitung vertrauenswürdiger Identitäten nutzen zu können, müssen AWS verwaltete Anwendungen mit dem IAM Identity Center verbunden sein.

Überlegungen

Beachten Sie bei der Konfiguration und Verwendung von Trusted Identity Propagation die folgenden Überlegungen:

- Organisations- und Kontoinstanz von IAM Identity Center
 - Eine [Organisationsinstanz](#) von IAM Identity Center bietet Ihnen die größtmögliche Kontrolle und Flexibilität, um Ihre Anwendungsfälle auf mehrere Benutzer und AWS-Konten auszudehnen. AWS-Services Wenn Sie eine Organisationsinstanz nicht verwenden können, wird Ihr Anwendungsfall möglicherweise mit Kontoinstanzen von IAM Identity Center unterstützt. Weitere

Informationen darüber, welche Kontoinstanzen von IAM Identity Center AWS-Services in Ihrem Anwendungsfall unterstützen, finden Sie unter. [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#)

- Multi-account Berechtigungen (Berechtigungssätze) sind nicht erforderlich
- Für die Weitergabe vertrauenswürdiger Identitäten müssen Sie keine Berechtigungen für [mehrere Konten](#) (Berechtigungssätze) einrichten. Sie können IAM Identity Center aktivieren und es nur für die Weitergabe vertrauenswürdiger Identitäten verwenden.

Überlegungen zu vom Kunden verwalteten Anwendungen

Ihre Mitarbeiter können von der Verbreitung vertrauenswürdiger Identitäten profitieren, selbst wenn Ihre Benutzer mit kundenseitigen Anwendungen interagieren, die beispielsweise Tableau nicht von AWS Ihren speziell entwickelten Anwendungen verwaltet werden. Die Benutzer dieser Anwendungen werden möglicherweise nicht im IAM Identity Center bereitgestellt. Um die reibungslose Erkennung und Autorisierung des Benutzerzugriffs auf AWS Ressourcen zu ermöglichen, können Sie mit IAM Identity Center eine vertrauenswürdige Beziehung zwischen dem Identitätsanbieter, der Ihre Benutzer authentifiziert, und IAM Identity Center konfigurieren. Weitere Informationen finden Sie unter [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#).

Darüber hinaus erfordert die Konfiguration der Verbreitung vertrauenswürdiger Identitäten für Ihre Anwendung:

- Ihre Anwendung muss das OAuth 2.0-Framework für die Authentifizierung verwenden. Die Verbreitung vertrauenswürdiger Identitäten unterstützt keine SAML 2.0-Integrationen.
- Ihre Anwendung muss vom IAM Identity Center erkannt werden. Folgen Sie den für Ihren [Anwendungsfall](#) spezifischen Anweisungen.

Anwendungsfälle für vertrauenswürdige Identitätsverbreitung

Als IAM Identity Center-Administrator werden Sie möglicherweise gebeten, bei der Konfiguration der vertrauenswürdigen Identitätsweitergabe von benutzerseitigen Anwendungen zu helfen. AWS-Services Zur Unterstützung dieser Anfrage benötigen Sie die folgenden Informationen:

- Mit welcher kundenseitigen Anwendung werden Ihre Benutzer interagieren?
- Welche AWS-Services werden verwendet, um die Daten abzufragen und den Zugriff auf die Daten zu autorisieren?

- Was AWS-Service autorisiert den Zugriff auf die Daten?

Ihre Aufgabe bei der Aktivierung von Anwendungsfällen zur Verbreitung vertrauenswürdiger Identitäten, an denen keine Anwendungen von Drittanbietern oder speziell entwickelte Anwendungen beteiligt sind, besteht darin,

1. [Aktivieren Sie IAM Identity Center.](#)
2. [Verbinden Sie Ihre bestehende Identitätsquelle mit dem IAM Identity Center.](#)

Die verbleibenden Schritte der Konfiguration der vertrauenswürdigen Identität für diese Anwendungsfälle werden innerhalb der verbundenen Geräte AWS-Services und Anwendungen ausgeführt. Umfassende dienstspezifische Anleitungen finden die Administratoren der verbundenen Geräte AWS-Services oder Anwendungen in den jeweiligen Benutzerhandbüchern.

Ihre Rolle bei der Aktivierung von Anwendungsfällen zur Verbreitung vertrauenswürdiger Identitäten, an denen Drittanbieteranwendungen oder speziell entwickelte Anwendungen beteiligt sind, umfasst die Schritte [zum Verbinden Ihrer Identitätsquelle](#) sowie die folgenden Schritte: [IAM Identity Center aktivieren](#)

1. Konfiguration der Verbindung Ihres Identitätsanbieters (IdP) zur Drittanbieter- oder kundenspezifischen Anwendung.
2. Aktivieren Sie IAM Identity Center, um die Drittanbieteranwendung oder die speziell entwickelte Anwendung zu erkennen.
3. Konfiguration Ihres IdP als vertrauenswürdigen Token-Aussteller im IAM Identity Center. Weitere Informationen finden Sie unter [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#).

Umfassende dienstspezifische Anleitungen finden die Administratoren der verbundenen Anwendungen in den jeweiligen Benutzerhandbüchern. AWS-Services

Anwendungsfälle in den Bereichen Analytik, Data Lakehouse und maschinelles Lernen

Mit den folgenden Analyse- und Machine-Learning-Diensten können Sie Anwendungsfälle für vertrauenswürdige Propagierung aktivieren:

- Amazon Redshift — Anleitungen finden Sie unter [Vertrauenswürdige Identitätsverbreitung mit Amazon Redshift](#).

- Amazon EMR — Anleitungen finden Sie unter. [Vertrauenswürdige Identitätsverbreitung mit Amazon EMR](#)
- Amazon Athena — Anleitungen finden Sie unter. [Vertrauenswürdige Identitätsverbreitung mit Amazon Athena](#)
- SageMaker Studio — Eine Anleitung finden Sie unter [Vertrauenswürdige Identitätsverbreitung mit Amazon Studio SageMaker](#).

Zusätzliche Anwendungsfälle

Sie können IAM Identity Center und die Verbreitung vertrauenswürdiger Identitäten mit folgenden zusätzlichen AWS-Services Funktionen aktivieren:

- Amazon Q Business — Anleitungen finden Sie unter:
 - [Admin-Workflow für Apps, die IAM Identity Center](#) verwenden.
 - [Konfiguration einer Amazon Q Business-Anwendung mithilfe von IAM Identity Center](#).
 - [Konfigurieren Sie Amazon Q Business mit der Verbreitung vertrauenswürdiger Identitäten im IAM Identity Center](#).
- Amazon OpenSearch Service — Anleitungen finden Sie unter:
 - [Unterstützung für Trusted Identity Propagation durch IAM Identity Center für Amazon OpenSearch Service](#).
 - [Zentralisierte OpenSearch Benutzeroberfläche \(Dashboards\) mit Amazon OpenSearch Service](#).
- AWS Transfer Family— Anleitungen finden Sie unter:
 - [Übertragen Sie die Web-Apps der Familie](#).

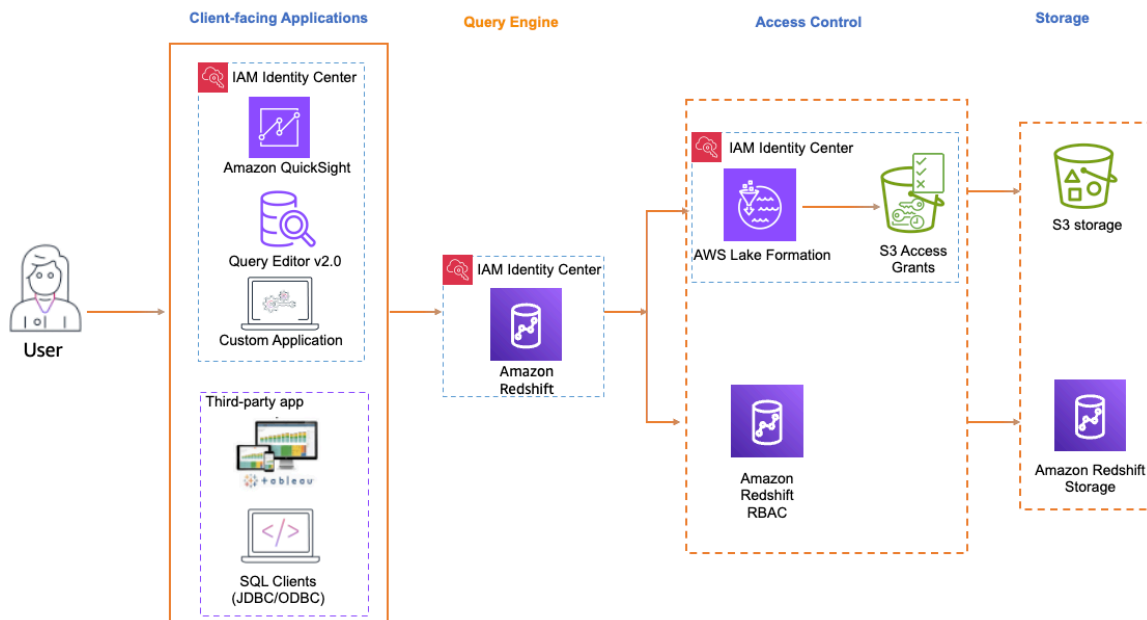
Themen

- [Vertrauenswürdige Identitätsverbreitung mit Amazon Redshift](#)
- [Vertrauenswürdige Identitätsverbreitung mit Amazon EMR](#)
- [Vertrauenswürdige Identitätsverbreitung mit Amazon Athena](#)
- [Vertrauenswürdige Identitätsverbreitung mit Amazon Studio SageMaker](#)

Vertrauenswürdige Identitätsverbreitung mit Amazon Redshift

Die Schritte zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten hängen davon ab, ob Ihre Benutzer mit AWS verwalteten Anwendungen oder mit vom Kunden verwalteten

Anwendungen interagieren. Das folgende Diagramm zeigt eine Konfiguration für vertrauenswürdige Identitätsverbreitung für clientseitige Anwendungen — entweder AWS verwaltet oder extern AWS —, die Amazon Redshift-Daten abfragen, wobei die Zugriffskontrolle entweder von Amazon Redshift oder von Autorisierungsdiensten wie AWS Lake Formation Amazon S3 bereitgestellt wird. Access Grants



Wenn die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift aktiviert ist, können Redshift-Administratoren Redshift so konfigurieren, dass [automatisch Rollen](#) für IAM Identity Center als Identitätsanbieter erstellt werden, Redshift-Rollen Gruppen im IAM Identity Center zugeordnet werden und mithilfe [der rollenbasierten Zugriffskontrolle von Redshift Zugriff gewährt wird](#).

Unterstützte Anwendungen mit Kundenkontakt

AWS verwaltete Anwendungen

Die folgenden AWS verwalteten, kundenseitigen Anwendungen unterstützen die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift:

- [Amazon Redshift Query Editor V2](#)
- [Schnell](#)

 Note

Wenn Sie Amazon Redshift Spectrum für den Zugriff auf externe Datenbanken oder Tabellen verwenden, sollten Sie in Betracht ziehen AWS Glue Data Catalog, [Lake Formation](#) und [Amazon S3 einzurichten, Access Grants](#) um eine präzise Zugriffskontrolle zu ermöglichen.

Vom Kunden verwaltete Anwendungen

Die folgenden vom Kunden verwalteten Anwendungen unterstützen die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift:

- Tableaueinschließlich Tableau Desktop TableauServer, und Tableau Prep
 - Informationen zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten für Benutzer von Tableau finden Sie [im AWS Big Data-Blog unter](#) Integration Tableau und Okta mit Amazon Redshift mithilfe von IAM Identity Center.
- SQL-Clients (DBEaverund) DBVisualizer
 - Informationen zum Aktivieren der vertrauenswürdigen Identitätsverbreitung für Benutzer von SQL-Clients (DBEaverundDBVisualizer) finden Sie im AWS Big Data-Blog unter [Integrate Identity Provider \(IdP\) with Amazon Redshift Query Editor V2 and SQL Client using IAM Identity Center for Seamless Single Sign-On](#).

Einrichtung der Weitergabe vertrauenswürdiger Identitäten mit Amazon Redshift Query Editor V2

Im folgenden Verfahren erfahren Sie, wie Sie eine vertrauenswürdige Identitätsweitergabe von Amazon Redshift Query Editor V2 an Amazon Redshift erreichen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie Folgendes einrichten:

1. [Aktivieren Sie IAM Identity Center. Eine Organisationsinstanz](#) wird empfohlen. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).
2. [Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit](#).

Die Aktivierung der Weitergabe vertrauenswürdiger Identitäten umfasst Aufgaben, die von einem IAM Identity Center-Administrator in der IAM Identity Center-Konsole ausgeführt werden, sowie Aufgaben, die von einem Amazon Redshift-Administrator in der Amazon Redshift-Konsole ausgeführt werden.

Aufgaben, die vom IAM Identity Center-Administrator ausgeführt werden

Die folgenden Aufgaben mussten vom IAM Identity Center-Administrator ausgeführt werden:

1. Erstellen Sie eine [IAM-Rolle](#) in dem Konto, in dem der Amazon Redshift-Cluster oder die Serverless-Instance vorhanden ist, mit der folgenden Berechtigungsrichtlinie. Weitere Informationen finden Sie unter Erstellung von [IAM-Rollen](#).
- Die folgenden Richtlinienbeispiele enthalten die erforderlichen Berechtigungen, um dieses Tutorial abzuschließen. Um diese Richtlinie zu verwenden, ersetzen Sie die Richtlinie *italicized placeholder text* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie [erstellen](#) oder Richtlinie [bearbeiten](#).

Genehmigungsrichtlinie:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
ID",
```

```

        "arn:aws:sso::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
    ]
}

```

Vertrauensrichtlinie:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

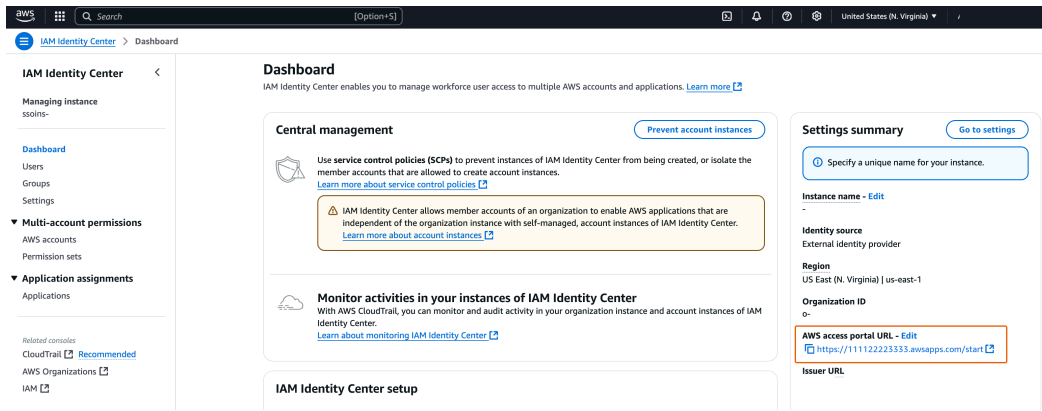
2. Erstellen Sie einen Berechtigungssatz in dem AWS Organizations Verwaltungskonto, in dem IAM Identity Center aktiviert ist. Sie werden es im nächsten Schritt verwenden, um Verbundbenutzern den Zugriff auf Redshift Query Editor V2 zu ermöglichen.
 - a. Gehen Sie zur IAM Identity Center-Konsole und wählen Sie unter Multi-Account Berechtigungen die Option Berechtigungssätze aus.
 - b. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
 - c. Wählen Sie Benutzerdefinierter Berechtigungssatz und dann Weiter aus.

- d. Wählen Sie unter AWS Verwaltete Richtlinien die Option **AmazonRedshiftQueryEditorV2ReadSharing**.
- e. Fügen Sie unter Inline-Richtlinie die folgende Richtlinie hinzu:

JSON

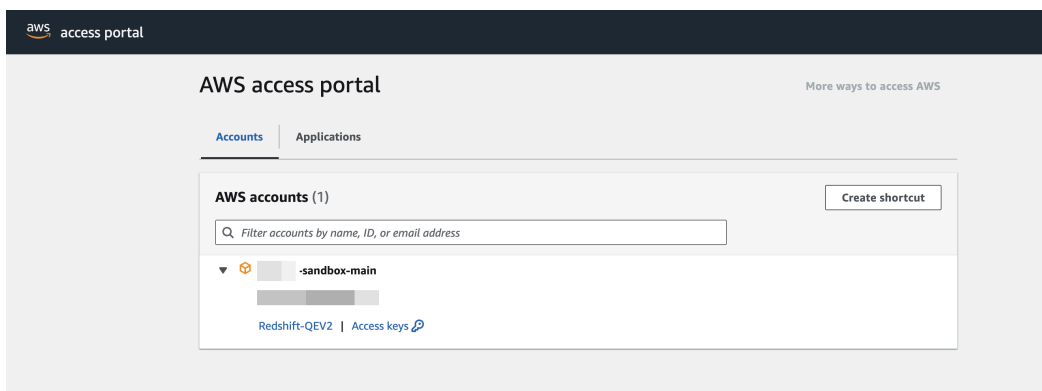
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}
```

- f. Wählen Sie Weiter aus und geben Sie dann einen Namen für den Berechtigungssatznamen ein. Beispiel, **Redshift-Query-Editor-V2**.
- g. Legen Sie unter Relay-Status — optional den Standard-Relay-Status auf die URL des Abfrage-Editors V2 fest. Verwenden Sie dazu das Format: `https://your-region.console.aws.amazon.com/sqlworkbench/home`.
- h. Überprüfen Sie die Einstellungen und wählen Sie Erstellen.
- i. Navigieren Sie zum IAM Identity Center Dashboard und kopieren Sie die URL des AWS Zugriffsportals aus dem Abschnitt Einstellungsübersicht.



- j. Öffnen Sie ein neues Inkognito-Browserfenster und fügen Sie die URL ein.

Dadurch gelangen Sie zu Ihrem AWS Zugriffsportal und stellen sicher, dass Sie sich mit einem IAM Identity Center-Benutzer anmelden.



Weitere Informationen zum Berechtigungssatz finden Sie unter [Verwalten AWS-Konten mit Berechtigungssätzen](#).

3. Ermöglichen Sie Verbundbenutzern den Zugriff auf Redshift Query Editor V2.
 - a. Öffnen Sie im AWS Organizations Verwaltungskonto die IAM Identity Center-Konsole.
 - b. Wählen Sie im Navigationsbereich unter Multi-account Berechtigungen die Option AWS-Konten.
 - c. Wählen Sie auf der AWS-Konten Seite AWS-Konto die aus, der Sie Zugriff gewähren möchten.
 - d. Wählen Sie Benutzer oder Gruppen zuweisen aus.
 - e. Wählen Sie auf der Seite Benutzer und Gruppen zuweisen die Benutzer und/oder Gruppen aus, für die Sie den Berechtigungssatz erstellen möchten. Wählen Sie anschließend Weiter.
 - f. Wählen Sie auf der Seite „Berechtigungssätze zuweisen“ den Berechtigungssatz aus, den Sie im vorherigen Schritt erstellt haben. Wählen Sie anschließend Weiter.

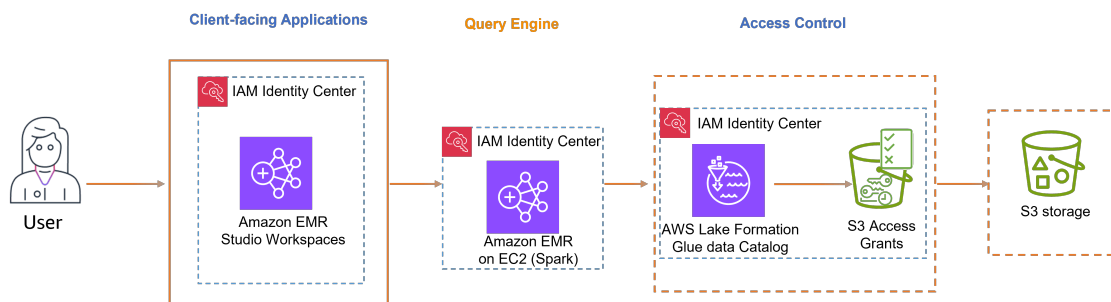
- g. Überprüfen Sie auf der Seite „Aufgaben überprüfen und einreichen“ Ihre Auswahl und wählen Sie **Senden** aus.

Aufgaben, die von einem Amazon Redshift-Administrator ausgeführt werden

Um die Weitergabe vertrauenswürdiger Identitäten an Amazon Redshift zu aktivieren, muss ein Amazon Redshift-Cluster-Administrator oder Amazon Redshift Serverless-Administrator eine Reihe von Aufgaben in der Amazon Redshift-Konsole ausführen. Weitere Informationen finden Sie im [Big Data-Blog unter Integrieren von Identity Provider \(IdP\) mit Amazon Redshift Query Editor V2 und SQL Client mithilfe von IAM Identity Center for Seamless Single. Sign-On](#) [AWS](#)

Vertrauenswürdige Identitätsverbreitung mit Amazon EMR

Das folgende Diagramm zeigt eine Konfiguration der vertrauenswürdigen Identitätsverbreitung für Amazon EMR Studio unter Verwendung von Amazon EMR auf Amazon EC2 mit Zugriffskontrolle durch AWS Lake Formation Amazon S3. Access Grants



Unterstützte Anwendungen mit Kundenkontakt

- Amazon EMR Studio

Gehen Sie folgendermaßen vor, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren:

- [Richten Sie Amazon EMR Studio](#) als clientseitige Anwendung für den Amazon EMR-Cluster ein.
- Richten Sie [Amazon EMR Cluster auf Amazon EC2 mit ein. Apache Spark](#)
- Empfohlen: [AWS Lake Formation](#) und [Amazon S3 Access Grants](#), um eine detaillierte Zugriffskontrolle für AWS Glue Data Catalog und die zugrunde liegenden Datenspeicherorte in S3 zu ermöglichen.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit Amazon EMR Studio

Das folgende Verfahren führt Sie durch die Einrichtung von Amazon EMR Studio für die Verbreitung vertrauenswürdiger Identitäten bei Abfragen laufender Amazon Athena-Arbeitsgruppen oder Amazon EMR-Cluster. Apache Spark

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie Folgendes einrichten:

1. [Aktivieren Sie IAM Identity Center](#). [Eine Organisationsinstanz](#) wird empfohlen. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).
2. [Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit](#).

Um die Einrichtung der vertrauenswürdigen Identitätsverbreitung von Amazon EMR Studio aus abzuschließen, muss der EMR Studio-Administrator die folgenden Schritte ausführen.

Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio

In diesem Schritt erstellt der Amazon Studio EMR-Administrator eine IAM-Servicerolle und eine IAM-Benutzerrolle für EMR. Studio

1. [Erstellen Sie eine EMR Studio-Servicerolle](#) — EMR Studio übernimmt diese IAM-Rolle, um Arbeitsbereiche und Notebooks sicher zu verwalten, Verbindungen zu Clustern herzustellen und Dateninteraktionen abzuwickeln.
 - a. Navigieren Sie zur IAM-Konsole (<https://console.aws.amazon.com/iam/>) und erstellen Sie eine IAM-Rolle.
 - b. Wählen Sie AWS-Service als vertrauenswürdige Entität aus und wählen Sie dann Amazon EMR. Fügen Sie die folgenden Richtlinien hinzu, um die Berechtigungen und das Vertrauensverhältnis der Rolle zu definieren.

Um diese Richtlinie zu verwenden, ersetzen Sie die Richtlinie *italicized placeholder text* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie [erstellen](#) oder Richtlinie [bearbeiten](#).

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ObjectActions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "Your-AWS-Account-ID"
      }
    }
  },
  {
    "Sid": "BucketActions",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetEncryptionConfiguration"
    ],
    "Resource": [
      "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "Your-AWS-Account-ID"
      }
    }
  }
]
}

```

Eine Referenz aller Servicerollenberechtigungen finden Sie unter [EMR Studio-Servicerollenberechtigungen](#).

2. [Erstellen Sie eine EMR Studio-Benutzerrolle für die IAM Identity Center-Authentifizierung](#) — EMR Studio übernimmt diese Rolle, wenn sich ein Benutzer über IAM Identity Center anmeldet,

um Workspaces, EMR-Cluster, Jobs und Git-Repositorys zu verwalten. Diese Rolle wird verwendet, um den Workflow zur Verbreitung vertrauenswürdiger Identitäten zu initiieren.

Note

Die EMR Studio-Benutzerrolle muss keine Berechtigungen für den Zugriff auf die Amazon S3-Speicherorte der Tabellen im AWS Glue Katalog enthalten. AWS Lake Formation Berechtigungen und registrierte See-Standorte werden verwendet, um temporäre Berechtigungen zu erhalten.

Die folgende Beispielrichtlinie kann in einer Rolle verwendet werden, die es einem Benutzer von EMR Studio ermöglicht, Athena-Arbeitsgruppen zum Ausführen von Abfragen zu verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],

```

```

        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                "ec2:CreateAction": "CreateSecurityGroup"
            }
        },
        {
            "Sid": "AllowSecretManagerListSecrets",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:CreateSecret",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
                }
            }
        },
        {
            "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
            "Effect": "Allow",
            "Action": "secretsmanager:TagResource",
            "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
        },
        {
            "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
            ],
            "Effect": "Allow"
        },
    ],

```

```

    {
      "Sid": "AllowS3ListAndLocationPermissions",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*",
      "Effect": "Allow"
    },
    {
      "Sid": "AllowS3ReadOnlyAccessToLogs",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowAthenaQueryExecutions",
      "Effect": "Allow",
      "Action": [
        "athena:StartQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StopQueryExecution",
        "athena:ListQueryExecutions",
        "athena:GetQueryResultsStream",
        "athena:ListWorkGroups",
        "athena:GetWorkGroup",
        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena>DeletePreparedStatement"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowGlueSchemaManipulations",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",

```

```

        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowQueryEditorToAccessWorkGroup",
    "Effect": "Allow",
    "Action": "athena:GetWorkGroup",
    "Resource": "arn:aws:athena:*:111122223333:workgroup*"
},
{
    "Sid": "AllowConfigurationForWorkspaceCollaboration",
    "Action": [
        "elasticmapreduce:UpdateEditor",
        "elasticmapreduce:PutWorkspaceAccess",
        "elasticmapreduce>DeleteWorkspaceAccess",
        "elasticmapreduce:ListWorkspaceAccessIdentities"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
        }
    }
},
{
    "Sid": "DescribeNetwork",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "ListIAMRoles",
    "Effect": "Allow",

```

```
        "Action": [
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AssumeRole",
        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole"
        ],
        "Resource": "*"
    }
]
```

Die folgende Vertrauensrichtlinie ermöglicht es EMR Studio, die Rolle zu übernehmen:

 Note

Für die Nutzung von EMR Studio Workspaces und EMR Notebooks sind zusätzliche Berechtigungen erforderlich. Weitere Informationen finden [Sie unter Erstellen von Berechtigungsrichtlinien für EMR Studio-Benutzer](#).

Weitere Informationen finden Sie unter den folgenden Links:

- [Benutzerdefinierte IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien definieren](#)
- [Berechtigungen für EMR Studio-Servicerollen](#)

Schritt 2. Erstellen und konfigurieren Sie Ihr EMR Studio

In diesem Schritt erstellen Sie ein Amazon EMR Studio in der EMR Studio-Konsole und verwenden die IAM-Rollen, in denen Sie erstellt haben. [Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio](#)

1. Navigieren Sie zur EMR Studio-Konsole, wählen Sie **Create Studio** und die Option **Custom Setup** aus. Sie können entweder einen neuen S3-Bucket erstellen oder einen vorhandenen Bucket verwenden. Sie können das Kästchen zum **Verschlüsseln von Workspace-Dateien** mit

Ihren eigenen KMS-Schlüsseln ☐ ankreuzen. Weitere Informationen finden Sie unter [AWS Key Management Service](#).

Create a Studio [Info](#)

Setup options [Info](#)

☐ Interactive workloads ☐ Batch jobs ☒ Custom

Studio settings [Info](#)

Studio name

Studio_1

Use up to 256 characters (alphanumeric, hyphens, or underscores).

Description - optional

The description below will be visible to your studio teams.

Describe the Studio

256 characters maximum

S3 location for Workspace storage

Specify an Amazon S3 location where Workspace work will be saved.

☒ Create new bucket ☐ Select existing location

We'll create a new bucket and use the location `s3://aws-emr-studio-225989353012-us-east-1/1735848818523`.

☐ Encrypt Workspace files with your own AWS KMS key

EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation.

- Wählen Sie unter **Servicerolle**, damit Studio auf Ihre Ressourcen zugreifen kann, die in erstellte Servicerolle [Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio](#) aus dem Menü aus.
- Wählen Sie unter **Authentifizierung** die Option **IAM Identity Center** aus. Wählen Sie die Benutzerrolle aus, die in [Schritt 1. Erstellen Sie die erforderlichen IAM-Rollen für EMR Studio](#) erstellt wurde.

Service role to let Studio access your AWS resources

AmazonEMRStudio_ [View permission details](#)

Authentication [Info](#)

Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)

Authenticate with single sign-on using IAM identity federation or IAM credentials.

☒ IAM Identity Center (AWS Single Sign-On)

Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

User role

Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#).

emrstudio-userrole-idx [Create IAM role](#)

Connect EMR Studio to IAM Identity Center

Instance of IAM Identity Center

Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

[iam:aws:sso::instance/ssolsins-](#)

- Markieren Sie das Kästchen **Vertrauenswürdige Identitätsweitergabe**. Wählen Sie im Abschnitt **Anwendungszugriff** die Option **Nur zugewiesene Benutzer und Gruppen** aus. Dadurch können Sie nur autorisierten Benutzern und Gruppen den Zugriff auf dieses Studio gewähren.
- (Optional) — Sie können VPC und Subnetz konfigurieren, wenn Sie dieses Studio mit EMR-Clustern verwenden.

Trusted identity propagation [Info](#)
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

Application access [Info](#)
Choose who can access your application
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ **All users and groups**
Any user or group from your IAM Identity Center directory can access this application.

▼ Networking and security - optional

VPC [Info](#)
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

Subnets [Info](#)
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

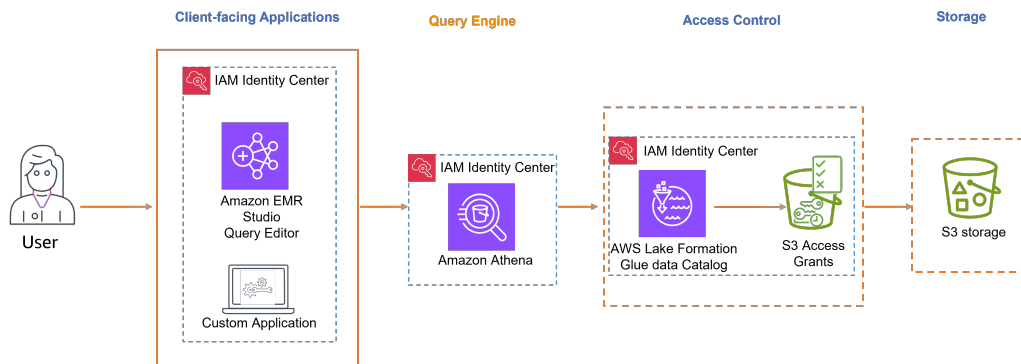
6. Überprüfen Sie alle Details und wählen Sie **Create Studio** aus.
7. Melden Sie sich nach der Konfiguration eines Athena WorkGroup - oder EMR-Clusters bei der Studio-URL an, um:
 - a. Führen Sie Athena-Abfragen mit dem Abfrage-Editor aus.
 - b. Führen Sie Spark-Jobs im Workspace mithilfe von Jupyter Notebook aus.

Vertrauenswürdige Identitätsverbreitung mit Amazon Athena

Die Schritte zur Aktivierung der Verbreitung vertrauenswürdiger Identitäten hängen davon ab, ob Ihre Benutzer mit AWS verwalteten Anwendungen oder mit vom Kunden verwalteten Anwendungen interagieren. Das folgende Diagramm zeigt eine Konfiguration für vertrauenswürdige Identitätsverbreitung für clientseitige Anwendungen — entweder AWS verwaltet oder extern AWS —, die Amazon Athena zur Abfrage von Amazon S3-Daten verwendet, wobei die Zugriffskontrolle von Amazon S3 bereitgestellt wird AWS Lake Formation . Access Grants

Note

- Für die vertrauenswürdige Identitätsverbreitung mit Amazon Athena ist die Verwendung von Trino erforderlich.
- Apache Spark- und SQL-Clients, die über ODBC- und JDBC-Treiber mit Amazon Athena verbunden sind, werden nicht unterstützt.



AWS verwaltete Anwendungen

Die folgende AWS verwaltete, clientseitige Anwendung unterstützt die Verbreitung vertrauenswürdiger Identitäten mit Athena:

- Amazon EMR Studio

Gehen Sie folgendermaßen vor, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren:

- [Richten Sie Amazon EMR Studio](#) als clientseitige Anwendung für Athena ein. Der Abfrage-Editor in EMR Studio wird benötigt, um Athena-Abfragen auszuführen, wenn die Weitergabe vertrauenswürdiger Identitäten aktiviert ist.
- [Richten Sie Athena Workgroup ein.](#)
- [Richten Sie es ein AWS Lake Formation](#), um eine detaillierte Zugriffskontrolle für AWS Glue Tabellen auf der Grundlage des Benutzers oder der Gruppe im IAM Identity Center zu ermöglichen.
- [Richten Sie Amazon S3 ein Access Grants](#), um den temporären Zugriff auf die zugrunde liegenden Datenspeicherorte in S3 zu ermöglichen.

Note

Sowohl Lake Formation als auch Amazon S3 Access Grants sind für die Zugriffskontrolle auf AWS Glue Data Catalog und für Athena-Abfrageergebnisse in Amazon S3 erforderlich.

Vom Kunden verwaltete Anwendungen

Informationen zur Aktivierung der Weitergabe vertrauenswürdiger Identitäten für Benutzer benutzerdefinierter Anwendungen finden Sie [im Sicherheitsblog](#) unter AWS-Services Programmgesteuertes Verwenden der AWS Weitergabe vertrauenswürdiger Identitäten.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit Amazon Athena-Arbeitsgruppen

Das folgende Verfahren führt Sie durch die Einrichtung von Amazon Athena-Arbeitsgruppen für die Weitergabe vertrauenswürdiger Identitäten.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie Folgendes einrichten:

1. [Aktivieren Sie IAM Identity Center](#). [Eine Organisationsinstanz](#) wird empfohlen. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).
2. [Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit](#).
3. Für diese Konfiguration sind [Amazon EMR Studio](#) und [Amazon S3 AWS Lake Formation Access Grants erforderlich](#).

Einrichtung einer vertrauenswürdigen Identitätsverbreitung mit Athena

Um die Verbreitung vertrauenswürdiger Identitäten mit Athena einzurichten, muss der Athena-Administrator:

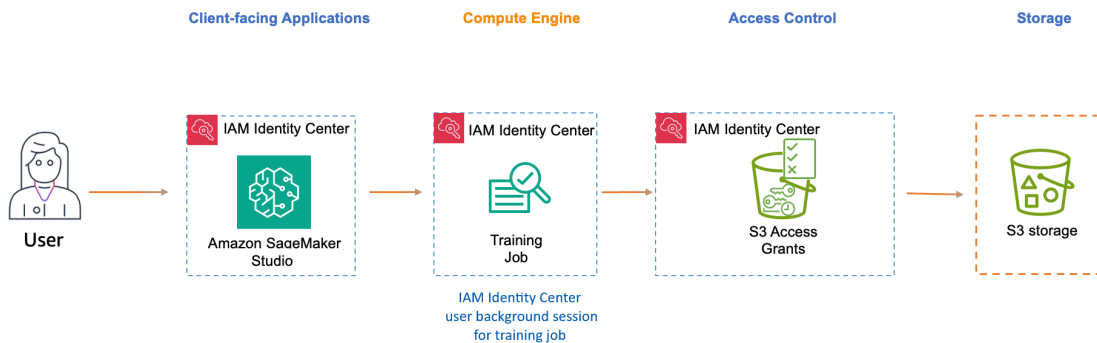
1. Lesen Sie die [Überlegungen und Einschränkungen bei der Verwendung von IAM Identity Center-fähigen Athena-Arbeitsgruppen](#).
2. [Erstellen Sie eine IAM Identity Center-fähige Athena-Arbeitsgruppe](#).

Vertrauenswürdige Identitätsverbreitung mit Amazon Studio SageMaker

[Amazon SageMaker Studio ist in IAM Identity Center](#) integriert und unterstützt [Benutzersitzungen im Hintergrund](#) sowie die Verbreitung vertrauenswürdiger Identitäten. Benutzersitzungen im Hintergrund ermöglichen es einem Benutzer, einen Job mit langer Laufzeit in SageMaker Studio zu initiieren, ohne dass dieser Benutzer angemeldet bleiben muss, während der Job ausgeführt wird. Der Job wird sofort und im Hintergrund ausgeführt, wobei die Berechtigungen des Benutzers verwendet werden, der den Job initiiert hat. Der Job kann auch dann weiter ausgeführt werden, wenn der Benutzer seinen Computer ausschaltet, seine IAM Identity Center-Anmeldesitzung abläuft oder der

Benutzer sich vom AWS Access Portal abmeldet. Die Standardsitzungsdauer für Benutzersitzungen im Hintergrund beträgt 7 Tage, Sie können jedoch eine maximale Dauer von 90 Tagen angeben. Trusted Identity Propagation ermöglicht einen fein abgestuften Zugriff auf AWS Ressourcen wie Amazon S3-Buckets auf der Grundlage der Benutzeridentität oder Gruppenmitgliedschaft.

Das folgende Diagramm zeigt eine Konfiguration für die Verbreitung vertrauenswürdiger Identitäten für SageMaker Studio mit Zugriff auf Daten, die in einem Amazon S3-Bucket gespeichert sind. Benutzersitzungen im Hintergrund sind für IAM Identity Center aktiviert, sodass der SageMaker Studio-Trainingsjob im Hintergrund ausgeführt werden kann. Die Zugriffskontrolle für die Trainingsdaten wird von Amazon S3 Access Grants bereitgestellt.



AWS verwaltete Anwendung

Die folgende AWS verwaltete, clientseitige Anwendung unterstützt die Verbreitung vertrauenswürdiger Identitäten:

- [Amazon Studio SageMaker](#)

Gehen Sie wie folgt vor, um die Verbreitung vertrauenswürdiger Identitäten und Benutzersitzungen im Hintergrund zu aktivieren:

- [Richten Sie SageMaker Studio als clientseitige Anwendung ein.](#)
- [Richten Sie Amazon S3 ein Access Grants](#), um den temporären Zugriff auf die zugrunde liegenden Datenspeicherorte in Amazon S3 zu ermöglichen.

Einrichtung der Verbreitung vertrauenswürdiger Identitäten mit SageMaker Studio

Das folgende Verfahren führt Sie Schritt für Schritt durch die Einrichtung von SageMaker Studio für vertrauenswürdige Identitäten und Hintergrund Sitzungen für Benutzer.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie die folgenden Aufgaben erledigen:

1. [Aktivieren Sie IAM Identity Center](#). Eine Organisationsinstanz ist erforderlich. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).
2. [Stellen Sie die Benutzer und Gruppen aus Ihrer Identitätsquelle im IAM Identity Center bereit](#).
3. [Vergewissern Sie sich, dass Benutzersitzungen im Hintergrund](#) in der IAM Identity Center-Konsole aktiviert sind. Standardmäßig sind Benutzer-Hintergrundsitzungen aktiviert und die Sitzungsdauer ist auf 7 Tage festgelegt. Sie können diese Dauer ändern.

Um die Weitergabe vertrauenswürdiger Identitäten von SageMaker Studio aus einzurichten, muss der SageMaker Studio-Administrator die folgenden Schritte ausführen.

Schritt 1: Aktivieren Sie die Weitergabe vertrauenswürdiger Identitäten in einer neuen oder vorhandenen SageMaker Studio-Domäne

SageMaker Studio verwendet Domänen, um Benutzerprofile, Anwendungen und die zugehörigen Ressourcen zu organisieren. Um die Weitergabe vertrauenswürdiger Identitäten zu aktivieren, müssen Sie eine SageMaker Studio-Domäne erstellen oder eine vorhandene Domäne ändern, wie im folgenden Verfahren beschrieben.

1. Öffnen Sie die SageMaker AI-Konsole, navigieren Sie zu **Domains** und führen Sie eine der folgenden Aktionen aus.
 - Erstellen Sie mithilfe von [Setup für Organisationen eine neue SageMaker Studio-Domain](#).

Wählen Sie **Für Organisationen einrichten** aus, und gehen Sie dann wie folgt vor:

- Wählen Sie **AWS Identity Center** als Authentifizierungsmethode.
- Aktivieren Sie das Kontrollkästchen **Weitergabe vertrauenswürdiger Identitäten für alle Benutzer dieser Domäne aktivieren**.
- Ändern Sie eine bestehende SageMaker Studio-Domäne.
 - Wählen Sie eine vorhandene Domain aus, die IAM Identity Center für die Authentifizierung verwendet.

 Important

Die Weitergabe vertrauenswürdiger Identitäten wird nur in SageMaker Studio-Domänen unterstützt, die IAM Identity Center für die Authentifizierung verwenden. Wenn die Domain IAM für die Authentifizierung verwendet, können Sie die Authentifizierungsmethode nicht ändern und daher die Weitergabe vertrauenswürdiger Identitäten nicht aktivieren.

- [Bearbeiten Sie die Domain-Einstellungen](#). Bearbeiten Sie die Authentifizierungs- und Berechtigungseinstellungen, um die Verbreitung vertrauenswürdiger Identitäten zu aktivieren.
2. Fahren Sie mit [Schritt 2 fort: Konfigurieren Sie die Standard-Domain-Ausführungsrolle](#). Diese Rolle ist erforderlich, damit Benutzer einer SageMaker Studio-Domain auf andere AWS Dienste wie Amazon S3 zugreifen können.

Schritt 2: Konfigurieren Sie die standardmäßige Domänenausführungsrolle und die Rollenvertrauensrichtlinie

Eine Domänenausführungsrolle ist eine [IAM-Rolle](#), die eine SageMaker Studio-Domäne im Namen aller Benutzer in der Domäne übernimmt. Die Berechtigungen, die Sie dieser Rolle zuweisen, bestimmen, welche Aktionen SageMaker Studio ausführen kann.

1. Gehen Sie wie folgt vor, um eine Domänenausführungsrolle zu erstellen oder auszuwählen:
 - Erstellen Sie mithilfe von [Setup für Organisationen eine Rolle oder wählen Sie sie aus](#).
 - Öffnen Sie die SageMaker AI-Konsole und folgen Sie den Anweisungen der Konsole in Schritt 2: Rollen und ML-Aktivitäten konfigurieren, um eine neue Domänenausführungsrolle zu erstellen, oder wählen Sie eine vorhandene Rolle aus.
 - Führen Sie die restlichen Einrichtungsschritte durch, um Ihre SageMaker Studio-Domain zu erstellen.
 - Erstellen Sie manuell eine Ausführungsrolle.
 - Öffnen Sie die IAM-Konsole und [erstellen Sie die Ausführungsrolle selbst](#).
2. [Aktualisieren Sie die Vertrauensrichtlinie](#), die der Domänenausführungsrolle zugeordnet ist, sodass sie die folgenden beiden Aktionen umfasst: [sts:AssumeRole](#) und [sts:SetContext](#). Informationen dazu, wie Sie die Ausführungsrolle für Ihre SageMaker Studio-Domain finden, finden [Sie unter Domain-Ausführungsrolle abrufen](#).

Eine Vertrauensrichtlinie gibt die Identität an, die eine Rolle übernehmen kann. Diese Richtlinie ist erforderlich, damit der SageMaker Studio-Dienst die Rolle der Domänenausführung übernehmen kann. Fügen Sie diese beiden Aktionen hinzu, sodass sie in Ihrer Richtlinie wie folgt angezeigt werden.

```
{
  "Version": "2012-10-17",

  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "sagemaker.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

Schritt 3: Überprüfen Sie die erforderlichen Amazon S3 Access Grant-Berechtigungen für die Domain-Ausführungsrolle

Um Amazon S3 Access Grants verwenden zu können, muss Ihrer SageMaker Studio-Domain-Ausführungsrolle eine Berechtigungsrichtlinie (entweder als Inline-Richtlinie oder als vom Kunden verwaltete Richtlinie) beigefügt sein, die die folgenden Berechtigungen enthält.

```
{
  "Version": "2012-10-17",

  "Statement": [
    {
      "Effect": "Allow",
```

```
        "Action": [
            "s3:GetDataAccess",
            "s3:GetAccessGrantsInstanceForPrefix"
        ],
        "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
]
```

Wenn Sie keine Richtlinie haben, die diese Berechtigungen enthält, folgen Sie den Anweisungen unter [Hinzufügen und Entfernen von IAM-Identitätsberechtigungen](#) im AWS Identity and Access Management Benutzerhandbuch.

Schritt 4: Weisen Sie der Domain Gruppen und Benutzer zu

Weisen Sie der SageMaker Studio-Domäne Gruppen und Benutzer zu, indem Sie den Schritten unter Gruppen und Benutzer [hinzufügen folgen](#).

Schritt 5: Richten Sie Amazon S3 Access Grants ein

Um Amazon S3 Access Grants einzurichten, folgen Sie den Schritten [unter Konfiguration von Amazon S3 Access Grants für die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center](#). Folgen Sie den schrittweisen Anweisungen, um die folgenden Aufgaben auszuführen:

1. Erstellen Sie eine Amazon S3 Access Grants-Instance.
2. Registrieren Sie einen Standort in dieser Instance.
3. Erstellen Sie Zuschüsse, um bestimmten IAM Identity Center-Benutzern oder -Gruppen den Zugriff auf bestimmte Amazon S3-Standorte oder Untergruppen (z. B. bestimmte Präfixe) innerhalb dieser Standorte zu ermöglichen.

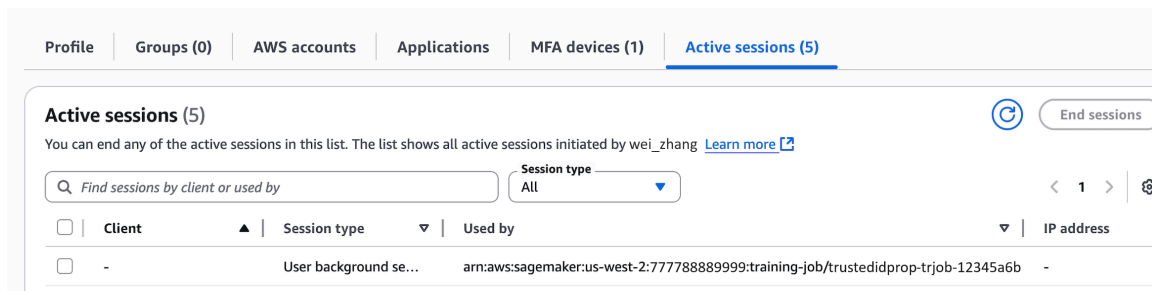
Schritt 6: Reichen Sie einen SageMaker Schulungsauftrag ein und sehen Sie sich die Hintergrundinformationen der Benutzer an

Starten Sie in SageMaker Studio ein neues Jupyter-Notizbuch und reichen Sie einen Trainingsjob ein. Führen Sie während der Ausführung des Jobs die folgenden Schritte aus, um die Sitzungsinformationen anzuzeigen und zu überprüfen, ob der Hintergrundkontext des Benutzers aktiv ist.

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.

3. Wählen Sie auf der Seite **Benutzer** den Benutzernamen des Benutzers aus, dessen Sitzungen Sie verwalten möchten. Dadurch gelangen Sie zu einer Seite mit den Benutzerinformationen.
4. Wählen Sie auf der Benutzerseite den Tab **Aktive Sitzungen**. Die Zahl in Klammern neben **Aktive Sitzungen** gibt die Anzahl der aktiven Sitzungen für diesen Benutzer an.
5. Um anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen zu suchen, wählen Sie in der Liste **Sitzungstyp** die Option **Benutzerhintergrundsitzungen** aus, und geben Sie dann die Job-ARN in das Suchfeld ein.

Im Folgenden finden Sie ein Beispiel dafür, wie ein Trainingsjob, der eine Benutzersitzung im Hintergrund verwendet, auf der Registerkarte **Aktive Sitzungen** für einen Benutzer angezeigt wird.



Schritt 7: Sehen Sie sich die CloudTrail Protokolle an, um die Verbreitung vertrauenswürdiger Identitäten in zu überprüfen CloudTrail

Wenn die Weitergabe vertrauenswürdiger Identitäten aktiviert ist, werden Aktionen in den CloudTrail Ereignisprotokollen unter dem `onBehalfOf` Element angezeigt. Das `userId` gibt die ID des IAM Identity Center-Benutzers wieder, der den Schulungsjob initiiert hat. Das folgende CloudTrail Ereignis erfasst den Prozess der Weitergabe vertrauenswürdiger Identitäten.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",

```

```

        "accountId": "111122223333",
        "userName": "SageMaker-ExecutionRole-20250728T125817"
    },
    "attributes": {
        "creationDate": "2025-07-29T17:17:10Z",
        "mfaAuthenticated": "false"
    }
},
"onBehalfOf": {
    "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",
    "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/d-1234567890"
}
},

```

Überlegungen zur Laufzeit

Wenn ein Administrator langwierige Schulungs- oder Verarbeitungsaufträge festlegt `MaxRuntimeInSeconds`, die kürzer als die Dauer der Benutzersitzung im Hintergrund sind, führt SageMaker Studio den Auftrag mindestens für die Dauer der Hintergrund Sitzung des Benutzers aus. `MaxRuntimeInSeconds`

Weitere Informationen `MaxRuntimeInSeconds` dazu finden Sie in der Anleitung für den `CreateTrainingJob` [StoppingCondition](#) Parameter in der SageMaker Amazon-API-Referenz.

Autorisierungsdienste

In allen Anwendungsfällen [in den Bereichen](#) Analytik und Data Lakehouse können Sie mithilfe der folgenden Methoden eine feinkörnige Zugriffskontrolle erreichen:

- AWS Lake Formation - Hinweise finden Sie unter [Einrichtung AWS Lake Formation mit IAM Identity Center](#)
- Amazon S3 Access Grants — Anleitungen finden Sie unter [Einrichtung von Amazon S3 Access Grants mit IAM Identity Center](#).

Einrichtung AWS Lake Formation mit IAM Identity Center

[AWS Lake Formation](#) ist ein verwalteter Dienst, der die Erstellung und Verwaltung von Data Lakes on AWS vereinfacht. Er automatisiert die Datenerfassung, Katalogisierung und Sicherheit und bietet ein

zentrales Repository für die Speicherung und Analyse verschiedener Datentypen. Lake Formation bietet detaillierte Zugriffskontrollen und lässt sich in verschiedene AWS Analysedienste integrieren, sodass Unternehmen ihre Data Lakes effizient einrichten, sichern und Erkenntnisse aus ihnen ableiten können.

Folgen Sie diesen Schritten, damit Lake Formation mithilfe von IAM Identity Center und Trusted Identity Propagation Datenberechtigungen auf der Grundlage der Benutzeridentität gewähren kann.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie Folgendes einrichten:

- [Aktivieren Sie IAM Identity Center](#). [Eine Organisationsinstanz](#) wird empfohlen. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).

Schritte zum Einrichten der Verbreitung vertrauenswürdiger Identitäten

1. Integrieren Sie IAM Identity Center, indem AWS Lake Formation Sie die Anweisungen unter [Verbinden von Lake Formation mit IAM Identity Center befolgen](#).

Important

Wenn Sie keine AWS Glue Data Catalog Tabellen haben, müssen Sie diese erstellen, um IAM Identity Center-Benutzern und -Gruppen Zugriff zu gewähren. AWS Lake Formation Weitere Informationen finden Sie unter [Objekte erstellen in AWS Glue Data Catalog](#).

2. Registrieren Sie die Standorte von Data Lake.

[Registrieren Sie die S3-Speicherorte](#), an denen die Daten der Glue-Tabellen gespeichert sind. Auf diese Weise gewährt Lake Formation temporären Zugriff auf die erforderlichen S3-Speicherorte, wenn die Tabellen abgefragt werden. Dadurch entfällt die Notwendigkeit, S3-Berechtigungen in die Servicerolle aufzunehmen (z. B. die auf der konfigurierte Athena-Servicerolle). WorkGroup

- a. Navigieren Sie im Navigationsbereich der Konsole im Abschnitt Administration zu den Data Lake-Speicherorten. AWS Lake Formation Wählen Sie Standort registrieren aus.

Dadurch kann Lake Formation temporäre IAM-Anmeldeinformationen mit den erforderlichen Berechtigungen für den Zugriff auf S3-Datenspeicherorte bereitstellen.

Register location

Amazon S3 location
Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path
Choose an Amazon S3 path for your data lake.
 [Browse](#)

Review location permissions - strongly recommended
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.
[Review location permissions](#)

IAM role
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

☐ **Enable Data Catalog Federation**
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Permission mode
Select the permission mode you want to use to manage access.

☒ **Hybrid access mode**
Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access.
[Learn more](#)

☐ **Lake Formation**
Only Lake Formation permissions are enforced.

[Cancel](#) [Register location](#)

- b. Geben Sie den S3-Pfad der Datenspeicherorte der AWS Glue Tabellen in das Amazon S3-Pfadfeld ein.
- c. Wählen Sie im Abschnitt „IAM-Rolle“ nicht die mit dem Service verknüpfte Rolle aus, wenn Sie sie für die Weitergabe vertrauenswürdiger Identitäten verwenden möchten. Erstellen Sie eine separate Rolle mit den folgenden Berechtigungen.

Um diese Richtlinien zu verwenden, ersetzen Sie die Richtlinie *italicized placeholder text* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie [erstellen](#) oder Richtlinie [bearbeiten](#). Die Berechtigungsrichtlinie sollte den Zugriff auf den im Pfad angegebenen S3-Speicherort gewähren:

- i. Genehmigungsrichtlinie:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    }
  ]
}
```

```

    ],
    },
    {
        "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket"
        ]
    },
    {
        "Sid": "LakeFormationDataAccessServiceRolePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
]
}

```

- ii. Vertrauensbeziehung: Dazu sollte gehören `sts:SectContext`, was für die Verbreitung vertrauenswürdiger Identitäten erforderlich ist.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}

```

```
}  
  }  
    ]  
      ]  
        }
```

 Note

Bei der vom Assistenten erstellten IAM-Rolle handelt es sich um eine dienstbezogene Rolle, die Folgendes nicht umfasst: `sts:SetContext`

- d. Wählen Sie nach dem Erstellen der IAM-Rolle die Option `Standort registrieren` aus.

Vertrauenswürdige Identitätsverbreitung mit Lake Formation Across AWS-Konten

AWS Lake Formation unterstützt die Verwendung von [AWS Resource Access Manager \(RAM\)](#) zur gemeinsamen Nutzung von Tabellen AWS-Konten und funktioniert mit der Weitergabe vertrauenswürdiger Identitäten, wenn sich das Konto des Zuschussempfängers und das Konto des Empfängers in derselben AWS-Region, derselben Organisationsinstanz von IAM Identity Center befinden und dieselbe Organisationsinstanz verwenden. AWS Organizations Weitere Informationen finden Sie unter [Cross-account Datenaustausch in Lake](#) Formation.

Einrichtung von Amazon S3 Access Grants mit IAM Identity Center

[Amazon S3 Access Grants](#) bietet die Flexibilität, eine identitätsbasierte, detaillierte Zugriffskontrolle für S3-Standorte zu gewähren. Sie können Amazon S3 verwendenAccess Grants, um Ihren Unternehmensbenutzern und -gruppen direkt Zugriff auf Amazon S3-Buckets zu gewähren. Folgen Sie diesen Schritten, um S3 Access Grants mit IAM Identity Center zu aktivieren und eine vertrauenswürdige Identitätsverbreitung zu erreichen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie Folgendes einrichten:

- [Aktivieren Sie IAM Identity Center](#). [Eine Organisationsinstanz](#) wird empfohlen. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).

Konfiguration von S3 Access Grants für die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center

Wenn Sie bereits ein Amazon S3 haben Zugang zu Zuschüssen Gehen Sie bei einer Instanz mit einem registrierten Standort wie folgt vor:

1. [Verknüpfen Sie Ihre IAM Identity Center-Instanz.](#)
2. [Erstellen Sie einen Zuschuss.](#)

Wenn Sie kein Amazon S3 erstellt haben Zugriff auf Zuschüsse Folgen Sie jedoch diesen Schritten:

1. [Erstellen Sie eine Access Grants S3-Instanz](#) — Sie können pro Access Grants Instanz eine S3-Instanz erstellen AWS-Region. Wenn Sie die Access Grants S3-Instanz erstellen, achten Sie darauf, das Kästchen IAM Identity Center-Instanz hinzufügen zu aktivieren und den ARN Ihrer IAM Identity Center-Instanz anzugeben. Klicken Sie auf Weiter.

Die folgende Abbildung zeigt die Seite „Access GrantsS3-Instance erstellen“ in der Amazon Access Grants S3-Konsole:

2. Standort registrieren — Nachdem Sie eine Amazon Access Grants S3-Instanz [AWS-Region in Ihrem Konto](#) erstellt und erstellt haben, [registrieren Sie einen S3-Standort](#) in dieser Instanz. Ein Access Grants S3-Standort ordnet einer IAM-Rolle die Standard-S3-Region (S3://), einen Bucket oder ein Präfix zu. S3 Access Grants übernimmt diese Amazon S3-Rolle, um temporäre Anmeldeinformationen an den Empfänger weiterzugeben, der auf diesen bestimmten Standort zugreift. Sie müssen zuerst mindestens einen Standort in Ihrer Access Grants S3-Instanz registrieren, bevor Sie eine Zugriffsgewährung einrichten können.

Geben Sie für den Geltungsbereich Standort an `s3://`, welcher alle Ihre Buckets in dieser Region umfasst. Dies ist der empfohlene Standortbereich für die meisten Anwendungsfälle. Wenn Sie einen erweiterten Anwendungsfall für Zugriffsmanagement haben, können Sie den Standortbereich auf einen bestimmten Bucket `s3://bucket` oder ein bestimmtes Präfix innerhalb eines Buckets festlegen `s3://bucket/prefix-with-path`. Weitere Informationen finden Sie unter Standort [registrieren](#) im Amazon Simple Storage Service-Benutzerhandbuch.

 Note

Stellen Sie sicher, dass die S3-Speicherorte der AWS Glue Tabellen, auf die Sie Zugriff gewähren möchten, in diesem Pfad enthalten sind.

Für das Verfahren müssen Sie eine IAM-Rolle für den Standort konfigurieren. Diese Rolle sollte Berechtigungen für den Zugriff auf den Standortbereich enthalten. Sie können den S3-Konsolenassistenten verwenden, um die Rolle zu erstellen. Sie müssen Ihren Access Grants S3-Instance-ARN in den Richtlinien für diese IAM-Rolle angeben. Der Standardwert Ihres Access Grants S3-Instance-ARN ist `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`.

Das folgende Beispiel für eine Berechtigungsrichtlinie erteilt Amazon S3-Berechtigungen für die IAM-Rolle, die Sie erstellt haben. Und das folgende Beispiel für eine Vertrauensrichtlinie ermöglicht es dem Access Grants S3-Serviceprinzipal, die IAM-Rolle zu übernehmen.

a. Berechtigungsrichtlinie

Um diese Richtlinien zu verwenden, ersetzen Sie die Richtlinie *italicized placeholder text* im Beispiel durch Ihre eigenen Informationen. Weitere Anweisungen finden Sie unter Richtlinie [erstellen](#) oder Richtlinie [bearbeiten](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
```

```

    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:GetObjectAcl",
      "s3:GetObjectVersionAcl",
      "s3:ListMultipartUploadParts"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "111122223333"
      },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": [
          "arn:aws:s3:::access-grants/instance-id"
        ]
      }
    }
  },
  {
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:AbortMultipartUpload"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "111122223333"
      },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": [
          "arn:aws:s3:::access-grants/instance-id"
        ]
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid": "BucketLevelReadPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "111122223333"
      },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": [
          "arn:aws:s3:::access-grants/instance-id"
        ]
      }
    }
  },
  {
    "Sid": "OptionalKMSPermissionsForSSEEncryption",
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

b. Vertrauensrichtlinie

Gewähren Sie in der Vertrauensrichtlinie für IAM-Rollen dem S3-Access-Grants-Service (`access-grants.s3.amazonaws.com`)-Prinzipal Zugriff auf die IAM-Rolle, die Sie erstellt haben. Hierzu können Sie eine JSON-Datei mit den folgenden Anweisungen erstellen. Informationen zum Hinzufügen der Vertrauensrichtlinie zu Ihrem Konto finden Sie unter [Erstellen einer Rolle mit benutzerdefinierten Vertrauensrichtlinien](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}
```

Erstellen Sie einen Amazon S3 Access Grant

Wenn Sie eine Amazon Access Grants S3-Instance mit einem registrierten Standort haben und Sie Ihre IAM Identity Center-Instance damit verknüpft haben, können [Sie einen Zuschuss gewähren](#). Gehen Sie auf der Seite **Create Grant** in der S3-Konsole wie folgt vor:

Erstellen einer Erteilung

1. Wählen Sie den im vorherigen Schritt erstellten Standort aus. Sie können den Umfang des Zuschusses reduzieren, indem Sie ein Unterpräfix hinzufügen. Das Unterpräfix kann einbucket,bucket/prefix, oder ein Objekt im Bucket sein. Weitere Informationen finden Sie unter [Subprefix](#) im Amazon Simple Storage Service-Benutzerhandbuch.
2. Wählen Sie unter **Berechtigungen und Zugriff** je nach Bedarf **Lesen** und/oder **Schreiben** aus.
3. Wählen Sie unter **Granter-Typ** die Option **Verzeichnisidentität aus IAM Identity Center** aus.
4. Geben Sie die IAM Identity Center-Benutzer- oder Gruppen-ID an. Sie finden die Benutzer- und Gruppen-IDs in der IAM Identity Center-Konsole in den Abschnitten [Benutzer und Gruppe](#). Klicken Sie auf **Weiter**.
5. Überprüfen Sie auf der Seite „Überprüfen und beenden“ die Einstellungen für S3 Access Grant und wählen Sie dann **Create Grant** aus.

Die folgende Abbildung zeigt die Seite „Grant erstellen“ in der Amazon Access Grants S3-Konsole:

The screenshot shows the 'Create Grant' page in the Amazon S3 console. The page is titled 'Create Grant' and includes several sections for configuring the grant:

- Grant**: A section with an 'info' icon, stating 'Grant a user or role a specific level of access to your S3 data.'
- Grant scope**: A section with an 'info' icon, stating 'The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.'
- Location**: A text input field containing 's3://'. Below it are buttons for 'Browse locations' and 'Register location'.
- Subprefix - optional**: A section with an 'info' icon, stating 'Further scope the grant to a bucket, prefix, or an individual object.' Below it is a text input field containing 'bucket-name/prefix/'.
- Grant scope**: A section with an 'info' icon, showing the resulting scope 's3://'. Below it is a checkbox labeled 'The grant scope is an object'.
- Permissions and access**: A section with an 'info' icon, stating 'Grant a user or role a specific level of access to your S3 data.'
- Permissions**: A section with checkboxes for 'Read' (checked) and 'Write'.
- Grantee type**: A section with an 'info' icon, showing 'Directory identity from IAM Identity Center' selected.
- Directory identity type**: A section with an 'info' icon, showing 'User' selected.
- IAM Identity Center group ID**: A section with an 'info' icon, stating 'The group that you want to grant this level of access to. You can find the ID in the IAM Identity Center console.' Below it is a text input field.

Richten Sie Ihre eigene OAuth 2.0-Anwendung ein

Vertrauenswürdige Identitätsverbreitung ermöglicht es einer vom Kunden verwalteten Anwendung, im Namen eines Benutzers Zugriff auf Daten in AWS Diensten anzufordern. Die Verwaltung des Datenzugriffs basiert auf der Identität eines Benutzers, sodass Administratoren den Zugriff auf der Grundlage der bestehenden Benutzer- und Gruppenmitgliedschaften gewähren können. Die Identität des Benutzers, in seinem Namen ausgeführte Aktionen und andere Ereignisse werden in dienstspezifischen Protokollen und CloudTrail Ereignissen aufgezeichnet.

Bei der Weitergabe vertrauenswürdiger Identitäten kann sich ein Benutzer bei einer vom Kunden verwalteten Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Zugriff auf Daten weitergeben. AWS-Services

Important

Um auf eine vom Kunden verwaltete Anwendung zugreifen zu können AWS-Service, müssen Sie ein Token von einem vertrauenswürdigen Token-Aussteller erhalten, der nicht zum IAM Identity Center gehört. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Zugriffsanfragen auf AWS-Services (empfangende Anwendungen) initiieren. Weitere Informationen finden Sie unter [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#).

Themen

- [Richten Sie vom Kunden verwaltete OAuth 2.0-Anwendungen für die Verbreitung vertrauenswürdiger Identitäten ein](#)
- [Geben Sie vertrauenswürdige Anwendungen an](#)
- [Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller](#)

Richten Sie vom Kunden verwaltete OAuth 2.0-Anwendungen für die Verbreitung vertrauenswürdiger Identitäten ein

Um eine vom Kunden verwaltete OAuth 2.0-Anwendung für die Verbreitung vertrauenswürdiger Identitäten einzurichten, müssen Sie sie zuerst zum IAM Identity Center hinzufügen. Gehen Sie wie folgt vor, um Ihre Anwendung zum IAM Identity Center hinzuzufügen.

Themen

- [Schritt 1: Wählen Sie den Anwendungstyp](#)
- [Schritt 2: Geben Sie die Anwendungsdetails an](#)
- [Schritt 3: Geben Sie die Authentifizierungseinstellungen an](#)
- [Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an](#)
- [Schritt 5: Überprüfen und konfigurieren](#)

Schritt 1: Wählen Sie den Anwendungstyp

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte Vom Kunden verwaltet aus.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Einrichtungspräferenz die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
6. Wählen Sie unter Anwendungstyp die Option OAuth 2.0 aus.
7. Wählen Sie Weiter, um zur nächsten Seite zu gelangen [Schritt 2: Geben Sie die Anwendungsdetails an](#).

Schritt 2: Geben Sie die Anwendungsdetails an

1. Geben Sie auf der Seite Anwendungsdetails angeben unter Anwendungsname und Beschreibung einen Anzeigenamen für die Anwendung ein, z. **MyApp** B. Geben Sie dann eine Beschreibung ein.
2. Wählen Sie unter Zuweisungsmethode für Benutzer und Gruppe eine der folgenden Optionen aus:
 - Zuweisungen erforderlich — Erlauben Sie nur IAM Identity Center-Benutzern und -Gruppen, die dieser Anwendung zugewiesen sind, den Zugriff auf die Anwendung.

Sichtbarkeit der Anwendungskachel — Nur Benutzer, die der Anwendung direkt oder über eine Gruppenzuweisung zugewiesen sind, können die Anwendungskachel im AWS Access Portal anzeigen, sofern die Sichtbarkeit der Anwendung im AWS Access Portal auf Sichtbar gesetzt ist.

- Keine Zuweisungen erforderlich — Erlauben Sie allen autorisierten IAM Identity Center-Benutzern und -Gruppen den Zugriff auf diese Anwendung.

Sichtbarkeit der Anwendungskachel — Die Anwendungskachel ist für alle Benutzer sichtbar, die sich beim AWS Access Portal anmelden, es sei denn, die Sichtbarkeit der Anwendung im AWS Access Portal ist auf Nicht sichtbar gesetzt.

3. Geben Sie unter AWS Zugriffsportal die URL ein, über die Benutzer auf die Anwendung zugreifen können, und geben Sie an, ob die Anwendungskachel im AWS Zugriffsportal sichtbar sein soll oder nicht. Wenn Sie Nicht sichtbar wählen, können nicht einmal zugewiesene Benutzer die Anwendungskachel sehen.
4. Wählen Sie unter Tags (optional) die Option Neues Tag hinzufügen aus , und geben Sie dann Werte für Schlüssel und Wert (optional) an.

Informationen zu Tags siehe [Ressourcen taggen AWS IAM Identity Center](#).

5. Wählen Sie Weiter und fahren Sie mit der nächsten Seite fort [Schritt 3: Geben Sie die Authentifizierungseinstellungen an](#).

Schritt 3: Geben Sie die Authentifizierungseinstellungen an

Um eine vom Kunden verwaltete Anwendung, die OAuth 2.0 unterstützt, zum IAM Identity Center hinzuzufügen, müssen Sie einen vertrauenswürdigen Token-Aussteller angeben. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Anforderungen (anfordernde Anwendungen) für den Zugriff auf von AWS verwaltete Anwendungen (empfangende Anwendungen) initiieren.

1. Führen Sie auf der Seite Authentifizierungseinstellungen angeben unter Vertrauenswürdige Token-Aussteller eine der folgenden Aktionen aus:

- So verwenden Sie einen vorhandenen Aussteller für vertrauenswürdige Tokens:

Markieren Sie das Kontrollkästchen neben dem Namen des vertrauenswürdigen Token-Ausstellers, den Sie verwenden möchten.

- So fügen Sie einen neuen Aussteller für vertrauenswürdige Tokens hinzu:

1. Wählen Sie Vertrauenswürdigen Token-Aussteller erstellen aus.

2. Ein neuer Browser-Tab wird geöffnet. Folgen Sie den Schritten 5 bis 8 in [Wie füge ich der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzu](#).

3. Nachdem Sie diese Schritte abgeschlossen haben, kehren Sie zu dem Browserfenster zurück, das Sie für die Anwendungseinrichtung verwenden, und wählen Sie den vertrauenswürdigen Token-Aussteller aus, den Sie gerade hinzugefügt haben.
4. Aktivieren Sie in der Liste der vertrauenswürdigen Token-Aussteller das Kontrollkästchen neben dem Namen des vertrauenswürdigen Token-Ausstellers, den Sie gerade hinzugefügt haben.

Nachdem Sie einen vertrauenswürdigen Token-Aussteller ausgewählt haben, wird der Abschnitt **Ausgewählte vertrauenswürdige Token-Aussteller konfigurieren** angezeigt.

2. Geben Sie unter **Ausgewählte vertrauenswürdige Token-Aussteller konfigurieren** den **Aud-Anspruch** ein. Der Aud-Anspruch identifiziert die Zielgruppe (Empfänger) des Tokens, das vom Aussteller des vertrauenswürdigen Tokens generiert wurde. Weitere Informationen finden Sie unter [Anspruch erheben](#).
3. Um zu verhindern, dass sich Ihre Benutzer erneut authentifizieren müssen, wenn sie diese Anwendung verwenden, wählen Sie „Aktualisierungstoken gewähren“ aus. Wenn diese Option ausgewählt ist, aktualisiert diese Option das Zugriffstoken für die Sitzung alle 60 Minuten, bis die Sitzung abläuft oder der Benutzer die Sitzung beendet.
4. Wählen Sie **Weiter** und fahren Sie mit der nächsten Seite fort. [Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an](#)

Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an

Gehen Sie wie in diesem Verfahren beschrieben vor, um die Anmeldeinformationen anzugeben, die Ihre Anwendung für den Token-Austausch mit vertrauenswürdigen Anwendungen verwendet. Diese Anmeldeinformationen werden in einer ressourcenbasierten Richtlinie verwendet. Die Richtlinie erfordert, dass Sie einen Prinzipal angeben, der über die Berechtigungen zum Ausführen der in der Richtlinie angegebenen Aktionen verfügt. Sie müssen einen Prinzipal angeben, auch wenn sich die vertrauenswürdigen Anwendungen in derselben Gruppe befinden AWS-Konto.

Note

Wenn Sie Berechtigungen mithilfe von Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen.

Für diese Richtlinie ist die [CreateTokenWithIAM](#) API-Aktion erforderlich. Weitere Informationen zu dieser Richtlinie und ein Beispiel, das Sie je nach Bedarf an Ihre Umgebung anpassen können, finden Sie unter [Resource-based Beispiel für eine Richtlinie für IAM Identity Center](#).

1. Führen Sie auf der Seite Anmeldeinformationen für die Anwendung angeben eine der folgenden Aktionen aus:

- So geben Sie schnell eine oder mehrere IAM-Rollen an:
 1. Wählen Sie Geben Sie eine oder mehrere IAM-Rollen ein.
 2. Geben Sie unter IAM-Rollen eingeben den Amazon-Ressourcennamen (ARN) einer vorhandenen IAM-Rolle an. Verwenden Sie die folgende Syntax, um den ARN anzugeben. Der Teil zur Angabe der Region im ARN ist leer, da IAM-Ressourcen globale Ressourcen sind.

```
arn:aws:iam::account:role/role-name-with-path
```

Weitere Informationen finden Sie im Benutzerhandbuch unter [Cross-account Zugriff mithilfe ressourcenbasierter Richtlinien](#) und [IAM-ARNs](#). AWS Identity and Access Management

- So bearbeiten Sie die Richtlinie manuell (erforderlich, wenn Sie keine Anmeldeinformationen angeben):AWS
 1. Wählen Sie Anwendungsrichtlinie bearbeiten aus.
 2. Ändern Sie Ihre Richtlinie, indem Sie Text in das JSON-Textfeld eingeben oder einfügen.
 3. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvvalidierung generiert wurden. Weitere Informationen finden Sie unter [Validieren von IAM-Richtlinien](#) im AWS Identity and Access Management Benutzerhandbuch.
2. Wählen Sie Weiter und fahren Sie mit der nächsten Seite fort., [Schritt 5: Überprüfen und konfigurieren](#)

Schritt 5: Überprüfen und konfigurieren

1. Überprüfen Sie auf der Seite Überprüfen und konfigurieren die von Ihnen getroffenen Entscheidungen. Um Änderungen vorzunehmen, wählen Sie den gewünschten Konfigurationsabschnitt aus, klicken Sie auf Bearbeiten, und nehmen Sie dann die erforderlichen Änderungen vor.

2. Wenn Sie fertig sind, wählen Sie **Anwendung** hinzufügen.
3. Die Anwendung, die Sie hinzugefügt haben, wird in der Liste der vom Kunden verwalteten Anwendungen angezeigt.
4. Nachdem Sie Ihre vom Kunden verwaltete Anwendung im IAM Identity Center eingerichtet haben, müssen Sie eine oder mehrere AWS-Services oder vertrauenswürdige Anwendungen für die Identitätsverbreitung angeben. Auf diese Weise können sich Benutzer bei Ihrer vom Kunden verwalteten Anwendung anmelden und auf Daten in der vertrauenswürdigen Anwendung zugreifen.

Weitere Informationen finden Sie unter [Geben Sie vertrauenswürdige Anwendungen an](#).

Geben Sie vertrauenswürdige Anwendungen an

Nachdem Sie Ihre vom Kunden verwaltete Anwendung [eingerichtet haben](#), müssen Sie einen oder mehrere vertrauenswürdige AWS Dienste oder vertrauenswürdige Anwendungen für die Identitätsverbreitung angeben. Geben Sie einen AWS Dienst an, der Daten enthält, auf die Benutzer Ihrer vom Kunden verwalteten Anwendungen zugreifen müssen. Wenn sich Ihre Benutzer bei Ihrer vom Kunden verwalteten Anwendung anmelden, gibt diese Anwendung die Identität Ihrer Benutzer an die vertrauenswürdige Anwendung weiter.

Gehen Sie wie folgt vor, um einen Dienst auszuwählen, und geben Sie dann einzelne Anwendungen an, denen Sie für diesen Dienst vertrauen sollen.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie **Applications (Anwendungen)**.
3. Wählen Sie die Registerkarte **Vom Kunden verwaltet** aus.
4. Wählen Sie in der Liste vom Kunden verwaltete Anwendungen die **OAuth 2.0-Anwendung** aus, für die Sie Zugriffsanfragen initiieren möchten. Dies ist die Anwendung, bei der sich Ihre Benutzer anmelden.
5. Wählen Sie auf der Detailseite unter **Vertrauenswürdige Anwendungen für die Verbreitung von Identitäten** die Option **Vertrauenswürdige Anwendungen** angeben aus.
6. Wählen Sie unter **Setuptyp** die Option **Einzelne Anwendungen** aus, geben Sie den Zugriff an, und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite „Dienst auswählen“ den AWS Dienst aus, der Anwendungen enthält, denen Ihre vom Kunden verwaltete Anwendung für die Identitätsverbreitung vertrauen kann, und klicken Sie dann auf **Weiter**.

Der Dienst, den Sie auswählen, definiert die Anwendungen, denen vertraut werden kann. Im nächsten Schritt wählen Sie Anwendungen aus.

8. Wählen Sie auf der Seite „Anwendungen auswählen“ die Option Einzelne Anwendungen aus, aktivieren Sie das Kontrollkästchen für jede Anwendung, die Zugriffsanfragen empfangen kann, und klicken Sie dann auf Weiter.
9. Führen Sie auf der Seite „Zugriff konfigurieren“ unter Konfigurationsmethode eine der folgenden Aktionen aus:
 - Zugriff pro Anwendung auswählen – Wählen Sie diese Option aus, um für jede Anwendung unterschiedliche Zugriffsebenen zu konfigurieren. Wählen Sie die Anwendung aus, für die Sie die Zugriffsebene konfigurieren möchten, und klicken Sie dann auf Zugriff bearbeiten. Ändern Sie unter Anzuwendende Zugriffsebene die Zugriffsebenen nach Bedarf und wählen Sie dann Änderungen speichern aus.
 - Gleiche Zugriffsebene auf alle Anwendungen anwenden — Wählen Sie diese Option, wenn Sie die Zugriffsebenen nicht pro Anwendung konfigurieren müssen.
10. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Konfiguration überprüfen die von Ihnen getroffenen Entscheidungen. Um Änderungen vorzunehmen, wählen Sie den gewünschten Konfigurationsabschnitt aus, wählen Sie Zugriff bearbeiten aus, und nehmen Sie dann die erforderlichen Änderungen vor.
12. Wenn Sie fertig sind, wählen Sie Anwendungen vertrauen aus.

Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Aussteller

Vertrauenswürdige Token-Aussteller ermöglichen es Ihnen, die Weitergabe vertrauenswürdiger Identitäten mit Anwendungen zu verwenden, die sich außerhalb von authentifizieren. AWS Mit vertrauenswürdigen Token-Ausstellern können Sie diese Anwendungen autorisieren, im Namen ihrer Benutzer Anfragen für den Zugriff auf verwaltete Anwendungen zu stellen. AWS

Die folgenden Themen beschreiben, wie vertrauenswürdige Token-Aussteller arbeiten, und bieten Anleitungen zur Einrichtung.

Themen

- [Überblick über vertrauenswürdige Token-Emittenten](#)

- [Voraussetzungen und Überlegungen für vertrauenswürdige Token-Aussteller](#)
- [Einzelheiten des JTI-Antrags](#)
- [Konfigurationseinstellungen für vertrauenswürdige Token-Aussteller](#)
- [Einen vertrauenswürdigen Token-Emittenten einrichten](#)
- [Identity-enhanced IAM-Rollensitzungen](#)

Überblick über vertrauenswürdige Token-Emittenten

Die Weitergabe vertrauenswürdiger Identitäten bietet einen Mechanismus, der es Anwendungen, die sich außerhalb von authentifizieren AWS , ermöglicht, mithilfe eines vertrauenswürdigen Token-Ausstellers Anfragen im Namen ihrer Benutzer zu stellen. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Anfragen für den Zugriff auf (Empfangen von Anwendungen) initiieren AWS-Services (Anwendungen anfordern). Anfordernde Anwendungen initiieren Zugriffsanfragen im Namen von Benutzern, die der vertrauenswürdige Token-Aussteller authentifiziert. Die Benutzer sind sowohl dem Aussteller des vertrauenswürdigen Tokens als auch dem IAM Identity Center bekannt.

AWS-Services Die Empfänger von Anfragen verwalten eine detaillierte Autorisierung für ihre Ressourcen auf der Grundlage ihrer Benutzer und Gruppenzugehörigkeit, wie sie im Identity Center-Verzeichnis dargestellt sind. AWS-Services kann die Token des externen Token-Ausstellers nicht direkt verwenden.

Um dieses Problem zu lösen, bietet IAM Identity Center der anfordernden Anwendung oder einem AWS Treiber, den die anfordernde Anwendung verwendet, die Möglichkeit, das vom vertrauenswürdigen Token-Aussteller ausgegebene Token gegen ein vom IAM Identity Center generiertes Token auszutauschen. Das vom IAM Identity Center generierte Token bezieht sich auf den entsprechenden IAM Identity Center-Benutzer. Die anfordernde Anwendung oder der Treiber verwendet das neue Token, um eine Anfrage an die empfangende Anwendung zu initiieren. Da das neue Token auf den entsprechenden Benutzer im IAM Identity Center verweist, kann die empfangende Anwendung den angeforderten Zugriff auf der Grundlage des Benutzers oder seiner Gruppenmitgliedschaft autorisieren, wie sie im IAM Identity Center dargestellt wird.

Important

Die Auswahl eines OAuth 2.0-Autorisierungsservers, der als vertrauenswürdiger Token-Aussteller hinzugefügt werden soll, ist eine Sicherheitsentscheidung, die sorgfältig

abgewogen werden muss. Wählen Sie nur vertrauenswürdige Token-Aussteller aus, denen Sie vertrauen, um die folgenden Aufgaben auszuführen:

- Authentifizieren Sie den Benutzer, der im Token angegeben ist.
- Autorisieren Sie den Zugriff dieses Benutzers auf die empfangende Anwendung.
- Generieren Sie ein Token, das IAM Identity Center gegen ein von IAM Identity Center erstelltes Token austauschen kann.

Voraussetzungen und Überlegungen für vertrauenswürdige Token-Aussteller

Bevor Sie einen vertrauenswürdigen Token-Aussteller einrichten, sollten Sie die folgenden Voraussetzungen und Überlegungen überprüfen.

- Konfiguration eines vertrauenswürdigen Token-Ausstellers

Sie müssen einen OAuth 2.0-Autorisierungsserver (den vertrauenswürdigen Token-Aussteller) konfigurieren. Obwohl der vertrauenswürdige Token-Aussteller in der Regel der Identitätsanbieter ist, den Sie als Identitätsquelle für IAM Identity Center verwenden, muss dies nicht der Fall sein. Informationen zur Einrichtung des vertrauenswürdigen Token-Ausstellers finden Sie in der Dokumentation des entsprechenden Identitätsanbieters.

Note

Sie können bis zu 10 vertrauenswürdige Token-Aussteller für die Verwendung mit IAM Identity Center konfigurieren, sofern Sie die Identität jedes Benutzers im vertrauenswürdigen Token-Aussteller einem entsprechenden Benutzer im IAM Identity Center zuordnen.

- Der OAuth 2.0-Autorisierungsserver (der vertrauenswürdige Token-Aussteller), der das Token erstellt, muss über einen [OpenID Connect \(OIDC\)](#) -Discovery-Endpunkt verfügen, den IAM Identity Center verwenden kann, um öffentliche Schlüssel zur Überprüfung der Tokensignaturen abzurufen. Weitere Informationen finden Sie unter [URL des OIDC-Discovery-Endpunkts \(Aussteller-URL\)](#).
- Vom vertrauenswürdigen Token-Emittenten ausgestellte Token

Token des vertrauenswürdigen Token-Emittenten müssen die folgenden Anforderungen erfüllen:

- Das Token muss signiert sein und im [JSON Web Token \(JWT\)](#) -Format unter Verwendung des RS256-Algorithmus vorliegen.
- Das Token muss die folgenden Ansprüche enthalten:
 - [Emittent](#) (iss) — Die Entität, die das Token ausgestellt hat. Dieser Wert muss mit dem Wert übereinstimmen, der im OIDC-Erkennungsendpunkt (Aussteller-URL) im vertrauenswürdigen Token-Aussteller konfiguriert ist.
 - [Betreff](#) (Sub) — Der authentifizierte Benutzer.
 - [Zielgruppe](#) (aud) — Der beabsichtigte Empfänger des Tokens. Dies ist der AWS-Service , auf den zugegriffen wird, nachdem das Token gegen ein Token von IAM Identity Center ausgetauscht wurde. Weitere Informationen finden Sie unter [Anspruch erheben](#).
 - [Ablaufzeit](#) (Exp) — Die Zeit, nach der das Token abläuft.
- Das Token kann ein Identitätstoken oder ein Zugriffstoken sein.
- Das Token muss über ein Attribut verfügen, das eindeutig einem IAM Identity Center-Benutzer zugeordnet werden kann.

 Note

Die Verwendung eines benutzerdefinierten Signaturschlüssels für JWTs von Microsoft Entra ID wird nicht unterstützt. Um Token von Microsoft Entra ID einem vertrauenswürdigen Token-Aussteller zu verwenden, können Sie keinen benutzerdefinierten Signaturschlüssel verwenden.

- Optionale Ansprüche

IAM Identity Center unterstützt alle optionalen Ansprüche, die in RFC 7523 definiert sind. Weitere Informationen finden Sie in [Abschnitt 3: JWT-Format- und Verarbeitungsanforderungen](#) dieses RFC.

Das Token kann beispielsweise einen [JTI-Anspruch \(JWT-ID\) enthalten](#). Dieser Anspruch, sofern vorhanden, verhindert, dass Token, die denselben JTI haben, für den Token-Austausch wiederverwendet werden. Weitere Informationen zu JTI-Ansprüchen finden Sie unter [Einzelheiten des JTI-Antrags](#)

- IAM Identity Center-Konfiguration für die Zusammenarbeit mit einem vertrauenswürdigen Token-Aussteller

Sie müssen außerdem IAM Identity Center aktivieren, die Identitätsquelle für IAM Identity Center konfigurieren und Benutzer bereitstellen, die den Benutzern im Verzeichnis des vertrauenswürdigen Token-Ausstellers entsprechen.

Dazu müssen Sie einen der folgenden Schritte ausführen:

- Synchronisieren Sie Benutzer mithilfe des Systems for Identity Management (SCIM) 2.0-Protokoll in IAM Cross-domain Identity Center.
- Erstellen Sie die Benutzer direkt im IAM Identity Center.

Einzelheiten des JTI-Antrags

Wenn IAM Identity Center eine Anfrage zum Austausch eines Tokens erhält, das IAM Identity Center bereits ausgetauscht hat, schlägt die Anfrage fehl. Um die Wiederverwendung eines Tokens für den Token-Austausch zu erkennen und zu verhindern, können Sie einen JTI-Anspruch einreichen. IAM Identity Center schützt vor der Wiederholung von Tokens auf der Grundlage der im Token enthaltenen Ansprüche.

Nicht alle OAuth 2.0-Autorisierungsserver fügen Tokens einen JTI-Anspruch hinzu. Auf einigen OAuth 2.0-Autorisierungsservern ist es möglicherweise nicht möglich, einen JTI als benutzerdefinierten Anspruch hinzuzufügen. OAuth 2.0-Autorisierungsserver, die die Verwendung eines JTI-Anspruchs unterstützen, fügen diesen Anspruch möglicherweise nur zu Identitätstoken, nur Zugriffstoken oder zu beiden hinzu. Weitere Informationen finden Sie in der Dokumentation zu Ihrem OAuth 2.0-Autorisierungsserver.

Informationen zum Erstellen von Anwendungen, die Tokens austauschen, finden Sie in der IAM Identity Center API-Dokumentation. Informationen zur Konfiguration einer vom Kunden verwalteten Anwendung zum Abrufen und Austauschen der richtigen Token finden Sie in der Dokumentation zur Anwendung.

Konfigurationseinstellungen für vertrauenswürdige Token-Aussteller

In den folgenden Abschnitten werden die Einstellungen beschrieben, die für die Einrichtung und Verwendung eines vertrauenswürdigen Token-Ausstellers erforderlich sind.

Themen

- [URL des OIDC-Discovery-Endpunkts \(Aussteller-URL\)](#)
- [Attributzuordnung](#)

- [Anspruch erheben](#)

URL des OIDC-Discovery-Endpunkts (Aussteller-URL)

Wenn Sie der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzufügen, müssen Sie die URL des OIDC-Discovery-Endpunkts angeben. Diese URL wird üblicherweise mit ihrer relativen URL bezeichnet. `/.well-known/openid-configuration` In der IAM Identity Center-Konsole wird diese URL als Aussteller-URL bezeichnet.

Note

Sie müssen die URL des Discovery-Endpunkts bis zum Ende einfügen. `/.well-known/openid-configuration` Wenn sie in der URL enthalten `/.well-known/openid-configuration` ist, funktioniert die Konfiguration des vertrauenswürdigen Token-Ausstellers nicht. Da IAM Identity Center diese URL nicht validiert, schlägt die Einrichtung des vertrauenswürdigen Token-Ausstellers ohne Benachrichtigung fehl, wenn die URL nicht korrekt geformt ist.

Die URL des OIDC-Discovery-Endpunkts darf nur über die Ports 80 und 443 erreichbar sein.

IAM Identity Center verwendet diese URL, um zusätzliche Informationen über den vertrauenswürdigen Token-Aussteller abzurufen. IAM Identity Center verwendet diese URL beispielsweise, um die Informationen abzurufen, die zur Überprüfung der Token erforderlich sind, die der vertrauenswürdige Token-Aussteller generiert. Wenn Sie dem IAM Identity Center einen vertrauenswürdigen Token-Aussteller hinzufügen, müssen Sie diese URL angeben. Die URL finden Sie in der Dokumentation zum OAuth 2.0-Autorisierungsserver-Anbieter, den Sie zum Generieren von Tokens für Ihre Anwendung verwenden, oder wenden Sie sich direkt an den Anbieter, um Unterstützung zu erhalten.

Attributzuordnung

Mithilfe von Attributzuordnungen kann IAM Identity Center den Benutzer, der in einem von einem vertrauenswürdigen Token-Aussteller ausgestellten Token dargestellt wird, einem einzelnen Benutzer im IAM Identity Center zuordnen. Sie müssen die Attributzuordnung angeben, wenn Sie den vertrauenswürdigen Token-Aussteller zu IAM Identity Center hinzufügen. Diese Attributzuordnung wird in einem Anspruch in dem Token verwendet, der vom Aussteller des vertrauenswürdigen Tokens generiert wird. Der Wert im Anspruch wird für die Suche im IAM Identity Center verwendet. Die Suche verwendet das angegebene Attribut, um einen einzelnen Benutzer in IAM Identity Center abzurufen,

der als der darin enthaltene Benutzer verwendet wird. AWS Der von Ihnen gewählte Anspruch muss einem Attribut in einer festen Liste verfügbarer Attribute im IAM Identity Center Identity Store zugeordnet werden. Sie können eines der folgenden IAM Identity Center-Identitätsspeicher-Attribute auswählen: Benutzername, E-Mail und externe ID. Der Wert für das Attribut, das Sie in IAM Identity Center angeben, muss für jeden Benutzer eindeutig sein.

Anspruch erheben

Ein Aud-Antrag identifiziert die Zielgruppe (Empfänger), für die ein Token bestimmt ist. Wenn sich die Anwendung, die den Zugriff anfordert, über einen Identitätsanbieter authentifiziert, der nicht mit dem IAM Identity Center verbunden ist, muss dieser Identitätsanbieter als vertrauenswürdiger Token-Aussteller eingerichtet werden. Die Anwendung, die die Zugriffsanforderung empfängt (die empfangende Anwendung), muss das vom Aussteller des vertrauenswürdigen Tokens generierte Token gegen ein vom IAM Identity Center generiertes Token austauschen.

Informationen dazu, wie Sie die AUD-Anspruchswerte für die empfangende Anwendung abrufen können, sobald diese beim Aussteller des vertrauenswürdigen Tokens registriert sind, finden Sie in der Dokumentation Ihres vertrauenswürdigen Token-Ausstellers oder wenden Sie sich an den Administrator des vertrauenswürdigen Tokens, um Unterstützung zu erhalten.

Einen vertrauenswürdigen Token-Emittenten einrichten

Um die Weitergabe vertrauenswürdiger Identitäten für eine Anwendung zu ermöglichen, die sich extern beim IAM Identity Center authentifiziert, müssen ein oder mehrere Administratoren einen vertrauenswürdigen Token-Aussteller einrichten. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der Token an Anwendungen ausgibt, die Anfragen initiieren (Anwendungen anfordern). Die Token autorisieren diese Anwendungen, im Namen ihrer Benutzer Anfragen an eine (n) empfangende Anwendung (an) zu initiieren. AWS-Service

Themen

- [Koordination der administrativen Rollen und Zuständigkeiten](#)
- [Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Ausstellers](#)
- [Wie füge ich der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzu](#)
- [Wie kann ich die Einstellungen für den Aussteller eines vertrauenswürdigen Tokens in der IAM Identity Center-Konsole anzeigen oder bearbeiten](#)
- [Einrichtungsprozess und Anforderungsablauf für Anwendungen, die einen vertrauenswürdigen Token-Aussteller verwenden](#)

Koordination der administrativen Rollen und Zuständigkeiten

In einigen Fällen kann ein einziger Administrator alle notwendigen Aufgaben für die Einrichtung eines vertrauenswürdigen Token-Ausstellers ausführen. Wenn mehrere Administratoren diese Aufgaben ausführen, ist eine enge Abstimmung erforderlich. In der folgenden Tabelle wird beschrieben, wie sich mehrere Administratoren abstimmen können, um einen vertrauenswürdigen Token-Aussteller einzurichten und den AWS Dienst für dessen Verwendung zu konfigurieren.

Note

Bei der Anwendung kann es sich um einen beliebigen AWS Dienst handeln, der in IAM Identity Center integriert ist und die Verbreitung vertrauenswürdiger Identitäten unterstützt.

Weitere Informationen finden Sie unter [Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Ausstellers](#).

Rolle	Führt diese Aufgaben aus	Koordiniert mit
IAM Identity Center-Administrator	Fügt den externen IdP als vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzu.	Externer IdP-Administrator (Trusted Token Issuer)
	Hilft beim Einrichten der korrekten Attributzuordnung zwischen IAM Identity Center und dem externen IdP.	AWS Dienstadministrator
	Benachrichtigt den AWS Dienstadministrator, wenn der vertrauenswürdige Token-Aussteller zur IAM Identity Center-Konsole hinzugefügt wird.	
Externer IdP-Administrator (vertrauenswürdig)	Konfiguriert den externen IdP für die Ausgabe von Tokens. Hilft beim Einrichten der korrekten Attributzuordnung zwischen IAM	IAM Identity Center-Administrator AWS Dienstadministrator

Rolle	Führt diese Aufgaben aus	Koordiniert mit
Vertrauenswürdiger Token-Aussteller)	<p>Identity Center und dem externen IdP.</p> <p>Stellt dem Serviceadministrator den Namen der Zielgruppe (Aud-Anspruch) zur AWS Verfügung.</p>	
AWS Dienstadministrator	<p>Überprüft die AWS Servicekonsole auf den Aussteller des vertrauenswürdigen Tokens. Der Aussteller des vertrauenswürdigen Tokens wird in der AWS Servicekonsole angezeigt, nachdem der IAM Identity Center-Administrator ihn zur IAM Identity Center-Konsole hinzugefügt hat.</p> <p>Konfiguriert den AWS Dienst so, dass er den vertrauenswürdigen Token-Aussteller verwendet.</p>	<p>IAM Identity Center-Administrator</p> <p>Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller)</p>

Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Ausstellers

Um einen vertrauenswürdigen Token-Aussteller einzurichten, müssen ein IAM Identity Center-Administrator, ein externer IdP-Administrator (Trusted Token Issuer) und ein Anwendungsadministrator die folgenden Aufgaben ausführen.

Note

Bei der Anwendung kann es sich um einen beliebigen AWS Dienst handeln, der in IAM Identity Center integriert ist und die Verbreitung vertrauenswürdiger Identitäten unterstützt.

1. Den vertrauenswürdigen Token-Aussteller zu IAM Identity Center hinzufügen — Der IAM Identity Center-Administrator [fügt den vertrauenswürdigen Token-Aussteller mithilfe der IAM](#)

[Identity Center-Konsole oder der APIs hinzu. https://docs.aws.amazon.com/singlesignon/latest/APIReference/API_Operations.html](https://docs.aws.amazon.com/singlesignon/latest/APIReference/API_Operations.html) Für diese Konfiguration müssen Sie Folgendes angeben:

- Ein Name für den vertrauenswürdigen Token-Aussteller.
 - Die URL des OIDC-Discovery-Endpunkts (in der IAM Identity Center-Konsole wird diese URL als Aussteller-URL bezeichnet). Der Discovery-Endpunkt darf nur über die Ports 80 und 443 erreichbar sein.
 - Attributzuordnung für die Benutzersuche. Diese Attributzuordnung wird in einem Anspruch in dem Token verwendet, der vom vertrauenswürdigen Token-Aussteller generiert wird. Der Wert im Anspruch wird für die Suche im IAM Identity Center verwendet. Bei der Suche wird das angegebene Attribut verwendet, um einen einzelnen Benutzer im IAM Identity Center abzurufen.
2. Den AWS Dienst mit IAM Identity Center verbinden — Der AWS Dienstadministrator muss die Anwendung mit dem IAM Identity Center verbinden, indem er die Konsole für die Anwendung oder die Anwendungs-APIs verwendet.

Nachdem der vertrauenswürdige Token-Aussteller zur IAM Identity Center-Konsole hinzugefügt wurde, ist er auch in der AWS Servicekonsole sichtbar und kann vom Serviceadministrator ausgewählt werden. AWS

3. Konfiguration der Verwendung des Tokenaustauschs — In der AWS Servicekonsole konfiguriert AWS der AWS Dienstadministrator den Dienst so, dass er vom vertrauenswürdigen Token-Aussteller ausgegebene Token akzeptiert. Diese Token werden gegen Tokens ausgetauscht, die vom IAM Identity Center generiert wurden. Dazu müssen Sie den Namen des vertrauenswürdigen Token-Ausstellers aus Schritt 1 sowie den Aud-Anspruchswert angeben, der AWS dem Service entspricht.

Der Aussteller des vertrauenswürdigen Tokens platziert den Aud-Anspruchswert in das ausgegebene Token, um anzuzeigen, dass das Token für die Verwendung durch den AWS Dienst vorgesehen ist. Um diesen Wert zu erhalten, wenden Sie sich an den Administrator des vertrauenswürdigen Token-Ausstellers.

Wie füge ich der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzu

In einer Organisation mit mehreren Administratoren wird diese Aufgabe von einem IAM Identity Center-Administrator ausgeführt. Wenn Sie der IAM Identity Center-Administrator sind, müssen Sie auswählen, welcher externe IdP als vertrauenswürdiger Token-Aussteller verwendet werden soll.

So fügen Sie der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Authentifizierung“.
4. Wählen Sie unter Vertrauenswürdige Token-Aussteller die Option Vertrauenswürdigen Token-Aussteller erstellen aus.
5. Gehen Sie auf der Seite Einen externen IdP für die Ausgabe vertrauenswürdiger Token einrichten unter Details zum Aussteller des vertrauenswürdigen Tokens wie folgt vor:
 - Geben Sie unter Aussteller-URL die [OIDC-Discovery-URL](#) des externen IdP an, der Token für die Weitergabe vertrauenswürdiger Identitäten ausstellt. Sie müssen die URL des Discovery-Endpunkts bis zum Ende angeben. `.well-known/openid-configuration` Der Administrator des externen IdP kann diese URL bereitstellen.

 Note

Hinweis: Diese URL muss mit der URL im Issuer (iss) -Anspruch in Tokens übereinstimmen, die für die Verbreitung vertrauenswürdiger Identitäten ausgegeben werden.

- Geben Sie im IAM Identity Center und in der Anwendungskonsole unter Name des vertrauenswürdigen Token-Ausstellers einen Namen ein, mit dem dieser vertrauenswürdige Token-Aussteller identifiziert werden kann.
6. Gehen Sie unter Zuordnungsattribute wie folgt vor:
 - Wählen Sie für das Identitätsanbieterattribut ein Attribut aus der Liste aus, das einem Attribut im IAM Identity Center-Identitätsspeicher zugeordnet werden soll.
 - Wählen Sie für das IAM Identity Center-Attribut das entsprechende Attribut für die Attributzuordnung aus.
 7. Wählen Sie unter Tags (optional) die Option Neues Tag hinzufügen aus , geben Sie einen Wert für Schlüssel und optional für Value an.

Informationen zu Tags siehe [Ressourcen taggen AWS IAM Identity Center](#).

8. Wählen Sie Vertrauenswürdigen Token-Aussteller erstellen aus.

9. Wenn Sie mit der Erstellung des vertrauenswürdigen Token-Ausstellers fertig sind, wenden Sie sich an den Anwendungsadministrator, um ihm den Namen des vertrauenswürdigen Token-Ausstellers mitzuteilen, damit er bestätigen kann, dass der vertrauenswürdige Token-Aussteller in der entsprechenden Konsole sichtbar ist.
10. Der Anwendungsadministrator muss diesen vertrauenswürdigen Token-Aussteller in der entsprechenden Konsole auswählen, um Benutzern den Zugriff auf die Anwendung über Anwendungen zu ermöglichen, die für die Weitergabe vertrauenswürdiger Identitäten konfiguriert sind.

Wie kann ich die Einstellungen für den Aussteller eines vertrauenswürdigen Tokens in der IAM Identity Center-Konsole anzeigen oder bearbeiten

Nachdem Sie der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzugefügt haben, können Sie die entsprechenden Einstellungen anzeigen und bearbeiten.

Wenn Sie vorhaben, die Einstellungen für den Aussteller des vertrauenswürdigen Tokens zu bearbeiten, beachten Sie, dass Benutzer dadurch möglicherweise den Zugriff auf alle Anwendungen verlieren, die für die Verwendung des vertrauenswürdigen Tokens konfiguriert sind. Um zu verhindern, dass der Benutzerzugriff unterbrochen wird, empfehlen wir Ihnen, sich mit den Administratoren über alle Anwendungen abzustimmen, die für die Verwendung des vertrauenswürdigen Tokens konfiguriert sind, bevor Sie die Einstellungen bearbeiten.

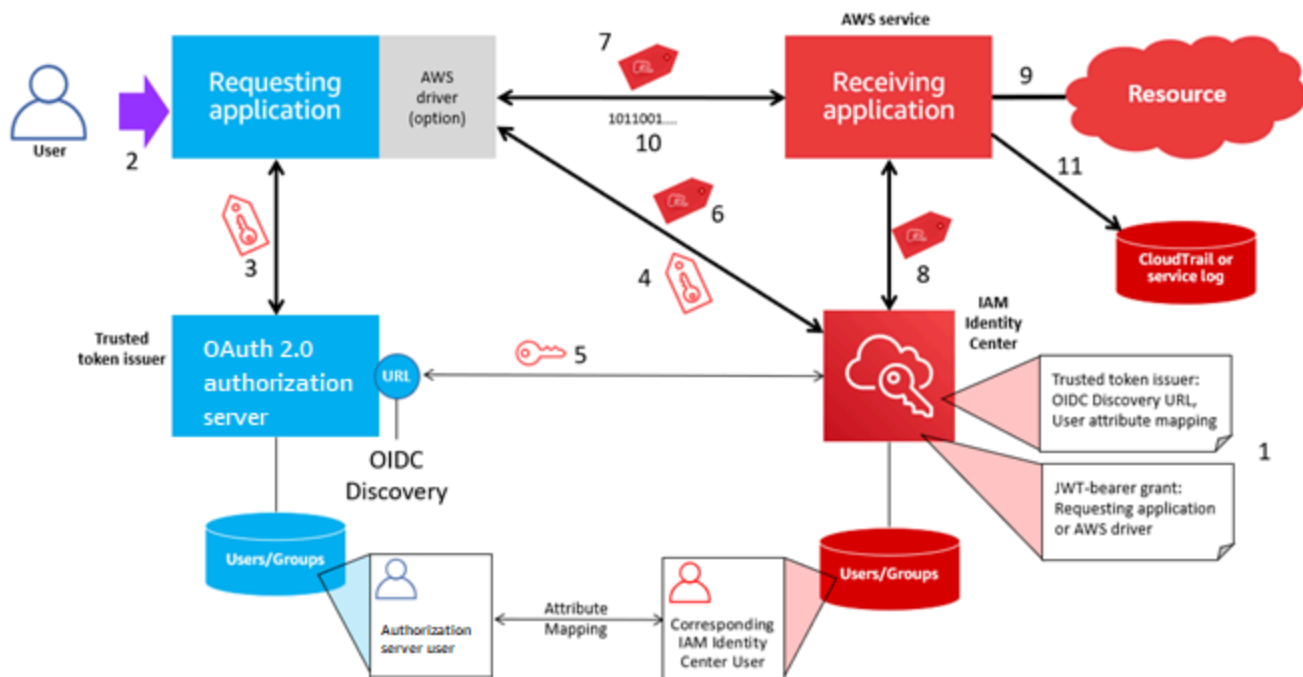
So können Sie die Einstellungen für den Aussteller des vertrauenswürdigen Tokens in der IAM Identity Center-Konsole anzeigen oder bearbeiten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Authentifizierung“.
4. Wählen Sie unter Vertrauenswürdige Token-Aussteller den vertrauenswürdigen Token-Aussteller aus, den Sie anzeigen oder bearbeiten möchten.
5. Wählen Sie Actions und anschließend Bearbeiten.
6. Auf der Seite „Aussteller des vertrauenswürdigen Tokens bearbeiten“ können Sie die Einstellungen nach Bedarf anzeigen oder bearbeiten. Sie können den Namen des Herausgebers des vertrauenswürdigen Tokens, die Attributzuordnungen und die Tags bearbeiten.
7. Wählen Sie Änderungen speichern aus.

8. Im Dialogfeld „Herausgeber des vertrauenswürdigen Tokens bearbeiten“ werden Sie aufgefordert, zu bestätigen, dass Sie Änderungen vornehmen möchten. Wählen Sie Bestätigen aus.

Einrichtungsprozess und Anforderungsablauf für Anwendungen, die einen vertrauenswürdigen Token-Aussteller verwenden

In diesem Abschnitt werden der Einrichtungsprozess und der Anforderungsablauf für Anwendungen beschrieben, die einen vertrauenswürdigen Token-Aussteller für die Weitergabe vertrauenswürdiger Identitäten verwenden. Das folgende Diagramm gibt einen Überblick über diesen Prozess.



Die folgenden Schritte enthalten zusätzliche Informationen zu diesem Prozess.

1. Richten Sie IAM Identity Center und die empfangende AWS verwaltete Anwendung so ein, dass sie einen vertrauenswürdigen Token-Aussteller verwenden. Weitere Informationen finden Sie unter [Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Ausstellers](#).
2. Der Anforderungsablauf beginnt, wenn ein Benutzer die anfordernde Anwendung öffnet.
3. Die anfordernde Anwendung fordert ein Token vom vertrauenswürdigen Token-Aussteller an, um Anfragen an die empfangende AWS verwaltete Anwendung zu initiieren. Wenn sich der Benutzer noch nicht authentifiziert hat, löst dieser Prozess einen Authentifizierungsablauf aus. Das Token enthält die folgenden Informationen:

- Der Betreff (Sub) des Benutzers.
 - Das Attribut, das IAM Identity Center verwendet, um den entsprechenden Benutzer in IAM Identity Center zu suchen.
 - Ein Audience-Anspruch (Aud), der einen Wert enthält, den der vertrauenswürdige Token-Aussteller der empfangenden AWS verwalteten Anwendung zuordnet. Wenn andere Ansprüche vorliegen, werden sie vom IAM Identity Center nicht verwendet.
4. Die anfordernde Anwendung oder der von ihr verwendete AWS Treiber übergibt das Token an IAM Identity Center und fordert an, dass das Token gegen ein von IAM Identity Center generiertes Token ausgetauscht wird. Wenn Sie einen AWS Treiber verwenden, müssen Sie den Treiber möglicherweise für diesen Anwendungsfall konfigurieren. Weitere Informationen finden Sie in der Dokumentation der jeweiligen AWS verwalteten Anwendung.
5. IAM Identity Center verwendet den OIDC Discovery-Endpunkt, um den öffentlichen Schlüssel abzurufen, mit dem es die Echtheit des Tokens überprüfen kann. IAM Identity Center führt dann Folgendes aus:
- Überprüft das Token.
 - Durchsucht das Identity Center-Verzeichnis. Dazu verwendet IAM Identity Center das zugeordnete Attribut, das im Token angegeben ist.
 - Überprüft, ob der Benutzer berechtigt ist, auf die empfangende Anwendung zuzugreifen. Wenn die AWS verwaltete Anwendung so konfiguriert ist, dass Zuweisungen an Benutzer und Gruppen erforderlich sind, muss der Benutzer der Anwendung direkt oder gruppenbasiert zugewiesen sein. Andernfalls wird die Anfrage abgelehnt. Wenn die AWS verwaltete Anwendung so konfiguriert ist, dass keine Benutzer- und Gruppenzuweisungen erforderlich sind, wird die Verarbeitung fortgesetzt.

 Note

AWS Dienste verfügen über eine Standardeinstellungskonfiguration, die bestimmt, ob Zuweisungen für Benutzer und Gruppen erforderlich sind. Es wird empfohlen, die Einstellung „Zuweisungen erforderlich“ für diese Anwendungen nicht zu ändern, wenn Sie sie für die Weitergabe vertrauenswürdiger Identitäten verwenden möchten. Selbst wenn Sie detaillierte Berechtigungen konfiguriert haben, die Benutzern den Zugriff auf bestimmte Anwendungsressourcen ermöglichen, kann eine Änderung der Einstellung „Zuweisungen erforderlich“ zu unerwartetem Verhalten führen, einschließlich einer Unterbrechung des Benutzerzugriffs auf diese Ressourcen.

- Überprüft, ob die anfordernde Anwendung so konfiguriert ist, dass sie gültige Bereiche für die empfangende verwaltete Anwendung verwendet. AWS
6. Wenn die vorherigen Überprüfungsschritte erfolgreich sind, erstellt IAM Identity Center ein neues Token. Das neue Token ist ein undurchsichtiges (verschlüsseltes) Token, das die Identität des entsprechenden Benutzers im IAM Identity Center, die Zielgruppe (Aud) der empfangenden AWS verwalteten Anwendung und die Bereiche enthält, die die anfordernde Anwendung verwenden kann, wenn sie Anfragen an die empfangende verwaltete Anwendung stellt. AWS
 7. Die anfordernde Anwendung oder der von ihr verwendete Treiber initiiert eine Ressourcenanforderung an die empfangende Anwendung und übergibt das von IAM Identity Center generierte Token an die empfangende Anwendung.
 8. Die empfangende Anwendung ruft das IAM Identity Center auf, um die Identität des Benutzers und die im Token kodierten Bereiche zu ermitteln. Sie kann auch Anfragen stellen, um Benutzerattribute oder die Gruppenmitgliedschaften des Benutzers aus dem Identity Center-Verzeichnis abzurufen.
 9. Die empfangende Anwendung verwendet ihre Autorisierungsconfiguration, um zu ermitteln, ob der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen.
 10. Wenn der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen, reagiert die empfangende Anwendung auf die Anfrage.
 11. Die Identität des Benutzers, in seinem Namen ausgeführte Aktionen und andere Ereignisse werden in den Protokollen und CloudTrail Ereignissen der empfangenden Anwendung aufgezeichnet. Die genaue Art und Weise, wie diese Informationen protokolliert werden, ist je nach Anwendung unterschiedlich.

Identity-enhanced IAM-Rollensitzungen

Das [AWS -Security-Token-Service](#) (STS) ermöglicht es einer Anwendung, eine IAM-Rollensitzung mit erweiterter Identität abzurufen. Identity-enhanced Rollensitzungen verfügen über einen zusätzlichen Identitätskontext, der eine Benutzerkennung zu dem Kontext enthält AWS-Service, den sie aufrufen. AWS-Services kann die Gruppenmitgliedschaften und Attribute des Benutzers im IAM Identity Center nachschlagen und sie verwenden, um den Zugriff des Benutzers auf Ressourcen zu autorisieren.

AWS Anwendungen erhalten Rollensitzungen mit erweiterter Identität, indem sie Anfragen an die AWS STS [AssumeRole](#) API-Aktion stellen und eine Kontext-Assertion mit der Benutzerkennung (userId) im Parameter der ProvidedContexts Anfrage an übergeben. AssumeRole Die Kontext-Assertion wird aus dem idToken Anspruch abgeleitet, der als Antwort auf eine Anfrage

an an eingegangen ist. SSO OIDC [CreateTokenWithIAM](#) Wenn eine AWS Anwendung eine Rollensitzung mit erweiterter Identität für den Zugriff auf eine Ressource verwendet, werden die `userId` initiiierende Sitzung und die ausgeführte Aktion CloudTrail protokolliert. Weitere Informationen finden Sie unter [Identity-enhanced IAM-Rolle, Sitzungsprotokollierung](#).

Themen

- [Arten von IAM-Rollensitzungen mit erweiterter Identität](#)
- [Identity-enhanced IAM-Rolle, Sitzungsprotokollierung](#)

Arten von IAM-Rollensitzungen mit erweiterter Identität

AWS STS kann zwei verschiedene Typen von IAM-Rollensitzungen mit erweiterter Identität erstellen, abhängig von der Kontext-Assertion, die für die Anfrage bereitgestellt wird. `AssumeRole` Anwendungen, die ID-Token vom IAM Identity Center erhalten haben, können IAM-Rollensitzungen hinzufügen `sts:identity_context` (empfohlen) oder `sts:audit_context` (aus Gründen der Abwärtskompatibilität unterstützt). Eine IAM-Rollensitzung mit erweiterter Identität kann nur eine dieser Kontextzusicherungen enthalten, nicht beide.

Identity-enhanced IAM-Rollensitzungen, die mit `sts:identity_context` erstellt wurden

Wenn eine Rollensitzung mit erweiterter Identität `sts:identity_context` den Aufgerufenen enthält, wird AWS-Service bestimmt, ob die Ressourcenautorisierung auf dem Benutzer basiert, der in der Rollensitzung vertreten ist, oder ob sie auf der Rolle basiert. AWS-Services die die benutzerbasierte Autorisierung unterstützen, bieten dem Administrator der Anwendung Steuerelemente, mit denen er dem Benutzer oder Gruppen, denen der Benutzer angehört, Zugriff gewähren kann.

AWS-Services die keine benutzerbasierte Autorisierung unterstützen, ignorieren Sie die. `sts:identity_context` CloudTrail protokolliert die Benutzer-ID des IAM Identity Center-Benutzers mit allen von der Rolle ausgeführten Aktionen. Weitere Informationen finden Sie unter [Identity-enhanced IAM-Rolle, Sitzungsprotokollierung](#).

Um diese Art von Sitzung mit erweiterter Identität abzurufen AWS STS, stellen Anwendungen den Wert des `sts:identity_context` Felds in der Anforderung mithilfe des [AssumeRole](#) Anforderungsparameters bereit. `ProvidedContexts` Verwenden Sie `arn:aws:iam::aws:contextProvider/IdentityCenter` als Wert für. `ProviderArn`

Weitere Informationen zum Verhalten der Autorisierung finden Sie in der Dokumentation zum Empfang AWS-Service.

Identity-enhanced IAM-Rollensitzungen, die mit sts:audit_context erstellt wurden

In der Vergangenheit `sts:audit_context` wurde es verwendet, um die Benutzeridentität protokollieren AWS-Services zu können, ohne sie für eine Autorisierungsentscheidung zu verwenden. AWS-Services sind jetzt in der Lage, einen einzigen Kontext zu `sts:identity_context` verwenden, um dies zu erreichen und Autorisierungsentscheidungen zu treffen. Wir empfehlen, `sts:identity_context` in allen neuen Bereitstellungen vertrauenswürdige Identitätsverbreitung zu verwenden.

Identity-enhanced IAM-Rolle, Sitzungsprotokollierung

Wenn eine Anfrage an eine Sitzung AWS-Service mit erweiterter IAM-Rollenfunktion gestellt wird, `userId` wird das IAM Identity Center des Benutzers in dem Element angemeldet. CloudTrail `OnBehalfOf` Die Art und Weise, wie Ereignisse angemeldet werden, CloudTrail variiert je nach AWS-Service Nicht alle AWS-Services protokollieren das `onBehalfOf` Element.

Im Folgenden finden Sie ein Beispiel dafür, wie eine Anfrage an eine Sitzung AWS-Service mit erweiterter Identität angemeldet wird. CloudTrail

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
```

```
}  
}
```

IAM Identity Center-Zertifikate rotieren

IAM Identity Center verwendet Zertifikate, um eine SAML-Vertrauensbeziehung zwischen IAM Identity Center und dem Dienstanbieter Ihrer Anwendung einzurichten. Wenn Sie eine Anwendung in IAM Identity Center hinzufügen, wird während des Einrichtungsvorgangs automatisch ein IAM Identity Center-Zertifikat für die Verwendung mit dieser Anwendung erstellt. Dieses automatisch generierte IAM Identity Center-Zertifikat ist standardmäßig für einen Zeitraum von fünf Jahren gültig.

Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere Zertifikate für eine bestimmte Anwendung durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein Zertifikat ersetzen, wenn sich das Ablaufdatum des Zertifikats nähert. Das Ersetzen eines älteren Zertifikats durch ein neueres wird als Zertifikatsrotation bezeichnet.

Überlegungen vor der Rotation eines Zertifikats

Bevor Sie mit der Rotation eines Zertifikats im IAM Identity Center beginnen, sollten Sie Folgendes berücksichtigen:

- Der Zertifizierungsrotationsprozess erfordert, dass Sie das Vertrauen zwischen IAM Identity Center und dem Dienstanbieter wiederherstellen. Verwenden Sie die unter beschriebenen Verfahren, um das Vertrauen wiederherzustellen. [Rotieren Sie ein IAM Identity Center-Zertifikat](#)
- Wenn Sie das Zertifikat beim Dienstanbieter aktualisieren, kann dies zu einer vorübergehenden Dienstunterbrechung für Ihre Benutzer führen, bis die Vertrauensstellung erfolgreich wiederhergestellt wurde. Planen Sie diesen Vorgang nach Möglichkeit sorgfältig außerhalb der Spitzenzeiten.

Rotieren Sie ein IAM Identity Center-Zertifikat

Das Rotieren eines IAM Identity Center-Zertifikats ist ein mehrstufiger Prozess, der Folgendes umfasst:

- Generieren eines neuen Zertifikats
- Hinzufügen des neuen Zertifikats zur Website des Dienstanbieters
- Das neue Zertifikat auf aktiv setzen

- Löschen des inaktiven Zertifikats

Verwenden Sie alle folgenden Verfahren in der folgenden Reihenfolge, um den Zertifikatsrotationsprozess für eine bestimmte Anwendung abzuschließen.

Schritt 1: Generieren Sie ein neues Zertifikat

Neue IAM Identity Center-Zertifikate, die Sie generieren, können so konfiguriert werden, dass sie die folgenden Eigenschaften verwenden:

- **Gültigkeitszeitraum** — Gibt die Zeit an (in Monaten), bis ein neues IAM Identity Center-Zertifikat abläuft.
- **Schlüsselgröße** — Bestimmt die Anzahl der Bits, die ein Schlüssel mit seinem kryptografischen Algorithmus verwenden muss. Sie können diesen Wert entweder auf 1024-Bit-RSA oder 2048-Bit-RSA festlegen. Allgemeine Informationen zur Funktionsweise von Schlüsselgrößen in der Kryptografie finden Sie unter [Schlüsselgröße](#).
- **Algorithmus** — Gibt den Algorithmus an, den IAM Identity Center beim Signieren der SAML assertion/response verwendet. Sie können diesen Wert auf entweder SHA-1 oder SHA-256 setzen. AWS empfiehlt die Verwendung von SHA-256, sofern dies möglich ist, sofern Ihr Dienstanbieter dies nicht verlangt SHA-1. Allgemeine Informationen zur Funktionsweise von Kryptografiealgorithmen finden Sie unter [Public-key](#) Kryptografie.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen die Anwendung aus, für die Sie ein neues Zertifikat generieren möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Registerkarte Konfiguration aus. Wählen Sie unter IAM Identity Center-Metadaten die Option Zertifikat verwalten aus. Wenn Sie nicht über eine Registerkarte „Konfiguration“ verfügen oder die Konfigurationseinstellung nicht verfügbar ist, müssen Sie das Zertifikat für diese Anwendung nicht rotieren.
5. Wählen Sie auf der Seite mit dem IAM Identity Center-Zertifikat die Option Neues Zertifikat generieren aus.
6. Geben Sie im Dialogfeld Neues IAM Identity Center-Zertifikat generieren die entsprechenden Werte für Gültigkeitszeitraum, Algorithmus und Schlüsselgröße an. Wählen Sie dann Generieren aus.

Schritt 2: Aktualisieren Sie die Website des Diensteanbieters

Gehen Sie wie folgt vor, um die Vertrauensstellung mit dem Diensteanbieter der Anwendung wiederherzustellen.

Important

Wenn Sie das neue Zertifikat zum Diensteanbieter hochladen, können sich Ihre Benutzer möglicherweise nicht authentifizieren. Um diese Situation zu korrigieren, legen Sie das neue Zertifikat wie im nächsten Schritt beschrieben als aktiv fest.

1. Wählen Sie in der [IAM Identity Center-Konsole die Anwendung aus](#), für die Sie gerade ein neues Zertifikat generiert haben.
2. Wählen Sie auf der Seite mit den Anwendungsdetails die Option **Konfiguration bearbeiten** aus.
3. Wählen Sie **Anweisungen anzeigen** aus und folgen Sie dann den Anweisungen auf der Website Ihres jeweiligen Anwendungsdiensteanbieters, um das neu generierte Zertifikat hinzuzufügen.

Schritt 3: Setzen Sie das neue Zertifikat auf aktiv

Einer Anwendung können bis zu zwei Zertifikate zugewiesen werden. IAM Identity Center verwendet die als aktiv eingestellte Zertifizierung, um alle SAML-Assertionen zu signieren.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie **Applications (Anwendungen)**.
3. Wählen Sie in der Liste der Anwendungen Ihre Anwendung aus.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die **Registerkarte Konfiguration** aus. Wählen Sie unter **IAM Identity Center-Metadaten** die Option **Zertifikat verwalten** aus.
5. Wählen Sie auf der Seite mit dem **IAM Identity Center-Zertifikat** das Zertifikat aus, das Sie als aktiv festlegen möchten, wählen Sie **Aktionen** und dann **Als aktiv festlegen** aus.
6. Bestätigen Sie im Dialogfeld **Ausgewähltes Zertifikat als aktiv festlegen**, dass Sie verstehen, dass Sie möglicherweise die Vertrauensstellung erneut einrichten müssen, wenn Sie ein Zertifikat auf aktiv setzen, und wählen Sie dann **Make active** aus.

Schritt 4: Löschen Sie das alte Zertifikat

Gehen Sie wie folgt vor, um den Zertifikatsrotationsprozess für Ihre Bewerbung abzuschließen. Sie können nur ein Zertifikat löschen, das sich im Status `Inaktiv` befindet.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie `Applications` (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen Ihre Anwendung aus.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Registerkarte `Konfiguration` aus. Wählen Sie unter `IAM Identity Center-Metadaten` die Option `Zertifikat verwalten` aus.
5. Wählen Sie auf der Seite mit dem `IAM Identity Center-Zertifikat` das Zertifikat aus, das Sie löschen möchten. Wählen Sie `Actions` und dann `Delete` aus.
6. Wählen Sie im Dialogfeld `Zertifikat löschen` die Option `Löschen` aus.

Indikatoren für den Ablaufstatus des Zertifikats

In der IAM Identity Center-Konsole werden auf der Seite „Anwendungen“ Statusanzeigesymbole in den Eigenschaften der einzelnen Anwendungen angezeigt. Diese Symbole werden in der Spalte `Läuft ab am` neben jedem Zertifikat in der Liste angezeigt. Im Folgenden werden die Kriterien beschrieben, anhand derer IAM Identity Center bestimmt, welches Symbol für jedes Zertifikat angezeigt wird.

- Rot — Zeigt an, dass ein Zertifikat derzeit abgelaufen ist.
- Gelb — Zeigt an, dass ein Zertifikat in 90 Tagen oder weniger abläuft.
- Grün — Zeigt an, dass ein Zertifikat derzeit gültig ist und noch mindestens 90 Tage gültig bleibt.

Um den Status eines Zertifikats zu überprüfen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie `Applications` (Anwendungen).
3. Überprüfen Sie in der Liste der Anträge den Status der Zertifikate in der Liste, wie in der Spalte `Läuft ab am` angegeben.

Machen Sie sich mit den Anwendungseigenschaften in der IAM Identity Center-Konsole vertraut

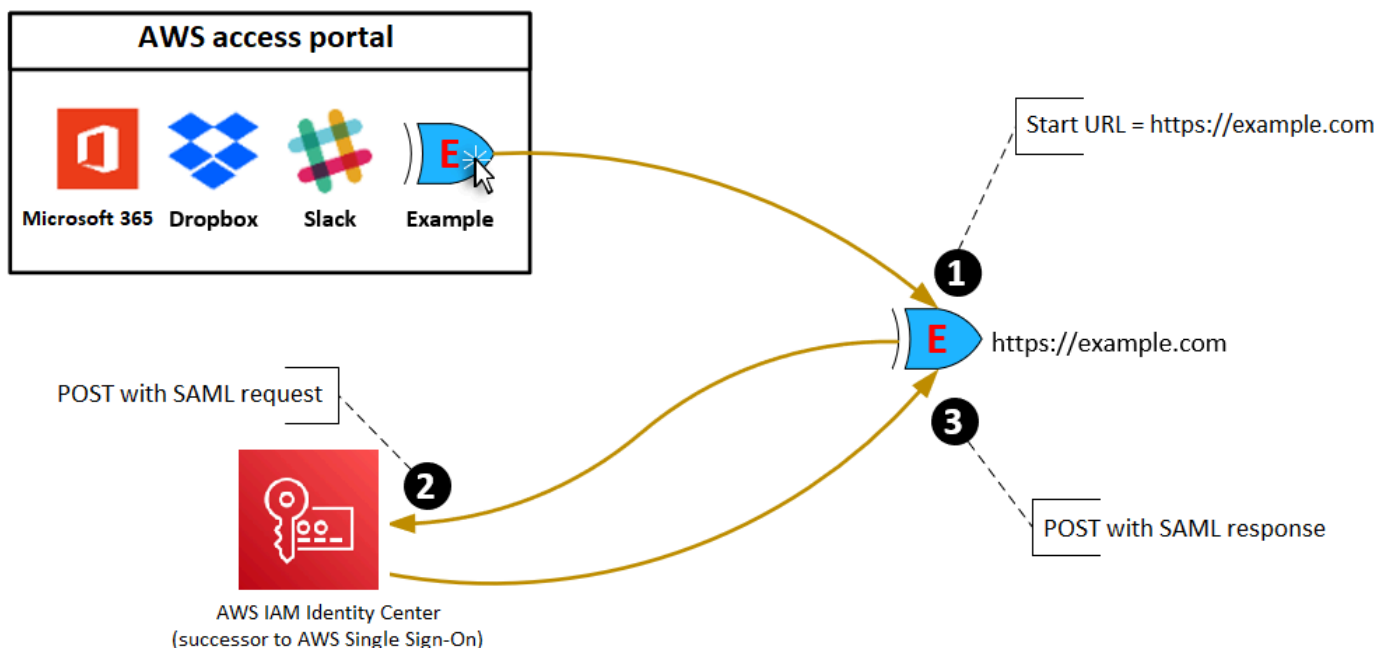
In IAM Identity Center können Sie die Benutzererfahrung anpassen, indem Sie die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer konfigurieren.

URL zum Starten der Anwendung

Sie verwenden eine Anwendungs-Start-URL, um den Verbundprozess mit Ihrer Anwendung zu starten. In der Regel wird eine Anwendung verwendet, die nur vom Service Provider (SP) initiierte Bindungen unterstützt.

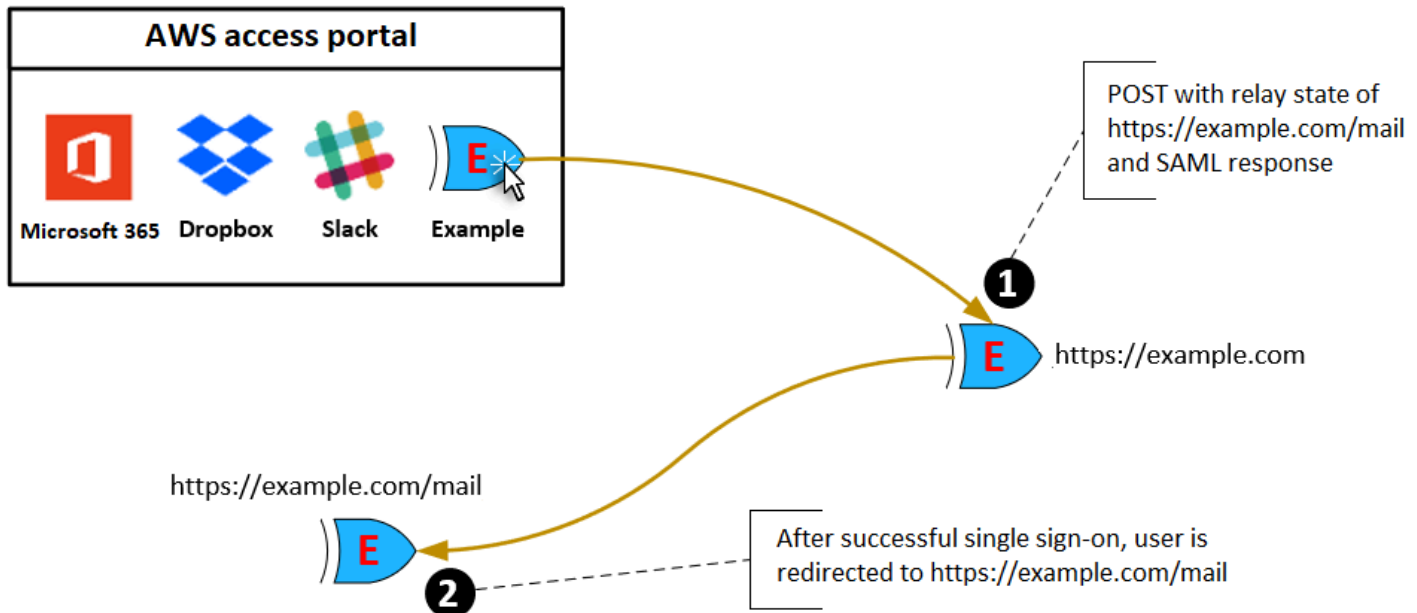
Die folgenden Schritte und das folgende Diagramm veranschaulichen den Workflow zur URL-Authentifizierung beim Start einer Anwendung, wenn ein Benutzer im AWS Access Portal eine Anwendung auswählt:

1. Der Browser des Benutzers leitet die Authentifizierungsanforderung unter Verwendung des Werts für die Anwendungsstart-URL um (in diesem Fall `https://example.com`).
2. Die Anwendung sendet eine HTML POST mit einer SAMLRequest an das IAM Identity Center.
3. IAM Identity Center sendet dann eine Nachricht HTML POST mit einem SAMLResponse zurück an die Anwendung.



Status weiterleiten

Während des Verbund-Authentifizierungsprozesses leitet der Relais-Status Benutzer innerhalb der Anwendung um. Für SAML 2.0 wird dieser Wert unverändert an die Anwendung übergeben. Nachdem die Anwendungseigenschaften konfiguriert wurden, sendet IAM Identity Center den Relay-Statuswert zusammen mit einer SAML-Antwort an die Anwendung.



Sitzungsdauer

Die Sitzungsdauer ist der Zeitraum, für den eine Anwendungsbenutzersitzung gültig ist. Für SAML 2.0 wird dies verwendet, um das `SessionNotOnOrAfter` Datum des Elements der SAML-Assertion festzulegen. `saml2:AuthNStatement`

Die Sitzungsdauer kann von Anwendungen auf eine der folgenden Arten interpretiert werden:

- Anwendungen können es verwenden, um die maximale Zeit zu ermitteln, die für die Sitzung des Benutzers zulässig ist. Anwendungen generieren möglicherweise eine Benutzersitzung mit einer kürzeren Dauer. Dies kann der Fall sein, wenn die Anwendung nur Benutzersitzungen mit einer Dauer unterstützt, die kürzer ist als die konfigurierte Länge der Sitzung ist.
- Anwendungen können sie als exakte Dauer ansehen und Administratoren möglicherweise nicht erlauben, den Wert zu konfigurieren. Dies kann der Fall sein, wenn die Anwendung nur eine bestimmte Sitzungsdauer unterstützt.

Weitere Informationen darüber, wie die Sitzungsdauer verwendet wird, finden Sie in der Dokumentation der betreffenden Anwendung.

Weisen Sie den Benutzerzugriff auf Anwendungen in der IAM Identity Center-Konsole zu

Sie können Benutzern Single-Sign-On-Zugriff auf SAML 2.0-Anwendungen im Anwendungskatalog oder auf benutzerdefinierte SAML 2.0-Anwendungen zuweisen.

Überlegungen zu Gruppenzuweisungen:

- Weisen Sie Gruppen den Zugriff direkt zu. Um die Verwaltung der Zugriffsberechtigungen zu vereinfachen, empfehlen wir, den Zugriff direkt Gruppen und nicht einzelnen Benutzern zuzuweisen. Mit Gruppen können Sie Benutzergruppen Berechtigungen gewähren oder verweigern, anstatt diese Berechtigungen auf jeden einzelnen Benutzer anzuwenden. Wenn ein Benutzer in eine andere Organisation wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe. Der Benutzer erhält dann automatisch die erforderlichen Berechtigungen für die neue Organisation.
- Verschachtelte Gruppen werden nicht unterstützt. Beim Zuweisen von Benutzerzugriff auf Anwendungen unterstützt IAM Identity Center nicht, dass Benutzer zu verschachtelten Gruppen hinzugefügt werden. Wenn ein Benutzer zu einer verschachtelten Gruppe hinzugefügt wird, erhält er möglicherweise bei der Anmeldung die Meldung „Sie haben keine Anwendungen“. Zuweisungen müssen für die unmittelbare Gruppe vorgenommen werden, der der Benutzer angehört.

Um Benutzern oder Gruppen Zugriff auf Anwendungen zu gewähren

Important

Für AWS verwaltete Anwendungen müssen Sie Benutzer direkt von den entsprechenden Anwendungskonsolen aus oder über die APIs hinzufügen.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

 Note

Wenn Sie Benutzer dort verwalten AWS Managed Microsoft AD, stellen Sie sicher, dass die IAM Identity Center-Konsole die AWS Region verwendet, in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen den Namen der Anwendung aus, der Sie Zugriff zuweisen möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails im Abschnitt Zugewiesene Benutzer die Option Benutzer zuweisen aus.
5. Geben Sie im Dialogfeld „Benutzer zuweisen“ einen Benutzer- oder Gruppennamen ein. Sie können mehrere Benutzer oder Gruppen angeben, indem Sie die entsprechenden Konten so auswählen, wie sie in den Suchergebnissen angezeigt werden.
6. Wählen Sie Assign users (Benutzer zuweisen) aus.

Entfernen Sie den Benutzerzugriff auf SAML 2.0-Anwendungen

Gehen Sie wie folgt vor, um den Benutzerzugriff auf SAML 2.0-Anwendungen im Anwendungskatalog oder auf benutzerdefinierte SAML 2.0-Anwendungen zu entfernen. Weitere Informationen zu Authentifizierungssitzungen und -dauern finden Sie unter [Grundlegendes zu Authentifizierungssitzungen in IAM Identity Center](#)

Um den Benutzerzugriff auf eine Anwendung zu entfernen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen die Anwendung aus, für die Sie den Benutzerzugriff entfernen möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails im Abschnitt Zugewiesene Benutzer den Benutzer oder die Gruppe aus, den Sie entfernen möchten, und klicken Sie dann auf die Schaltfläche Zugriff entfernen.
5. Überprüfen Sie im Dialogfeld Remove access (Zugriff entfernen) den Benutzer- oder Gruppennamen. Klicken Sie abschließend auf Remove access (Zugriff entfernen).

Ordnen Sie Attribute in Ihrer Anwendung den IAM Identity Center-Attributen zu

Einige Service-Anbieter erfordern benutzerdefinierte SAML-Zusicherungen, um zusätzliche Daten zu Ihren Benutzeranmeldungen zu übergeben. Verwenden Sie in diesem Fall das folgende Verfahren, um anzugeben, wie die Benutzerattribute Ihrer Anwendungen den entsprechenden Attributen in IAM Identity Center zugeordnet werden sollen.

So ordnen Sie Anwendungsattribute Attributen in IAM Identity Center zu

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen diejenige aus, für die Attribute zugeordnet werden sollen.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Option Aktionen aus und klicken Sie dann auf Attributzuordnung bearbeiten.
5. Wählen Sie Neue Attributzuordnung hinzufügen aus.
6. Geben Sie im ersten Textfeld das Anwendungsattribut ein.
7. Geben Sie im zweiten Textfeld das Attribut in IAM Identity Center ein, das Sie dem Anwendungsattribut zuordnen möchten. Beispielsweise möchten Sie möglicherweise das Anwendungsattribut **Username** dem IAM Identity Center-Benutzerattribut zuordnen **email**. Die Liste der zulässigen Benutzerattribute in IAM Identity Center finden Sie in der Tabelle unter [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#)
8. Wählen Sie in der dritten Spalte der Tabelle das entsprechende Format für das Attribut aus dem Menü aus.
9. Wählen Sie Änderungen speichern aus.

Konfigurieren Sie den Zugriff auf AWS-Konten

Organisationsinstanzen von IAM Identity Center sind integriert in AWS Organizations. Auf diese Weise können Sie mehrere Berechtigungen zentral verwalten, AWS-Konten ohne den Zugriff auf jedes Konto einzeln konfigurieren zu müssen.

In der folgenden Tabelle werden die Optionen zur Kontozugriffsverwaltung verglichen, die Sie in Betracht ziehen sollten:

	IAM-Rollen mit Kontozugriffsmanager	IAM Identity Center-Berechtigungssätze	IAM-Rollen mit direktem IAM-Verbindung
Am besten geeignet für	Workforce-Benutzer und Gruppen mit benutzerdefinierten IAM-Rollen, die je nach Konto unterschiedlich sind. Dezentrale Rollenerstellung und Bereitstellung mit zentraler Rollenzuweisung an Benutzer.	Einheitlicher Basiszugriff für Mitarbeiter, z. B. Schreibgeschützt und für Administratoren. Zentralisierte Rollenerstellung und Bereitstellung.	Workloads
Scope	Mehrere Konten in einer Organisation AWS	Mehrere Konten in einer AWS Organisation	Pro Konto
Bereitstellung von IAM-Rollen	<ul style="list-style-type: none"> Infrastructure as Code (IaC) Manuelle Bereitstellung über die IAM-Konsole AWS 	Automatisch bereitgestellt	<ul style="list-style-type: none"> Infrastructure as Code (IaC) Manuelle Bereitstellung über die AWS IAM-Konsole oder externe IdP-Konsolen

	IAM-Rollen mit Kontozugriffsmanager	IAM Identity Center- Berechtigungssätze	IAM-Rollen mit direktem IAM-Verbu nd
Role-to-identity Die Zuordnung befindet sich in	Kontozugriffsmanager	IAM Identity Center	Externer IdP
Erfahrung für Endbenutzer	Benutzer greifen AWS-Konten über die URL des Kontozugr iffsportals zu. Erfordert die IAM Identity Center-Au thentifizierung.	Benutzer greifen AWS-Konten über die URL des AWS Zugriffsportals zu.	Benutzer greifen AWS-Konten über kontospezifische SAML-Anwendungen (Symbole) in ihrem IdP-Portal zu.

	IAM-Rollen mit Kontozugriffsmanager	IAM Identity Center-Berechtigungssätze	IAM-Rollen mit direktem IAM-Verbund
AWS CLI Benutzererfahrung	Der Benutzer meldet sich in einem Webbrowser an AWS und greift auf ein AWS-Konto mit einer bestimmten Rolle zu. Der Benutzer gibt in <code>aws login</code> der Befehlszeile ein, um die Anmeldeinformationen für die IAM-Rollensitzung aus dem Browser abzurufen. Während der Dauer der IAM-Rollensitzung kann der Benutzer mit dem arbeiten, AWS CLI ohne sich erneut zu authentifizieren.	Der Benutzer konfiguriert ein Profil, das das gewünschte Konto- und Rollenpaar enthält, indem er Folgendes eingibt. <code>aws configure sso</code> Der Benutzer gibt <code>aws sso login</code> , um eine neue Sitzung mithilfe eines Profils zu initiieren. Wenn es keine aktive IAM Identity Center-Sitzung gibt, authentifiziert sich der Benutzer in einem Browser. Weitere Informationen finden Sie im AWS IAM Identity Center Benutzerhandbuch.	Benutzerdefinierte Integrationen mithilfe von AWS SDK-Anmeldeinformationsanbietern

AWS-Konto Typen

Es gibt zwei Arten von AWS-Konten In AWS Organizations:

- Verwaltungskonto — Das Konto AWS-Konto , das zur Erstellung der Organisation verwendet wird.
- Mitgliedskonten — Die übrigen Konten AWS-Konten , die zu einer Organisation gehören.

Weitere Informationen zu AWS-Konto Typen finden Sie [im AWS Organizations Benutzerhandbuch unter](#) AWS Organizations Terminologie und Konzepte.

Sie können sich auch dafür entscheiden, ein Mitgliedskonto als delegierten Administrator für IAM Identity Center zu registrieren. Benutzer in diesem Konto können die meisten Verwaltungsaufgaben von IAM Identity Center ausführen. Weitere Informationen finden Sie unter [Delegierte Verwaltung](#).

In der folgenden Tabelle wird für jede Aufgabe und jeden Kontotyp angegeben, ob die IAM Identity Center-Verwaltungsaufgabe von Benutzern im Konto ausgeführt werden kann.

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
Benutzer oder Gruppen lesen (die Gruppe selbst und die Gruppenmitgliedschaft lesen)	✔ Ja	✔ Ja	✔ Ja
Benutzer oder Gruppen hinzufügen, bearbeiten oder löschen	✘ Nein	✔ Ja*	✔ Ja
Benutzerzugriff aktivieren oder deaktivieren	✘ Nein	✔ Ja	✔ Ja
Eingehende Attribute aktivieren, deaktivieren oder verwalten	✘ Nein	✔ Ja	✔ Ja
Identitätsquellen ändern oder verwalten	✘ Nein	✔ Ja	✔ Ja
Kundenverwaltete Anwendungen erstellen, bearbeiten oder löschen	✘ Nein	✔ Ja	✔ Ja

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
AWS Verwaltete Anwendungen erstellen, bearbeiten oder löschen	✔ Ja	✔ Ja	✔ Ja
MFA konfigurieren	✘ Nein	✔ Ja	✔ Ja
Berechtigungssätze verwalten, die nicht im Verwaltungskonto bereitgestellt wurden	✘ Nein	✔ Ja	✔ Ja
Im Verwaltungskonto bereitgestellte Berechtigungssätze verwalten	✘ Nein	✘ Nein	✔ Ja
IAM Identity Center aktivieren	✘ Nein	✘ Nein	✔ Ja
Löschen Sie die IAM Identity Center-Konfiguration	✘ Nein	✘ Nein	✔ Ja
Aktivieren oder deaktivieren Sie den Benutzerzugriff im Verwaltungskonto	✘ Nein	✘ Nein	✔ Ja
Registriere oder deregistriere ein Mitgliedskonto als delegierter Administrator	✘ Nein	✘ Nein	✔ Ja

*Lesen Sie die bewährten Methoden für die delegierte Verwaltung bezüglich der Benutzer- und Gruppenzuweisung zum Verwaltungskonto.

Status "Assigning" AWS-Konto access

Mithilfe von Berechtigungssätzen können Sie Benutzern und Gruppen in Ihrer Organisation den Zugriff auf Folgendes vereinfachen AWS-Konten. Berechtigungssätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, auf die Benutzer und Gruppen Zugriff haben. AWS-Konto Sie können einen einzelnen Berechtigungssatz erstellen und ihn mehreren Personen AWS-Konten innerhalb Ihrer Organisation zuweisen. Sie können demselben Benutzer auch mehrere Berechtigungssätze zuweisen.

Sie können den [Account Access Manager](#) — eine IAM-Funktion — auch verwenden, um IAM Identity Center-Benutzern und -Gruppen in den Konten Ihrer Organisation vorhandene IAM-Rollen zuzuweisen. Sie können den Account Access Manager einzeln oder zusammen mit Berechtigungssätzen verwenden. Mit dem Account Access Manager haben Sie Zugriff auf den gesamten Funktionsumfang der IAM-Rollen, einschließlich benutzerdefinierter Vertrauensrichtlinien, Rollentags für ABAC und konfigurierbarer Rollenpfade.

Weitere Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze erstellen, verwalten und löschen](#).

Note

Sie können Ihren Benutzern auch Single-Sign-On-Zugriff auf Anwendungen zuweisen. Weitere Informationen finden Sie unter [Zugriff auf Anwendungen konfigurieren](#).

End-user Erfahrung

Das AWS Zugriffsportal bietet IAM Identity Center-Benutzern über ein Webportal Single-Sign-On-Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen. Das AWS Zugriffsportal unterscheidet sich von dem [AWS-Managementkonsole](#), bei dem es sich um eine Sammlung von Servicekonsolen zur Verwaltung AWS von Ressourcen handelt.

Wenn Sie einen Berechtigungssatz erstellen, wird der Name, den Sie für den Berechtigungssatz angeben, im AWS Access Portal als verfügbare Rolle angezeigt. Benutzer melden sich beim

AWS Access-Portal an, wählen eine AWS-Konto und dann die Rolle aus. Nachdem sie die Rolle ausgewählt haben, können sie auf AWS Dienste zugreifen, indem sie die temporären Anmeldeinformationen verwenden AWS-Managementkonsole oder temporäre Anmeldeinformationen abrufen, um programmgesteuert auf AWS Dienste zuzugreifen.

Um die temporären Anmeldeinformationen für den AWS programmgesteuerten Zugriff zu öffnen AWS-Managementkonsole oder abzurufen, führen Benutzer die folgenden Schritte aus:

1. Benutzer öffnen ein Browserfenster und verwenden die von Ihnen angegebene Anmelde-URL, um zum Zugriffsportal zu navigieren. AWS
2. Mit ihren Verzeichnisanmeldeinformationen melden sie sich beim AWS Zugriffsportal an.
3. Nach der Authentifizierung wählen sie auf der AWS Access-Portalseite die Registerkarte Konten, um die Liste AWS-Konten anzuzeigen, auf die sie Zugriff haben.
4. Die Benutzer wählen dann AWS-Konto die aus, die sie verwenden möchten.
5. Unter dem Namen von werden alle Berechtigungssätze AWS-Konto, denen Benutzer zugewiesen sind, als verfügbare Rollen angezeigt. Wenn Sie dem PowerUser Berechtigungssatz beispielsweise john_styles einen Benutzer zugewiesen haben, wird die Rolle im AWS Access-Portal als angezeigtPowerUser/john_styles. Benutzer mit mehreren Berechtigungssätzen wählen aus, welche -Rolle verwendet werden soll. Benutzer können ihre Rolle für den Zugriff auf auswählen AWS-Managementkonsole.
6. Zusätzlich zur Rolle können AWS Access-Portal-Benutzer temporäre Anmeldeinformationen für den Befehlszeilen- oder programmgesteuerten Zugriff abrufen, indem sie Zugriffstasten wählen.

Eine schrittweise Anleitung, die Sie den Benutzern Ihrer Belegschaft zur Verfügung stellen können, finden Sie unter [Einrichtung und Verwendung des AWS auf das Portal zugreifen](#) und [Abrufen der IAM Identity Center-Benutzeranmeldedaten für AWS CLI oder AWS SDKs](#).

Durchsetzung und Beschränkung des Zugriffs

Wenn Sie IAM Identity Center aktivieren, erstellt IAM Identity Center eine serviceverknüpfte Rolle. Sie können auch Service Control Policies (SCPs) verwenden.

Delegieren und Durchsetzen des Zugriffs

Eine dienstgebundene Rolle ist eine Art von IAM-Rolle, die direkt mit einem Dienst verknüpft ist. AWS Nachdem Sie IAM Identity Center aktiviert haben, kann IAM Identity Center für jede Rolle in

Ihrer Organisation eine dienstverknüpfte Rolle erstellen. AWS-Konto Diese Rolle bietet vordefinierte Berechtigungen, die es IAM Identity Center ermöglichen, zu delegieren und durchzusetzen, welche Benutzer Single-Sign-On-Zugriff auf bestimmte Benutzer in Ihrer Organisation haben. AWS-Konten AWS Organizations Sie müssen einem oder mehreren Benutzern Zugriff auf ein Konto zuweisen, um diese Rolle verwenden zu können. Weitere Informationen erhalten Sie unter [Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center](#) und [Verwenden von dienstverknüpften Rollen für IAM Identity Center](#).

Beschränken Sie den Zugriff auf den Identitätsspeicher von Mitgliedskonten aus

Für den vom IAM Identity Center verwendeten Identitätsspeicherdienst können Benutzer, die Zugriff auf ein Mitgliedskonto haben, API-Aktionen verwenden, für die Leseberechtigungen erforderlich sind. Mitgliedskonten haben Zugriff auf Lese-Aktionen sowohl im SSO-Verzeichnis als auch im Identitystore-Namespace. Weitere Informationen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center Verzeichnisse und Aktionen, Ressourcen und Bedingungsschlüssel für Identity Store in der Serviceautorisierungsreferenz. AWS](#)

Um zu verhindern, dass Benutzer in Mitgliedskonten API-Operationen im Identitätsspeicher verwenden, können Sie eine Service Control Policy (SCP) https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_attach.html anhängen. Ein SCP ist eine Art von Organisationsrichtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können. Das folgende SCP-Beispiel verhindert, dass Benutzer in Mitgliedskonten auf API-Operationen im Identitätsspeicher zugreifen.

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

Note

Um sicherzustellen, dass Ihre AWS verwalteten Anwendungen problemlos mit Ihrem IAM Identity Center funktionieren, sollten Sie vermeiden, diesen SCP auf den Ort anzuwenden, an AWS-Konten dem Sie diese Anwendungen bereitgestellt haben. Wenn Sie die delegierte Administration verwenden, sollten Sie außerdem vermeiden, diesen SCP auf das Konto der

delegierten Administration anzuwenden. Weitere Informationen finden Sie unter [Bewährte Methoden](#).

Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien \(SCPs\)](#) im AWS Organizations - Benutzerhandbuch.

Delegierte Verwaltung

Die delegierte Administration bietet zugewiesenen Benutzern in einem registrierten Mitgliedskonto eine bequeme Möglichkeit, die meisten Verwaltungsaufgaben im IAM Identity Center auszuführen. Wenn Sie IAM Identity Center aktivieren, wird Ihre IAM Identity Center-Instanz standardmäßig im Verwaltungskonto erstellt. AWS Organizations Dies wurde ursprünglich so konzipiert, dass IAM Identity Center Rollen für alle Mitgliedskonten Ihrer Organisation bereitstellen, die Bereitstellung aufheben und aktualisieren kann. Obwohl sich Ihre IAM Identity Center-Instanz immer im Verwaltungskonto befinden muss, können Sie die Verwaltung von IAM Identity Center an ein Mitgliedskonto in delegieren und so die Möglichkeiten erweitern AWS Organizations, IAM Identity Center von außerhalb des Verwaltungskontos zu verwalten.

Die Aktivierung der delegierten Administration bietet die folgenden Vorteile:

- Minimiert die Anzahl der Personen, die Zugriff auf das Verwaltungskonto benötigen, um Sicherheitsbedenken auszuräumen
- Ermöglicht ausgewählten Administratoren das Zuweisen von Benutzern und Gruppen zu Anwendungen und Mitgliedskonten Ihrer Organisation

Weitere Informationen darüber, wie IAM Identity Center mit IAM Identity Center zusammenarbeitet AWS Organizations, finden Sie unter [Konfigurieren Sie den Zugriff auf AWS-Konten](#). Weitere Informationen und ein Beispiel für ein Unternehmensszenario zur Konfiguration der delegierten Administration finden Sie im Security Blog unter [Erste Schritte mit der delegierten IAM Identity Center-Administration](#). AWS

Themen

- [Bewährte Methoden](#)
- [Voraussetzungen](#)
- [Registrieren Sie ein Mitgliedskonto](#)
- [Aufheben der Registrierung eines Mitgliedskontos](#)

- [Sehen Sie sich an, welches Mitgliedskonto als delegierter Administrator registriert wurde](#)

Bewährte Methoden

Hier sind einige bewährte Methoden, die Sie berücksichtigen sollten, bevor Sie die delegierte Administration konfigurieren:

- Gewähren Sie dem Verwaltungskonto die geringsten Rechte — Da es sich bei dem Verwaltungskonto um ein Konto mit hohen Rechten handelt, und um das Prinzip der geringsten Rechte einzuhalten, empfehlen wir dringend, den Zugriff auf das Verwaltungskonto auf so wenige Personen wie möglich zu beschränken. Mit der Funktion für delegierte Administratoren soll die Anzahl der Personen minimiert werden, die Zugriff auf das Verwaltungskonto benötigen. Sie können auch erwägen, [vorübergehend erhöhten Zugriff](#) zu verwenden, um diesen Zugriff nur bei Bedarf zu gewähren.
- Dedizierte Berechtigungssätze für das Verwaltungskonto — Verwenden Sie dedizierte Berechtigungssätze für das Verwaltungskonto. Aus Sicherheitsgründen kann ein Berechtigungssatz, der für den Zugriff auf das Verwaltungskonto verwendet wird, nur von einem IAM Identity Center-Administrator vom Verwaltungskonto aus geändert werden. Der delegierte Administrator kann die im Verwaltungskonto bereitgestellten Berechtigungssätze nicht ändern.
- Nur Benutzer (keine Gruppen) Berechtigungssätzen im Verwaltungskonto zuweisen — Da das Verwaltungskonto über besondere Rechte verfügt, müssen Sie vorsichtig sein, wenn Sie diesem Konto in der Konsole oder AWS Command Line Interface (CLI) Zugriff gewähren. Wenn Sie Gruppen Berechtigungssätzen mit Zugriff auf das Verwaltungskonto zuweisen, kann add/remove jeder, der berechtigt ist, die Mitgliedschaften in diesen Gruppen zu ändern, to/from diese Gruppen verwenden und somit beeinflussen, wer Zugriff auf das Verwaltungskonto hat. Dies ist jeder Gruppenadministrator mit Kontrolle über Ihre Identitätsquelle, einschließlich Ihres Identitätsanbieters (IdP) -Administrators, Microsoft Active Directory-Domänendienst (AD DS) -Administrators oder IAM Identity Center-Administrators. Daher sollten Sie Benutzern direkt Berechtigungssätzen zuweisen, die den Zugriff auf das Verwaltungskonto gewähren, und Gruppen vermeiden. Wenn Sie Gruppen verwenden, um den Zugriff auf das Verwaltungskonto zu verwalten, stellen Sie sicher, dass der IdP über angemessene Kontrollen verfügt, um einzuschränken, wer diese Gruppen ändern darf, und stellen Sie sicher, dass Änderungen an diesen Gruppen (oder Änderungen der Anmeldeinformationen für die Benutzer im Verwaltungskonto) protokolliert und bei Bedarf überprüft werden.
- Berücksichtigen Sie Ihren Active Directory-Standort — Wenn Sie Active Directory als Ihre IAM Identity Center-Identitätsquelle verwenden möchten, suchen Sie das Verzeichnis im Mitgliedskonto,

in dem Sie die Funktion für delegierte Administratoren von IAM Identity Center aktiviert haben. Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle auf Active Directory oder von Active Directory auf eine andere Quelle zu ändern, muss sich das Verzeichnis im Mitgliedskonto für delegierte Administratoren von IAM Identity Center befinden. Wenn Sie möchten, dass sich Ihr Active Directory im Verwaltungskonto befindet, müssen Sie das Setup im Verwaltungskonto durchführen, da der delegierte Administrator nicht über die erforderlichen Berechtigungen verfügt, um es abzuschließen.

Beschränken Sie die Aktionen des IAM Identity Center-Identitätsspeichers im Konto für delegierte Administration auf externe Identitätsquellen

Wenn Sie eine externe Identitätsquelle wie einen IdP oder verwenden, sollten Sie Richtlinien implementieren Directory Service, die die Identitätsspeicheraktionen einschränken, die ein IAM Identity Center-Administrator innerhalb des Kontos für delegierte Administration ausführen kann. Schreib- und Löschvorgänge sollten sorgfältig abgewogen werden. Im Allgemeinen ist die externe Identitätsquelle die Informationsquelle für Benutzer und ihre Attribute sowie für Gruppenmitgliedschaften. Wenn Sie diese mithilfe der Identitätsspeicher-APIs oder der Konsole ändern, werden Ihre Änderungen während der normalen Synchronisierungszyklen überschrieben. Überlassen Sie diese Vorgänge am besten der alleinigen Kontrolle Ihrer Identitätsquelle. Dies schützt auch davor, dass ein IAM Identity Center-Administrator Gruppenmitgliedschaften ändert, um Zugriff auf einen der Gruppe zugewiesenen Berechtigungssatz oder eine Anwendung zu gewähren, anstatt die Kontrolle über die Gruppenmitgliedschaft Ihrem IdP-Administrator zu überlassen. Sie sollten auch darauf achten, wer SCIM-Bearer-Token vom Konto für delegierte Administratoren aus erstellen kann, da diese es einem Administrator eines Mitgliedskontos ermöglichen könnten, Gruppen und Benutzer über einen SCIM-Client zu ändern.

Es kann vorkommen, dass Schreib- oder Löschvorgänge vom Konto des delegierten Administrators aus angemessen sind. Sie können beispielsweise eine Gruppe erstellen, ohne Mitglieder hinzuzufügen, und dann einem Berechtigungssatz zuweisen, ohne darauf warten zu müssen, dass der IdP-Administrator die Gruppe erstellt. Niemand hat Zugriff auf diese Aufgabe, bis der IdP-Administrator die Gruppe bereitstellt und der IdP-Synchronisierungsprozess die Gruppenmitglieder festlegt. Es kann auch angemessen sein, einen Benutzer oder eine Gruppe zu löschen, um die Anmeldung oder Autorisierung zu verhindern, wenn Sie nicht auf den IdP-Synchronisierungsvorgang warten können, um dem Benutzer oder der Gruppe den Zugriff zu entziehen. Ein Missbrauch dieser Erlaubnis kann sich jedoch negativ auf die Nutzer auswirken. Bei der Zuweisung von Identitätsspeicherberechtigungen sollten Sie das Prinzip der geringsten Rechte verwenden. Mithilfe

einer Service Control Policy (SCP) können Sie steuern, welche Identitätsspeicher-Aktionen von den Administratoren Ihres delegierten Administrationskontos zugelassen werden.

Das folgende SCP-Beispiel verhindert das Zuweisen von Benutzern zu Gruppen über die Identity Store-API und die. Dies wird empfohlen AWS-Managementkonsole, wenn es sich bei Ihrer Identitätsquelle um eine externe Identitätsquelle handelt. Dies hat keinen Einfluss auf die Benutzersynchronisierung von Directory Service oder von einem externen IdP (über SCIM).

 Note

Es ist möglich, dass Ihre Organisation, obwohl Sie eine externe Identitätsquelle verwenden, ganz oder teilweise auf die Identity Store-APIs für die Bereitstellung von Benutzern und Gruppen angewiesen ist. Bevor Sie diesen SCP aktivieren, sollten Sie daher sicherstellen, dass Ihr Benutzerbereitstellungsprozess diesen Identity Store-API-Vorgang nicht verwendet. Im nächsten Abschnitt finden Sie außerdem Informationen dazu, wie Sie die Verwaltung von Gruppenmitgliedschaften auf bestimmte Gruppen beschränken können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

Wenn Sie verhindern möchten, dass Benutzer nur zu Gruppen hinzugefügt werden, die Zugriff auf das Verwaltungskonto gewähren, können Sie mithilfe des Gruppen-ARN im folgenden Format auf diese spezifischen Gruppen verweisen: `arn:${Partition}:identitystore:::group/${GroupId}`. Dieser und andere im Identity Store verfügbare Ressourcentypen sind in der [Service Authorization Reference](#) unter [Von AWS Identity Store definierte Ressourcentypen](#) dokumentiert. Sie können auch erwägen, zusätzliche Identity Store-APIs in den SCP aufzunehmen. Weitere Informationen finden Sie unter [Aktionen](#) in der Identity Store-API-Referenz.

Indem Sie Ihrem SCP die folgende Richtlinienerklärung hinzufügen, können Sie verhindern, dass der delegierte Administrator SCIM-Bearer-Token erstellt. Sie können dies für beide externen Identitätsquellen anwenden.

 Note

Wenn Ihr delegierter Administrator die Benutzerbereitstellung mit SCIM einrichten oder die regelmäßige SCIM-Inhaber-Token-Rotation durchführen muss, müssen Sie vorübergehend den Zugriff auf diese API zulassen, damit der delegierte Administrator diese Aufgaben ausführen kann.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

Beschränken Sie die Aktionen im IAM Identity Center-Identitätsspeicher im Konto für delegierte Administratoren für lokal verwaltete Benutzer

Wenn Sie Ihre Benutzer und Gruppen direkt in IAM Identity Center erstellen, anstatt einen externen IdP zu verwenden Directory Service, sollten Sie Vorkehrungen treffen, um festzulegen, wer Benutzer erstellen, Passwörter zurücksetzen und die Gruppenmitgliedschaft kontrollieren kann. Diese Aktionen geben dem Administrator umfangreiche Möglichkeiten, festzulegen, wer sich anmelden kann und wer über die Mitgliedschaft in Gruppen Zugriff erhält. Diese Richtlinien lassen sich am besten als Inline-Richtlinien innerhalb der Berechtigungssätze implementieren, die Sie für Ihre IAM Identity Center-Administratoren verwenden, und nicht als SCPs. Das folgende Beispiel für eine Inline-Richtlinie verfolgt zwei Ziele. Erstens wird verhindert, dass Benutzer zu bestimmten Gruppen hinzugefügt werden. Sie können dies verwenden, um zu verhindern, dass delegierte Administratoren Benutzer zu Gruppen hinzufügen, die Zugriff auf das Verwaltungskonto gewähren. Zweitens verhindert es die Ausgabe von SCIM-Bearer-Token.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore::group/${GroupId1},
                    arn:${Partition}:identitystore::group/${GroupId2}
                  ]
    }
  ]
}
```

```
],  
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ] }  
]  
}
```

Trennen Sie das IAM Identity Center-Konfigurationsmanagement vom Management PermissionSet

Trennen Sie die administrativen Aufgaben wie die Änderung der externen Identitätsquelle, die SCIM-Token-Verwaltung und die Konfiguration des Sitzungs-Timeouts von den Aufgaben zum Erstellen, Ändern und Zuweisen von Berechtigungssätzen, indem Sie separate Administratorberechtigungssätze von Ihrem Verwaltungskonto aus erstellen.

Beschränken Sie die Ausgabe von SCIM-Bearer-Token

SCIM-Bearer-Token ermöglichen es einer externen Identitätsquelle, Benutzer, Gruppen und Gruppenmitgliedschaften über das SCIM-Protokoll bereitzustellen, wenn die Identitätsquelle Ihres IAM Identity Centers ein externer IdP wie Okta oder Entra ID ist. Sie können das folgende SCP einrichten, um die Erstellung von SCIM-Bearer-Token durch delegierte Administratoren zu verhindern. Wenn Ihr delegierter Administrator die Benutzerbereitstellung mit SCIM einrichten oder die regelmäßige SCIM-Inhaber-Token-Rotation durchführen muss, müssen Sie vorübergehend den Zugriff auf diese API zulassen, damit der delegierte Administrator diese Aufgaben ausführen kann.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Verwenden Sie Berechtigungssätze, Tags und Kontolisten, um die Verwaltung bestimmter Konten zu delegieren

Sie können Berechtigungssätze erstellen, die Sie Ihren IAM Identity Center-Administratoren zuweisen, um zu delegieren, wer Berechtigungssätze erstellen kann und wer welche Berechtigungssätze welchen Konten zuweisen kann. Dazu kennzeichnen Sie Berechtigungssätze und verwenden Richtlinienbedingungen in Berechtigungssätzen, die Sie Ihren Administratoren zuweisen. Sie können beispielsweise Berechtigungssätze erstellen, die es einem Benutzer

ermöglichen, Berechtigungssätze zu erstellen, sofern sie auf eine bestimmte Weise gekennzeichnet sind. Sie können auch Richtlinien erstellen, die es einem Administrator ermöglichen, bestimmten Konten Berechtigungssätze zuzuweisen, die mit einem bestimmten Tag versehen sind. Dies kann Ihnen helfen, die Verwaltung von Konten zu delegieren, ohne einem Administrator die Rechte zu geben, seinen Zugriff und seine Rechte für das delegierte Administratorkonto zu ändern. Indem Sie beispielsweise Berechtigungssätze kennzeichnen, die Sie nur im Konto für delegierte Administratoren verwenden, können Sie eine Richtlinie angeben, die nur bestimmten Personen die Berechtigung erteilt, Berechtigungssätze und Zuweisungen zu ändern, die sich auf das Konto der delegierten Administration auswirken. Sie können auch anderen Personen die Berechtigung geben, eine Liste von Konten außerhalb des Kontos für delegierte Administratoren zu verwalten. Weitere Informationen finden Sie im AWS Sicherheitsblog unter [Delegieren der Verwaltung von Berechtigungssätzen und Kontozuweisungen. AWS IAM Identity Center](#)

Voraussetzungen

Bevor Sie ein Konto als delegierter Administrator registrieren können, müssen Sie zunächst die folgende Umgebung bereitstellen:

- AWS Organizations muss zusätzlich zu Ihrem Standard-Verwaltungskonto mit mindestens einem Mitgliedskonto aktiviert und konfiguriert sein.
- Wenn Ihre Identitätsquelle auf Active Directory eingestellt ist, muss die [IAM Identity Center, konfigurierbare AD-Synchronisierung](#) Funktion aktiviert sein.

Registrieren Sie ein Mitgliedskonto

Um die delegierte Administration zu konfigurieren, müssen Sie zunächst ein Mitgliedskonto in Ihrer Organisation als delegierter Administrator registrieren. Benutzer in diesem Mitgliedskonto, die über ausreichende Berechtigungen verfügen, erhalten Administratorzugriff auf IAM Identity Center. Nachdem ein Mitgliedskonto erfolgreich für die delegierte Administration registriert wurde, wird es als delegiertes Administratorkonto bezeichnet. Weitere Informationen zu Aufgaben, die das delegierte Administratorkonto ausführen kann, finden Sie unter [AWS-Konto Typen](#)

IAM Identity Center unterstützt die Registrierung jeweils nur eines Mitgliedskontos als delegierter Administrator. Sie können ein Mitgliedskonto nur registrieren, wenn Sie mit den Anmeldeinformationen des Verwaltungskontos angemeldet sind.

Gehen Sie wie folgt vor, um Administratorzugriff auf IAM Identity Center zu gewähren, indem Sie ein bestimmtes Mitgliedskonto in Ihrer AWS Organisation als delegierter Administrator registrieren.

⚠ Important

Dieser Vorgang delegiert den Administratorzugriff von IAM Identity Center an Administratorbenutzer in diesem Mitgliedskonto. Alle Benutzer, die über ausreichende Berechtigungen für dieses delegierte Administratorkonto verfügen, können alle Verwaltungsaufgaben von IAM Identity Center von diesem Konto aus ausführen, mit Ausnahme von:

- IAM Identity Center aktivieren
- Löschen von IAM Identity Center-Konfigurationen
- Verwaltung von Berechtigungssätzen, die im Verwaltungskonto bereitgestellt wurden
- Registrierung oder Abmeldung anderer Mitgliedskonten als delegierte Administratoren
- Aktivieren oder Deaktivieren des Benutzerzugriffs im Verwaltungskonto

Der delegierte Administrator kann die Gruppenmitgliedschaft bearbeiten.

Um ein Mitgliedskonto zu registrieren

1. Melden Sie sich AWS-Managementkonsole mit den Anmeldeinformationen Ihres Verwaltungskontos an AWS Organizations. Anmeldeinformationen für das Verwaltungskonto sind erforderlich, um die [RegisterDelegatedAdministrator](#) API auszuführen.
2. Wählen Sie die Region aus, in der IAM Identity Center aktiviert ist, und öffnen Sie dann die [IAM Identity Center-Konsole](#).
3. Wählen Sie **Einstellungen** und dann die Registerkarte **Verwaltung** aus.
4. Wählen Sie im Bereich **Delegierter Administrator** die Option **Konto registrieren** aus.
5. Wählen Sie auf der Seite **Delegierten Administrator registrieren** den Benutzer aus, den AWS-Konto Sie registrieren möchten, und klicken Sie dann auf **Konto registrieren**.

Aufheben der Registrierung eines Mitgliedskontos

Sie können ein Mitgliedskonto nur abmelden, wenn Sie mit den Anmeldedaten des Verwaltungskontos angemeldet sind.

Gehen Sie wie folgt vor, um den Administratorzugriff von IAM Identity Center zu entfernen, indem Sie ein Mitgliedskonto in Ihrer AWS Organisation abmelden, das zuvor als delegierter Administrator benannt wurde.

 Important

Wenn Sie ein Konto deregistrieren, nehmen Sie praktisch allen Administratorbenutzern die Möglichkeit, IAM Identity Center von diesem Konto aus zu verwalten. Daher können sie IAM Identity Center-Identitäten, Zugriffsverwaltung, Authentifizierung oder Anwendungszugriff nicht mehr von diesem Konto aus verwalten. Dieser Vorgang wirkt sich nicht auf die im IAM Identity Center konfigurierten Berechtigungen oder Zuweisungen AWS-Konten aus und hat daher keine Auswirkungen auf Ihre Endbenutzer, da diese weiterhin über das Zugriffsportal auf ihre Apps zugreifen können. AWS

Um ein Mitgliedskonto abzumelden

1. Melden Sie sich AWS-Managementkonsole mit den Anmeldeinformationen Ihres Verwaltungskontos an. AWS Organizations Anmeldeinformationen für das Verwaltungskonto sind erforderlich, um die [DeregisterDelegatedAdministrator](#) API auszuführen.
2. Wählen Sie die Region aus, in der IAM Identity Center aktiviert ist, und öffnen Sie dann die [IAM Identity Center-Konsole](#).
3. Wählen Sie **Einstellungen** und dann die Registerkarte **Verwaltung** aus.
4. Wählen Sie im Abschnitt **Delegierter Administrator** die Option **Konto abmelden** aus.
5. Prüfen Sie im Dialogfeld **Konto abmelden** die Auswirkungen auf die Sicherheit und geben Sie dann den Namen des Mitgliedskontos ein, um zu bestätigen, dass Sie verstanden haben.
6. Wählen Sie **Konto abmelden**.

Sehen Sie sich an, welches Mitgliedskonto als delegierter Administrator registriert wurde

Gehen Sie wie folgt vor, um herauszufinden, welches Mitgliedskonto in Ihrem Konto als delegierter Administrator für IAM Identity Center konfiguriert AWS Organizations wurde.

Um Ihr registriertes Mitgliedskonto einzusehen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

2. Wählen Sie Einstellungen aus.
3. Suchen Sie im Abschnitt Details unter Delegierter Administrator nach dem Namen des registrierten Kontos. Sie können diese Informationen auch finden, indem Sie die Registerkarte Verwaltung auswählen und sie im Bereich Delegierter Administrator einsehen.

Temporärer erhöhter Zugriff für AWS-Konten

Jeder Zugriff auf Sie AWS-Konto beinhaltet ein gewisses Maß an Privilegien. Sensible Vorgänge, wie z. B. die Änderung der Konfiguration für eine Produktionsumgebung, erfordern aufgrund des Umfangs und der möglichen Auswirkungen eine besondere Behandlung. Temporärer Zugriff mit erhöhten Rechten (auch bekannt als Just-in-Time-Zugriff) ist eine Möglichkeit, die Verwendung einer Berechtigung zur Ausführung einer bestimmten Aufgabe während einer bestimmten Zeit anzufordern, zu genehmigen und nachzuverfolgen. Temporärer Zugriff mit erhöhten Rechten ergänzt andere Formen der Zugriffskontrolle, z. B. Berechtigungssätze und die mehrstufige Authentifizierung.

Note

Um die Geschäftskontinuität zu gewährleisten, empfehlen wir Ihnen, den Notfallzugriff auf den [AWS-Managementkonsole](#) einzurichten.

Lässt sich in die Lösungen von AWS Security Competency-Partnern AWS IAM Identity Center integrieren, um einer Reihe von Kundenanforderungen gerecht zu werden. AWS bestätigt, dass diese Lösungen eine Reihe gängiger temporärer erhöhter Zugriffsanforderungen erfüllen. Wir empfehlen Ihnen, jede Partnerlösung sorgfältig zu prüfen, damit Sie eine auswählen können, die Ihren individuellen Anforderungen und Präferenzen am besten entspricht, einschließlich Ihres Unternehmens, der Architektur Ihrer Cloud-Umgebung und Ihres Budgets.

Zu den validierten Lösungen gehören [Apono Access Management Platform](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#) und [Tenable](#) (ehemals Ermetic).

Partner können mithilfe der AWS Security Competency-Anwendung im Partner Center Lösungen nominieren. Weitere Informationen finden Sie unter [AWS Sicherheitskompetenzpartner](#).

Note

Wenn Sie den ressourcenbasierten Amazon Elastic Kubernetes Service verwenden, finden Sie weitere Informationen unter [Referenzieren von Berechtigungssätzen](#)

[in Ressourcenrichtlinien AWS Key Management Service, Amazon EKS-Cluster-Konfigurationszuordnungen und AWS KMS wichtigen Richtlinien](#), bevor Sie sich für Ihre Just-in-Time-Lösung entscheiden.

Single-Sign-On-Zugriff auf AWS-Konten

Sie können Benutzern in Ihrem verbundenen Verzeichnis Berechtigungen auf der AWS Organizations Grundlage [üblicher Aufgaben](#) dem Verwaltungskonto oder den Mitgliedskonten in Ihrer Organisation zuweisen. Alternativ können Sie benutzerdefinierte Berechtigungen verwenden, um Ihre spezifischen Sicherheitsanforderungen zu erfüllen. Beispielsweise können Sie Datenbankadministratoren weitreichende Berechtigungen für Amazon RDS in Entwicklungskonten gewähren, ihre Berechtigungen jedoch in Produktionskonten einschränken. IAM Identity Center konfiguriert automatisch alle erforderlichen Benutzerberechtigungen in Ihrem AWS-Konten System.

Note

Möglicherweise müssen Sie Benutzern oder Gruppen Berechtigungen gewähren, um im AWS Organizations Verwaltungskonto arbeiten zu können. Da es sich um ein Konto mit hohen Rechten handelt, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen über die [IAMFullAccess](#) Richtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

Themen

- [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#)
- [Entfernen Sie den Benutzer- und Gruppenzugriff auf eine AWS-Konto](#)
- [Widerrufen Sie den Benutzerzugriff](#)
- [Delegieren Sie, wer Benutzern und Gruppen im Verwaltungskonto den Single-Sign-On-Zugriff gewähren kann](#)

Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten

Gehen Sie wie folgt vor, um Benutzern und Gruppen in Ihrem verbundenen Verzeichnis den Single-Sign-On-Zugriff zuzuweisen, und legen Sie anhand von Berechtigungssätzen deren Zugriffsebene fest.

Informationen zur Überprüfung des bestehenden Benutzer- und Gruppenzugriffs finden Sie unter [Einen Berechtigungssatz anzeigen und ändern](#).

Note

Zur vereinfachten Administration der Zugriffsberechtigungen wird empfohlen, den Zugriff direkt den Gruppen zuzuweisen (und nicht einzelnen Benutzern). Bei Gruppen können Sie Berechtigungen für Benutzergruppen gewähren oder verweigern, anstatt dies für jede Einzelperson individuell zu tun. Wenn ein Benutzer zu einer anderen Organisation wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe. Er erhält dann automatisch die Berechtigungen für die neue Organisation.

So weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

Note

Stellen Sie sicher, dass die IAM Identity Center-Konsole die Region verwendet, in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie im Navigationsbereich unter **Multi-account Berechtigungen** die Option **AWS-Konten**.
3. Auf der **AWS-Konten** Seite wird eine Baumstrukturliste Ihrer Organisation angezeigt. Markieren Sie das Kontrollkästchen **AWS-Konto** neben dem, dem Sie Zugriff gewähren möchten. Wenn Sie den Administratorzugriff für IAM Identity Center einrichten, aktivieren Sie das Kontrollkästchen neben dem **Verwaltungskonto**.

Note

Sie können pro Berechtigungssatz bis zu 10 AWS-Konten gleichzeitig auswählen, wenn Sie Benutzern und Gruppen den Single-Sign-On-Zugriff zuweisen. Um derselben Gruppe

von Benutzern und Gruppen mehr als 10 AWS-Konten zuzuweisen, wiederholen Sie dieses Verfahren bei Bedarf für die zusätzlichen Konten. Wenn Sie dazu aufgefordert werden, wählen Sie dieselben Benutzer, Gruppen und denselben Berechtigungssatz aus.

4. Wählen Sie „Benutzer oder Gruppen zuweisen“.
5. Gehen Sie für Schritt 1: Benutzer und Gruppen auswählen auf der Seite Benutzer und Gruppen zu **AWS-account-name** zuweisen wie folgt vor:

1. Wählen Sie auf der Registerkarte Benutzer einen oder mehrere Benutzer aus, denen Sie Single Sign-On-Zugriff gewähren möchten.

Um die Ergebnisse zu filtern, geben Sie zunächst den Namen des gewünschten Benutzers in das Suchfeld ein.

2. Wählen Sie auf der Registerkarte Gruppen eine oder mehrere Gruppen aus, denen Sie Single Sign-On-Zugriff gewähren möchten.

Um die Ergebnisse zu filtern, geben Sie zunächst den Namen der gewünschten Gruppe in das Suchfeld ein.

3. Um die Benutzer und Gruppen anzuzeigen, die Sie ausgewählt haben, wählen Sie das seitliche Dreieck neben Ausgewählte Benutzer und Gruppen.
 4. Nachdem Sie bestätigt haben, dass die richtigen Benutzer und Gruppen ausgewählt sind, wählen Sie Weiter.
6. Gehen Sie für Schritt 2: Berechtigungssätze auswählen auf der Seite „Berechtigungssätze zuweisen zu **AWS-account-name**“ wie folgt vor:

1. Wählen Sie einen oder mehrere Berechtigungssätze aus. Bei Bedarf können Sie neue Berechtigungssätze erstellen und auswählen.
 - Um einen oder mehrere vorhandene Berechtigungssätze auszuwählen, wählen Sie unter Berechtigungssätze die Berechtigungssätze aus, die Sie auf die Benutzer und Gruppen anwenden möchten, die Sie im vorherigen Schritt ausgewählt haben.
 - Um einen oder mehrere neue Berechtigungssätze zu erstellen, wählen Sie Berechtigungssatz erstellen aus und folgen Sie den Schritten unter [Erstellen Sie einen Berechtigungssatz](#). Nachdem Sie die Berechtigungssätze erstellt haben, die Sie anwenden möchten, kehren Sie in der IAM Identity Center-Konsole zu AWS-Konten und folgen Sie den Anweisungen, bis Sie zu Schritt 2: Berechtigungssätze auswählen gelangen. Wenn Sie

diesen Schritt erreicht haben, wählen Sie die neuen Berechtigungssätze aus, die Sie erstellt haben, und fahren Sie mit dem nächsten Schritt in diesem Verfahren fort.

2. Nachdem Sie bestätigt haben, dass die richtigen Berechtigungssätze ausgewählt sind, wählen Sie **Weiter** aus.
7. Gehen Sie für Schritt 3: Prüfen und Absenden auf der Seite **Aufgaben** überprüfen und einreichen an **AWS-account-name** wie folgt vor:
 1. Überprüfen Sie die ausgewählten Benutzer, Gruppen und Berechtigungssätze.
 2. Nachdem Sie bestätigt haben, dass die richtigen Benutzer, Gruppen und Berechtigungssätze ausgewählt wurden, wählen Sie **Senden** aus.

Überlegungen

- Das Zuweisen von Benutzern und Gruppen kann einige Minuten in Anspruch nehmen. Lassen Sie diese Seite geöffnet, bis der Vorgang erfolgreich abgeschlossen ist.

Note

Möglicherweise müssen Sie Benutzern oder Gruppen Berechtigungen gewähren, um mit dem AWS Organizations Verwaltungskonto arbeiten zu können. Da es sich um ein Konto mit hohen Rechten handelt, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen über die [IAMFullAccess](#) Richtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

8. Wenn eine der folgenden Bedingungen zutrifft, folgen Sie den Schritten unter [Benutzer zur MFA auffordern](#) So aktivieren Sie MFA für IAM Identity Center:
 - Sie verwenden das Identity Center-Standardverzeichnis als Identitätsquelle.
 - Sie verwenden ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory als Identitätsquelle und Sie verwenden RADIUS MFA nicht mit AWS Directory Service

 Note

Wenn Sie einen externen Identitätsanbieter verwenden, beachten Sie, dass der externe IdP, nicht IAM Identity Center, die MFA-Einstellungen verwaltet. MFA im IAM Identity Center wird nicht für die Verwendung durch externe Benutzer unterstützt. IdPs

Wenn Sie den Kontozugriff für den Administratorbenutzer einrichten, erstellt IAM Identity Center eine entsprechende IAM-Rolle. Diese Rolle, die von IAM Identity Center gesteuert wird, wird in der entsprechenden Instanz erstellt AWS-Konto, und die im Berechtigungssatz angegebenen Richtlinien werden der Rolle zugeordnet.

Sie können es auch verwenden, [AWS CloudFormation](#) um Berechtigungssätze zu erstellen und zuzuweisen und diesen Berechtigungssätzen Benutzer zuzuweisen. Benutzer können [sich dann im AWS Access-Portal anmelden](#) oder [AWS Command Line Interface \(AWS CLI\)](#) -Befehle verwenden.

 Note

In diesem Thema wird das Zuweisen von Zugriffen mithilfe von Berechtigungssätzen behandelt. Informationen zum Zuweisen vorhandener IAM-Rollen zu IAM Identity Center-Benutzern und -Gruppen — mit dem vollständigen Funktionsumfang der IAM-Rollen — finden Sie unter [Account Access Manager](#) im IAM-Benutzerhandbuch.

Entfernen Sie den Benutzer- und Gruppenzugriff auf eine AWS-Konto

Gehen Sie wie folgt vor, um den Single-Sign-On-Zugriff auf und AWS-Konto für einen oder mehrere Benutzer und Gruppen in Ihrem verbundenen Verzeichnis zu entfernen. Alternativ können Sie die <https://docs.aws.amazon.com/cli/latest/reference/sso-admin/delete-account-assignment.html> AWS CLI Delete-Account-Assignment verwenden.

 Note

Wenn Sie die Bereitstellung von IAM Identity Center-Benutzern oder -Gruppen aufheben müssen, sollten Sie zunächst alle Zuweisungen von Berechtigungssätzen [für Ihre Benutzer und Gruppen](#) entfernen, bevor Sie die Benutzer und Gruppen löschen.

So entfernen Sie den Benutzer- und Gruppenzugriff auf AWS-Konto

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich unter **Multi-account Berechtigungen** die Option **AWS-Konten**.
3. Auf der **AWS-Konten** Seite wird eine Strukturansicht Ihrer Organisation angezeigt. Wählen Sie den Namen der aus **AWS-Konto** , der die Benutzer und Gruppen enthält, für die Sie den **Single-Sign-On-Zugriff** entfernen möchten.
4. Wählen Sie auf der **Übersichtsseite** für die **AWS-Konto** unter **Zugewiesene Benutzer und Gruppen** den Namen eines oder mehrerer Benutzer oder Gruppen aus und klicken Sie auf **Zugriff entfernen**.
5. Vergewissern Sie sich im Dialogfeld „**Zugriff entfernen**“, dass die Namen der Benutzer oder Gruppen korrekt sind, und wählen Sie **Zugriff entfernen** aus.

Widerrufen Sie den Benutzerzugriff

Im Folgenden finden Sie ein allgemeines Verfahren zum Widerrufen einer aktiven Berechtigungssatzsitzung für einen IAM Identity Center-Benutzer. Das Verfahren geht davon aus, dass Sie einem Benutzer, dessen Anmeldeinformationen kompromittiert wurden, oder einem böswilligen Akteur, der sich im System befindet, jeglichen Zugriff entziehen möchten. Voraussetzung ist, dass Sie die Anweisungen in [Bereiten Sie sich darauf vor, eine aktive IAM-Rollensitzung zu widerrufen, die mit einem Berechtigungssatz erstellt wurde](#) befolgt haben. Wir gehen davon aus, dass die Deny-All-Richtlinie in einer Service Control Policy (SCP) enthalten ist.

Note

AWS empfiehlt, eine Automatisierung zu erstellen, die alle Schritte außer reinen Konsolenoperationen abwickelt.

1. Besorgen Sie sich die Benutzer-ID der Person, deren Zugriff Sie widerrufen müssen. Sie können die Identity Store-APIs verwenden, um den Benutzer anhand seines Benutzernamens zu finden.
2. Aktualisieren Sie die Deny-Richtlinie, um die Benutzer-ID aus Schritt 1 zu Ihrer Service Control-Richtlinie (SCP) hinzuzufügen. Nach Abschluss dieses Schritts verliert der Zielbenutzer den Zugriff und kann keine Aktionen mit Rollen ausführen, die von der Richtlinie betroffen sind.
3. Entfernt alle Zuweisungen von Berechtigungssätzen für den Benutzer. Wenn der Zugriff über Gruppenmitgliedschaften gewährt wird, entfernen Sie den Benutzer aus allen Gruppen und

allen direkten Berechtigungssatzzuweisungen. Dieser Schritt verhindert, dass der Benutzer zusätzliche IAM-Rollen übernimmt. Wenn ein Benutzer eine aktive AWS Access-Portalsitzung hat und Sie den Benutzer deaktivieren, kann er weiterhin neue Rollen annehmen, bis Sie ihm den Zugriff entziehen.

4. Entfernen Sie alle IAM-Rollenzuweisungen für den Benutzer im Account Access Manager. Wenn der Zugriff über Gruppenmitgliedschaften gewährt wird, entfernen Sie den Benutzer aus allen Gruppen und allen direkten IAM-Rollenzuweisungen. Dieser Schritt verhindert, dass der Benutzer zusätzliche IAM-Rollen übernimmt, die im Account Access Manager verwaltet werden. Wenn ein Benutzer eine aktive AWS Kontozugriffsportalsitzung hat und Sie den Benutzer deaktivieren, kann er weiterhin neue Rollen annehmen, bis Sie ihm den Zugriff entziehen.
5. Wenn Sie einen Identitätsanbieter (IdP) oder Microsoft Active Directory als Identitätsquelle verwenden, deaktivieren Sie den Benutzer in der Identitätsquelle. Die Deaktivierung des Benutzers verhindert die Erstellung zusätzlicher AWS Zugriffsportalsitzungen. Erfahren Sie in Ihrer IdP- oder Microsoft Active Directory-API-Dokumentation, wie Sie diesen Schritt automatisieren können. Wenn Sie das IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, deaktivieren Sie den Benutzerzugriff noch nicht. In Schritt 7 deaktivieren Sie den Benutzerzugriff.
6. Suchen Sie in der IAM Identity Center-Konsole den Benutzer und löschen Sie seine aktive Sitzung.
 - a. Wählen Sie Users (Benutzer) aus.
 - b. Wählen Sie den Benutzer aus, dessen aktive Sitzung Sie löschen möchten.
 - c. Wählen Sie auf der Detailseite des Benutzers den Tab **Aktive Sitzungen**.
 - d. Markieren Sie die Kontrollkästchen neben den Sitzungen, die Sie löschen möchten, und wählen Sie **Sitzung löschen** aus.

Nach dem Löschen einer Benutzersitzung verliert der Benutzer sofort den Zugriff auf das AWS Zugriffsportal. Erfahren Sie mehr über die [Sitzungsdauer](#).

7. Deaktivieren Sie in der IAM Identity Center-Konsole den Benutzerzugriff.
 - a. Wählen Sie Users (Benutzer) aus.
 - b. Wählen Sie den Benutzer aus, dessen Zugriff Sie deaktivieren möchten.
 - c. Erweitern Sie auf der Detailseite des Benutzers die Option **Allgemeine Informationen** und wählen Sie die Schaltfläche **Benutzerzugriff deaktivieren**, um weitere Anmeldungen des Benutzers zu verhindern.

8. Lassen Sie die Ablehnungsrichtlinie mindestens 12 Stunden lang in Kraft. Andernfalls hat der Benutzer mit einer aktiven IAM-Rollensitzung Aktionen mit der IAM-Rolle wiederhergestellt. Wenn Sie 12 Stunden warten, laufen aktive Sitzungen ab und der Benutzer kann nicht mehr auf die IAM-Rolle zugreifen.

 Important

Wenn Sie den Zugriff eines Benutzers deaktivieren, bevor Sie die Benutzersitzung beenden (Sie haben Schritt 7 abgeschlossen, ohne Schritt 6 abzuschließen), können Sie die Benutzersitzung nicht mehr über die IAM Identity Center-Konsole beenden. Wenn Sie versehentlich den Benutzerzugriff deaktivieren, bevor Sie die Benutzersitzung beenden, können Sie den Benutzer erneut aktivieren, seine Sitzung beenden und dann seinen Zugriff erneut deaktivieren.

Sie können jetzt die Anmeldeinformationen des Benutzers ändern, falls sein Passwort kompromittiert wurde, und seine Zuweisungen wiederherstellen. [???](#)

Delegieren Sie, wer Benutzern und Gruppen im Verwaltungskonto den Single-Sign-On-Zugriff gewähren kann

Das Zuweisen des Single-Sign-On-Zugriffs zum Verwaltungskonto mithilfe der IAM Identity Center-Konsole ist eine privilegierte Aktion. Standardmäßig kann nur ein Root-Benutzer des AWS-Kontos oder mehrere Benutzer, denen die Richtlinien `AWSSSOMasterAccountAdministrator` und die `IAMFullAccess` AWS verwalteten Richtlinien zugeordnet sind, dem Verwaltungskonto den Single-Sign-On-Zugriff zuweisen. Die `AWSSSOMasterAccountAdministrator` `IAMFullAccess` AND-Richtlinien verwalten den Single-Sign-On-Zugriff auf das Verwaltungskonto innerhalb einer AWS Organizations Organisation.

Sie können sie auch verwenden, AWS CLI um Berechtigungssätze zu erstellen, Richtlinien anzuhängen und ihnen zuzuweisen. Im Folgenden sind die Befehle für jeden Schritt aufgeführt:

- So erstellen Sie einen Berechtigungssatz: [create-permission-set](#)
- Um einen Berechtigungssatz anzuhängen: AWS Managed Policy attach-managed-policy-to-permission-set <https://docs.aws.amazon.com/cli/latest/reference/sso-admin/attach-managed-policy-to-permission-set.html>

- Um eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz anzuhängen: attach-customer-managed-policy-to-permission-set <https://docs.aws.amazon.com/cli/latest/reference/sso-admin/attach-customer-managed-policy-reference-to-permission-set.html>
- So weisen Sie einem Principal einen Berechtigungssatz zu: create-account-assignment <https://docs.aws.amazon.com/cli/latest/reference/sso-admin/create-account-assignment.html>

Gehen Sie wie folgt vor, um Berechtigungen für die Verwaltung des Single-Sign-On-Zugriffs auf Benutzer und Gruppen in Ihrem Verzeichnis zu delegieren.

Um Benutzern und Gruppen in Ihrem Verzeichnis Berechtigungen für die Verwaltung des Single-Sign-On-Zugriffs zu gewähren

1. Melden Sie sich bei der IAM Identity Center-Konsole als Root-Benutzer des Verwaltungskontos oder mit einem anderen Benutzer an, der über Administratorberechtigungen für das Verwaltungskonto verfügt.
2. Folgen Sie den Schritten unter [Erstellen Sie einen Berechtigungssatz](#), um einen Berechtigungssatz zu erstellen, und gehen Sie dann wie folgt vor:
 1. Aktivieren Sie auf der Seite **Neuen Berechtigungssatz erstellen** das Kontrollkästchen **Benutzerdefinierten Berechtigungssatz erstellen**, und wählen Sie dann **Weiter: Details** aus.
 2. Geben Sie auf der Seite **Neuen Berechtigungssatz erstellen** einen Namen für den benutzerdefinierten Berechtigungssatz und optional eine Beschreibung an. Ändern Sie bei Bedarf die Sitzungsdauer und geben Sie eine Relay-Status-URL an.

 Note

Für die Relay-Status-URL müssen Sie eine URL angeben, die sich in der befindet AWS-Managementkonsole. Beispiel:

<https://console.aws.amazon.com/ec2/>

Weitere Informationen finden Sie unter [Stellen Sie den Relay-Status für den schnellen Zugriff auf den ein AWS-Managementkonsole](#).

3. Unter **Welche Richtlinien möchten Sie in Ihren Berechtigungssatz aufnehmen?**, aktivieren Sie das Kontrollkästchen **AWS Verwaltete Richtlinien** anhängen.
4. Wählen Sie in der Liste der IAM-Richtlinien sowohl die **SOMasterAccountAdministrator** **AWSS-Richtlinien** als auch die **IAMFullAccess** **AWS** verwalteten Richtlinien aus. Diese

Richtlinien gewähren allen Benutzern und Gruppen, denen in Zukunft Zugriff auf diesen Berechtigungssatz zugewiesen wird, Berechtigungen.

5. Wählen Sie Weiter: Tags aus.
6. Geben Sie unter Tags hinzufügen (optional) Werte für Schlüssel und Wert (optional) an, und wählen Sie dann Weiter: Überprüfen aus. Weitere Informationen zu Tags erhalten Sie unter [Ressourcen taggen AWS IAM Identity Center](#).
7. Überprüfen Sie die von Ihnen getroffenen Auswahlen und wählen Sie dann Erstellen aus.
3. Folgen Sie den Schritten unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#), um dem soeben erstellten Berechtigungssatz die entsprechenden Benutzer und Gruppen zuzuweisen.
4. Teilen Sie den zugewiesenen Benutzern Folgendes mit: Wenn sie sich beim AWS Access Portal anmelden und die Registerkarte Konten auswählen, müssen sie den entsprechenden Rollennamen auswählen, um mit den Berechtigungen, die Sie gerade delegiert haben, authentifiziert zu werden.

Verwalten AWS-Konten mit Berechtigungssätzen

Ein Berechtigungssatz ist eine Vorlage, die Sie erstellen und verwalten und die eine Sammlung von einer oder mehreren [IAM-Richtlinien definiert](#). Berechtigungssätze vereinfachen die Zuweisung von AWS-Konto Zugriffen für Benutzer und Gruppen in Ihrer Organisation. Sie können beispielsweise einen Datenbankadministrator-Berechtigungssatz erstellen, der Richtlinien für die Verwaltung von AWS RDS-, DynamoDB- und Aurora-Diensten enthält, und diesen einzigen Berechtigungssatz verwenden, um Ihren Datenbankadministratoren Zugriff auf eine Liste von Zielen AWS-Konten innerhalb Ihrer [AWS Organisation](#) zu gewähren.

Note

Für Ihre Organisations-Instance müssen Berechtigungen für mehrere Konten aktiviert sein, damit Berechtigungssätze funktionieren. Wenn Sie Ihre Organisationsinstanz erstellen, sind die Berechtigungen für mehrere Konten standardmäßig aktiviert. Falls nicht zuvor aktiviert, verwenden Sie den Tab „Verwaltung“ auf der Seite „Einstellungen“, um Berechtigungen für mehrere Konten zu aktivieren, sodass Sie Berechtigungssätze erstellen können. Sie können die [UpdateInstance](#) API auch verwenden, um Berechtigungen für mehrere Konten zu aktivieren.

IAM Identity Center weist einem Benutzer oder einer Gruppe in einer oder mehreren Gruppen AWS-Konten mit Berechtigungssätzen Zugriff zu. Wenn Sie einen Berechtigungssatz zuweisen, erstellt IAM Identity Center entsprechende IAM Identity Center-controlled IAM-Rollen in jedem Konto und hängt die im Berechtigungssatz angegebenen Richtlinien an diese Rollen an. IAM Identity Center verwaltet die Rolle und ermöglicht den autorisierten Benutzern, die Sie definiert haben, die Rolle mithilfe des IAM Identity Center-Benutzerportals oder der CLI zu übernehmen. AWS Wenn Sie den Berechtigungssatz ändern, stellt IAM Identity Center sicher, dass die entsprechenden IAM-Richtlinien und -Rollen entsprechend aktualisiert werden.

Sie können Ihren [Berechtigungssätzen verwaltete Richtlinien, vom Kunden verwaltete Richtlinien, integrierte Richtlinien und AWS verwaltete Richtlinien für Aufgabenfunktionen hinzufügen](#) AWS . Sie können auch eine AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie als [Berechtigungsgrenze zuweisen](#).

Informationen zum Erstellen eines Berechtigungssatzes finden Sie unter [Berechtigungssätze erstellen, verwalten und löschen](#).

Wenn Ihre Zugriffsverwaltung Funktionen erfordert, die über das hinausgehen, was Berechtigungssätze bieten, wie z. B. benutzerdefinierte Vertrauensrichtlinien, Rollentags oder konfigurierbare Rollenpfade, können Sie den [Account Access Manager](#) in IAM verwenden. Mit dem Account Access Manager können Sie IAM Identity Center-Benutzern und -Gruppen vorhandene IAM-Rollen zuweisen. Sie können ihn unabhängig oder zusammen mit Berechtigungssätzen verwenden, um Zugriff auf den gesamten Funktionsumfang der IAM-Rollen zu erhalten.

Erstellen Sie einen Berechtigungssatz, der Berechtigungen mit geringsten Rechten anwendet

Nach dem Erstellen eines Administratorberechtigungssatzes erstellen Sie nach dem Erstellen eines Administratorberechtigungssatzes einen restriktiveren Berechtigungssatz und weisen ihn einem oder mehreren Benutzern zu. Die im vorherigen Verfahren erstellten Berechtigungssätze bieten Ihnen einen Ausgangspunkt, um abzuschätzen, wie viel Zugriff auf Ressourcen Ihre Benutzer benötigen. Um zu den Berechtigungen mit den geringsten Rechten zu wechseln, können Sie IAM Access Analyzer ausführen, um Prinzipale mit AWS verwalteten Richtlinien zu überwachen. Nachdem Sie erfahren haben, welche Berechtigungen sie verwenden, können Sie eine benutzerdefinierte Richtlinie schreiben oder eine Richtlinie mit nur den erforderlichen Berechtigungen für Ihr Team erstellen.

Mit IAM Identity Center können Sie demselben Benutzer mehrere Berechtigungssätze zuweisen. Ihrem Administratorbenutzer sollten auch zusätzliche, restriktivere Berechtigungssätze zugewiesen

werden. Auf diese Weise können sie nur AWS-Konto mit den erforderlichen Berechtigungen auf Sie zugreifen, anstatt immer ihre Administratorberechtigungen zu verwenden.

Wenn Sie beispielsweise ein Entwickler sind, können Sie, nachdem Sie Ihren Administratorbenutzer in IAM Identity Center erstellt haben, einen neuen Berechtigungssatz erstellen, der `PowerUserAccess` Berechtigungen gewährt, und diesen Berechtigungssatz dann sich selbst zuweisen. Im Gegensatz zum Administratorberechtigungsatz, der `AdministratorAccess` Berechtigungen verwendet, ermöglicht der `PowerUserAccess` Berechtigungssatz keine Verwaltung von IAM-Benutzern und -Gruppen. Wenn Sie sich beim AWS Zugriffsportal anmelden, um auf Ihr AWS Konto zuzugreifen, können Sie `PowerUserAccess` wählen, ob `AdministratorAccess` Sie Entwicklungsaufgaben im Konto ausführen möchten.

Beachten Sie folgende Überlegungen:

- Verwenden Sie einen vordefinierten Berechtigungssatz anstelle eines benutzerdefinierten Berechtigungssatzes, um schnell mit der Erstellung eines restriktiveren Berechtigungssatzes zu beginnen.

Mit einem vordefinierten Berechtigungssatz, der [vordefinierte Berechtigungen verwendet](#), wählen Sie eine einzelne AWS verwaltete Richtlinie aus einer Liste verfügbarer Richtlinien aus. Jede Richtlinie gewährt eine bestimmte Zugriffsebene auf AWS Dienste und Ressourcen oder Berechtigungen für eine allgemeine Aufgabenfunktion. Informationen zu jeder dieser Richtlinien finden Sie unter [AWS Verwaltete Richtlinien für Jobfunktionen](#).

- Sie können die Sitzungsdauer für einen Berechtigungssatz konfigurieren, um zu steuern, wie lange ein Benutzer angemeldet ist AWS-Konto.

Wenn Benutzer sich mit ihrer verbinden AWS-Konto und die AWS Management Console oder die AWS Befehlszeilenschnittstelle (AWS CLI) verwenden, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Standardmäßig ist der Wert für die Sitzungsdauer, der bestimmt, wie lange ein Benutzer angemeldet werden kann, AWS-Konto bevor er sich von der Sitzung AWS abmeldet, auf eine Stunde festgelegt. Sie können einen Höchstwert von 12 Stunden angeben. Weitere Informationen finden Sie unter [Legen Sie die Sitzungsdauer fest für AWS-Konten](#).

- Sie können auch die Sitzungsdauer des AWS Access Portals konfigurieren, um zu steuern, wie lange ein Workforce-Benutzer im Portal angemeldet ist.

Standardmäßig beträgt der Wert für Maximale Sitzungsdauer, der bestimmt, wie lange ein Workforce-Benutzer am AWS Access Portal angemeldet werden kann, bevor er sich erneut

authentifizieren muss, acht Stunden. Sie können einen Höchstwert von 90 Tagen angeben. Weitere Informationen finden Sie unter [Konfigurieren Sie die Sitzungsdauer im IAM Identity Center](#).

- Wenn Sie sich beim AWS Access Portal anmelden, wählen Sie die Rolle aus, die Berechtigungen mit den geringsten Rechten gewährt.

Jeder Berechtigungssatz, den Sie erstellen und Ihrem Benutzer zuweisen, wird als verfügbare Rolle im AWS Access-Portal angezeigt. Wenn Sie sich als dieser Benutzer beim Portal anmelden, wählen Sie nicht die Rolle aus, die dem restriktivsten Berechtigungssatz entspricht, den Sie für die Ausführung von Aufgaben im Konto verwenden können `AdministratorAccess`.

- Sie können weitere Benutzer zu IAM Identity Center hinzufügen und diesen Benutzern vorhandene oder neue Berechtigungssätze zuweisen.

Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).

Themen

- [Vordefinierte Berechtigungen für AWS Verwaltete Richtlinien](#)
- [Benutzerdefinierte Berechtigungen für AWS verwaltete und vom Kunden verwaltete Richtlinien](#)
- [Berechtigungssätze erstellen, verwalten und löschen](#)
- [Konfigurieren Sie die Eigenschaften von Berechtigungssätzen](#)

Vordefinierte Berechtigungen für AWS Verwaltete Richtlinien

Sie können einen vordefinierten Berechtigungssatz mit AWS verwalteten Richtlinien erstellen.

Wenn Sie einen Berechtigungssatz mit vordefinierten Berechtigungen erstellen, wählen Sie eine Richtlinie aus einer Liste AWS verwalteter Richtlinien aus. Innerhalb der verfügbaren Richtlinien können Sie zwischen `allgemeinen Berechtigungsrichtlinien` und Richtlinien für `berufliche Funktionen` wählen.

Allgemeine Genehmigungsrichtlinien

Wählen Sie aus einer Liste AWS verwalteter Richtlinien, die Ihnen den Zugriff auf Ihre gesamten Ressourcen ermöglichen AWS-Konto. Sie können eine der folgenden Richtlinien hinzufügen:

- `AdministratorAccess`
- `PowerUserAccess`
- `ReadOnlyAccess`

- ViewOnlyAccess

Richtlinien für Aufgaben und Funktionen

Wählen Sie aus einer Liste AWS verwalteter Richtlinien aus, die den Zugriff auf Ressourcen in Ihrem Unternehmen ermöglichen AWS-Konto , die für eine Stelle in Ihrem Unternehmen relevant sein könnten. Sie können eine der folgenden Richtlinien hinzufügen:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Eine ausführliche Beschreibung der verfügbaren allgemeinen Berechtigungsrichtlinien und Richtlinien für Jobfunktionen finden Sie [im AWS Identity and Access Management Benutzerhandbuch unter AWS Verwaltete Richtlinien für Jobfunktionen](#).

Anweisungen zum Erstellen eines Berechtigungssatzes finden Sie unter [Berechtigungssätze erstellen, verwalten und löschen](#).

Benutzerdefinierte Berechtigungen für AWS verwaltete und vom Kunden verwaltete Richtlinien

Sie können einen Berechtigungssatz mit benutzerdefinierten Berechtigungen erstellen und dabei alle AWS verwalteten und vom Kunden verwalteten Richtlinien, die Sie in AWS Identity and Access Management (IAM) haben, mit integrierten Richtlinien kombinieren. Sie können auch eine Berechtigungsgrenze angeben, um die maximal möglichen Berechtigungen festzulegen, die andere Richtlinien Benutzern Ihres Berechtigungssatzes gewähren können.

Anweisungen zum Erstellen eines Berechtigungssatzes finden Sie unter [Berechtigungssätze erstellen, verwalten und löschen](#).

Richtlinientypen, die Sie Ihrem Berechtigungssatz hinzufügen können

Themen

- [Eingebundene Richtlinien](#)
- [AWS Verwaltete Richtlinien](#)
- [Kundenverwaltete Richtlinien](#)
- [Berechtigungsgrenzen](#)

Eingebundene Richtlinien

Sie können eine integrierte Richtlinie an einen Berechtigungssatz anhängen. Eine Inline-Richtlinie ist ein Textblock, der als IAM-Richtlinie formatiert ist und den Sie direkt zu Ihrem Berechtigungssatz hinzufügen. Sie können eine Richtlinie einfügen oder mit dem Tool zur Richtlinienerstellung in der IAM Identity Center-Konsole eine neue generieren, wenn Sie einen neuen Berechtigungssatz erstellen. Sie können IAM-Richtlinien auch mit dem [AWS Policy Generator erstellen](#).

Wenn Sie einen Berechtigungssatz mit einer integrierten Richtlinie bereitstellen, erstellt IAM Identity Center eine IAM-Richtlinie an der AWS-Konten Stelle, an der Sie Ihren Berechtigungssatz zuweisen. IAM Identity Center erstellt die Richtlinie, wenn Sie den Berechtigungssatz dem Konto zuweisen. Die Richtlinie wird dann an die IAM-Rolle in Ihrem angehängt AWS-Konto, die Ihr Benutzer annimmt.

Wenn Sie eine Inline-Richtlinie erstellen und Ihren Berechtigungssatz zuweisen, konfiguriert IAM Identity Center die darin enthaltenen Richtlinien für Sie AWS-Konten. Wenn Sie Ihren Berechtigungssatz mit erstellen [Kundenverwaltete Richtlinien](#), müssen Sie die Richtlinien AWS-Konten selbst erstellen, bevor Sie den Berechtigungssatz zuweisen.

AWS Verwaltete Richtlinien

Sie können AWS verwaltete Richtlinien an Ihren Berechtigungssatz anhängen. AWS Verwaltete Richtlinien sind IAM-Richtlinien, die AWS verwaltet werden. Im Gegensatz dazu [Kundenverwaltete Richtlinien](#) gibt es in Ihrem Konto IAM-Richtlinien, die Sie erstellen und verwalten. AWS verwaltete Richtlinien befassen sich mit den häufigsten Anwendungsfällen mit den geringsten Rechten in Ihrem AWS-Konto Unternehmen. Sie können eine AWS verwaltete Richtlinie als Berechtigungen für die Rolle, die IAM Identity Center erstellt, oder als [Berechtigungsgrenze](#) zuweisen.

AWS verwaltet [AWS verwaltete Richtlinien für Jobfunktionen](#), die Ihren Ressourcen auftragsspezifische Zugriffsberechtigungen zuweisen. AWS Sie können eine Jobfunktionsrichtlinie hinzufügen, wenn Sie sich dafür entscheiden, vordefinierte Berechtigungen zusammen mit Ihrem Berechtigungssatz zu verwenden. Wenn Sie Benutzerdefinierte Berechtigungen auswählen, können Sie mehr als eine Job-/Funktionsrichtlinie hinzufügen.

Ihre enthält AWS-Konto auch eine große Anzahl AWS verwalteter IAM-Richtlinien für bestimmte AWS-Services und Kombinationen von. AWS-Services Wenn Sie einen Berechtigungssatz mit benutzerdefinierten Berechtigungen erstellen, können Sie aus vielen zusätzlichen AWS verwalteten Richtlinien wählen, die Sie Ihrem Berechtigungssatz zuweisen möchten.

AWS füllt jede AWS-Konto mit AWS verwalteten Richtlinien auf. Um einen Berechtigungssatz mit AWS verwalteten Richtlinien bereitzustellen, müssen Sie nicht zuerst eine Richtlinie in Ihrem AWS-Konten erstellen. Wenn Sie Ihren Berechtigungssatz mit erstellen [Kundenverwaltete Richtlinien](#), müssen Sie die Richtlinien AWS-Konten selbst erstellen, bevor Sie den Berechtigungssatz zuweisen.

Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter [AWS Verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

Kundenverwaltete Richtlinien

Sie können von Kunden verwaltete Richtlinien an Ihren Berechtigungssatz anhängen. Von Kunden verwaltete Richtlinien sind IAM-Richtlinien in Ihrem Konto, die Sie erstellen und verwalten. Werden in Ihrem Konto dagegen die IAM-Richtlinien eingehalten? [AWS Verwaltete Richtlinien](#) AWS Sie können eine vom Kunden verwaltete Richtlinie als Berechtigungen für die Rolle, die IAM Identity Center erstellt, oder als [Berechtigungsgrenze zuweisen](#).

Wenn Sie einen Berechtigungssatz mit einer vom Kunden verwalteten Richtlinie erstellen, müssen Sie in allen Bereichen, in AWS-Konto denen IAM Identity Center Ihren Berechtigungssatz zuweist, eine IAM-Richtlinie mit demselben Namen und Pfad erstellen. Wenn Sie einen benutzerdefinierten Pfad angeben, stellen Sie sicher, dass Sie in jedem Pfad denselben Pfad angeben. AWS-Konto Weitere Informationen finden Sie unter [Anzeigenamen und -pfade](#) im IAM-Benutzerhandbuch. IAM Identity Center hängt die IAM-Richtlinie an die IAM-Rolle an, die es in Ihrem erstellt. AWS-Konto Es hat sich bewährt, in jedem Konto, dem Sie den Berechtigungssatz zuweisen, dieselben Berechtigungen auf die Richtlinie anzuwenden. Weitere Informationen finden Sie unter [Verwenden Sie IAM-Richtlinien in Berechtigungssätzen](#).

Note

Wenn eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz angehängt ist, wird beim Namen der Richtlinie nicht zwischen Groß- und Kleinschreibung unterschieden.

Weitere Informationen finden Sie [im IAM-Benutzerhandbuch unter Vom Kunden verwaltete Richtlinien](#).

Berechtigungsgrenzen

Sie können Ihrem Berechtigungssatz eine Berechtigungsgrenze hinzufügen. Eine Berechtigungsgrenze ist eine AWS verwaltete oder vom Kunden verwaltete IAM-Richtlinie, die die maximale Anzahl von Berechtigungen festlegt, die eine identitätsbasierte Richtlinie einem IAM-Prinzipal gewähren kann. Wenn Sie eine Berechtigungsgrenze anwenden, können Ihre und [AWS Verwaltete Richtlinien](#) keine Berechtigungen gewähren [Eingebundene Richtlinien](#)[Kundenverwaltete Richtlinien](#), die die von Ihrer Berechtigungsgrenze gewährten Berechtigungen überschreiten. Eine Berechtigungsgrenze gewährt keine Berechtigungen, sondern sorgt stattdessen dafür, dass IAM alle Berechtigungen außerhalb der Grenze ignoriert.

Wenn Sie einen Berechtigungssatz mit einer vom Kunden verwalteten Richtlinie als Berechtigungsgrenze erstellen, müssen Sie für jede AWS-Konto Stelle, an der IAM Identity Center Ihren Berechtigungssatz zuweist, eine IAM-Richtlinie mit demselben Namen erstellen. IAM Identity Center hängt die IAM-Richtlinie als Berechtigungsgrenze an die IAM-Rolle an, die es in Ihrem erstellt. AWS-Konto

Weitere Informationen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.

Berechtigungssätze erstellen, verwalten und löschen

Berechtigungssätze definieren die Zugriffsebene, auf die Benutzer und Gruppen Zugriff haben. AWS-Konto Berechtigungssätze werden im IAM Identity Center gespeichert und können für einen oder mehrere Benutzer bereitgestellt werden. AWS-Konten Sie können einem Benutzer mehrere Berechtigungssätze zuweisen. Weitere Informationen zu Berechtigungssätzen und ihrer Verwendung in IAM Identity Center finden Sie unter. [Verwalten AWS-Konten mit Berechtigungssätzen](#)

Note

In der IAM Identity Center-Konsole können Sie Berechtigungssätze nach Namen suchen und sortieren.

Beachten Sie beim Erstellen von Berechtigungssätzen die folgenden Überlegungen:

- Instanz der Organisation

Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

- Beginnen Sie mit einem vordefinierten Berechtigungssatz

Mit einem vordefinierten Berechtigungssatz, der [vordefinierte Berechtigungen verwendet](#), wählen Sie eine einzelne AWS verwaltete Richtlinie aus einer Liste verfügbarer Richtlinien aus. Jede Richtlinie gewährt eine bestimmte Zugriffsebene auf AWS Dienste und Ressourcen oder Berechtigungen für eine allgemeine Aufgabenfunktion. Informationen zu jeder dieser Richtlinien finden Sie unter [AWS Verwaltete Richtlinien für Jobfunktionen](#). Nachdem Sie Nutzungsdaten gesammelt haben, können Sie den Berechtigungssatz so verfeinern, dass er restriktiver ist.

- Beschränken Sie die Dauer der Verwaltungssitzung auf angemessene Arbeitszeiten

Wenn Benutzer sich zu ihrem Netzwerk AWS-Konto zusammenschließen und die AWS-Managementkonsole AWS Befehlszeilenschnittstelle (AWS CLI) verwenden, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Wenn die Benutzersitzung die Sitzungsdauer erreicht, werden sie von der Konsole abgemeldet und aufgefordert, sich erneut anzumelden. Als bewährte Sicherheitsmaßnahme empfehlen wir Ihnen, die Sitzungsdauer nicht länger als für die Ausführung der Rolle nötig festzulegen. Standardmäßig ist der Wert für die Sitzungsdauer eine Stunde. Sie können einen Höchstwert von 12 Stunden angeben. Weitere Informationen finden Sie unter [Legen Sie die Sitzungsdauer fest für AWS-Konten](#).

- Begrenzen Sie die Dauer der Sitzung im Workforce-Benutzerportal

Workforce-Benutzer verwenden Portalsitzungen, um Rollen auszuwählen und auf Anwendungen zuzugreifen. Standardmäßig beträgt der Wert für Maximale Sitzungsdauer, der bestimmt, wie lange ein Workforce-Benutzer am AWS Access Portal angemeldet werden kann, bevor er sich erneut authentifizieren muss, acht Stunden. Sie können einen Höchstwert von 90 Tagen angeben. Weitere Informationen finden Sie unter [Konfigurieren Sie die Sitzungsdauer im IAM Identity Center](#).

- Verwenden Sie die Rolle, die Berechtigungen mit den geringsten Rechten gewährt

Jeder Berechtigungssatz, den Sie erstellen und Ihrem Benutzer zuweisen, wird als verfügbare Rolle im AWS Access-Portal angezeigt. Wenn Sie sich als dieser Benutzer beim Portal anmelden, wählen Sie nicht die Rolle aus, die dem restriktivsten Berechtigungssatz entspricht, den Sie für die Ausführung von Aufgaben im Konto verwenden können AdministratorAccess. Testen Sie Ihre

Berechtigungssätze, um sicherzustellen, dass sie den erforderlichen Zugriff gewähren, bevor Sie die Benutzereinladung senden.

 Note

Sie können es auch verwenden [AWS CloudFormation](#), um Berechtigungssätze zu erstellen und zuzuweisen und diesen Berechtigungssätzen Benutzer zuzuweisen.

Themen

- [Erstellen Sie einen Berechtigungssatz](#)
- [Einen Berechtigungssatz anzeigen und ändern](#)
- [Delegieren Sie die Verwaltung von Berechtigungssätzen](#)
- [Verwenden Sie IAM-Richtlinien in Berechtigungssätzen](#)
- [Entfernen Sie Berechtigungssätze im IAM Identity Center](#)
- [Löschen Sie Berechtigungssätze im IAM Identity Center](#)

Erstellen Sie einen Berechtigungssatz

Gehen Sie wie folgt vor, um einen vordefinierten Berechtigungssatz zu erstellen, der eine einzelne AWS verwaltete Richtlinie verwendet, oder einen benutzerdefinierten Berechtigungssatz, der bis zu 10 AWS verwaltete oder vom Kunden verwaltete Richtlinien und eine integrierte Richtlinie verwendet. Sie können in der [Service Quota-Konsole](#) für IAM eine Anpassung an die maximale Anzahl von 10 Richtlinien anfordern. Sie können einen Berechtigungssatz in der IAM Identity Center-Konsole erstellen.

 Note

Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

So erstellen Sie einen Berechtigungssatz

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).

2. Wählen Sie unter **Multi-account Berechtigungen** die Option **Berechtigungssätze** aus.
3. Wählen Sie **Create permission set (Berechtigungssatz erstellen)** aus.
4. Wählen Sie auf der **Seite Berechtigungssatztyp** auswählen unter **Berechtigungssatztyp** einen **Berechtigungssatztyp** aus.
5. Wählen Sie je nach Typ des Berechtigungssatzes eine oder mehrere Richtlinien aus, die Sie für den Berechtigungssatz verwenden möchten:

- **Vordefinierter Berechtigungssatz**

1. Wählen Sie unter **Richtlinie für vordefinierten Berechtigungssatz** eine der **IAM-Jobfunktionsrichtlinien** oder **Allgemeine Berechtigungsrichtlinien** in der Liste aus, und klicken Sie dann auf **Weiter**. Weitere Informationen finden Sie unter [AWS Verwaltete Richtlinien für Jobfunktionen](#) und [AWS verwaltete Richtlinien](#) im AWS Identity and Access Management Benutzerhandbuch.
2. Fahren Sie mit Schritt 6 fort, um die **Seite „Details zum Berechtigungssatz angeben“** abzuschließen.

- **Benutzerdefinierter Berechtigungssatz**

1. Wählen Sie **Weiter** aus.
 2. Wählen Sie auf der **Seite Richtlinien und Berechtigungsgrenzen** angeben die Typen von IAM-Richtlinien aus, die Sie auf Ihren neuen Berechtigungssatz anwenden möchten. Standardmäßig können Sie Ihrem Berechtigungssatz eine beliebige Kombination aus bis zu 10 AWS verwalteten Richtlinien und vom Kunden verwalteten Richtlinien hinzufügen. Dieses Kontingent wird von IAM festgelegt. Um es zu erhöhen, fordern Sie eine Erhöhung der IAM-Quote an. Verwaltete Richtlinien, die einer IAM-Rolle zugeordnet sind, können Sie in der Konsole **„Dienstkontingente“** in allen Bereichen, in AWS-Konto denen Sie den Berechtigungssatz zuweisen möchten, eine Erhöhung des IAM-Kontingents beantragen.
- Erweitern Sie die AWS verwalteten Richtlinien, um Richtlinien von IAM hinzuzufügen, das diese AWS erstellt und verwaltet. Weitere Informationen finden Sie unter [AWS Verwaltete Richtlinien](#).
 - a. Suchen Sie im Berechtigungssatz nach AWS verwalteten Richtlinien, die Sie auf Ihre Benutzer anwenden möchten, und wählen Sie sie aus.
 - b. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie dessen Container aus und treffen Sie Ihre Auswahl. Wählen Sie **Weiter**, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die **Seite „Details zum Berechtigungssatz angeben“** abzuschließen.

- Erweitern Sie vom Kunden verwaltete Richtlinien, um Richtlinien aus IAM hinzuzufügen, die Sie erstellen und verwalten. Weitere Informationen finden Sie unter [Kundenverwaltete Richtlinien](#).
 - a. Wählen Sie Richtlinien anhängen aus und geben Sie den Namen einer Richtlinie ein, die Sie Ihrem Berechtigungssatz hinzufügen möchten. Erstellen Sie in jedem Konto, dem Sie den Berechtigungssatz zuweisen möchten, eine Richtlinie mit dem von Ihnen eingegebenen Namen. Es hat sich bewährt, der Richtlinie in jedem Konto dieselben Berechtigungen zuzuweisen.
 - b. Wählen Sie Weitere anhängen, um eine weitere Richtlinie hinzuzufügen.
 - c. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie dessen Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.
- Erweitern Sie Inline-Richtlinie, um benutzerdefinierten JSON-formatted Richtlinientext hinzuzufügen. Inline-Richtlinien entsprechen nicht den vorhandenen IAM-Ressourcen. Um eine Inline-Richtlinie zu erstellen, geben Sie die benutzerdefinierte Richtliniensprache in das bereitgestellte Formular ein. IAM Identity Center fügt die Richtlinie zu den IAM-Ressourcen hinzu, die es in Ihren Mitgliedskonten erstellt. Weitere Informationen finden Sie unter [Eingebundene Richtlinien](#).
 - a. Fügen Sie Ihrer Inline-Richtlinie die gewünschten Aktionen und Ressourcen im interaktiven Editor hinzu. Zusätzliche Aussagen können mit Neue Aussage hinzufügen hinzugefügt werden.
 - b. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie dessen Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.
- Erweitern Sie die Grenze für Berechtigungen, um eine AWS verwaltete oder vom Kunden verwaltete IAM-Richtlinie als maximale Anzahl von Berechtigungen hinzuzufügen, die Ihre anderen Richtlinien im Berechtigungssatz zuweisen können. Weitere Informationen finden Sie unter [Berechtigungsgrenzen](#).
 - a. Wählen Sie Eine Berechtigungsgrenze verwenden aus, um die maximale Anzahl an Berechtigungen festzulegen.
 - b. Wählen Sie eine AWS verwaltete Richtlinie, um eine Richtlinie von IAM festzulegen, die als Berechtigungsgrenze AWS erstellt und verwaltet wird. Wählen Sie vom Kunden

verwaltete Richtlinien, um eine von IAM erstellte und verwaltete Richtlinie als Ihre Berechtigungsgrenze festzulegen.

- c. Wenn Sie einen anderen Richtlinienentyp hinzufügen möchten, wählen Sie dessen Container aus und treffen Sie Ihre Auswahl. Wählen Sie **Weiter**, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.

6. Gehen Sie auf der Seite „Details zum Berechtigungssatz angeben“ wie folgt vor:

1. Geben Sie unter **Name des Berechtigungssatzes** einen Namen ein, um diesen Berechtigungssatz in IAM Identity Center zu identifizieren. Der Name, den Sie für diesen Berechtigungssatz angeben, wird im AWS Access Portal als verfügbare Rolle angezeigt. Benutzer melden sich im AWS Access-Portal an, wählen eine aus AWS-Konto, und wählen Sie dann die Rolle aus.

 Note

Die Namen von Berechtigungssätzen müssen innerhalb Ihrer IAM Identity Center-Instanz eindeutig sein.

2. (Optional) Sie können auch eine Beschreibung eingeben. Die Beschreibung wird nur in der IAM Identity Center-Konsole angezeigt, nicht im AWS Access-Portal.
3. (Optional) Geben Sie den Wert für die **Sitzungsdauer** an. Dieser Wert bestimmt, wie lange ein Benutzer angemeldet werden kann, bevor ihn die Konsole von seiner Sitzung abmeldet. Weitere Informationen finden Sie unter [Legen Sie die Sitzungsdauer fest für AWS-Konten](#).
4. (Optional) Geben Sie den Wert für den **Relay-Status** an. Dieser Wert wird im Verbundprozess verwendet, um Benutzer innerhalb des Kontos umzuleiten. Weitere Informationen finden Sie unter [Stellen Sie den Relay-Status für den schnellen Zugriff auf den ein AWS-Managementkonsole](#).

 Note

Die Relay-Status-URL muss innerhalb von liegen AWS-Managementkonsole. Beispiel:
`https://console.aws.amazon.com/ec2/`

5. Erweitern Sie **Tags (optional)**, wählen Sie **Tag hinzufügen** aus, und geben Sie dann Werte für **Schlüssel** und **Wert** an (optional).

Informationen zu Tags siehe [Ressourcen taggen AWS IAM Identity Center](#).

6. Wählen Sie Weiter aus.

7. Überprüfen Sie auf der Seite „Überprüfen und erstellen“ die von Ihnen getroffenen Auswahlen und wählen Sie dann „Erstellen“.
8. Wenn Sie einen Berechtigungssatz erstellen, wird der Berechtigungssatz standardmäßig nicht bereitgestellt (er wird in keinem AWS-Konto verwendet). Um einen Berechtigungssatz in einem bereitzustellenden AWS-Konto, müssen Sie Benutzern und Gruppen im Konto IAM Identity Center-Zugriff zuweisen und dann den Berechtigungssatz auf diese Benutzer und Gruppen anwenden. Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).

Einen Berechtigungssatz anzeigen und ändern

Sie können Berechtigungssätze verwenden, um Benutzern Zugriff darauf zu AWS-Konten gewähren. Sie können einen Berechtigungssatz mit der AWS IAM Identity Center Konsole anzeigen und ändern. In der IAM Identity Center-Konsole können Sie Berechtigungssätze nach Namen suchen und sortieren. Weitere Informationen zu Berechtigungssätzen und ihrer Verwendung in IAM Identity Center finden Sie unter [the section called “Berechtigungssätze”](#)

Berechtigungssätze sind nicht erforderlich, um den Benutzerzugriff auf Anwendungen zu verwalten.

Note

Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Zuweisungen von Berechtigungssätzen anzeigen

Gehen Sie wie folgt vor, um den angewendeten Berechtigungssatz in der AWS IAM Identity Center Konsole anzuzeigen.

All AWS-Konten where a permission set is provisioned

Gehen Sie wie folgt vor, um alle Zuweisungen für einen Berechtigungssatz anzuzeigen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter Multi-account Berechtigungen die Option Berechtigungssätze aus.
3. Wählen Sie auf der Seite Berechtigungssätze den Berechtigungssatz aus, den Sie anzeigen möchten.
4. Auf der Seite mit den ausgewählten Berechtigungssätzen können Sie auf der Registerkarte Konten die Konten sehen, für die der Berechtigungssatz verwendet wird. Sie können das Konto auswählen, um zu sehen, wie der Berechtigungssatz innerhalb des Kontos bereitgestellt wird. Sie können Richtlinien [löschen](#), bearbeiten und an den Berechtigungssatz anhängen.

All permission sets for an AWS-Konto

Gehen Sie wie folgt vor, um alle Zuweisungen für einen Berechtigungssatz anzuzeigen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter Multi-account Berechtigungen die Option AWS-Konten. Wählen Sie das Konto aus, für das Sie die bereitgestellten Berechtigungssätze anzeigen möchten.
3. Sobald Sie auf der ausgewählten AWS-Konto Seite auf der Registerkarte Berechtigungssätze sind, können Sie die verschiedenen Berechtigungssätze einsehen, die den ausgewählten AWS-Konto Berechtigungen zugewiesen wurden. Sie können den Hyperlink zum Berechtigungssatz auswählen, um mehr über den Berechtigungssatz zu erfahren.

All applied permission sets to users and groups

Gehen Sie wie folgt vor, um alle Berechtigungssätze anzuzeigen, die Benutzern oder Gruppen zugewiesen sind:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter Dashboard entweder Benutzer oder Gruppen aus, um IAM Identity Center-Benutzer oder -Gruppen anzuzeigen.
 - a. Wählen Sie auf der Seite Benutzer den Benutzer aus, für den Sie die angewendeten Berechtigungssätze sehen möchten. Wählen Sie als Nächstes die AWS-Konten

Registerkarte und dann den AWS-Konto Abschnitt AWS Kontozugriff aus. Sie können die angewendeten Berechtigungssätze AWS-Konto für den ausgewählten Benutzer sehen.

- b. Wählen Sie auf der Seite Gruppen die Gruppe aus, für die Sie die angewendeten Berechtigungssätze anzeigen möchten. Wählen Sie als Nächstes die AWS-Konten Registerkarte und dann den AWS-Konto Abschnitt „AWS-Konto Zugriff“ aus. Sie können die angewendeten Berechtigungssätze AWS-Konto für die ausgewählte Gruppe sehen.

Einen Berechtigungssatz ändern

Gehen Sie wie folgt vor, um einen [Berechtigungssatz](#) mit der IAM Identity Center-Konsole zu ändern. Sie können Berechtigungssätze für Benutzer oder Gruppen hinzufügen oder daraus entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter Multi-account Berechtigungen die Option AWS-Konten.
3. Auf der AWS-Konto Seite wird eine Baumstrukturliste Ihrer Organisation angezeigt. Wählen Sie den Namen der Person AWS-Konto aus, von der aus Sie den Berechtigungssatz ändern möchten.
4. Wählen Sie auf der Übersichtsseite von unter Zugewiesene Benutzer und Gruppen den Benutzernamen oder Gruppennamen des Berechtigungssatzes aus, den Sie ändern möchten. AWS-Konto Wählen Sie dann Berechtigungssätze ändern aus.
5. Nehmen Sie die gewünschten Änderungen am Berechtigungssatz vor und wählen Sie dann Änderungen speichern aus.
6. Navigieren Sie zur Registerkarte „Berechtigungssätze“, wählen Sie den kürzlich geänderten Berechtigungssatz aus und wählen Sie „Aktualisieren“.
7. Wählen Sie auf der Seite „Berechtigungen aktualisieren“ die Option Aktualisieren aus.

Delegieren Sie die Verwaltung von Berechtigungssätzen

Mit IAM Identity Center können Sie die Verwaltung von Berechtigungssätzen und Zuweisungen in Konten delegieren, indem Sie [IAM-Richtlinien erstellen, die auf die Amazon-Ressourcennamen \(ARNs\)](#) der IAM Identity Center-Ressourcen verweisen. Sie können beispielsweise Richtlinien erstellen, die es verschiedenen Administratoren ermöglichen, Zuweisungen für Berechtigungssätze mit bestimmten Stichwörtern in bestimmten Konten zu verwalten.

 Note

Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

Sie können eine der folgenden Methoden verwenden, um diese Arten von Richtlinien zu erstellen.

- (Empfohlen) Erstellen Sie [in IAM Identity Center](#) Berechtigungssätze mit jeweils einer anderen Richtlinie, und weisen Sie die Berechtigungssätze verschiedenen Benutzern oder Gruppen zu. Auf diese Weise können Sie Administratorberechtigungen für Benutzer verwalten, die sich mit der von Ihnen ausgewählten [IAM Identity Center-Identitätsquelle anmelden](#).
- Erstellen Sie benutzerdefinierte Richtlinien in IAM und fügen Sie sie dann den IAM-Rollen hinzu, die Ihre Administratoren übernehmen. Informationen zu Rollen finden Sie unter [IAM-Rollen](#), um die ihnen zugewiesenen IAM Identity Center-Administratorberechtigungen zu erhalten.

 Important

Bei den ARNs von IAM Identity Center-Ressourcen wird zwischen Groß- und Kleinschreibung unterschieden.

Im Folgenden wird die korrekte Schreibweise für die Referenzierung des IAM Identity Center-Berechtigungssatzes und der Kontoressourcentypen veranschaulicht.

Ressourcentypen	ARN	Kontextschlüssel
PermissionSet	arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId}	aws:ResourceTag/\${TagKey}
Account	arn:\${Partition}:sso::account/\${AccountId}	Nicht zutreffend

Verwenden Sie IAM-Richtlinien in Berechtigungssätzen

In haben Sie gelernt [Erstellen Sie einen Berechtigungssatz](#), wie Sie Richtlinien, einschließlich vom Kunden verwalteter Richtlinien und Berechtigungsgrenzen, zu einem Berechtigungssatz hinzufügen. Wenn Sie einem Berechtigungssatz vom Kunden verwaltete Richtlinien und Berechtigungen hinzufügen, erstellt IAM Identity Center in keinem dieser AWS-Konten Bereiche eine Richtlinie. Stattdessen müssen Sie diese Richtlinien im Voraus in jedem Konto erstellen, dem Sie Ihren Berechtigungssatz zuweisen möchten, und sie mit den Namen und Pfadangaben Ihres Berechtigungssatzes abgleichen. Wenn Sie einer AWS-Konto in Ihrer Organisation einen Berechtigungssatz zuweisen, erstellt IAM Identity Center eine [AWS Identity and Access Management \(IAM-\) Rolle](#) und hängt Ihre [IAM-Richtlinien](#) an diese Rolle an.

Überlegungen

- Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).
- Bevor Sie Ihren Berechtigungssatz den IAM-Richtlinien zuweisen, müssen Sie Ihr Mitgliedskonto vorbereiten. Der Name einer IAM-Richtlinie in Ihrem Mitgliedskonto muss mit dem Namen der Richtlinie in Ihrem Verwaltungskonto übereinstimmen. IAM Identity Center kann den Berechtigungssatz nicht zuweisen, wenn die Richtlinie in Ihrem Mitgliedskonto nicht vorhanden ist.

Note

Wenn eine vom Kunden verwaltete Richtlinie an einen Berechtigungssatz angehängt ist, wird beim Namen der Richtlinie nicht zwischen Groß- und Kleinschreibung unterschieden.

- Die Berechtigungen, die die Richtlinie gewährt, müssen nicht exakt den Konten entsprechen.

Weisen Sie einem Berechtigungssatz eine IAM-Richtlinie zu

1. Erstellen Sie in jedem Bereich, AWS-Konten dem Sie den Berechtigungssatz zuweisen möchten, eine IAM-Richtlinie.
2. Weisen Sie der IAM-Richtlinie Berechtigungen zu. Sie können verschiedenen Konten unterschiedliche Berechtigungen zuweisen. Für ein einheitliches Nutzererlebnis sollten Sie in jeder Richtlinie identische Berechtigungen konfigurieren und verwalten. Sie können Automatisierungsressourcen verwenden AWS CloudFormation StackSets , um beispielsweise Kopien einer IAM-Richtlinie mit demselben Namen und denselben Berechtigungen in

jedem Mitgliedskonto zu erstellen. Weitere Informationen CloudFormation StackSets dazu finden Sie unter [Arbeiten mit AWS CloudFormation StackSets](#) im AWS CloudFormation Benutzerhandbuch.

3. Erstellen Sie einen Berechtigungssatz in Ihrem Verwaltungskonto und fügen Sie Ihre IAM-Richtlinie unter „Vom Kunden verwaltete Richtlinien“ oder „Berechtigungsgrenze“ hinzu. Weitere Informationen zum Erstellen eines Berechtigungssatzes finden Sie unter [Erstellen Sie einen Berechtigungssatz](#).
4. Fügen Sie alle integrierten Richtlinien, AWS verwalteten Richtlinien oder zusätzlichen IAM-Richtlinien hinzu, die Sie vorbereitet haben.
5. Erstellen Sie Ihren Berechtigungssatz und weisen Sie ihn zu.

Entfernen Sie Berechtigungssätze im IAM Identity Center

Sie können einen Berechtigungssatz von IAM Identity Center-Benutzern und -Gruppen in der IAM Identity Center-Konsole entfernen. Sie können auch einen Berechtigungssatz aus einem entfernen. AWS-Konto Weitere Informationen zu Berechtigungssätzen und ihrer Verwendung in IAM Identity Center finden Sie unter [Verwalten AWS-Konten mit Berechtigungssätzen](#).

Note

Um Berechtigungssätze verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).

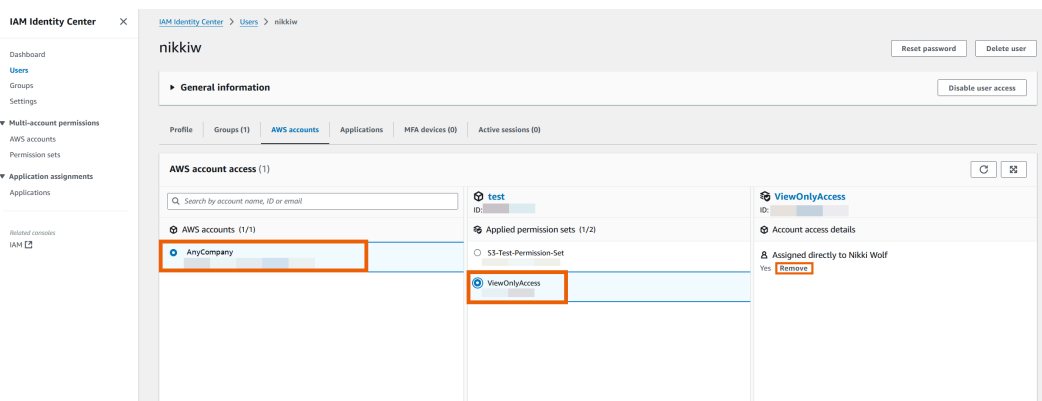
Remove permission set from a user

Berechtigungssatz von einem Benutzer entfernen

Gehen Sie wie folgt vor, um mit der IAM Identity Center-Konsole einen Berechtigungssatz von einem Benutzer zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter IAM Identity Center die Option Benutzer aus.
3. Wählen Sie den Benutzernamen des Benutzers aus, von dem Sie einen Berechtigungssatz entfernen möchten.

4. Wählen Sie auf der Seite mit den Benutzerdetails die AWS-Konten Registerkarte aus. Wählen Sie unter AWS-Konto Zugriff Ihre aus AWS-Konto.
5. Im rechten Bereich werden die angewendeten Berechtigungen für den ausgewählten Benutzer angezeigt. Wählen Sie den Berechtigungssatz aus, den Sie entfernen möchten. Wählen Sie unter Kontozugriffsdetails die Option Entfernen aus.
6. In einem Dialogfeld werden Sie gefragt, ob Sie diesen Berechtigungssatz entfernen möchten. Wählen Sie Entfernen aus.

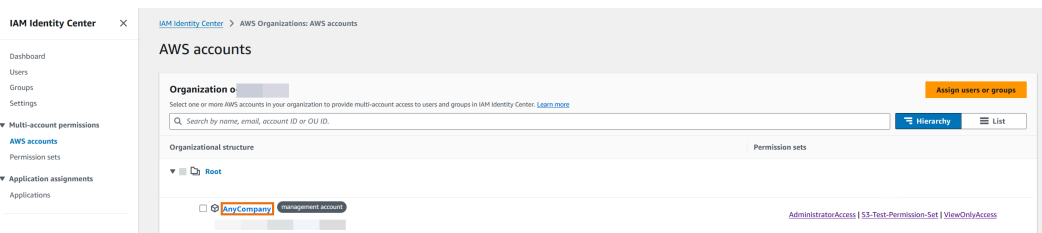


Remove permission set from a group

Berechtigungssatz aus einer Gruppe entfernen

Gehen Sie wie folgt vor, um einen Berechtigungssatz mit der IAM Identity Center-Konsole aus einer Gruppe zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter Multi-account Berechtigungen die Option aus AWS-Konten. Wählen Sie den Link zu Ihrem Verwaltungskonto aus.



3. Wählen Sie auf der Registerkarte Zugewiesene Benutzer und Gruppen die Gruppe aus, aus der Sie den Berechtigungssatz entfernen möchten, und wählen Sie dann Berechtigungssatz ändern aus.

4. Löschen Sie auf der Seite **Berechtigungssätze** ändern den **Berechtigungssatz**, den Sie entfernen möchten, und wählen Sie dann **Änderungen speichern** aus.

Remove permission set from an AWS-Konto

Gehen Sie wie folgt vor, um AWS-Konto mit der IAM Identity Center-Konsole einen **Berechtigungssatz** aus der IAM Identity Center-Konsole zu entfernen.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie unter **Multi-account Berechtigungen** die Option aus AWS-Konten. Wählen Sie den Namen der Person AWS-Konto aus, aus der Sie den **Berechtigungssatz** entfernen möchten.
3. Wählen Sie auf der **Übersichtsseite** von die AWS-Konto **Registerkarte** **Berechtigungssätze** aus. Wählen Sie den **Berechtigungssatz** aus, den Sie entfernen möchten. Wählen Sie dann **Entfernen** aus.
4. Bestätigen Sie im Dialogfeld „**Berechtigungssatz entfernen**“, dass der richtige **Berechtigungssatz** ausgewählt ist, geben Sie ein, **Delete** um das Entfernen zu bestätigen, und wählen Sie dann **Zugriff entfernen** aus.

Löschen Sie Berechtigungssätze im IAM Identity Center

Bevor Sie einen **Berechtigungssatz** aus IAM Identity Center löschen können, sollten Sie [ihn von allen](#) Benutzern entfernen AWS-Konten , die den **Berechtigungssatz** verwenden. Informationen zur Überprüfung des bestehenden Benutzer- und Gruppenzugriffs finden Sie unter [Einen Berechtigungssatz anzeigen und ändern](#).

Überlegungen

- Um **Berechtigungssätze** verwenden zu können, müssen Sie eine Organisationsinstanz von IAM Identity Center verwenden. Weitere Informationen finden Sie unter [Organisations- und Kontoinstanzen von IAM Identity Center](#).
- Informationen zum Widerrufen einer aktiven **Berechtigungssatzsitzung** finden Sie unter [the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”](#).
- Sie sollten **Berechtigungssätze** und **Anwendungszuweisungen** von Benutzern oder Gruppen entfernen, die Sie löschen möchten, bevor Sie sie löschen. Andernfalls stehen Ihnen im IAM

Identity Center nicht zugewiesene und ungenutzte Berechtigungssätze und Anwendungen zur Verfügung.

Gehen Sie wie folgt vor, um einen oder mehrere Berechtigungssätze zu löschen, sodass sie von niemandem AWS-Konto in der Organisation mehr verwendet werden können.

 Important

Alle Benutzer und Gruppen, denen dieser Berechtigungssatz zugewiesen wurde, können AWS-Konto sich nicht mehr anmelden, unabhängig davon, wer ihn verwendet. Informationen zur Überprüfung des bestehenden Benutzer- und Gruppenzugriffs finden Sie unter [Einen Berechtigungssatz anzeigen und ändern](#).

So löschen Sie einen Berechtigungssatz aus einem AWS-Konto

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie unter Multi-account Berechtigungen die Option Berechtigungssätze aus.
3. Wählen Sie den Berechtigungssatz aus, den Sie löschen möchten, und klicken Sie dann auf Löschen.
4. Geben Sie im Dialogfeld „Berechtigungssatz löschen“ den Namen des Berechtigungssatzes ein, um das Löschen zu bestätigen, und wählen Sie dann Löschen aus. Der Name berücksichtigt Groß- und Kleinschreibung.

Konfigurieren Sie die Eigenschaften von Berechtigungssätzen

In IAM Identity Center können Administratoren die folgenden Konfigurations- und Verwaltungsaufgaben ausführen, um den Benutzerzugriff und die Sitzungsdauer zu steuern.

Aufgabe	Weitere Informationen
Administratoren können die maximale Dauer für Benutzersitzungen festlegen, wenn sie über IAM Identity Center auf AWS Ressourcen zugreifen.	Legen Sie die Sitzungsdauer fest für AWS-Konten

Aufgabe	Weitere Informationen
Administratoren können die Landingpage anpassen, die Benutzern nach erfolgreicher Authentifizierung über IAM Identity Center angezeigt wird.	Stellen Sie den Relay-Status für den schnellen Zugriff auf den ein AWS-Managementkonsole
Stellen Sie sicher, dass Benutzer keinen Zugriff mehr auf AWS Ressourcen haben, wenn ihre Berechtigungen widerrufen werden.	Verwenden Sie eine Ablehnungsrichtlinie, um aktive Benutzerberechtigungen zu entziehen

Legen Sie die Sitzungsdauer fest für AWS-Konten

Für jeden [Berechtigungssatz](#) können Sie eine Sitzungsdauer angeben, um zu steuern, wie lange ein Benutzer angemeldet werden kann AWS-Konto. Wenn die angegebene Dauer abgelaufen ist, AWS meldet sich der Benutzer von der Sitzung ab.

Wenn Sie einen neuen Berechtigungssatz erstellen, ist die Sitzungsdauer standardmäßig auf 1 Stunde (in Sekunden) festgelegt. Die Minstdauer der Sitzung beträgt 1 Stunde und kann auf ein Maximum von 12 Stunden festgelegt werden. IAM Identity Center erstellt automatisch IAM-Rollen in jedem zugewiesenen Konto für jeden Berechtigungssatz und konfiguriert diese Rollen mit einer maximalen Sitzungsdauer von 12 Stunden.

Wenn Benutzer eine Verbindung zu ihrer AWS-Konto Konsole herstellen oder wenn AWS Command Line Interface (AWS CLI) verwendet wird, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Standardmäßig können IAM-Rollen, die von IAM Identity Center für Berechtigungssätze generiert wurden, nur von IAM Identity Center-Benutzern übernommen werden. Dadurch wird sichergestellt, dass die im IAM Identity Center-Berechtigungssatz angegebene Sitzungsdauer durchgesetzt wird.

Important

Als bewährte Sicherheitsmaßnahme empfehlen wir Ihnen, die Sitzungsdauer nicht länger als für die Ausführung der Rolle nötig festzulegen.

Nachdem Sie einen Berechtigungssatz erstellt haben, können Sie ihn aktualisieren, um eine neue Sitzungsdauer anzuwenden. Gehen Sie wie folgt vor, um die Länge der Sitzungsdauer für einen Berechtigungssatz zu ändern.

So legen Sie die Sitzungsdauer fest

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie unter **Multi-account Berechtigungen** die Option **Berechtigungssätze** aus.
3. Wählen Sie den Namen des Berechtigungssatzes, für den Sie die Sitzungsdauer ändern möchten.
4. Wählen Sie auf der Detailseite für den Berechtigungssatz rechts neben der Überschrift **Allgemeine Einstellungen** die Option **Bearbeiten** aus.
5. Wählen Sie auf der Seite „Allgemeine Berechtigungssatz-Einstellungen bearbeiten“ einen neuen Wert für die **Sitzungsdauer** aus.
6. Wenn der Berechtigungssatz für einen beliebigen Berechtigungssatz bereitgestellt wurde AWS-Konten, werden die Namen der Konten darunter angezeigt, die automatisch erneut bereitgestellt werden AWS-Konten sollen. Nachdem der Wert für die Sitzungsdauer für den Berechtigungssatz aktualisiert wurde, werden alle Benutzer, AWS-Konten die den Berechtigungssatz verwenden, erneut bereitgestellt. Das bedeutet, dass der neue Wert für diese Einstellung auf alle angewendet wird AWS-Konten , die den Berechtigungssatz verwenden.
7. Wählen Sie **Änderungen speichern** aus.
8. Oben auf der AWS-Konten Seite wird eine Benachrichtigung angezeigt.
 - Wenn der Berechtigungssatz in einem oder mehreren Fällen bereitgestellt wurde AWS-Konten, bestätigt die Benachrichtigung, dass die Berechtigungen erfolgreich erneut bereitgestellt AWS-Konten wurden und dass der aktualisierte Berechtigungssatz auf die Konten angewendet wurde.
 - Wenn der Berechtigungssatz nicht in einem bereitgestellt wird, bestätigt die Benachrichtigung AWS-Konto, dass die Einstellungen für den Berechtigungssatz aktualisiert wurden.

Stellen Sie den Relay-Status für den schnellen Zugriff auf den ein AWS-Managementkonsole

Wenn sich ein Benutzer beim AWS Zugriffsportal anmeldet, ein Konto auswählt und dann die Rolle auswählt, die aus dem zugewiesenen Berechtigungssatz AWS erstellt wird, leitet IAM Identity Center

den Browser des Benutzers standardmäßig an den weiter. AWS-Managementkonsole Sie können dieses Verhalten ändern, indem Sie den Relay-Status auf eine andere Konsolen-URL setzen.

Wenn Sie den Relay-Status festlegen, können Sie dem Benutzer schnellen Zugriff auf die Konsole gewähren, die für seine Rolle am besten geeignet ist. Beispielsweise können Sie den Relay-Status auf die Amazon EC2-Konsolen-URL (**<https://console.aws.amazon.com/ec2/>**) setzen, um den Benutzer zu dieser Konsole weiterzuleiten, wenn er die Amazon EC2-Administratorrolle wählt. Während der Umleitung zur Standard-URL oder Relay-Status-URL leitet IAM Identity Center den Browser des Benutzers an den Konsolenendpunkt weiter, den der Benutzer zuletzt AWS-Region verwendet hat. Wenn ein Benutzer beispielsweise seine letzte Konsolensitzung in der Region Europa (Stockholm) (eu-north-1) beendet hat, wird der Benutzer zur Amazon EC2-Konsole in dieser Region weitergeleitet.



Um IAM Identity Center so zu konfigurieren, dass der Benutzer zu einer Konsole in einer bestimmten Region umgeleitet wird AWS-Region, geben Sie die Regionsspezifikation als Teil der URL an. Um beispielsweise den Benutzer zur Amazon EC2-Konsole in der Region USA Ost (Ohio) (us-east-2) umzuleiten, geben Sie die URL für die Amazon EC2-Konsole in dieser Region an (). **<https://us-east-2.console.aws.amazon.com/ec2/>** Wenn Sie IAM Identity Center in der Region USA West (Oregon) (us-west-2) aktiviert haben und Sie den Benutzer zu dieser Region weiterleiten möchten, geben Sie Folgendes an. **<https://us-west-2.console.aws.amazon.com/>**

Konfigurieren Sie den Relay-Status

Gehen Sie wie folgt vor, um die Relay-Status-URL für einen Berechtigungssatz zu konfigurieren.

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie unter Multi-account Berechtigungen die Option Berechtigungssätze aus.
3. Wählen Sie den Namen des Berechtigungssatzes, für den Sie die neue Relay-Status-URL festlegen möchten.
4. Wählen Sie auf der Detailseite für den Berechtigungssatz rechts neben der Überschrift Allgemeine Einstellungen die Option Bearbeiten aus.
5. Geben Sie auf der Seite Allgemeine Berechtigungssatz-Einstellungen bearbeiten unter Relay-Status eine Konsolen-URL für einen der AWS Dienste ein. Beispiel:

<https://console.aws.amazon.com/ec2/>

 Note

Die Relay-Status-URL muss innerhalb von liegen AWS-Managementkonsole.

6. Wenn der Berechtigungssatz in einem beliebigen Fall bereitgestellt wurde AWS-Konten, werden die Namen der Konten unter angezeigt, die automatisch neu bereitgestellt werden AWS-Konten sollen. Nachdem die Relay-Status-URL für den Berechtigungssatz aktualisiert wurde, werden alle Benutzer, AWS-Konten die den Berechtigungssatz verwenden, erneut bereitgestellt. Das bedeutet, dass der neue Wert für diese Einstellung auf alle angewendet wird AWS-Konten , die den Berechtigungssatz verwenden.
7. Wählen Sie Änderungen speichern aus.
8. Oben auf der Seite „AWS Organisation“ wird eine Benachrichtigung angezeigt.
 - Wenn der Berechtigungssatz in einem oder mehreren Fällen bereitgestellt wurde AWS-Konten, bestätigt die Benachrichtigung, dass die Berechtigungen erfolgreich erneut bereitgestellt AWS-Konten wurden und dass der aktualisierte Berechtigungssatz auf die Konten angewendet wurde.
 - Wenn der Berechtigungssatz nicht in einem bereitgestellt wird, bestätigt die Benachrichtigung AWS-Konto, dass die Einstellungen für den Berechtigungssatz aktualisiert wurden.

 Note

Sie können diesen Prozess automatisieren, indem Sie die AWS API, ein AWS SDK oder das AWS Command Line Interface(AWS CLI) verwenden. Weitere Informationen finden Sie unter:

- Die CreatePermissionSet oder UpdatePermissionSet Aktionen in der [IAM Identity Center API-Referenz](#)
- Die create-permission-set update-permission-set OR-Befehle im [sso-admin](#) Abschnitt der AWS CLI Befehlsreferenz.

Verwenden Sie eine Ablehnungsrichtlinie, um aktive Benutzerberechtigungen zu entziehen

Möglicherweise müssen Sie einem IAM Identity Center-Benutzer den Zugriff entziehen, AWS-Konten während der Benutzer einen Berechtigungssatz aktiv verwendet. Sie können ihnen die

Möglichkeit nehmen, ihre aktiven IAM-Rollensitzungen zu verwenden, indem Sie im Voraus eine Ablehnungsrichtlinie für einen nicht angegebenen Benutzer implementieren. Bei Bedarf können Sie dann die Ablehnungsrichtlinie aktualisieren, um den Benutzer anzugeben, dessen Zugriff Sie blockieren möchten. In diesem Thema wird erläutert, wie eine Ablehnungsrichtlinie erstellt wird, und es werden Überlegungen zur Bereitstellung der Richtlinie getroffen.

Bereiten Sie sich darauf vor, eine aktive IAM-Rollensitzung zu widerrufen, die mit einem Berechtigungssatz erstellt wurde

Sie können verhindern, dass der Benutzer mit einer IAM-Rolle, die er aktiv verwendet, Aktionen ausführt, indem Sie für einen bestimmten Benutzer mithilfe einer Service Control-Richtlinie eine Deny-All-Richtlinie anwenden. Sie können auch verhindern, dass ein Benutzer einen beliebigen Berechtigungssatz verwendet, bis Sie sein Passwort ändern. Dadurch wird verhindert, dass ein böswilliger Akteur gestohlene Anmeldeinformationen missbraucht. Wenn Sie den Zugriff generell verweigern und verhindern müssen, dass ein Benutzer erneut einen Berechtigungssatz betritt oder auf andere Berechtigungssätze zugreift, können Sie auch den gesamten Benutzerzugriff entfernen, die aktive AWS Access-Portalsitzung beenden und die Benutzeranmeldung deaktivieren. Unter erfahren [the section called “Beenden Sie aktive Sitzungen für Workforce-Benutzer”](#) Sie, wie Sie die Verweigerungsrichtlinie in Verbindung mit zusätzlichen Aktionen für eine umfassendere Sperrung des Zugriffs verwenden können.

Richtlinie „Ablehnen“

Sie können eine Ablehnungsrichtlinie mit einer Bedingung verwenden, die mit der Bedingung des Benutzers `UserID` aus dem IAM Identity Center-Identitätsspeicher übereinstimmt, um weitere Aktionen durch eine IAM-Rolle zu verhindern, die der Benutzer aktiv verwendet. Durch die Verwendung dieser Richtlinie werden Auswirkungen auf andere Benutzer vermieden, die möglicherweise denselben Berechtigungssatz verwenden, wenn Sie die Ablehnungsrichtlinie bereitstellen. Diese Richtlinie verwendet die Platzhalter-Benutzer-ID *Add user ID here*, `"identitystore:userId"` die Sie mit der Benutzer-ID aktualisieren, für die Sie den Zugriff sperren möchten.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```



```
    "Effect": "Deny",
    "Action": [
        "*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "identitystore:userId": "Add user ID here"
        }
    }
}
```

Sie könnten zwar einen anderen Bedingungsschlüssel verwenden `aws:userId`, wie z. B., `identitystore:userId` ist sicher, da es sich um einen global eindeutigen Wert handelt, der einer Person zugeordnet ist. Die Verwendung `aws:userId` in der Bedingung kann davon abhängen, wie Benutzerattribute anhand Ihrer Identitätsquelle synchronisiert werden, und kann sich ändern, wenn sich der Benutzername oder die E-Mail-Adresse des Benutzers ändern.

In der IAM Identity Center-Konsole können Sie die eines Benutzers finden, `identitystore:userId` indem Sie zu Benutzer navigieren, anhand des Namens nach dem Benutzer suchen, den Abschnitt Allgemeine Informationen erweitern und die Benutzer-ID kopieren. Es ist auch praktisch, die AWS Access-Portal-Sitzung eines Benutzers zu beenden und seinen Anmeldezugriff im gleichen Abschnitt zu deaktivieren, während Sie nach der Benutzer-ID suchen. Sie können den Prozess zur Erstellung einer Ablehnungsrichtlinie automatisieren, indem Sie die Benutzer-ID des Benutzers durch Abfragen der Identitätsspeicher-APIs abrufen.

Bereitstellung der Ablehnungsrichtlinie

Sie können eine Platzhalter-Benutzer-ID verwenden, die nicht gültig ist, z. B. *Add user ID here* um die Ablehnungsrichtlinie im Voraus mithilfe einer Service Control Policy (SCP) bereitzustellen, die Sie den AWS-Konten Benutzern zuordnen, auf die möglicherweise Zugriff haben. Diese Vorgehensweise wird aufgrund ihrer Einfachheit und Schnelligkeit empfohlen. Wenn Sie einem Benutzer den Zugriff mit der Richtlinie „Verweigern“ entziehen, bearbeiten Sie die Richtlinie so, dass die Platzhalter-Benutzer-ID durch die Benutzer-ID der Person ersetzt wird, deren Zugriff Sie entziehen möchten. Dadurch wird verhindert, dass der Benutzer in jedem Konto, an das Sie den SCP anhängen, Aktionen ausführt, für die Berechtigungen festgelegt wurden. Es blockiert die Aktionen des Benutzers, auch wenn er seine aktive AWS Access-Portalsitzung verwendet, um zu

verschiedenen Konten zu navigieren und unterschiedliche Rollen zu übernehmen. Wenn der Zugriff des Benutzers vollständig durch den SCP gesperrt ist, können Sie ihm dann die Möglichkeit zur Anmeldung deaktivieren, seine Zuweisungen widerrufen und seine AWS Zugriffsportalsitzung bei Bedarf beenden.

Als Alternative zur Verwendung von SCPs können Sie die Richtlinie „Ablehnen“ auch in die Inline-Richtlinie für Berechtigungssätze und in vom Kunden verwaltete Richtlinien aufnehmen, die von den Berechtigungssätzen verwendet werden, auf die der Benutzer zugreifen kann.

Wenn Sie den Zugriff für mehrere Personen sperren müssen, können Sie eine Liste von Werten im Bedingungsblock verwenden, z. B.:

```
"Condition": {
  "StringEquals": {
    "identitystore:userId": [" user1 userId", "user2 userId"...]
  }
}
```

Important

Unabhängig von der Methode (n), die Sie verwenden, müssen Sie alle anderen Korrekturmaßnahmen ergreifen und die Benutzer-ID des Benutzers mindestens 12 Stunden lang in der Richtlinie aufbewahren. Nach Ablauf dieser Zeit laufen alle Rollen ab, die der Benutzer übernommen hat, und Sie können dann seine Benutzer-ID aus der Deny-Richtlinie entfernen.

Verweisen auf Berechtigungssätze in Ressourcenrichtlinien, Amazon EKS-Cluster-Konfigurationszuordnungen und AWS KMS Schlüsselrichtlinien

Wenn Sie einem AWS Konto einen Berechtigungssatz zuweisen, erstellt IAM Identity Center eine Rolle mit einem Namen, der mit beginnt. `AWSReservedSSO_`

Der vollständige Name und der Amazon-Ressourcenname (ARN) für die Rolle verwenden das folgende Format:

Name	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Wenn Ihre Identitätsquelle im IAM Identity Center in us-east-1 gehostet wird, enthält die ARN keine *aws-region*. Der vollständige Name und der ARN für die Rolle verwenden das folgende Format:

Name	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Wenn Sie beispielsweise einen Berechtigungssatz erstellen, der Datenbankadministratoren AWS Kontozugriff gewährt, wird eine entsprechende Rolle mit dem folgenden Namen und der folgenden ARN erstellt:

Name	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

Wenn Sie alle Zuweisungen zu diesem Berechtigungssatz im AWS Konto löschen, wird die entsprechende Rolle, die IAM Identity Center erstellt hat, ebenfalls gelöscht. Wenn Sie demselben Berechtigungssatz später eine neue Zuweisung vornehmen, erstellt IAM Identity Center eine neue

Rolle für den Berechtigungssatz. Der Name und der ARN der neuen Rolle enthalten ein anderes, eindeutiges Suffix. In diesem Beispiel lautet das eindeutige Suffix `abcdef0123456789`.

Name	ARN
<code>AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789</code>	<code>arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789</code>

Die Änderung des Suffixes im neuen Namen und ARN für die Rolle führt dazu, dass alle Richtlinien, die auf den ursprünglichen Namen und ARN verweisen, veraltet sind. Dadurch wird der Zugriff für Personen unterbrochen, die den entsprechenden Berechtigungssatz verwenden. Beispielsweise beeinträchtigt eine Änderung des ARN für die Rolle den Zugriff für Benutzer des Berechtigungssatzes, wenn in den folgenden Konfigurationen auf den ursprünglichen ARN verwiesen wird:

- In der `aws-auth ConfigMap` Datei für Amazon Elastic Kubernetes Service (Amazon EKS) - Cluster, wenn Sie den `aws-auth ConfigMap` für den Clusterzugriff verwenden.
- In einer ressourcenbasierten Richtlinie für einen `()` -Schlüssel. AWS Key Management Service (AWS KMS) Diese Richtlinie wird auch als Schlüsselrichtlinie bezeichnet.

Note

Wir empfehlen, dass Sie [Amazon EKS-Zugriffseinträge verwenden](#), um den Zugriff auf Ihre Amazon EKS-Cluster zu verwalten. Auf diese Weise können Sie IAM-Berechtigungen verwenden, um die Principals zu verwalten, die Zugriff auf einen Amazon EKS-Cluster haben. Mithilfe von Amazon EKS-Zugriffseinträgen können Sie einen IAM-Prinzipal mit Amazon EKS-Berechtigungen verwenden, um wieder Zugriff auf einen Cluster zu erhalten, ohne Kontakt aufnehmen zu müssen. Support

Sie können zwar ressourcenbasierte Richtlinien für die meisten AWS Services so aktualisieren, dass sie auf einen neuen ARN für eine Rolle verweisen, die einem Berechtigungssatz entspricht, aber Sie müssen über eine Backup-Rolle verfügen, die Sie in IAM für Amazon EKS erstellen und AWS KMS

falls sich der ARN ändert. Für Amazon EKS muss die Backup-IAM-Rolle in der vorhanden sein. `aws-auth ConfigMap` Denn AWS KMS sie muss in Ihren wichtigsten Richtlinien enthalten sein. Wenn Sie keine Backup-IAM-Rolle mit Berechtigungen zur Aktualisierung der `aws-auth ConfigMap` oder der AWS KMS Schlüsselrichtlinie haben, wenden Sie sich an uns, Support um wieder Zugriff auf diese Ressourcen zu erhalten.

Empfehlungen zur Vermeidung von Zugriffsunterbrechungen

Um Zugriffsunterbrechungen aufgrund von Änderungen im ARN für eine Rolle zu vermeiden, die einem Berechtigungssatz entspricht, empfehlen wir Ihnen, Folgendes zu tun.

- Pflegen Sie mindestens eine Berechtigungssatzzuweisung.

Behalten Sie diese Zuweisung in den AWS Konten bei, die die Rollen enthalten, auf die Sie in Amazon EKS verweisen, wichtige Richtlinien in AWS KMS oder ressourcenbasierte Richtlinien `aws-auth ConfigMap` für andere. AWS-Services

Wenn Sie beispielsweise einen EKSAccess Berechtigungssatz erstellen und vom AWS Konto aus auf den entsprechenden Rollen-ARN verweisen `111122223333`, weisen Sie dem Berechtigungssatz in diesem Konto dauerhaft eine administrative Gruppe zu. Da es sich um eine permanente Zuweisung handelt, löscht IAM Identity Center die entsprechende Rolle nicht, sodass das Risiko einer Umbenennung ausgeschlossen ist. Die administrative Gruppe hat immer Zugriff, ohne dass das Risiko einer Rechteerweiterung besteht.

- Für Amazon EKS-Cluster, die **aws-auth ConfigMap** und verwenden AWS KMS: Schließen Sie eine in IAM erstellte Rolle ein.

Wenn Sie Rollen-ARNs für Berechtigungssätze in einem `aws-auth ConfigMap` Amazon EKS-Cluster oder in wichtigen Richtlinien für AWS KMS Schlüssel referenzieren, empfehlen wir, dass Sie auch mindestens eine Rolle einbeziehen, die Sie in IAM erstellen. Die Rolle muss Ihnen den Zugriff auf den Amazon EKS-Cluster oder die Verwaltung der AWS KMS Schlüsselrichtlinie ermöglichen. Der Berechtigungssatz muss in der Lage sein, diese Rolle zu übernehmen. Auf diese Weise können Sie, falls sich der Rollen-ARN für einen Berechtigungssatz ändert, den Verweis auf den ARN in der AWS KMS Schlüsselrichtlinie `aws-auth ConfigMap` oder aktualisieren. Der nächste Abschnitt enthält ein Beispiel dafür, wie Sie eine Vertrauensrichtlinie für eine Rolle erstellen können, die in IAM erstellt wird. Die Rolle kann nur von einem `AdministratorAccess` Berechtigungssatz übernommen werden.

Beispiel für eine benutzerdefinierte Vertrauensrichtlinie

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Vertrauensrichtlinie, die einem AdministratorAccess Berechtigungssatz den Zugriff auf eine Rolle gewährt, die in IAM erstellt wurde. Zu den wichtigsten Elementen dieser Richtlinie gehören:

- Das Hauptelement dieser Vertrauensrichtlinie legt einen AWS Hauptkontoinhaber fest. In dieser Richtlinie können Hauptbenutzer des AWS Kontos 111122223333 mit `sts:AssumeRole` Berechtigungen die Rolle übernehmen, die in IAM erstellt wurde.
- Die `Condition` element dieser Vertrauensrichtlinie legt zusätzliche Anforderungen für Prinzipale fest, die die in IAM erstellte Rolle übernehmen können. In dieser Richtlinie kann der Berechtigungssatz mit der folgenden Rolle ARN die Rolle übernehmen.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/  
AWSReservedSSO_AdministratorAccess_*
```

Note

Das `Condition` Element enthält den `ArnLike` Bedingungsoperator und verwendet statt eines eindeutigen Suffixes einen Platzhalter am Ende des Rollen-ARNS für den Berechtigungssatz. Das bedeutet, dass die Richtlinie es dem Berechtigungssatz ermöglicht, die in IAM erstellte Rolle zu übernehmen, auch wenn sich der Rollen-ARN für den Berechtigungssatz ändert.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::111122223333:root"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {  
        "ArnLike": {
```

```
    "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
  }
}
]
}
```

Wenn Sie eine Rolle, die Sie in IAM erstellen, in eine solche Richtlinie aufnehmen, erhalten Sie Notfallzugriff auf Ihre Amazon EKS-Cluster oder andere AWS Ressourcen AWS KMS keys, falls ein Berechtigungssatz oder alle Zuweisungen zu dem Berechtigungssatz versehentlich gelöscht und neu erstellt werden.

Attribute-based Zugriffskontrolle

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. Sie können IAM Identity Center verwenden, um den Zugriff auf Ihre AWS Ressourcen über mehrere Benutzer hinweg zu verwalten, indem Sie Benutzerattribute AWS-Konten verwenden, die aus einer beliebigen IAM Identity Center-Identitätsquelle stammen. In AWS werden diese Attribute als Tags bezeichnet. Durch die Verwendung von Benutzerattributen als Stichwörter können Sie den Prozess der Erstellung detaillierter Berechtigungen vereinfachen AWS und sicherstellen, dass Ihre Mitarbeiter nur auf die AWS Ressourcen mit den entsprechenden Stichwörtern zugreifen können. AWS

Beispielsweise können Sie den Entwicklern Bob und Sally, die aus zwei verschiedenen Teams stammen, demselben Berechtigungssatz im IAM Identity Center (oder derselben IAM-Rolle im Account Access Manager) zuweisen und dann das Teamnamenattribut für die Zugriffskontrolle auswählen. Wenn Bob und Sally sich bei ihrem anmelden AWS-Konten, sendet IAM Identity Center ihr Teamnamenattribut in der AWS Sitzung, sodass Bob und Sally nur dann auf AWS Projektressourcen zugreifen können, wenn ihr Teamnamenattribut mit dem Teamnamens-Tag auf der Projektressource übereinstimmt. Wenn Bob in Zukunft zu Sallys Team wechselt, können Sie seinen Zugriff ändern, indem Sie einfach sein Teamnamenattribut im Unternehmensverzeichnis aktualisieren. Wenn Bob sich das nächste Mal anmeldet, erhält er automatisch Zugriff auf die Projektressourcen seines neuen Teams, ohne dass die Berechtigungen aktualisiert werden müssen. AWS

Dieser Ansatz hilft auch dabei, die Anzahl der unterschiedlichen Berechtigungen zu reduzieren, die Sie im IAM Identity Center erstellen und verwalten müssen, da Benutzer, die denselben

Berechtigungssätzen zugeordnet sind (oder im Account Access Manager als Benutzer, die derselben IAM-Rolle zugeordnet sind), nun über eindeutige Berechtigungen verfügen können, die auf ihren Attributen basieren. Sie können diese Benutzerattribute in IAM Identity Center-Berechtigungssätzen (oder IAM-Rollen, wenn Sie Account Access Manager-Rollenzuweisungen verwenden) und ressourcenbasierten Richtlinien verwenden, um ABAC für AWS Ressourcen zu implementieren und die Verwaltung von Berechtigungen im großen Maßstab zu vereinfachen.

Vorteile

Im Folgenden finden Sie weitere Vorteile der Verwendung von ABAC in IAM Identity Center.

- **ABAC benötigt weniger Berechtigungssätze** — Da Sie keine unterschiedlichen Richtlinien für verschiedene Jobfunktionen erstellen müssen, erstellen Sie weniger Berechtigungssätze (oder IAM-Rollen, wenn Sie den Account Access Manager verwenden). Dies reduziert die Komplexität Ihrer Rechteverwaltung.
- **Mithilfe von ABAC können sich Teams schnell ändern und wachsen** — Berechtigungen für neue Ressourcen werden automatisch auf der Grundlage von Attributen erteilt, wenn Ressourcen bei der Erstellung entsprechend gekennzeichnet werden.
- **Verwenden Sie Mitarbeiterattribute aus Ihrem Unternehmensverzeichnis mit ABAC** — Sie können vorhandene Mitarbeiterattribute aus jeder in IAM Identity Center konfigurierten Identitätsquelle verwenden, um Entscheidungen zur Zugriffskontrolle in zu treffen. AWS
- **Verfolgen Sie, wer auf Ressourcen zugreift** — Sicherheitsadministratoren können die Identität einer Sitzung leicht ermitteln, indem sie die Benutzerattribute überprüfen, AWS CloudTrail um die Benutzeraktivitäten in nachzuverfolgen. AWS

Informationen zur Konfiguration von ABAC mithilfe der IAM Identity Center-Konsole finden Sie unter [Attribute für Zugriffskontrolle](#). Informationen zur Aktivierung und Konfiguration von ABAC mithilfe der IAM Identity Center APIs finden Sie [CreateInstanceAccessControlAttributeConfiguration](#) im IAM Identity Center API-Referenzhandbuch.

Themen

- [Checkliste: Konfiguration von ABAC in AWS mithilfe von IAM Identity Center](#)
- [Attribute für Zugriffskontrolle](#)

Checkliste: Konfiguration von ABAC in AWS mithilfe von IAM Identity Center

Diese Checkliste enthält die Konfigurationsaufgaben, die zur Vorbereitung Ihrer AWS Ressourcen und zur Einrichtung von IAM Identity Center für den ABAC-Zugriff erforderlich sind. Führen Sie die Aufgaben in dieser Checkliste der Reihe nach aus. Wenn ein Referenzlink Sie zu einem Thema führt, kehren Sie zu diesem Thema zurück, damit Sie mit den verbleibenden Aufgaben in dieser Checkliste fortfahren können.

Schritt	Aufgabe	Referenz
1	Lesen Sie, wie Sie Stichwörter zu all Ihren AWS Ressourcen hinzufügen. Um ABAC in IAM Identity Center zu implementieren, müssen Sie zunächst allen AWS Ressourcen, für die Sie ABAC implementieren möchten, Tags hinzufügen.	<ul style="list-style-type: none"> • Ressourcen taggen AWS
2	Erfahren Sie, wie Sie Ihre Identitätsquelle im IAM Identity Center mit den zugehörigen Benutzeridentitäten und Attributen in Ihrem Identitätsspeicher konfigurieren. Mit IAM Identity Center können Sie Benutzerattribute aus jeder unterstützten IAM Identity Center-Identitätsquelle für ABAC in verwenden. AWS	<ul style="list-style-type: none"> • Verwaltung Ihrer Identitätsquelle
3	Ermitteln Sie anhand der folgenden Kriterien, welche Attribute Sie für Entscheidungen zur Zugriffskontrolle in IAM Identity Center verwenden möchten, AWS und senden Sie sie an IAM Identity Center.	<ul style="list-style-type: none"> • Erste Schritte
	<ul style="list-style-type: none"> • Wenn Sie einen externen Identitätsanbieter (IdP) verwenden, entscheiden Sie, ob Sie vom IdP übergebene Attribute verwenden oder Attribute aus IAM Identity Center auswählen möchten. 	<ul style="list-style-type: none"> • Auswahl von Attributen, wenn Sie einen externen Identitätsanbieter als Identitätsquelle verwenden
	<ul style="list-style-type: none"> • Wenn Sie sich dafür entscheiden, dass Ihr IdP Attribute sendet, konfigurieren Sie Ihren IdP so, dass er die Attribute in SAML-Assertionen überträgt. Lesen Sie die Optional Abschnitte im Tutorial für Ihren spezifischen IdP. 	<ul style="list-style-type: none"> • Tutorials zu Identitätsquellen im IAM Identity Center

Schritt	Aufgabe	Referenz
	<ul style="list-style-type: none"> Wenn Sie einen IdP als Identitätsquelle verwenden und Attribute im IAM Identity Center auswählen, sollten Sie untersuchen, wie Sie SCIM so konfigurieren, dass die Attributwerte von Ihrem IdP stammen. Wenn Sie SCIM nicht mit Ihrem IdP verwenden können, fügen Sie die Benutzer und ihre Attribute über die Benutzerseite der IAM Identity Center Console hinzu. 	<ul style="list-style-type: none"> Stellen Sie Benutzer und Gruppen von einem externen Identitätsanbieter mithilfe von SCIM bereit Unterstützte externe Identitätsanbieter-Attribute
	<ul style="list-style-type: none"> Wenn Sie Active Directory oder IAM Identity Center als Identitätsquelle verwenden oder einen IdP verwenden und Attribute im IAM Identity Center auswählen, überprüfen Sie die verfügbaren Attribute, die Sie konfigurieren können. Fahren Sie dann sofort mit Schritt 4 fort, um mit der Konfiguration Ihrer ABAC-Attribute mithilfe der IAM Identity Center-Konsole zu beginnen. 	<ul style="list-style-type: none"> Auswahl von Attributen, wenn Sie IAM Identity Center als Identitätsquelle verwenden Auswahl von Attributen bei der Verwendung AWS Managed Microsoft AD als Ihre Identitätsquelle Standardzuordnungen zwischen IAM Identity Center und Microsoft AD
4	Wählen Sie auf der Seite „Attribute für die Zugriffskontrolle“ in der IAM Identity Center-Konsole die Attribute aus, die für ABAC verwendet werden sollen. Auf dieser Seite können Sie Attribute für die Zugriffskontrolle aus der Identitätsquelle auswählen, die Sie in Schritt 2 konfiguriert haben. Nachdem Ihre Identitäten und ihre Attribute im IAM Identity Center gespeichert sind, müssen Sie Schlüssel-Wert-Paare (Zuordnungen) erstellen, die AWS-Konten zur Verwendung bei Zugriffskontrollentscheidungen an Sie weitergegeben werden.	<ul style="list-style-type: none"> Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle

Schritt	Aufgabe	Referenz
5	Erstellen Sie benutzerdefinierte Berechtigungsrichtlinien innerhalb Ihres Berechtigungssatzes (oder Ihrer IAM-Rolle, wenn Sie den Account Access Manager verwenden) und verwenden Sie Zugriffskontrollattribute, um ABAC-Regeln zu erstellen, sodass Benutzer nur mit passenden Stichwörtern auf Ressourcen zugreifen können. Benutzerattribute, die Sie in Schritt 4 konfiguriert haben, werden als Stichwörter AWS für Zugriffskontrollentscheidungen verwendet. Mithilfe der <code>aws:PrincipalTag/key</code> Bedingung können Sie auf die Attribute der Zugriffskontrolle in der Berechtigungsrichtlinie verweisen.	<ul style="list-style-type: none"> • Erstellen Sie Berechtigungsrichtlinien für ABAC im IAM Identity Center
6	Weisen Sie in Ihren verschiedenen AWS-Konten Optionen Benutzer den Berechtigungssätzen zu, die Sie in Schritt 5 erstellt haben. Auf diese Weise wird sichergestellt, dass sie beim Zusammenschluss mit ihren Konten und beim Zugriff auf AWS Ressourcen nur Zugriff erhalten, der mit passenden Stichwörtern verknüpft ist.	<ul style="list-style-type: none"> • Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten

Nachdem Sie diese Schritte abgeschlossen haben, erhalten Benutzer, die sich AWS-Konto über Single Sign-On zu einem Verbund zusammenschließen, auf der Grundlage übereinstimmender Attribute Zugriff auf ihre AWS Ressourcen.

Attribute für Zugriffskontrolle

Attribute für die Zugriffskontrolle ist der Name der Seite in der IAM Identity Center-Konsole, auf der Sie Benutzerattribute auswählen, die Sie in Richtlinien zur Steuerung des Zugriffs auf Ressourcen verwenden möchten. Sie können Benutzer Workloads auf der AWS Grundlage vorhandener Attribute in der Identitätsquelle der Benutzer zuweisen.

Angenommen, Sie möchten den Zugriff auf S3-Buckets anhand von Abteilungsamen zuweisen. Auf der Seite Attribute für die Zugriffskontrolle wählen Sie das Benutzerattribut Abteilung für die Verwendung mit der attributbasierten Zugriffskontrolle (ABAC) aus. Im IAM Identity Center-

Berechtigungssatz (oder in der IAM-Rolle, wenn Sie den Account Access Manager verwenden) schreiben Sie dann eine Richtlinie, die Benutzern nur dann Zugriff gewährt, wenn das Department-Attribut mit dem Abteilungs-Tag übereinstimmt, das Sie Ihren S3-Buckets zugewiesen haben. IAM Identity Center übergibt das Abteilungsattribut des Benutzers an das Konto, auf das zugegriffen wird. Das Attribut wird dann verwendet, um den Zugriff auf der Grundlage der Richtlinie zu bestimmen. Wenn IAM Identity Center diese Attribute an das Konto übergibt, werden sie als Sitzungs-Tags gesendet, auf die Sie mithilfe des `aws:PrincipalTag/tag-key` Bedingungsschlüssels in allen relevanten AWS IAM-Richtlinientypen verweisen können. Weitere Informationen zu ABAC finden Sie unter. [Attribute-based Zugriffskontrolle](#)

Erste Schritte

Wie Sie mit der Konfiguration von Attributen für die Zugriffskontrolle beginnen, hängt davon ab, welche Identitätsquelle Sie verwenden. Unabhängig von der ausgewählten Identitätsquelle müssen Sie, nachdem Sie Ihre Attribute ausgewählt haben, Berechtigungssatzrichtlinien (oder IAM-Rollenrichtlinien, wenn Sie den Account Access Manager verwenden) erstellen oder bearbeiten. Diese Richtlinien müssen Benutzeridentitäten Zugriff auf Ressourcen gewähren AWS .

Auswahl von Attributen, wenn Sie IAM Identity Center als Identitätsquelle verwenden

Wenn Sie IAM Identity Center als Identitätsquelle konfigurieren, fügen Sie zunächst Benutzer hinzu und konfigurieren deren Attribute. Navigieren Sie als Nächstes zur Seite „Attribute für die Zugriffskontrolle“ und wählen Sie die Attribute aus, die Sie in Richtlinien verwenden möchten. Navigieren Sie abschließend zu der AWS-Konten Seite, um Berechtigungssätze für die Verwendung der Attribute für ABAC zu erstellen oder zu bearbeiten.

Auswahl von Attributen bei der Verwendung AWS Managed Microsoft AD als Ihre Identitätsquelle

Wenn Sie IAM Identity Center AWS Managed Microsoft AD als Ihre Identitätsquelle konfigurieren, ordnen Sie zunächst eine Reihe von Attributen aus Active Directory den Benutzerattributen in IAM Identity Center zu. Navigieren Sie als Nächstes zur Seite „Attribute für die Zugriffskontrolle“. Wählen Sie dann aus, welche Attribute in Ihrer ABAC-Konfiguration verwendet werden sollen, basierend auf den vorhandenen SSO-Attributen, die aus Active Directory zugeordnet wurden. Erstellen Sie schließlich ABAC-Regeln mithilfe der Zugriffskontrollattribute in Berechtigungssätzen (oder IAM-Rollen, wenn Sie den Account Access Manager verwenden), um Benutzeridentitäten Zugriff auf Ressourcen zu gewähren. AWS Eine Liste der Standardzuordnungen von Benutzerattributen in IAM Identity Center zu den Benutzerattributen in Ihrem Verzeichnis finden Sie unter. AWS Managed Microsoft AD [Standardzuordnungen zwischen IAM Identity Center und Microsoft AD](#)

Auswahl von Attributen, wenn Sie einen externen Identitätsanbieter als Identitätsquelle verwenden

Wenn Sie IAM Identity Center mit einem externen Identitätsanbieter (IdP) als Identitätsquelle konfigurieren, gibt es zwei Möglichkeiten, Attribute für ABAC zu verwenden.

- Konfigurieren Sie Attributzuordnungen in der IAM Identity Center-Konsole. Sie können Attribute aus dem IAM Identity Center-Verzeichnis Sitzungs-Tags auf der Seite „Attribute für die Zugriffskontrolle“ in der IAM Identity Center-Konsole zuordnen. Die Attributwerte, die Sie hier auswählen, stammen aus dem Identity Center-Verzeichnis und ersetzen die Werte für alle passenden Attribute, die über eine SAML-Assertion von einem IdP stammen. Je nachdem, ob Sie SCIM verwenden, sollten Sie Folgendes beachten:
 - Wenn Sie SCIM verwenden, synchronisiert der IdP die Attributwerte automatisch mit IAM Identity Center. Sie können diese synchronisierten Attribute dann auf der Seite „Attribute für die Zugriffskontrolle“ auswählen, um sie als Sitzungs-Tags zu verwenden.
 - Wenn Sie SCIM nicht verwenden, müssen Sie die Benutzer manuell hinzufügen und ihre Attribute so einrichten, als ob Sie IAM Identity Center als Identitätsquelle verwenden würden. Navigieren Sie als Nächstes zur Seite „Attribute für die Zugriffskontrolle“ und wählen Sie die Attribute aus, die Sie in Richtlinien verwenden möchten.
- Übergeben Sie Attribute von Ihrem IdP über SAML-Assertionen. Sie können Ihren IdP so konfigurieren, dass Attribute als Sitzungs-Tags über SAML-Assertionen gesendet werden. Konfigurieren Sie dazu Ihren IdP so, dass er SAML-Assertionen mit dem Attributnamen auf sendet und diese durch den `https://aws.amazon.com/SAML/Attributes/AccessControl:TagKey` Sitzungs-Tag-Schlüssel `TagKey` ersetzt, den Sie ausfüllen möchten. IAM Identity Center leitet den Attributnamen und den Wert vom IdP zur Richtlinienbewertung weiter.

Es ist nicht erforderlich, auf der Seite „Attribute für die Zugriffskontrolle“ eine ABAC-Attributzuordnung für Attribute zu konfigurieren, die Sie über SAML-Assertionen von Ihrem externen IdP übergeben. Wenn Sie jedoch auf der Seite „Attribute für die Zugriffskontrolle“ eine ABAC-Zuordnung für dasselbe Attribut konfigurieren, hat die Zuordnung aus dem Identity Center-Verzeichnis Vorrang und ersetzt den von Ihrem IdP in der SAML-Assertion gesendeten Wert.

Note

Attribute in SAML-Assertionen sind für Sie auf der Seite „Attribute für die Zugriffskontrolle“ nicht sichtbar. Sie müssen diese Attribute im Voraus kennen und sie den Zugriffskontrollregeln hinzufügen, wenn Sie Richtlinien erstellen. Wenn Sie sich dafür

entscheiden, Ihren externen IdPs Attributen zu vertrauen, werden diese Attribute immer weitergegeben, wenn Benutzer sich AWS-Konten zusammenschließen. Informationen zur Konfiguration von Benutzerattributen für die Zugriffskontrolle in Ihrem IdP zum Senden über SAML-Assertionen finden Sie unter für Ihren IdP. [Tutorials zu Identitätsquellen im IAM Identity Center](#)

Eine vollständige Liste der unterstützten Attribute für Benutzerattribute in IAM Identity Center für die Benutzerattribute in Ihrem externen System finden Sie unter. IdPs [Unterstützte externe Identitätsanbieter-Attribute](#)

Informationen zu den ersten Schritten mit ABAC in IAM Identity Center finden Sie in den folgenden Themen.

Themen

- [Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle](#)
- [Erstellen Sie Berechtigungsrichtlinien für ABAC im IAM Identity Center](#)

Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle

Um die attributbasierte Zugriffskontrolle (ABAC) zu verwenden, müssen Sie sie zunächst entweder auf der Seite „Einstellungen“ der IAM Identity Center-Konsole oder in der IAM Identity Center-API aktivieren. https://docs.aws.amazon.com/singlesignon/latest/APIReference/API_CreateInstanceAccessControlAttributeConfiguration.html Unabhängig von der Identitätsquelle können Sie Benutzerattribute aus dem Identity Store jederzeit für die Verwendung in ABAC konfigurieren. In der Konsole können Sie dies tun, indem Sie auf der Seite „Einstellungen“ zur Registerkarte „Attribute für die Zugriffskontrolle“ navigieren. Wenn Sie einen externen Identitätsanbieter (IdP) als Identitätsquelle verwenden, haben Sie auch die Möglichkeit, Attribute vom externen IdP in SAML-Assertionen zu erhalten. In diesem Fall müssen Sie den externen IdP so konfigurieren, dass er die gewünschten Attribute sendet. Wenn ein Attribut aus einer SAML-Assertion in IAM Identity Center auch als ABAC-Attribut definiert ist, sendet IAM Identity Center den Wert aus seinem Identity Store als [Sitzungs-Tag bei der Anmeldung an ein](#). AWS-Konto

Note

Sie können die von einem externen IdP konfigurierten und gesendeten Attribute nicht auf der Seite „Attribute für die Zugriffskontrolle“ in der IAM Identity Center-Konsole anzeigen. Wenn

Sie Zugriffskontrollattribute in den SAML-Assertionen von Ihrem externen IdP übergeben, werden diese Attribute direkt an den AWS-Konto gesendet, wenn Benutzer sich verbinden. Die Attribute werden im IAM Identity Center nicht für die Zuordnung verfügbar sein.

Themen

- [Aktivieren Sie Attribute für die Zugriffskontrolle](#)
- [Wählen Sie Ihre Attribute für die Zugriffskontrolle](#)
- [Attribute für die Zugriffskontrolle deaktivieren](#)

Aktivieren Sie Attribute für die Zugriffskontrolle

Gehen Sie wie folgt vor, um die ABAC-Kontrollfunktion (Attributes for Access) mithilfe der IAM Identity Center-Konsole zu aktivieren.

Note

Wenn Sie bereits über Berechtigungssätze verfügen und ABAC in Ihrer IAM Identity Center-Instanz aktivieren möchten, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen zunächst über die Richtlinie verfügen. `iam:UpdateAssumeRolePolicy` Diese zusätzlichen Sicherheitseinschränkungen sind nicht erforderlich, wenn in Ihrem Konto keine Berechtigungssätze erstellt wurden.

Wenn Ihre IAM Identity Center-Instanz vor Dezember 2020 erstellt wurde und Sie beabsichtigen, ABAC darin zu aktivieren, müssen Sie die `iam:UpdateAssumeRolePolicy` Richtlinie haben, die der IAM Identity Center-Administratorrolle zugeordnet ist, unabhängig davon, ob Sie in Ihrem Konto Berechtigungssätze erstellt haben.

Um Attribute für die Zugriffskontrolle zu aktivieren

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie „Einstellungen“
3. Suchen Sie auf der Seite „Einstellungen“ das Feld „Attribute für die Zugriffskontrolle“ und wählen Sie dann „Aktivieren“. Fahren Sie mit dem nächsten Verfahren fort, um es zu konfigurieren.

Wählen Sie Ihre Attribute für die Zugriffskontrolle

Gehen Sie wie folgt vor, um Attribute für Ihre ABAC-Konfiguration einzurichten.

Note

Dieses Verfahren gilt nur, wenn Sie Attribute aus Ihrem IAM Identity Center-Verzeichnis zur Verwendung als Sitzungs-Tags zuordnen möchten. Wenn Sie Attribute von einem externen Identitätsanbieter (IdP) über SAML-Assertionen übergeben, müssen Sie hier keine Attributzuordnungen konfigurieren. Weitere Informationen finden Sie unter [Auswahl von Attributen, wenn Sie einen externen Identitätsanbieter als Identitätsquelle verwenden](#). Werte, die in der Zuordnung aus dem Identity Center-Verzeichnis festgelegt wurden, überschreiben Werte, die in SAML-Assertionen festgelegt sind.

Um Ihre Attribute mithilfe der IAM Identity Center-Konsole auszuwählen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie „Einstellungen“
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Attribute für die Zugriffskontrolle“ und dann „Attribute verwalten“.
4. Wählen Sie auf der Seite „Attribute für die Zugriffskontrolle“ die Option „Attribut hinzufügen“ aus und geben Sie die Schlüssel - und Wertdetails ein. Hier ordnen Sie das Attribut, das aus Ihrer Identitätsquelle stammt, einem Attribut zu, das IAM Identity Center als Sitzungs-Tag übergibt.

Key ⓘ	Value (optional) ⓘ	Remove
<input type="text" value="Department"/>	<input type="text" value="\${path:enterprise.department}"/>	✕
<input type="text" value="CostCenter"/>	<input type="text" value="\${path:enterprise.costCenter}"/>	✕
<input type="text" value="Add new key"/>	<input type="text" value="Add new value"/>	

Key steht für den Namen, den Sie dem Attribut zur Verwendung in Richtlinien geben. Dies kann ein beliebiger Name sein, aber Sie müssen diesen genauen Namen in den Richtlinien angeben, die Sie für die Zugriffskontrolle erstellen. Nehmen wir zum Beispiel an, Sie verwenden Okta (einen externen IdP) als Identitätsquelle und müssen die Kostenstellendaten Ihrer Organisation als Sitzungs-Tags weitergeben. Im Feld Schlüssel würden Sie einen ähnlich passenden Namen CostCenter wie Ihren Schlüsselnamen eingeben. Es ist wichtig zu beachten, dass der Name, den Sie hier wählen, auch in Ihrem [AWS: PrincipalTag Bedingungsschlüssel](#) (d.

h."ec2:ResourceTag/CostCenter": "\${aws:PrincipalTag/CostCenter}") exakt gleich benannt sein muss.

 Note

Verwenden Sie ein Einzelwertattribut für Ihren Schlüssel, z. B. **Manager** IAM Identity Center unterstützt beispielsweise keine Attribute mit mehreren Werten für ABAC.

Manager, IT Systems

Value steht für den Inhalt des Attributs, das aus Ihrer konfigurierten Identitätsquelle stammt. Hier können Sie einen beliebigen Wert aus der entsprechenden Identitätsquellentabelle eingeben, die unter aufgeführt ist [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#). Unter Verwendung des Kontextes aus dem oben genannten Beispiel würden Sie beispielsweise die Liste der unterstützten IdP-Attribute überprüfen und feststellen, dass einem unterstützten Attribut am nächsten kommt, **\${path:enterprise.costCenter}** und Sie würden es dann in das Feld Wert eingeben. Sehen Sie sich den obigen Screenshot als Referenz an. Beachten Sie, dass Sie keine externen IdP-Attributwerte außerhalb dieser Liste für ABAC verwenden können, es sei denn, Sie verwenden die Option, Attribute über die SAML-Assertion zu übergeben.

5. Wählen Sie **Änderungen speichern** aus.

Nachdem Sie die Zuordnung Ihrer Zugriffskontrollattribute konfiguriert haben, müssen Sie den ABAC-Konfigurationsprozess abschließen. Erstellen Sie dazu Ihre ABAC-Regeln und fügen Sie sie Ihren and/or ressourcenbasierten Richtlinien für Berechtigungssätze hinzu. Dies ist erforderlich, damit Sie Benutzeridentitäten Zugriff auf Ressourcen gewähren können. AWS Weitere Informationen finden Sie unter [Erstellen Sie Berechtigungsrichtlinien für ABAC im IAM Identity Center](#).

Attribute für die Zugriffskontrolle deaktivieren

Gehen Sie wie folgt vor, um die ABAC-Funktion zu deaktivieren und alle konfigurierten Attributzuordnungen zu löschen.

Um Attribute für die Zugriffskontrolle zu deaktivieren

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie **Einstellungen** aus.

3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Attribute für die Zugriffskontrolle“ und dann „Attribute verwalten“.
4. Wählen Sie auf der Seite Attribute für die Zugriffskontrolle verwalten die Option Deaktivieren aus.
5. Überprüfen Sie im Dialogfeld „Attribute für die Zugriffskontrolle deaktivieren“ die Informationen, geben Sie die Informationen ein, wenn Sie bereit sind **DISABLE**, und wählen Sie dann Bestätigen.

 Important

Bei diesem Schritt werden alle Attribute gelöscht und die Verwendung von Attributen für die Zugriffskontrolle bei einem Verbund eingestellt, AWS-Konten unabhängig davon, ob SAML-Assertionen von einem externen Identitätsquellenanbieter Attribute enthalten.

Erstellen Sie Berechtigungsrichtlinien für ABAC im IAM Identity Center

Sie können Berechtigungsrichtlinien erstellen, die anhand des konfigurierten Attributwerts festlegen, wer auf Ihre AWS Ressourcen zugreifen kann. Wenn Sie ABAC aktivieren und Attribute angeben, übergibt IAM Identity Center den Attributwert des authentifizierten Benutzers zur Verwendung bei der Richtlinienbewertung an IAM.

AWS: PrincipalTag Bedingungsschlüssel

Sie können Zugriffskontrollattribute in Ihren Berechtigungssätzen (oder IAM-Rollen, wenn Sie den Account Access Manager verwenden) verwenden, indem Sie den `aws:PrincipalTag` Bedingungsschlüssel zum Erstellen von Zugriffsregeln verwenden. In der folgenden Richtlinie können Sie beispielsweise alle Ressourcen in Ihrer Organisation mit ihren jeweiligen Kostenstellen kennzeichnen. Sie können auch einen einzigen Berechtigungssatz (oder eine IAM-Rolle, wenn Sie den Account Access Manager verwenden) verwenden, der Entwicklern Zugriff auf ihre Kostenstellenressourcen gewährt. Wenn Entwickler jetzt mithilfe von Single Sign-On und ihrem Kostenstellenattribut eine Verbindung zum Konto herstellen, erhalten sie nur Zugriff auf die Ressourcen in ihren jeweiligen Kostenstellen. Wenn das Team seinem Projekt weitere Entwickler und Ressourcen hinzufügt, müssen Sie die Ressourcen nur mit der richtigen Kostenstelle kennzeichnen. Dann geben Sie in der AWS Sitzung, in der sich die Entwickler zusammenschließen, Informationen zur Kostenstelle weiter. AWS-Konten Wenn das Unternehmen der Kostenstelle also neue Ressourcen und Entwickler hinzufügt, können Entwickler Ressourcen entsprechend ihrer Kostenstellen verwalten, ohne dass die Berechtigungen aktualisiert werden müssen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/
CostCenter}"
        }
      }
    }
  ]
}
```

Wenn Benutzer AWS-Konto über IAM Identity Center eine Verbindung zu einem Netzwerk herstellen, werden die konfigurierten Zugriffskontrollattribute als Sitzungs-Tags übergeben. Sie können in Ihren Richtlinien mithilfe des `aws:PrincipalTag/tag-key` Bedingungsschlüssels auf diese Sitzungs-Tags verweisen. Dieser Bedingungsschlüssel wird in allen relevanten AWS IAM-Richtlinientypen unterstützt, für die Sie Bedingungen verwenden können, einschließlich identitätsbasierter Richtlinien, ressourcenbasierter Richtlinien, Berechtigungsgrenzen, Service Control Policies (SCPs) und VPC-Endpunktrichtlinien. Auf diese Weise können Sie auf der Grundlage von Benutzerattributen in Ihrer gesamten Umgebung detaillierte Entscheidungen zur Zugriffskontrolle treffen. AWS

Weitere Informationen finden Sie unter [aws:PrincipalTag](#) und [EC2: Starten oder Stoppen von Instances auf der Grundlage übereinstimmender Principal- und Resource-Tags](#) im IAM-Benutzerhandbuch.

Wenn Richtlinien in ihren Bedingungen ungültige Attribute enthalten, schlägt die Richtlinienbedingung fehl und der Zugriff wird verweigert. Weitere Informationen finden Sie unter [Fehler „Ein unerwarteter Fehler ist aufgetreten“, wenn ein Benutzer versucht, sich mit einem externen Identitätsanbieter anzumelden](#).

Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center

[Service-linked Rollen](#) sind vordefinierte IAM-Berechtigungen, die es IAM Identity Center ermöglichen, zu delegieren und durchzusetzen, welche Benutzer Single-Sign-On-Zugriff auf bestimmte Benutzer AWS-Konten in Ihrer Organisation haben. AWS Organizations Der Service ermöglicht diese Funktionalität, indem er jedem innerhalb der Organisation eine dienstbezogene Rolle zuweist. AWS-Konto Der Service ermöglicht es dann anderen AWS Diensten wie IAM Identity Center, diese Rollen zu nutzen, um dienstbezogene Aufgaben auszuführen. Weitere Informationen finden Sie unter [AWS Organizations Und serviceverknüpfte Rollen](#).

Wenn Sie IAM Identity Center aktivieren, erstellt IAM Identity Center eine serviceverknüpfte Rolle in allen Konten innerhalb der Organisation in. AWS Organizations IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen. Weitere Informationen finden Sie unter [Konfigurieren Sie den Zugriff auf AWS-Konten](#).

Service-linked Die Rollen, die in den einzelnen Rollen erstellt werden, AWS-Konto sind benannt `AWSServiceRoleForSSO`. Weitere Informationen finden Sie unter [Verwenden von dienstverknüpften Rollen für IAM Identity Center](#).

Hinweise

- Wenn Sie beim AWS Organizations Verwaltungskonto angemeldet sind, verwendet es Ihre aktuell angemeldete Rolle und nicht die dienstverknüpfte Rolle. Dies verhindert die Eskalation von Rechten.
- Wenn IAM Identity Center IAM-Vorgänge im AWS Organizations Verwaltungskonto ausführt, werden für alle Vorgänge die Anmeldeinformationen des IAM-Prinzips

verwendet. Auf diese Weise können die Anmeldungen CloudTrail Aufschluss darüber geben, wer alle Rechteänderungen im Verwaltungskonto vorgenommen hat.

Einrichtung und Verwendung des AWS auf das Portal zugreifen

Das AWS Zugangsportal verbindet Ihre Mitarbeiter über IAM Identity Center mit Cloud-Anwendungen. AWS-Konten Administratoren konfigurieren das Portal und verwalten den Benutzerzugriff, während sich Endbenutzer einmal anmelden, um nahtlos auf alle ihre autorisierten Ressourcen zuzugreifen.

Das AWS Zugangsportal bietet Single-Sign-On-Zugriff auf:

- AWS-Konten in Ihrer Organisation.
- AWS verwaltete Anwendungen wie Amazon Quick und Kiro.
- Cloud-Anwendungen wie Office 365, Concur, Salesforce und andere.

Wenn Benutzer sich im Portal anmelden, finden sie die AWS-Konten Anwendungen, auf die sie ohne zusätzliche Anmeldung zugreifen dürfen.

Das AWS Zugriffsportal bietet auch Zugriff auf die AWS Kontozugriffsanwendung, in der Benutzer die ihnen zugewiesenen IAM-Rollen über den [Account Access Manager einsehen und darauf zugreifen können](#).

Erste Schritte mit dem AWS auf das Portal zugreifen

Für Administratoren:

Sie benötigen Administratorzugriff auf Ihre [Organisations](#) - oder [Kontoinstanz](#) von IAM Identity Center, um das AWS Zugriffsportal zu konfigurieren und den Benutzerzugriff zu verwalten.

1. Passen Sie optional die URL des AWS Zugriffsportals an.
2. Weisen Sie Benutzerzugriff auf AWS-Konten und Anwendungen zu. Zugewiesene AWS Ressourcen werden im Portal angezeigt.

Für Endbenutzer:

Ihr Administrator muss die Einrichtung des AWS Access Portals abgeschlossen und Ihnen Ihre Portal-URL und Anmeldeinformationen zur Verfügung gestellt haben.

1. Ihre Portal-URL erhalten Sie (in der Regel `https://your-company.awsapps.com/start`) von Ihrem Administrator.
2. Melden Sie sich mit den Anmeldeinformationen an, die Sie von Ihrem Administrator erhalten haben.
3. Greifen Sie in Ihrem Portal auf Ihre Ressourcen zu.

Konfigurieren Sie das AWS auf das Portal zugreifen

Als Administrator können Sie das AWS Zugangsportale an die Anforderungen Ihres Unternehmens anpassen und sicherstellen, dass Benutzer problemlos auf ihre autorisierten Ressourcen zugreifen können.

Was können Sie konfigurieren

AWS Aktivierung des Zugriffsportals: Richten Sie den ersten Benutzerzugriff auf das AWS Access Portal ein, einschließlich der Aktivierung der Benutzeranmeldeinformationen und der Erstanmeldung.

Benutzerdefinierte AWS Zugriffsportale-URL (optional): Personalisieren Sie die AWS Zugriffsportale-URL Ihrer Organisation vom Standardformat (`d-xxxxxxxxxx.awsapps.com/start`) zu einer besser erkennbaren Subdomain (`your-company.awsapps.com/start`).

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Administratorzugriff auf IAM Identity Center haben, stellen Sie sicher, dass IAM Identity Center entweder als [Organisations](#) - oder [Kontoinstanz eingerichtet ist](#), und planen Sie Ihren benutzerdefinierten Subdomainnamen (dies ist eine einmalige Konfiguration, die später nicht geändert werden kann).

Nach der Konfiguration können Benutzer über die benutzerdefinierte URL AWS auf das Zugriffsportale zugreifen und den Aktivierungsprozess verfolgen, den Sie für Ihre Organisation eingerichtet haben.

Themen

- [Aktivierung der AWS Zugriffsportale für Erstbenutzer von IAM Identity Center](#)
- [Anpassen der AWS auf die URL des Portals zugreifen](#)
- [Bestätigen Sie, dass sich Benutzer bei der anmelden können AWS auf das Portal zugreifen](#)

Aktivierung der AWS Zugriffsportal für Erstbenutzer von IAM Identity Center

Wenn Sie zum ersten Mal versuchen, sich beim AWS Access Portal anzumelden, finden Sie in Ihrer E-Mail Anweisungen zur Aktivierung Ihrer Benutzeranmeldeinformationen.

Um Ihre Benutzeranmeldeinformationen zu aktivieren

1. Wählen Sie je nach der E-Mail, die Sie von Ihrem Unternehmen erhalten haben, eine der folgenden Methoden, um Ihre Benutzeranmeldeinformationen zu aktivieren, damit Sie das AWS Zugangsportal verwenden können.
 - a. Wenn Sie eine E-Mail mit dem Betreff `Einladung zur Teilnahme an AWS IAM Identity Center` erhalten haben, öffnen Sie sie und wählen Sie `Einladung annehmen`. Geben Sie auf der Anmeldeseite für neue Benutzer ein Passwort ein, bestätigen Sie es und wählen Sie dann `Neues Passwort festlegen` aus. Sie verwenden dieses Passwort jedes Mal, wenn Sie sich im Portal anmelden.
 - b. Wenn Sie eine E-Mail vom IT-Support oder IT-Administrator Ihres Unternehmens erhalten haben, folgen Sie den dort bereitgestellten Anweisungen, um Ihre Benutzeranmeldeinformationen zu aktivieren.
2. Nachdem Sie Ihre Benutzeranmeldeinformationen durch Eingabe eines neuen Passworts aktiviert haben, meldet Sie das AWS Zugangsportal automatisch an. Wenn dies nicht der Fall ist, können Sie sich mithilfe der Anweisungen unter [manuell beim AWS Access Portal anmelden](#) [Melden Sie sich bei der an AWS auf das Portal zugreifen](#).

Anpassen der AWS auf die URL des Portals zugreifen

Standardmäßig können Sie auf das Access-Portal AWS zugreifen, indem Sie eine URL verwenden, die diesem Format folgt: `d-xxxxxxxxxx.awsapps.com/start`. Sie können die URL wie folgt anpassen: `your_subdomain.awsapps.com/start`.

Important

Wenn Sie die URL des AWS Access-Portals ändern, können Sie sie später nicht mehr bearbeiten.

Um Ihre URL anzupassen

1. Öffnen Sie die AWS IAM Identity Center Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie in der IAM Identity Center-Konsole im Navigationsbereich Dashboard aus und suchen Sie den Abschnitt mit der Zusammenfassung der Einstellungen.
3. Klicken Sie unter Ihrer AWS Access-Portal-URL auf die Schaltfläche „Anpassen“.

Note

Wenn die Schaltfläche „Anpassen“ nicht angezeigt wird, bedeutet dies, dass das AWS Zugangsportal bereits angepasst wurde. Das Anpassen der URL des AWS Zugangsportals ist ein einmaliger Vorgang, der nicht rückgängig gemacht werden kann.

4. Geben Sie den gewünschten Subdomainnamen ein und wählen Sie Speichern.

Sie können sich jetzt über Ihr AWS Zugangsportal mit Ihrer benutzerdefinierten URL bei der AWS Konsole anmelden.

Bestätigen Sie, dass sich Benutzer bei der anmelden können AWS auf das Portal zugreifen

Mit den folgenden Schritten muss der IAM Identity Center-Administrator bestätigen, dass sich der IAM Identity Center-Benutzer beim AWS Zugriffportal anmelden und auf das zugreifen kann. AWS-Konto

Melden Sie sich bei der AWS auf das Portal zugreifen

1. Führen Sie einen der folgenden Schritte aus, um sich bei der anzumelden AWS-Managementkonsole.
 - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
 - Bereits verwendet AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen an und wählen Sie eine Administratorrolle aus.
2. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
3. Wählen Sie im Navigationsbereich Dashboard (Dashboard).

4. Wählen Sie auf der Dashboard-Seite unter Zusammenfassung der Einstellungen die URL für das AWS Zugriffsportal aus.
5. Melden Sie sich mit einer der folgenden Methoden an:
 - Wenn Sie Active Directory oder einen externen Identitätsanbieter (IdP) als Identitätsquelle verwenden, melden Sie sich mit den Anmeldeinformationen des Active Directory- oder IdP-Benutzers an.
 - Wenn Sie das standardmäßige Identity Center-Verzeichnis als Identitätsquelle verwenden, melden Sie sich mit dem Benutzernamen an, den Sie bei der Erstellung des Benutzers angegeben haben, und dem neuen Passwort, das Sie für den Benutzer angegeben haben.
6. Suchen Sie auf der Registerkarte Konten nach Ihrem AWS-Konto und erweitern Sie es.
7. Die Rollen, die Ihnen zur Verfügung stehen, werden angezeigt. Wenn Ihnen beispielsweise sowohl der AdministratorAccess Berechtigungssatz als auch die Abrechnungsberechtigungssätze zugewiesen sind, werden diese Rollen im AWS Zugriffsportal angezeigt. Wählen Sie den IAM-Rollennamen, den Sie für die Sitzung verwenden möchten.
8. Wenn Sie zur AWS Managementkonsole weitergeleitet werden, haben Sie die Einrichtung des Zugriffs auf die AWS-Konto erfolgreich abgeschlossen.

 Note

Wenn Sie keine Rechte in der AWS-Konten Liste sehen, wurde dem Benutzer wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Anweisungen zum Zuweisen von Benutzern zu einem Berechtigungssatz finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).

Nachdem Sie nun bestätigt haben, dass Sie sich mit den IAM Identity Center-Anmeldeinformationen anmelden können, wechseln Sie zu dem Browser, mit dem Sie sich mit Ihrem Root-Benutzer oder Ihren IAM-Benutzeranmeldedaten an- AWS-Managementkonsole und abmelden.

 Important

Wir empfehlen dringend, die Anmeldeinformationen des IAM Identity Center-Administrators zu verwenden, wenn Sie sich beim AWS Access-Portal anmelden, um Verwaltungsaufgaben auszuführen, anstatt die Anmeldeinformationen des IAM-Benutzers oder des Root-Benutzers zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Um

anderen Benutzern den Zugriff auf Ihre Konten und Anwendungen zu ermöglichen und IAM Identity Center zu verwalten, erstellen und weisen Sie Berechtigungssätze nur über IAM Identity Center zu.

Verwenden Sie das AWS auf das Portal zugreifen

Sie können mehrere Anwendungen starten, indem Sie im Portal die Registerkarte AWS-Konto oder Anwendung auswählen. Das Vorhandensein von Anwendungssymbolen in Ihrem AWS Zugangsportal bedeutet, dass Ihnen ein Administrator Ihres Unternehmens Zugriff auf diese AWS-Konten oder Anwendungen gewährt hat. Es bedeutet auch, dass Sie vom Access Portal aus auf all diese Konten oder Anwendungen AWS zugreifen können, ohne dass Sie sich erneut anmelden müssen.

Wie benutzt man den AWS auf das Portal zugreifen

So verwenden Sie das AWS Zugangsportal:

1. Holen Sie sich Ihre Portal-URL von Ihrem Administrator (sieht normalerweise so aus `https://your-company.awsapps.com/start`).
2. Melden Sie sich mit den Anmeldeinformationen an, die Sie von Ihrem Administrator erhalten haben.
3. Wählen Sie die Konten und Anwendungen in Ihrem Portal aus, auf die Sie zugreifen möchten.

Ihr Administrator steuert, was Sie im Portal sehen, basierend auf Ihrer Rolle und Ihren Berechtigungen. Wenden Sie sich in den folgenden Situationen an Ihren Administrator, um zusätzlichen Zugriff anzufordern:

- Sie sehen keine AWS-Konto OR-Anwendung, auf die Sie zugreifen müssen.
- Der Zugriff, den Sie auf ein bestimmtes Konto oder eine bestimmte Anwendung haben, entspricht nicht Ihren Erwartungen.

Themen

- [Melden Sie sich bei der an AWS auf das Portal zugreifen](#)
- [Zurücksetzen Ihres AWS Passwort für den Zugriff auf das Portal](#)

- [Abrufen der IAM Identity Center-Benutzeranmeldedaten für AWS CLI oder AWS SDKs](#)
- [Erstellen von Verknüpfungen zu AWS-Managementkonsole Destinationen](#)
- [Registrieren Sie Ihr Gerät für MFA](#)
- [Ihre aktive Sitzung anzeigen und beenden](#)

Melden Sie sich bei der an AWS auf das Portal zugreifen

Das AWS Zugriffsportal bietet IAM Identity Center-Benutzern über ein Webportal Single-Sign-On-Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen. Im Folgenden wird beschrieben, wie Sie sich beim AWS Access-Portal anmelden können, sowie Tipps zur Anmeldung und zum Abmelden vom AWS Access-Portal.

Voraussetzungen

IAM Identity Center muss aktiviert sein, um das AWS Zugriffsportal verwenden zu können. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).

Note

Nach der Anmeldung beträgt die Standarddauer für Ihre AWS Access Portal-Sitzung 8 Stunden. Beachten Sie, dass ein Administrator die Dauer [dieser Sitzung](#) ändern kann.

Loggen Sie sich ein bei AWS auf das Portal zugreifen

Um sich beim anzumelden AWS auf das Portal zugreifen

1. Fügen Sie in Ihrem Browserfenster die Anmelde-URL ein, die Sie erhalten haben, und wählen Sie Enter. Die URL sieht aus wie `d-xxxxxxxxxx.awsapps.com/start` oder `your_subdomain.awsapps.com/start`. Wir empfehlen, diesen Link zum Portal jetzt als Lesezeichen zu setzen, sodass Sie später schnell darauf zugreifen können.
2. Melden Sie sich mit Ihren Standard-Unternehmensanmeldedaten an.

Note

Wenn Ihr Administrator Ihnen per E-Mail ein Einmalpasswort (OTP) geschickt hat und Sie sich zum ersten Mal anmelden, geben Sie dieses Passwort ein. Nachdem Sie

sich angemeldet haben, müssen Sie ein neues Passwort für zukünftige Anmeldungen erstellen.

Wenn Sie zur Eingabe eines Bestätigungscode aufgefordert werden, überprüfen Sie Ihre E-Mail, kopieren Sie den Code und fügen Sie ihn in die Anmeldeseite ein.

 Note

Bestätigungscode werden normalerweise per E-Mail gesendet, aber die Zustellungsmethode kann variieren. Weitere Einzelheiten erhalten Sie von Ihrem Administrator.

3. Sobald Sie angemeldet sind, können Sie auf jede AWS-Konto Anwendung zugreifen, die im Portal angezeigt wird.

Vertrauenswürdige Geräte

Wenn Sie auf der Anmeldeseite die Option **Dies ist ein vertrauenswürdige Gerät** auswählen, betrachtet IAM Identity Center alle zukünftigen Anmeldungen von diesem Gerät aus als autorisiert. Das bedeutet, dass IAM Identity Center keine Option zur Eingabe eines MFA-Codes anbietet, solange Sie dieses vertrauenswürdige Gerät verwenden. Es gibt jedoch einige Ausnahmen, z. B. wenn Sie sich über einen neuen Browser anmelden oder wenn Ihrem Gerät eine unbekannte IP-Adresse zugewiesen wurde.

Tipps zur Anmeldung für AWS auf das Portal zugreifen

Im Folgenden finden Sie einige Tipps, die Ihnen bei der Verwaltung Ihres AWS Access Portal-Erlebnisses helfen sollen.

- Gelegentlich müssen Sie sich möglicherweise vom AWS Access Portal abmelden und erneut anmelden. Dies kann eventuell notwendig sein, um auf neue Anwendungen zuzugreifen, die Ihnen vom Administrator erst kürzlich zugewiesen wurden. Es ist jedoch nicht zwingend erforderlich, da alle neuen Anwendungen stündlich aktualisiert werden.
- Wenn Sie sich beim AWS Access Portal anmelden, können Sie jede der im Portal aufgelisteten Anwendungen öffnen, indem Sie auf das Symbol der Anwendung klicken. Wenn Sie die Anwendung nicht mehr verwenden, können Sie die Anwendung entweder schließen oder sich vom AWS Zugangsportal abmelden. Durch das Schließen der Anwendung werden Sie nur von

dieser Anwendung abgemeldet. Alle anderen Anwendungen, die Sie über das AWS Access Portal geöffnet haben, bleiben geöffnet und werden ausgeführt.

- Bevor Sie sich als anderer Benutzer anmelden können, müssen Sie sich zuerst vom AWS Access Portal abmelden. Durch das Abmelden vom Portal werden Ihre Anmeldeinformationen vollständig aus der Browsersitzung entfernt.
- Sobald Sie sich beim AWS Access Portal angemeldet haben, können Sie zu einer Rolle wechseln. Wenn Sie die Rollen wechseln, werden Ihre ursprünglichen Benutzerberechtigungen vorübergehend aufgehoben und Sie erhalten stattdessen die der Rolle zugewiesenen Berechtigungen. Weitere Informationen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#).

Abmelden von AWS auf das Portal zugreifen

Wenn Sie sich vom Portal abmelden, werden Ihre Anmeldeinformationen vollständig aus der Browsersitzung entfernt. Weitere Informationen finden Sie [im AWS-Anmeldung Handbuch unter Vom AWS Zugangsportal](#) abmelden.

Um sich vom abzumelden AWS auf das Portal zugreifen

- Wählen Sie im AWS Access-Portal in der Navigationsleiste **Abmelden** aus.

Note

Wenn Sie sich als ein anderer Benutzer anmelden möchten, müssen Sie sich zuerst vom AWS Access Portal abmelden.

Zurücksetzen Ihres AWS Passwort für den Zugriff auf das Portal

Das AWS Zugangsportal bietet [IAM Identity](#) Center-Benutzern über ein Webportal Single-Sign-On-Zugriff auf alle ihnen zugewiesenen AWS Konten und Cloud-Anwendungen. Das AWS Zugriffportal unterscheidet sich von dem [AWS-Managementkonsole](#), bei dem es sich um eine Sammlung von Servicekonsolen zur Verwaltung AWS von Ressourcen handelt.

Gehen Sie wie folgt vor, um Ihr IAM Identity Center-Benutzerkennwort für das AWS Access Portal zurückzusetzen. Weitere Informationen zu [Benutzertypen finden Sie](#) im AWS-Anmeldung Benutzerhandbuch.

Überlegungen

Die Funktion zum Zurücksetzen Ihres Passworts für Ihr AWS Zugangsportal ist nur für Benutzer von Identity Center-Instanzen verfügbar, die das Identity Center-Verzeichnis oder [AWS Managed Microsoft AD](#) als Identitätsquelle verwenden. Wenn Ihr Benutzer mit einem externen Identitätsanbieter oder [AD Connector verbunden ist](#), muss das Zurücksetzen des Benutzerkennworts über den externen Identitätsanbieter oder über eine Verbindung Active Directory erfolgen.

- Wenn es sich bei Ihrer Identitätsquelle um ein IAM Identity Center-Verzeichnis handelt, finden Sie weitere Informationen unter [Kennwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center](#)
- Wenn es sich bei Ihrer Identitätsquelle um eine handelt AWS Managed Microsoft AD, finden Sie weitere Informationen unter [Kennwortanforderungen beim Zurücksetzen eines Kennworts in. AWS Managed Microsoft AD](#)

Um dein Passwort zurückzusetzen auf AWS auf das Portal zugreifen

1. Öffnen Sie einen Webbrowser und rufen Sie die Anmeldeseite für Ihr AWS Zugangsportal auf.

Wenn Sie Ihre AWS Zugriffsportal-URL nicht haben, überprüfen Sie Ihre E-Mails. Sie sollten per E-Mail eine Einladung zum Beitritt zum AWS IAM Identity Center erhalten haben, die eine bestimmte Anmelde-URL für das AWS Zugangsportal enthält. Alternativ hat Ihnen Ihr Administrator möglicherweise direkt ein Einmalkennwort und die URL des AWS Zugriffsportals zur Verfügung gestellt. Wenn Sie diese Informationen nicht finden können, bitten Sie Ihren Administrator, sie Ihnen zu senden.

Weitere Informationen zur Anmeldung beim AWS Access Portal finden [Sie im AWS-Anmeldung Benutzerhandbuch unter Beim AWS Access Portal](#) anmelden.

2. Geben Sie Ihren Benutzernamen ein und wählen Sie dann Weiter.
3. Wählen Sie unter Passwort die Option Passwort vergessen aus.

Bestätigen Sie Ihren Benutzernamen und geben Sie die Zeichen für das bereitgestellte Bild ein, um zu bestätigen, dass Sie kein Roboter sind. Klicken Sie anschließend auf Weiter. Möglicherweise müssen Sie die Werbeblocker-Software deaktivieren, wenn Sie keine Zeichen eingeben können.

4. Eine Meldung wird angezeigt, um zu bestätigen, dass eine E-Mail zum Zurücksetzen des Passworts gesendet wurde. Klicken Sie auf Weiter.
5. Sie erhalten eine E-Mail von `no-reply@signin.aws` mit dem Betreff Passwort zum Zurücksetzen des Passworts. Wählen Sie in Ihrer E-Mail die Option Passwort zurücksetzen.

6. Überprüfen Sie auf der Seite „Passwort zurücksetzen“ Ihren Benutzernamen, geben Sie ein neues Passwort für das AWS Zugangsportal an und wählen Sie dann Neues Passwort festlegen aus.
7. Sie erhalten eine E-Mail von `no-reply@signin.aws` mit dem Betreff Passwort aktualisiert.

Note

Ein Administrator kann Ihr Passwort zurücksetzen, indem er Ihnen entweder eine E-Mail mit Anweisungen zum Zurücksetzen Ihres Passworts sendet oder ein Einmalpasswort generiert und es Ihnen mitteilt. Wenn Sie Administrator sind, finden Sie weitere Informationen unter [Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück.](#)

Abrufen der IAM Identity Center-Benutzeranmeldedaten für AWS CLI oder AWS SDKs

Sie können programmgesteuert auf AWS Dienste zugreifen, indem Sie die AWS Command Line Interface oder die AWS Software Development Kits (SDKs) mit Benutzeranmeldeinformationen aus IAM Identity Center verwenden. In diesem Thema wird beschrieben, wie Sie temporäre Anmeldeinformationen für einen Benutzer in IAM Identity Center abrufen.

Das AWS Zugriffsportal bietet IAM Identity Center-Benutzern Single-Sign-On-Zugriff auf ihre AWS-Konten und Cloud-Anwendungen. Nachdem Sie sich als IAM Identity Center-Benutzer beim AWS Zugriffsportal angemeldet haben, können Sie temporäre Anmeldeinformationen abrufen. Anschließend können Sie die Anmeldeinformationen, die auch als IAM Identity Center-Benutzeranmeldeinformationen bezeichnet werden, in den AWS CLI oder AWS SDKs verwenden, um auf Ressourcen in einem zuzugreifen. AWS-Konto

Wenn Sie den verwenden AWS CLI , um programmgesteuert auf AWS Dienste zuzugreifen, können Sie die Verfahren in diesem Thema verwenden, um den Zugriff auf die zu initiieren. AWS CLI Informationen zu dem finden AWS CLI Sie im [AWS Command Line Interface Benutzerhandbuch.](#)

Wenn Sie die AWS SDKs verwenden, um programmgesteuert auf AWS Dienste zuzugreifen, wird durch Befolgen der Verfahren in diesem Thema auch direkt die Authentifizierung für die SDKs eingerichtet. AWS Informationen zu den SDKs finden Sie im AWS Referenzhandbuch für [AWS SDKs und Tools.](#)

 Note

Benutzer in IAM Identity Center unterscheiden sich von IAM-Benutzern. https://docs.aws.amazon.com/cli/latest/userguide/id_users.html IAM-Benutzern werden langfristige Anmeldeinformationen für Ressourcen gewährt. AWS Benutzern im IAM Identity Center werden temporäre Anmeldeinformationen gewährt. Wir empfehlen, temporäre Anmeldeinformationen als bewährte Sicherheitsmethode für den Zugriff auf Ihre zu verwenden AWS-Konten , da diese Anmeldeinformationen bei jeder Anmeldung generiert werden.

Voraussetzungen

Um temporäre Anmeldeinformationen für Ihren IAM Identity Center-Benutzer zu erhalten, benötigen Sie Folgendes:

- Ein IAM Identity Center-Benutzer — Sie melden sich als dieser Benutzer beim AWS Access-Portal an. Sie oder Ihr Administrator können diesen Benutzer erstellen. Informationen zum Aktivieren von IAM Identity Center und zum Erstellen eines IAM Identity Center-Benutzers finden Sie unter [Erste Schritte mit IAM Identity Center](#)
- Benutzerzugriff auf ein AWS-Konto — Um einem IAM Identity Center-Benutzer die Berechtigung zum Abrufen seiner temporären Anmeldeinformationen zu gewähren, müssen Sie oder ein Administrator dem IAM Identity Center-Benutzer einen Berechtigungssatz zuweisen. [???](#) Berechtigungssätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, die ein IAM Identity Center-Benutzer auf ein AWS-Konto hat. Wenn Ihr Administrator den IAM Identity Center-Benutzer für Sie erstellt hat, bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).
- AWS CLI installiert — Um die temporären Anmeldeinformationen verwenden zu können, müssen Sie den AWS CLI installieren. Weitere Anweisungen finden Sie unter [Installation oder Aktualisierung der aktuellen Version der AWS CLI](#) im Benutzerhandbuch zu AWS CLI .

Überlegungen

Bevor Sie die Schritte zum Abrufen der temporären Anmeldeinformationen für Ihren IAM Identity Center-Benutzer ausführen, sollten Sie die folgenden Überlegungen berücksichtigen:

- IAM Identity Center erstellt IAM-Rollen — Wenn Sie einen Benutzer in IAM Identity Center einem Berechtigungssatz zuweisen, erstellt IAM Identity Center eine entsprechende IAM-Rolle aus dem Berechtigungssatz. Durch Berechtigungssätze erstellte IAM-Rollen unterscheiden sich auf folgende Weise von IAM-Rollen, die mit erstellt wurden: AWS Identity and Access Management
- IAM Identity Center besitzt und schützt die Rollen, die durch Berechtigungssätze erstellt werden. Nur IAM Identity Center kann diese Rollen ändern.
- Nur Benutzer in IAM Identity Center können die Rollen übernehmen, die ihren zugewiesenen Berechtigungssätzen entsprechen. Sie können IAM-Benutzern, IAM-Verbundbenutzern oder Dienstkontoen keinen Berechtigungssatzzugriff zuweisen.
- Sie können eine Rollenvertrauensrichtlinie für diese Rollen nicht ändern, um [Principals](#) außerhalb von IAM Identity Center Zugriff zu gewähren.

Informationen zum Abrufen temporärer Anmeldeinformationen für eine Rolle, die Sie in IAM erstellen, finden Sie AWS CLI [im Benutzerhandbuch unter](#) Verwenden temporärer Sicherheitsanmeldeinformationen mit dem AWS Identity and Access Management .

- Sie können die Sitzungsdauer für Berechtigungssätze festlegen — Nachdem Sie sich beim AWS Access Portal angemeldet haben, wird der Berechtigungssatz, dem Ihr IAM Identity Center-Benutzer zugewiesen ist, als verfügbare Rolle angezeigt. IAM Identity Center erstellt eine separate Sitzung für diese Rolle. Diese Sitzung kann je nach der für den Berechtigungssatz konfigurierten Sitzungsdauer zwischen einer und 12 Stunden dauern. Die Standardsitzungsdauer beträgt eine Stunde. Weitere Informationen finden Sie unter [Legen Sie die Sitzungsdauer fest für AWS-Konten](#).

Temporäre Anmeldeinformationen abrufen und aktualisieren

Sie können temporäre Anmeldeinformationen für Ihren IAM Identity Center-Benutzer automatisch oder manuell abrufen und aktualisieren.

Themen

- [Automatische Aktualisierung der Anmeldeinformationen \(empfohlen\)](#)
- [Manuelles Aktualisieren der Anmeldeinformationen](#)

Automatische Aktualisierung der Anmeldeinformationen (empfohlen)

Die automatische Aktualisierung der Anmeldeinformationen verwendet den Gerätecode-Autorisierungsstandard Open ID Connect (OIDC). Bei dieser Methode initiieren Sie den Zugriff direkt, indem Sie den `aws configure sso` Befehl im verwenden. AWS CLI Mit diesem Befehl können Sie

automatisch auf jede Rolle zugreifen, die mit einem beliebigen Berechtigungssatz verknüpft ist, dem Sie für eine bestimmte Rolle zugewiesen sind AWS-Konto.

Um auf die Rolle zuzugreifen, die für Ihren IAM Identity Center-Benutzer erstellt wurde, führen Sie den `aws configure sso` Befehl AWS CLI aus und autorisieren Sie ihn dann in einem Browserfenster. Solange Sie eine aktive AWS Access-Portal-Sitzung haben, ruft das AWS CLI automatisch temporäre Anmeldeinformationen ab und aktualisiert die Anmeldeinformationen automatisch.

Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter [Konfigurieren Sie Ihr Profil mit `aws configure sso wizard`](#) dem.

Um temporäre Anmeldeinformationen zu erhalten, die automatisch aktualisiert werden

1. Melden Sie sich mit der spezifischen Anmelde-URL, die Sie von Ihrem Administrator erhalten haben, beim AWS Access-Portal an. Wenn Sie den IAM Identity Center-Benutzer erstellt haben, AWS haben Sie eine E-Mail-Einladung gesendet, die Ihre Anmelde-URL enthält. Weitere Informationen finden Sie im AWS Sign-In Benutzerhandbuch unter Beim AWS Access-Portal <https://docs.aws.amazon.com/signin/latest/userguide/iam-id-center-sign-in-tutorial.html> anmelden.
2. Suchen Sie auf der Registerkarte Konten das Konto, AWS-Konto von dem Sie die Anmeldeinformationen abrufen möchten. Wenn Sie das Konto auswählen, werden der Kontoname, die Konto-ID und die E-Mail-Adresse angezeigt, die dem Konto zugeordnet sind.

 Note

Wenn Sie keine Rechte in der AWS-Konten Liste sehen, wurde Ihnen wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Wenden Sie sich in diesem Fall an Ihren Administrator und bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten](#).

3. Unter dem Namen des Kontos wird der Berechtigungssatz, dem Ihr IAM Identity Center-Benutzer zugewiesen ist, als verfügbare Rolle angezeigt. Wenn Ihrem IAM Identity Center-Benutzer beispielsweise der `PowerUserAccess` Berechtigungssatz für das Konto zugewiesen ist, wird die Rolle im AWS Zugriffsportal als angezeigt. `PowerUserAccess`
4. Je nach Ihrer Option neben dem Rollennamen wählen Sie entweder Zugriffstasten oder Befehlszeilen- oder programmatischen Zugriff.

5. Wählen Sie im Dialogfeld „Anmeldeinformationen abrufen“ entweder macOS und Linux , Windows oder PowerShell, je nachdem, auf welchem Betriebssystem Sie den AWS CLI installiert haben.
6. Unter AWS IAM Identity Center-Anmeldeinformationen (empfohlen) SSO Region werden Ihre SSO Start URL und angezeigt. Diese Werte sind erforderlich, um sowohl ein für IAM Identity Center aktiviertes Profil als auch für Ihr Profil sso-session zu konfigurieren. AWS CLI Um diese Konfiguration abzuschließen, folgen Sie den Anweisungen unter [Konfigurieren Sie Ihr Profil mit dem aws configure sso wizard](#) im AWS Command Line Interface Benutzerhandbuch.

Verwenden Sie nach Bedarf AWS CLI so lange, AWS-Konto bis die Anmeldeinformationen abgelaufen sind.

Manuelles Aktualisieren der Anmeldeinformationen

Sie können die Methode zur manuellen Aktualisierung der Anmeldeinformationen verwenden, um temporäre Anmeldeinformationen für eine Rolle abzurufen, die einem bestimmten Berechtigungssatz in einer bestimmten Rolle zugeordnet ist. AWS-Konto Dazu kopieren Sie die erforderlichen Befehle für die temporären Anmeldeinformationen und fügen sie ein. Bei dieser Methode müssen Sie die temporären Anmeldeinformationen manuell aktualisieren.

Sie können AWS CLI Befehle ausführen, bis Ihre temporären Anmeldeinformationen ablaufen.

Um Anmeldeinformationen abzurufen, die Sie manuell aktualisieren

1. Melden Sie sich mit der spezifischen Anmelde-URL, die Sie von Ihrem Administrator erhalten haben, beim AWS Access-Portal an. Wenn Sie den IAM Identity Center-Benutzer erstellt haben, AWS haben Sie eine E-Mail-Einladung gesendet, die Ihre Anmelde-URL enthält. Weitere Informationen finden Sie im AWS Sign-In Benutzerhandbuch unter Beim AWS Access-Portal <https://docs.aws.amazon.com/signin/latest/userguide/iam-id-center-sign-in-tutorial.html> anmelden.
2. Suchen Sie auf der Registerkarte Konten das Verzeichnis, AWS-Konto von dem Sie die Zugangsdaten abrufen möchten, und erweitern Sie es, sodass der IAM-Rollenname angezeigt wird (z. B. Administrator). Wählen Sie je nach Ihrer Option neben dem IAM-Rollennamen entweder Zugriffstasten oder Befehlszeilen- oder programmatischen Zugriff aus.

 Note

Wenn Sie keine dieser Berechtigungen in der AWS-Konten Liste sehen, wurde Ihnen wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Wenden Sie sich in diesem Fall an Ihren Administrator und bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter [Weisen Sie Benutzer- oder Gruppengriff zu AWS-Konten](#).

3. Wählen Sie im Dialogfeld „Anmeldeinformationen abrufen“ macOS und Linux , Windows oder PowerShell, je nachdem, auf welchem Betriebssystem Sie den installiert haben AWS CLI.
4. Wählen Sie eine der folgenden Optionen:
 - Option 1: AWS Umgebungsvariablen festlegen

Wählen Sie diese Option, um alle Einstellungen für Anmeldeinformationen außer Kraft zu setzen, einschließlich aller Einstellungen in den `credentials` Dateien und `config` Dateien. Weitere Informationen finden Sie AWS CLI [im AWS CLI Benutzerhandbuch unter Umgebungsvariablen zur Konfiguration von](#).

Um diese Option zu verwenden, kopieren Sie die Befehle in Ihre Zwischenablage, fügen Sie die Befehle in Ihr AWS CLI Terminalfenster ein und drücken Sie dann die EINGABETASTE, um die erforderlichen Umgebungsvariablen festzulegen.

- Option 2: Fügen Sie Ihrer AWS Anmeldeinformationsdatei ein Profil hinzu

Wählen Sie diese Option, um Befehle mit unterschiedlichen Anmeldeinformationen auszuführen.

Um diese Option zu verwenden, kopieren Sie die Befehle in Ihre Zwischenablage und fügen Sie die Befehle dann in Ihre gemeinsame AWS `credentials` Datei ein, um ein neues benanntes Profil einzurichten. Weitere Informationen finden Sie unter [Gemeinsam genutzte Konfigurationsdateien und Anmeldeinformationen](#) im Referenzhandbuch für AWS SDKs und Tools. Um diese Anmeldeinformationen zu verwenden, geben Sie die `--profile` Option in Ihrem AWS CLI Befehl an. Dies wirkt sich auf alle Umgebungen aus, die dieselbe Anmeldeinformationsdatei verwenden.

- Option 3: Verwenden Sie individuelle Werte in Ihrem AWS Service Client

Wählen Sie diese Option, um von einem AWS Service-Client aus auf AWS Ressourcen zuzugreifen. Weitere Informationen finden Sie unter [Tools für AWS](#).

Um diese Option zu verwenden, kopieren Sie die Werte in Ihre Zwischenablage, fügen Sie die Werte in Ihren Code ein und weisen Sie sie den entsprechenden Variablen für Ihr SDK zu. Weitere Informationen finden Sie in der Dokumentation zu Ihrer spezifischen SDK-API.

Erstellen von Verknüpfungen zu AWS-Managementkonsole Destinationen

Im AWS Access-Portal erstellte Verknüpfungen führen IAM Identity Center-Benutzer zu einem bestimmten Ziel im AWS-Managementkonsole, mit einem bestimmten Berechtigungssatz und in einem bestimmten AWS-Konto.

Shortcut-Links sparen Zeit für Sie und Ihre Mitarbeiter. Anstatt über mehrere Seiten, einschließlich des AWS Access-Portals, zu einer gewünschten Ziel-URL auf der AWS-Managementkonsole (z. B. einer Amazon S3-Bucket-Instance-Seite) zu navigieren, können Sie einen Shortcut-Link verwenden, um automatisch zum gleichen Ziel zu gelangen.

Zieloptionen für den Shortcut-Link

Für Verknüpfungen gibt es drei Zieloptionen, die hier nach Priorität aufgelistet sind:

- (Optional) Jede Ziel-URL in dem im Shortcut AWS-Managementkonsole angegebenen Link. Zum Beispiel die Amazon S3-Bucket-Instance-Seite.
- (Optional) Administrator-configured Relay-Status-URL für den fraglichen Berechtigungssatz. Weitere Hinweise zum Einstellen des Relay-Status finden Sie unter [Stellen Sie den Relay-Status für den schnellen Zugriff auf den ein AWS-Managementkonsole](#).
- AWS-Managementkonsole Zuhause. Das Standardziel, falls Sie keines angeben.

Note

Die automatische Navigation zu einem Ziel ist nur erfolgreich, wenn Sie bei IAM Identity Center authentifiziert sind und Ihnen der erforderliche Berechtigungssatz für das AWS Konto und die Ziel-URL zugewiesen wurde.

Das AWS Access-Portal enthält die Schaltfläche „Verknüpfung erstellen“, mit der Sie einen gemeinsam nutzbaren Shortcut-Link erstellen können. Wenn Sie eine Ziel-URL angeben möchten (die erste Option in der vorherigen Liste), können Sie die URL in eine Zwischenablage kopieren, um sie zu teilen.

Erstellen Sie einen Shortcut-Link in der AWS auf das Portal zugreifen

1. Wählen Sie, während Sie im AWS Access Portal angemeldet sind, die Registerkarte **Konten** und dann die Schaltfläche **Verknüpfung erstellen**.
2. Im Dialogfeld:
 - a. Wählen Sie eine, AWS-Konto indem Sie die Konto-ID oder den Kontonamen verwenden. Während der Eingabe werden in einem Dropdownmenü die entsprechenden Konto-IDs und Namen angezeigt, auf die Sie zugreifen können. Sie können nur ein Konto auswählen, auf das Sie Zugriff haben.
 - b. Wählen Sie optional eine IAM-Rolle aus der Dropdownliste aus. Dies sind die Berechtigungssätze, die Ihnen für das ausgewählte Konto zugewiesen wurden. Wenn Sie die Rolle nicht auswählen, werden Benutzer aufgefordert, eine Rolle auszuwählen, die ihnen für das gewählte Konto zugewiesen ist, wenn sie den Shortcut-Link verwenden.

Note

Mit Shortcut-Links können Sie keinen neuen Zugriff gewähren. Verknüpfungen funktionieren nur mit den Berechtigungssätzen, die dem Benutzer bereits zugewiesen sind. Wenn dem Benutzer nicht die erforderlichen Berechtigungssätze für das Konto und die Ziel-URL zugewiesen wurden, wird ihm der Zugriff verweigert.

- c. Geben Sie optional die Ziel-URL des AWS Access Portals ein. Wenn Sie keine URL eingeben, wird das Ziel automatisch bestimmt, wenn Sie den Shortcut-Link verwenden, basierend auf den zuvor genannten Zieloptionen für den Shortcut-Link.
- d. Ihr Shortcut-Link wird auf der Grundlage Ihrer Eingabe am unteren Rand des Dialogfelds generiert. Wählen Sie die Schaltfläche „URL kopieren“. Sie können jetzt ein Lesezeichen mit dem kopierten Shortcut-Link erstellen oder es mit Ihren Mitarbeitern teilen, die mit demselben Berechtigungssatz oder einem anderen ausreichenden Berechtigungssatz Zugriff auf dasselbe Konto haben.

Sicher konstruieren AWS-Managementkonsole Shortcut-Links mit URL-Codierung

Alle Parameterwerte der URL, einschließlich der Konto-ID, des Namens des Berechtigungssatzes und der Ziel-URL, müssen URL-encoded

Shortcut-Links erweitern die URL des AWS Access-Portals um den folgenden Pfad:

```
/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Die vollständige URL in der klassischen AWS Partition folgt diesem Muster:

IPv4-Endpunkt:

```
https://[your_subdomain].awsapps.com/start/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Dual-stack Endpunkt

```
https://[identity_center_instance_id].portal.[region].app.aws/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Hier ist ein Beispiel für einen Shortcut-Link, der einen Benutzer 123456789012 mit dem S3FullAccess Berechtigungssatz anmeldet und ihn zur Startseite der S3-Konsole weiterleitet:

- IPv4-Endpunkt: `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Dual-stack Endpunkt: `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) IPv4-Endpunkt: `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) Dual-stack Endpunkt: `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registrieren Sie Ihr Gerät für MFA

Verwenden Sie für Benutzer im Identity Center-Verzeichnis das folgende Verfahren im AWS Access Portal, um Ihr neues Gerät für die Multifaktor-Authentifizierung (MFA) zu registrieren.

Important

MFA im IAM Identity Center wird derzeit für [externe Identitätsanbieter nicht unterstützt](#).

Bevor Sie beginnen

Wir empfehlen, dass Sie zuerst die entsprechende Authenticator-App auf Ihr Gerät herunterladen, bevor Sie mit den Schritten dieses Verfahrens beginnen. Eine Liste der Apps, die Sie für MFA-Geräte verwenden können, finden Sie unter: [Apps für virtuelle Authentifikatoren](#)

Registrieren Sie Ihr Gerät

Um Ihr Gerät für die Verwendung mit MFA zu registrieren

1. Melden Sie sich bei Ihrem AWS Zugangsportaal an. Weitere Informationen finden Sie unter [Melden Sie sich bei der an AWS auf das Portal zugreifen](#).
2. Wählen Sie oben rechts auf der Seite MFA-Geräte aus.
3. Wählen Sie auf der Seite mit Multi-factor Authentifizierungsgeräten (MFA) die Option Gerät registrieren aus.

Note

Wenn die Option MFA-Gerät registrieren ausgegraut ist, wenden Sie sich an Ihren Administrator, um Unterstützung bei der Registrierung Ihres Geräts zu erhalten.

4. Wählen Sie auf der Seite „MFA-Gerät registrieren“ einen der folgenden MFA-Gerätetypen aus und folgen Sie den Anweisungen:
 - Authenticator-App
 1. Auf der Seite „Authenticator-App einrichten“ finden Sie möglicherweise Konfigurationsinformationen für das neue MFA-Gerät, einschließlich einer QR-Code-Grafik. Die Grafik ist eine Darstellung des geheimen Schlüssels, der für die manuelle Eingabe auf Geräten verfügbar ist, die keine QR-Codes unterstützen.

2. Gehen Sie mit dem physischen MFA-Gerät wie folgt vor:
 - a. Öffnen Sie eine kompatible MFA-Authenticator-App. Eine Liste der getesteten Apps, die Sie mit MFA-Geräten verwenden können, finden Sie unter [Apps für virtuelle Authentifikatoren](#). Wenn die MFA-App mehrere Konten (mehrere MFA-Geräte) unterstützt, wählen Sie die Option zum Erstellen eines neuen Kontos (ein neues MFA-Gerät).
 - b. Stellen Sie fest, ob die MFA-App QR-Codes unterstützt, und führen Sie dann auf der Seite „Die Authenticator-App einrichten“ einen der folgenden Schritte aus:
 - i. Wählen Sie Show QR code (QR-Code anzeigen) und verwenden Sie anschließend die App, um den QR-Code zu scannen. Sie können beispielsweise das Kamerasymbol oder eine ähnliche Option wie Scan code (Code scannen) auswählen. Verwenden Sie anschließend die Kamera des Geräts, um den Code zu scannen.
 - ii. Wählen Sie „Geheimen Schlüssel anzeigen“ und geben Sie diesen geheimen Schlüssel dann in Ihre MFA-App ein.

 Important

Wenn Sie ein MFA-Gerät für IAM Identity Center konfigurieren, empfehlen wir Ihnen, eine Kopie des QR-Codes oder des geheimen Schlüssels an einem sicheren Ort aufzubewahren. Dies kann hilfreich sein, wenn Sie das Telefon verlieren oder die MFA-Authenticator-App neu installieren müssen. Wenn eines dieser Dinge passiert, können Sie die App schnell neu konfigurieren, um dieselbe MFA-Konfiguration zu verwenden.

3. Geben Sie auf der Seite „Authentifikator-App einrichten“ unter Authenticator-Code das Einmalkennwort ein, das derzeit auf dem physischen MFA-Gerät angezeigt wird.

 Important

Senden Sie die Anforderung direkt nach der Erzeugung der Codes. Wenn Sie den Code generieren und dann mit dem Absenden der Anfrage zu lange warten, wurde das MFA-Gerät erfolgreich mit Ihrem Benutzer verknüpft, das MFA-Gerät ist jedoch nicht synchronisiert. Dies liegt daran, weil die zeitgesteuerten Einmalpasswörter (TOTP) nach einer kurzen Zeit ungültig werden. In diesem Fall können Sie das Gerät erneut synchronisieren.

4. Klicken Sie auf **Assign MFA (MFA zuordnen)**. Das MFA-Gerät kann jetzt mit der Generierung von Einmalkennwörtern beginnen und ist jetzt einsatzbereit für AWS.

- **Sicherheitsschlüssel** oder **Authentifikator** **Built-in**

1. Folgen Sie auf der Seite „Den Sicherheitsschlüssel Ihres Benutzers registrieren“ den Anweisungen Ihres Browsers oder Ihrer Plattform.

 Note

Die Erfahrung variiert je nach Browser oder Plattform. Nachdem Ihr Gerät erfolgreich registriert wurde, können Sie Ihrem neu registrierten Gerät einen benutzerfreundlichen Anzeigenamen zuordnen. Um den Namen zu ändern, wählen Sie **Umbenennen**, geben Sie den neuen Namen ein und wählen Sie dann **Speichern**.

Ihre aktive Sitzung anzeigen und beenden

Sie können Ihr AWS Zugangsportal verwenden, um die Liste Ihrer aktiven Sitzungen einzusehen und bei Bedarf eine oder mehrere Sitzungen zu beenden.

Beenden Sie Ihre aktive Sitzung mit Ihrem AWS auf das Portal zugreifen

1. Melden Sie sich bei Ihrem AWS Zugangsportal an. Weitere Informationen finden Sie unter [Melden Sie sich bei der an AWS auf das Portal zugreifen](#).
2. Wählen Sie oben rechts auf der Seite **Sicherheit** aus.
3. Auf der Seite **Sicherheit** gibt die Zahl in Klammern neben **Aktive Sitzungen** an, wie viele aktive Sitzungen Sie haben. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann **Sitzungen beenden** aus.

 Tip

Für Benutzersitzungen im Hintergrund können Sie anhand des Amazon-Ressourcennamens (ARN) des Jobs, der die Sitzung verwendet, nach Sitzungen suchen. Wählen Sie in der Liste **Sitzungstyp** die Option **Benutzerhintergrundsitzungen** aus, und geben Sie dann den Job-ARN in das Suchfeld ein.

Sie können nur aktive Sitzungen beenden, die geladen sind. Wenn Sie viele Sitzungen haben, wählen Sie **Weitere aktive Sitzungen laden**, um weitere Sitzungen anzuzeigen.

4. Aktivieren Sie das Kontrollkästchen neben jeder Sitzung, die Sie beenden möchten, und wählen Sie dann **Sitzungen beenden** aus.
5. Ein Dialogfeld wird angezeigt, das bestätigt, dass Sie aktive Sitzungen beenden. Überprüfen Sie die Informationen. Wenn Sie fortfahren möchten, geben Sie Folgendes ein **confirm**, und wählen Sie dann **Sitzungen beenden** aus.
6. Sie kehren zu Ihrer Liste der aktiven Sitzungen zurück. Eine grüne Benachrichtigung wird angezeigt, um darauf hinzuweisen, dass die ausgewählten Sitzungen erfolgreich beendet wurden.

Verwenden von IAM Identity Center für mehrere AWS-Regionen

In diesem Thema wird die Verwendung von AWS IAM Identity Center Across Multiple AWS-Regionen erklärt. Erfahren Sie, wie Sie Ihre Instance in weitere Regionen replizieren, den Zugriff und die Sitzungen Ihrer Mitarbeiter verwalten, Anwendungen bereitstellen und den Kontozugriff bei Serviceunterbrechungen aufrechterhalten können.

Wenn Sie eine Organisationsinstanz von IAM Identity Center aktivieren, wählen Sie eine einzelne AWS-Region (primäre Region) aus. Sie können diese Instanz AWS-Regionen während der Instanzerstellung oder danach auf weitere Instanzen replizieren, sofern sie bestimmte Voraussetzungen erfüllt. IAM Identity Center repliziert automatisch Mitarbeiteridentitäten, Berechtigungssätze, Benutzer- und Gruppenzuweisungen, Sitzungen und andere Metadaten aus der primären Region in die ausgewählten zusätzlichen Regionen.

Vorteile des regionsübergreifenden Supports

Die Replikation von IAM Identity Center auf zusätzliche Systeme AWS-Regionen bietet zwei wichtige Vorteile:

- Verbesserte Ausfallsicherheit beim AWS-Konto Zugriff — Ihre Mitarbeiter können auch dann auf ihre AWS-Konto Daten zugreifen, wenn es bei der IAM Identity Center-Instanz in ihrer Hauptregion zu einer Serviceunterbrechung kommt. Dies gilt für Zugriffe mit Berechtigungen, die vor der Störung erteilt wurden.
- Höhere Flexibilität bei der Auswahl der Bereitstellungsregionen für AWS verwaltete Anwendungen — Sie können AWS verwaltete Anwendungen in Ihren bevorzugten Regionen bereitstellen, um die Anforderungen an den Speicherort der Anwendungsdaten zu erfüllen und die Leistung durch die Nähe zu den Benutzern zu verbessern. Anwendungen, die in weiteren Regionen bereitgestellt werden, greifen lokal auf replizierte Mitarbeiteridentitäten zu, um optimale Leistung und Zuverlässigkeit zu gewährleisten.

Voraussetzungen und Überlegungen

Bevor Sie Ihre IAM Identity Center-Instanz replizieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- **Instanztyp** — Ihre IAM Identity Center-Instanz muss eine [Organisationsinstanz sein](#). Multi-Region Unterstützung ist in [Kontoinstanzen](#) nicht verfügbar.
- **Identitätsquelle** — Ihre IAM Identity Center-Instanz muss mit einem externen Identitätsanbieter (IdP) verbunden sein, z. B. [Okta](#), oder das [Identity Center-Verzeichnis](#) als Identitätsquelle verwenden. Multi-Region Unterstützung ist nicht für Instanzen verfügbar, die [Active Directory](#) als Identitätsquelle verwenden.
- **AWS Regionen** — Multi-Region Support ist in [kommerziellen Regionen verfügbar, die standardmäßig](#) in Ihren aktiviert sind AWS-Konto. Opt-in Regionen werden derzeit nicht unterstützt.
- **KMS-Schlüsseltyp für Verschlüsselung im Ruhezustand** — Ihre IAM Identity Center-Instanz muss mit einem vom [Kunden verwalteten KMS-Schlüssel für mehrere Regionen konfiguriert sein](#). Der KMS-Schlüssel muss sich im selben AWS Konto wie IAM Identity Center befinden. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).
- **AWS Kompatibilität mit verwalteten Anwendungen** — Prüfen Sie die Anwendungstabelle unter [the section called “Anwendungen, die Sie mit IAM Identity Center verwenden können”](#), um die folgenden beiden Anwendungsanforderungen zu überprüfen:
 - Alle AWS verwalteten Anwendungen, die von Ihrem Unternehmen verwendet werden, müssen das IAM Identity Center unterstützen, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist.
 - Die AWS verwalteten Anwendungen, die Sie in weiteren Regionen bereitstellen möchten, müssen diese Art der Bereitstellung unterstützen.
- **Externe IdP-Kompatibilität (nur externe Identitätsanbieter)** — Wenn Sie einen externen Identitätsanbieter verwenden, muss der IdP mehrere ACS-URLs (Assertion Consumer Service) unterstützen, um die Unterstützung mehrerer Regionen in vollem Umfang nutzen zu können. Dies ist eine SAML-Funktion, die IdPs beispielsweise von Okta, Microsoft Entra ID und unterstützt wird. PingFederate PingOne JumpCloud

Wenn Sie beispielsweise einen IdP verwenden, der nicht mehrere ACS-URLs unterstützt, empfehlen wir Ihnen Google Workspace, mit Ihrem IdP-Anbieter zusammenzuarbeiten, um diese Funktion zu aktivieren. Diese Voraussetzung gilt nicht, wenn das Identity Center-Verzeichnis als Identitätsquelle verwendet wird. Optionen, die ohne mehrere ACS-URLs verfügbar sind, finden Sie unter [the section called “Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs”](#) und [the section called “AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu”](#).

Eine zusätzliche Region auswählen

Wenn Sie unter den standardmäßig aktivierten kommerziellen Regionen eine weitere Region auswählen, sollten Sie die folgenden Faktoren berücksichtigen:

- **Compliance-Anforderungen** — Wenn Sie AWS verwaltete Anwendungen ausführen müssen, die auf Datensätze zugreifen, die aus Compliance-Gründen auf eine bestimmte Region beschränkt sind, wählen Sie die Region aus, in der sich die Datensätze befinden.
- **Leistungsoptimierung** — Wenn die Datenresidenz keine Rolle spielt, wählen Sie eine Region aus, die Ihren Anwendungsbenutzern am nächsten ist, um deren Nutzererlebnis zu optimieren.
- **Anwendungssupport** — Stellen Sie sicher, dass Ihre erforderlichen AWS Anwendungen in der von Ihnen ausgewählten Region verfügbar sind.
- **AWS-Konto Zugriffssicherheit** — Wählen Sie für einen kontinuierlichen Zugriff auf AWS-Konto s eine Region aus, die geografisch weit von der Hauptregion Ihrer IAM Identity Center-Instance entfernt ist.

Note

IAM Identity Center hat ein Kontingent für die Anzahl von AWS-Regionen. Weitere Informationen finden Sie unter [the section called “Zusätzliche Kontingente”](#).

Replizieren Sie IAM Identity Center in eine zusätzliche Region

Wenn Ihre Umgebung die [Voraussetzungen erfüllt](#), z. B. die Konfiguration von IAM Identity Center mit einem vom Kunden verwalteten KMS-Schlüssel für mehrere Regionen, führen Sie die folgenden Schritte aus, um Ihre IAM Identity Center-Instanz in eine weitere Region zu replizieren. Ihre primäre Region funktioniert während und nach diesen Schritten weiterhin normal.

Note

Wenn Sie eine neue Organisationsinstanz erstellen, können Sie Multiregion bei der Instanzerstellung aktivieren. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).

Schritt 1: Erstellen Sie einen Replikatschlüssel in der zusätzlichen Region

Bevor Sie IAM Identity Center in eine Region replizieren, müssen Sie zunächst einen Replikatschlüssel Ihres vom Kunden verwalteten KMS-Schlüssels in dieser Region erstellen und den Replikatschlüssel mit den für den Betrieb von IAM Identity Center erforderlichen Berechtigungen konfigurieren. Anweisungen zum Erstellen von Replikatschlüsseln für mehrere Regionen finden Sie unter Erstellen von Replikatschlüsseln für mehrere Regionen. <https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-replicate.html>

Der empfohlene Ansatz für die KMS-Schlüsselberechtigungen besteht darin, die Schlüsselrichtlinie aus dem Primärschlüssel zu kopieren, wodurch dieselben Berechtigungen gewährt werden, die bereits für IAM Identity Center in der Primärregion eingerichtet wurden. Alternativ können Sie Region-specific wichtige Richtlinien definieren. Dieser Ansatz erhöht jedoch die Komplexität der regionsübergreifenden Verwaltung von Berechtigungen und erfordert möglicherweise zusätzliche Koordination, wenn Richtlinien in Zukunft aktualisiert werden.

Note

AWS KMS synchronisiert Ihre KMS-Schlüsselrichtlinie nicht zwischen den Regionen Ihres mehrregionalen KMS-Schlüssels. Damit die KMS-Schlüsselrichtlinie in allen KMS-Schlüsselregionen synchron bleibt, müssen Sie die Änderungen in jeder Region einzeln vornehmen.

Schritt 2: Fügen Sie die Region im IAM Identity Center hinzu

Das Hinzufügen einer Region in IAM Identity Center löst die automatische Replikation der IAM Identity Center-Daten in diese Region aus. Die Replikation erfolgt asynchron mit eventueller Konsistenz. Auf den folgenden Registerkarten finden Sie Anweisungen dazu im Feld und. AWS-Managementkonsole AWS CLI

Console

Um eine Region hinzuzufügen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie den Tab Management.

4. Wählen Sie im Abschnitt Regionen für IAM Identity Center die Option Region hinzufügen aus.
5. Wählen Sie im Abschnitt Für Replikation AWS-Regionen verfügbar Ihre bevorzugte AWS-Region Option aus. Wenn die Region nicht in der Liste erscheint, ist sie nicht für die Replikation verfügbar, da der KMS-Schlüssel dort nicht repliziert wurde. Weitere Informationen finden Sie unter [the section called “Implementierung von kundenverwalteten KMS-Schlüsseln”](#).
6. Wählen Sie Region hinzufügen.
7. Überwachen Sie im Abschnitt Regionen für IAM Identity Center den Status der Region. Verwenden Sie die Schaltfläche „Aktualisieren“ (runder Pfeil), um bei Bedarf den aktuellen Status der Region zu überprüfen. Fahren Sie nach Abschluss der Replikation mit Schritt 2 fort.

AWS CLI

Um eine Region hinzuzufügen

```
aws sso-admin add-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Um den aktuellen Status der Region zu überprüfen

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Wenn der Regionsstatus AKTIV ist, können Sie mit Schritt 2 fortfahren.

Die Dauer der ersten Replizierung in eine weitere Region hängt von der Datenmenge in Ihrer IAM Identity Center-Instance ab. Nachfolgende inkrementelle Änderungen werden in den meisten Fällen innerhalb von Sekunden repliziert.

Schritt 3 (nur externe Identitätsanbieter): Aktualisieren Sie das externe IdP-Setup

Dieser Schritt gilt nur, wenn Sie einen externen Identitätsanbieter (IdP) verwenden. Wenn Sie das Identity Center-Verzeichnis als Identitätsquelle verwenden, fahren Sie mit Schritt 4 fort.

Folgen Sie dem Tutorial für Ihren externen IdP [Tutorials zur Identitätsquelle](#) für die folgenden Schritte:

Schritt 3.a: Fügen Sie Ihrem externen IdP die URLs des Assertion Consumer Service (ACS) hinzu

Dieser Schritt ermöglicht die direkte Anmeldung bei jeder weiteren Region und ist erforderlich, um die Anmeldung bei AWS verwalteten Anwendungen zu ermöglichen, die in diesen Regionen bereitgestellt werden, sowie für den Zugriff AWS-Konto auf s über diese Regionen. Informationen dazu, wo Sie die ACS-URLs finden, finden Sie unter [ACS-Endpunkte im primären und zusätzlichen Bereich AWS-Regionen](#)

Schritt 3.b (optional): Stellen Sie die im externen IdP-Portal AWS-Zugangsportale zur Verfügung

Stellen Sie die App AWS-Zugangsportale in der zusätzlichen Region als Lesezeichen-App im externen IdP-Portal zur Verfügung. Lesezeichen-Apps enthalten nur einen Link (URL) zum gewünschten Ziel und ähneln einem Browser-Lesezeichen. Sie finden die AWS-Zugangsportale URLs in der Konsole, indem Sie im Abschnitt Regionen für IAM Identity Center die Option Alle AWS-Zugangsportale URLs anzeigen auswählen. Weitere Informationen finden Sie unter [the section called “AWS Greifen Sie auf die Portal-Endpunkte im primären und zusätzlichen Bereich zu AWS-Regionen”](#).

IAM Identity Center unterstützt IdP-initiiertes SAML SSO in jeder weiteren Region, extern wird dies jedoch in IdPs der Regel mit nur einer einzigen ACS-URL unterstützt. Aus Gründen der Kontinuität empfehlen wir, die ACS-URL der primären Region für IdP-initiiertes SAML-SSO beizubehalten und sich beim Zugriff auf weitere Regionen auf Lesezeichen-Apps und Browser-Lesezeichen zu verlassen.

Schritt 4: Bestätigen Sie die Zulassungslisten für Firewall und Gateway

Überprüfen Sie Ihre Zulassungslisten für Domänen in Firewalls oder Gateways und aktualisieren Sie sie auf der Grundlage der dokumentierten Zulassungslisten. [???](#)

Schritt 5: Stellen Sie Ihren Benutzern Informationen zur Verfügung

Stellen Sie Ihren Benutzern Informationen über das neue Setup zur Verfügung, einschließlich der AWS-Zugangsportal URL in der zusätzlichen Region und der Verwendung der zusätzlichen Regionen. In den folgenden Abschnitten finden Sie relevante Details:

- [the section called “Zugang zu Arbeitskräften über eine zusätzliche Region”](#)
- [the section called “Failover zu einer zusätzlichen Region für den Zugriff AWS-Konto ”](#)
- [the section called “Bereitstellung und Verwaltung von Anwendungen auf mehreren AWS-Regionen”](#)

Die Region ändert sich über das Hinzufügen der ersten Region hinaus

Sie können weitere Regionen hinzufügen und entfernen. Die primäre Region kann nur entfernt werden, indem die gesamte IAM Identity Center-Instanz gelöscht wird. Weitere Informationen zum Entfernen einer Region finden Sie unter [the section called “Eine Region aus dem IAM Identity Center entfernen”](#).

Sie können keine zusätzliche Region zur primären Region heraufstufen oder die primäre Region als zusätzliche Region herabstufen.

Welche Daten werden repliziert?

IAM Identity Center repliziert die folgenden Daten:

Daten	Quelle und Ziel der Replikation
Identitäten der Belegschaft (Benutzer, Gruppen, Gruppenmitgliedschaften)	Von der Hauptregion zu den zusätzlichen Regionen
Berechtigungssätze und ihre Zuweisungen an Benutzer und Gruppen	Von der Hauptregion zu den zusätzlichen Regionen
Konfiguration (z. B. SAML-Einstellungen für externe IdP)	Von der primären Region zu den zusätzlichen Regionen

Daten	Quelle und Ziel der Replikation
Anwendungsmetadaten und Anwendungszuweisungen an Benutzer und Gruppen	Von der verbundenen IAM Identity Center-Region einer Anwendung zu den anderen aktivierten Regionen
Vertrauenswürdige Token-Aussteller	Von der Hauptregion zu den zusätzlichen Regionen
Sitzungen	Von der ursprünglichen Region der Sitzung zu den anderen aktivierten Regionen

Note

IAM Identity Center repliziert keine Daten, die in AWS verwalteten Anwendungen gespeichert sind. Außerdem ändert es nichts an der regionalen Präsenz einer Anwendungsbereitstellung. Wenn sich Ihre IAM Identity Center-Instance beispielsweise in den USA Ost (Nord-Virginia) befindet und Sie Amazon Redshift in derselben Region bereitgestellt haben, wirkt sich die Replikation von IAM Identity Center nach USA West (Oregon) nicht auf die Bereitstellungsregion von Amazon Redshift und die darin gespeicherten Daten aus.

Überlegungen:

- Globale Ressourcenkennungen in aktivierten Regionen — Benutzer, Gruppen, Berechtigungssätze und andere Ressourcen haben in den aktivierten Regionen dieselben Identifikatoren.
- Die Replikation wirkt sich nicht auf bereitgestellte IAM-Rollen aus — Bestehende IAM-Rollen, die anhand von Berechtigungssatzzuweisungen bereitgestellt wurden, werden bei der Kontoanmeldung aus einer beliebigen aktivierten Region verwendet.

Zugriff für Mitarbeiter über eine zusätzliche Region

In diesem Abschnitt wird erklärt, wie Ihre Mitarbeiter auf die AWS-Zugangsportal, AWS-Konto s und Anwendungen zugreifen können, wenn Sie IAM Identity Center in mehreren Regionen aktiviert haben.

AWS-Zugangsportal In einer weiteren Region werden die AWS-Konto s und Anwendungen angezeigt, auf die Ihre Mitarbeiter auf die gleiche Weise wie in der primären Region Zugriff haben. Ihre Mitarbeiter können sich AWS-Zugangsportal in einer weiteren Region über einen direkten Link zum Endpunkt des regionalen Portals anmelden (z. B. <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>). Wenn Sie einen externen Identitätsanbieter verwenden, können sich Ihre Mitarbeiter auch über eine [Lesezeichen-App anmelden, die](#) Sie im externen IdP eingerichtet haben.

Sie können den AWS-Zugangsportal Endpunkt in einer zusätzlichen Region verwenden, um den AWS CLI Zugriff auf APIs als IAM Identity Center-Benutzer zu autorisieren. Diese Funktion funktioniert auf die gleiche Weise wie in der primären Region. CLI-Autorisierungen werden jedoch nicht in allen aktivierten Regionen repliziert. Daher müssen Sie die CLI in jeder Region einzeln autorisieren.

Benutzersitzungen über mehrere AWS-Regionen

IAM Identity Center repliziert Benutzersitzungen aus der ursprünglichen Region in die anderen aktivierten Regionen. Sitzungssperrung und Abmeldung in einer Region werden auch in den anderen Regionen repliziert.

Sitzungssperrung durch IAM Identity Center-Administratoren

IAM Identity Center-Administratoren können Benutzersitzungen in weiteren Regionen widerrufen. Da Sitzungen regionsübergreifend repliziert werden, reicht es unter normalen Bedingungen aus, eine Sitzung in einer einzelnen Region zu widerrufen und IAM Identity Center die Änderung auf die anderen aktivierten Regionen replizieren zu lassen. Wenn in der primären Region von IAM Identity Center eine Störung auftritt, können Administratoren diesen Vorgang in weiteren Regionen durchführen.

AWS-Zugangsportal Endpunkte in der primären und zusätzlichen AWS-Regionen

Gehen Sie folgendermaßen vor, wenn Sie die AWS Access Portal-URLs für die aktivierten Regionen nachschlagen müssen:

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie den Tab Management.

4. Wählen Sie im Abschnitt Regionen für IAM Identity Center die Option Alle AWS Zugriffsportal-URLs anzeigen aus.

In der folgenden Tabelle sind die AWS-Zugangsportal Endpunkte in den primären und zusätzlichen Regionen einer IAM Identity Center-Instance aufgeführt.

AWS-Zugangsportal Endpunkt	Primäre - Region	Zusätzliche Region	URL-Muster und Beispiel
Nur klassisches IPv4 1	Ja	Nein	<p>Muster: <code>https://[Identity Store ID].awsapps.com/start</code></p> <p>Beispiel: <code>https://d-12345678.awsapps.com/start</code></p>
Custom-alias Nur IPv4 1	Ja (optional)	Nein	<p>Muster: <code>https://[custom alias].awsapps.com/start</code></p> <p>Beispiel: <code>https://mycompany.awsapps.com/start</code></p>
Nur alternative IPv4 2	Ja	Ja	<p>Muster: <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code></p> <p>Beispiel: <code>https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com</code></p>
Dual-stack ²	Ja	Ja	<p>Muster: <code>https://[Identity Center instance ID].portal.[Region].app.aws</code></p>

AWS-Zugangsportal Endpunkt	Primäre - Region	Zusätzliche Region	URL-Muster und Beispiel
			Beispiel: <code>https://ssoins-111111h2222j33pp.porta1.eu-west-1.app.aws</code>

¹ In weiteren Regionen wird der benutzerdefinierte Alias nicht unterstützt und die `awsapps.com` übergeordnete Domain ist nicht verfügbar.

² Bei den alternativen Endpunkten „Nur IPv4“ und „Dual-Stack-Portal“ steht die URL nicht am Ende. / start

Assertion Consumer Service (ACS) -Endpunkte auf den primären und zusätzlichen Endpunkten AWS-Regionen

Note

Dieser Abschnitt gilt nur für Instances, die einen externen Identitätsanbieter (IdP) verwenden. Wenn Sie das Identity Center-Verzeichnis als Identitätsquelle verwenden, ist eine ACS-URL-Konfiguration nicht erforderlich.

Gehen Sie folgendermaßen vor, wenn Sie die ACS-URLs nachschlagen oder als Teil der SAML-Metadaten herunterladen müssen:

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie die Registerkarte „Identitätsquelle“.
4. Wählen Sie im Dropdownmenü Aktionen die Option Authentifizierung verwalten aus.
5. Im Abschnitt Metadaten des Dienstanbieters werden die AWS-Zugangsportal ACS-URL für jede aktivierte Region angezeigt. IPv4-only und Dual-Stack-URLs werden auf separaten Registerkarten angezeigt. Wenn Ihr IdP das Hochladen einer SAML-Metadatendatei unterstützt, können Sie Metadatendatei herunterladen wählen, um die SAML-Metadatendatei mit allen ACS-URLs herunterzuladen. Wenn Ihr IdP das Hochladen einer Metadatendatei nicht unterstützt oder Sie ACS-URLs lieber einzeln hinzufügen möchten, können Sie einzelne URLs aus der

Tabelle in der Konsole kopieren oder ACS-URLs anzeigen und dann Alle URLs kopieren auswählen. Behalten Sie die ACS-URL bei, die bereits für die primäre Region konfiguriert ist, um sicherzustellen, dass das vom Dienstanbieter initiierte SAML-Single-Sign-On aus der primären Region weiterhin funktioniert.

In der folgenden Tabelle sind die SAML Assertion Consumer Service (ACS) -Endpunkte in der primären und zusätzlichen Region einer IAM Identity Center-Instanz aufgeführt:

ACS-Endpunkt	Primäre - Region	Zusätzliche Region	URL-Muster und Beispiel
Nur IPv4	Ja	Ja	<p>Muster:</p> <p><code>https://[Region].signin.aws/platform/saml/acs/ [Tenant ID]</code></p> <p>Beispiel: <code>https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code></p>
Nur alternative IPv4*	Ja	Nein	<p>Muster: <code>https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID]</code></p> <p>Beispiel: <code>https://us-west-2.signin.aws.amazon.com/platform/saml/acs/111111111111111111-aaee-ffff-dddd-111111111111</code></p>
Dual-stack	Ja	Ja	<p>Muster:</p> <p><code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code></p> <p>Beispiel: <code>https://us-west-2.sso.signin.aws/platform/sam</code></p>

ACS-Endpunkt	Primäre - Region	Zusätzliche Region	URL-Muster und Beispiel
			1/acs/1111111111111111-aaee -ffff-dddd-1111111111

* Für Instances, die vor Februar 2026 aktiviert wurden, sollten Sie diesen Endpunkt beibehalten, da dies vom Dienstanbieter initiiertes SAML-Single-Sign-On für die primäre Region erforderlich ist. IAM Identity Center verwendet diesen Endpunkt nicht für Instances, die im Februar 2026 oder später aktiviert wurden.

Verwenden AWS verwaltete Anwendungen ohne mehrere ACS-URLs

Note

Dieser Abschnitt gilt nur für Instanzen, die einen externen Identitätsanbieter (IdP) verwenden. Wenn Sie das Identity Center-Verzeichnis als Ihre Identitätsquelle verwenden, gilt diese Einschränkung nicht.

Einige externe Identitätsanbieter (IdPs) unterstützen nicht mehrere ACS-URLs (Assertion Consumer Service) in ihrer IAM Identity Center-Anwendung. Mehrere ACS-URLs sind eine SAML-Funktion, die für die direkte Anmeldung in einer bestimmten Region in einem IAM Identity Center mit mehreren Regionen erforderlich ist.

Wenn Sie beispielsweise eine AWS verwaltete Anwendung über einen Anwendungslink starten, löst das System die Anmeldung über die mit der Anwendung verbundene IAM Identity Center-Region aus. Wenn die ACS-URL für diese Region jedoch nicht im externen IdP konfiguriert ist, schlägt die Anmeldung fehl.

Um dieses Problem zu beheben, wenden Sie sich an Ihren IdP-Anbieter, um die Unterstützung mehrerer ACS-URLs zu aktivieren. In der Zwischenzeit können Sie AWS verwaltete Anwendungen weiterhin in weiteren Regionen verwenden. Melden Sie sich zunächst bei der Region an, deren ACS-URL im externen IdP konfiguriert ist (standardmäßig die primäre Region). Nach einer aktiven Sitzung im IAM Identity Center können Sie die Anwendung über das AWS Zugriffsportal in jeder aktivierten Region oder über einen Anwendungslink starten.

Failover zu einer zusätzlichen Region für AWS-Konto access

Das Thema AWS-Konto Zugriff über IAM Identity Center wird ausführlich behandelt in. [AWS-Konto Zugriff](#) Dieser Abschnitt enthält zusätzliche Informationen, die für die Aufrechterhaltung des AWS-Konto Zugriffs auf mehrere Benutzer AWS-Regionen im Falle einer Dienstunterbrechung in der Hauptregion relevant sind.

Wenn es bei Ihrer IAM Identity Center-Instance in der Hauptregion zu einer Unterbrechung kommt (z. B. ist das AWS Zugriffsportal in der Hauptregion nicht verfügbar), können Ihre Mitarbeiter in eine weitere Region wechseln, um weiterhin auf Anwendungen zuzugreifen AWS-Konto, die nicht betroffen sind. Weitere Informationen finden Sie unter [the section called “Zugang zu Arbeitskräften über eine zusätzliche Region”](#).

Wir empfehlen, dass Sie Ihren Mitarbeitern die AWS-Zugangsportal Endpunkte in weiteren Regionen mitteilen, sobald Sie die Einrichtung abgeschlossen haben. [the section called “Replizieren Sie IAM Identity Center in eine zusätzliche Region”](#) Wenn Sie einen externen Identitätsanbieter verwenden, teilen Sie uns auch das IdP-Setup mit (z. B. indem Sie Apps für die zusätzlichen Regionen mit Lesezeichen versehen). Dadurch sind sie bei Bedarf für einen Failover in eine weitere Region bereit.

Ebenso empfehlen wir AWS CLI Benutzern, [für jedes der](#) AWS CLI Profile, die sie für die primäre Region haben, Profile für zusätzliche Regionen zu erstellen. Anschließend können sie zu diesem Profil wechseln, wenn es in der Hauptregion zu einer Dienstunterbrechung kommt.

Note

Die Kontinuität des Zugriffs auf AWS-Konto s hängt davon ab, ob Berechtigungen wie Berechtigungssätze, Zuweisungen und Gruppenmitgliedschaften vor einer Betriebsunterbrechung bereitgestellt und repliziert werden. Wenn Sie einen externen Identitätsanbieter verwenden, hängt die Kontinuität auch vom Zustand Ihres externen IdP ab. Wir empfehlen, dass Ihr Unternehmen auch einen [AWS Break-Glass-Zugriff einrichtet](#), um den AWS Zugriff für eine kleine Gruppe berechtigter Benutzer aufrechtzuerhalten, wenn es bei der Identitätsquelle zu einer Betriebsunterbrechung kommt. [Der Notfallzugriff](#) ist eine ähnliche Option, für die ein externer IdP erforderlich ist.

AWS-Konto greifen Sie ohne mehrere ACS-URLs auf Resilienz zu

Note

Dieser Abschnitt gilt nur für Instanzen, die einen externen Identitätsanbieter (IdP) verwenden. Wenn Sie das Identity Center-Verzeichnis als Ihre Identitätsquelle verwenden, gilt diese Einschränkung nicht.

Einige externe Identitätsanbieter (IdPs) unterstützen nicht mehrere ACS-URLs (Assertion Consumer Service) in ihrer IAM Identity Center-Anwendung. Mehrere ACS-URLs sind eine SAML-Funktion, die für die direkte Anmeldung in einer bestimmten Region in einem IAM Identity Center mit mehreren Regionen erforderlich ist.

Damit Ihre Benutzer AWS-Konten über mehrere IAM Identity Center-Regionen auf ihre Regionen zugreifen können, müssen Sie die entsprechenden regionalen ACS-URLs im externen IdP konfigurieren. Wenn der externe IdP jedoch nur eine einzige ACS-URL in seiner IAM Identity Center-Anwendung unterstützt, können sich Benutzer direkt bei einer einzelnen IAM Identity Center-Region anmelden.

Um dieses Problem zu lösen, wenden Sie sich an Ihren IdP-Anbieter, um die Unterstützung mehrerer ACS-URLs zu aktivieren. In der Zwischenzeit können Sie zusätzliche Regionen als Backup für den Zugriff auf diese AWS-Konten verwenden.

Wenn in der primären Region eine Unterbrechung des IAM Identity Center-Dienstes auftritt, müssen Sie die ACS-URL im externen IdP mit der ACS-URL einer zusätzlichen Region aktualisieren. Nach diesem Update können Ihre Benutzer mithilfe der vorhandenen IAM Identity Center-Anwendung im externen IDP-Portal oder über einen direkten Link, den Sie mit ihnen teilen, auf das AWS Zugriffsportal in der zusätzlichen Region zugreifen.

Wir empfehlen Ihnen, dieses Setup regelmäßig zu testen, um sicherzustellen, dass es bei Bedarf funktioniert, und dass Sie Ihren Betrieb über diesen Failover-Prozess informieren.

Note

Wenn Sie AWS-Konten in dieser Konfiguration eine zusätzliche Region für den Zugriff verwenden, können Ihre Benutzer möglicherweise nicht auf AWS verwaltete Anwendungen

zugreifen, die mit der primären Region verbunden sind. Daher empfehlen wir dies nur als vorübergehende Maßnahme, um den Zugriff darauf aufrechtzuerhalten AWS-Konten.

Bereitstellung und Verwaltung von Anwendungen auf mehreren AWS Regionen

Das Thema Anwendungszugriff über IAM Identity Center wird ausführlich behandelt in [Anwendungszugriff](#). Dieser Abschnitt enthält zusätzliche Informationen, die für die Bereitstellung und Verwaltung von Anwendungen auf mehreren AWS-Regionen Geräten relevant sind.

Bereitstellung und Verwaltung AWS verwaltete Anwendungen auf mehreren AWS-Regionen

Mit einer IAM Identity Center-Instance mit einer einzigen Region können Sie AWS verwaltete Anwendungen in derselben Region wie Ihre Instance bereitstellen. Einige Anwendungen wie Amazon Q Business unterstützen eine regionsübergreifende Verbindung zum IAM Identity Center, was ihre Bereitstellung außerhalb der Region des IAM Identity Center ermöglicht, sofern die entsprechende Anwendung dort verfügbar ist. Regionsübergreifende Aufrufe können jedoch zu einer langsameren Anwendungsleistung führen, und die meisten AWS verwalteten Anwendungen unterstützen diese Art von Verbindung nicht.

Mit einer IAM Identity Center-Instance mit mehreren Regionen können Sie AWS verwaltete Anwendungen in jeder aktivierten Region mit einer Verbindung zum IAM Identity Center in derselben Region bereitstellen („Verbindung“). Region-local Die Bereitstellung in der Primärregion wird von allen integrierten AWS verwalteten Anwendungen unterstützt. Informationen dazu, welche AWS verwalteten Anwendungen die Bereitstellung in weiteren Regionen von IAM Identity Center unterstützen, finden Sie in [the section called “Anwendungen, die Sie mit IAM Identity Center verwenden können”](#) der Anwendungstabelle unter. In jedem Fall muss die AWS verwaltete Anwendung in der Region verfügbar sein, in der Sie sie bereitstellen möchten.

Mit einer Region-local Verbindung zum IAM Identity Center greifen AWS verwaltete Anwendungen auf Mitarbeiteridentitäten in derselben Region zu, um optimale Leistung und Zuverlässigkeit zu gewährleisten. Wir empfehlen, bei der Bereitstellung einer AWS verwalteten Anwendung eine Region-local Verbindung zu wählen, wenn die [Voraussetzungen erfüllt](#) sind.

Um eine AWS verwaltete Anwendung in einer weiteren Region von IAM Identity Center bereitzustellen, starten Sie die Bereitstellung in dieser Region über die Anwendungskonsole oder API auf die gleiche Weise wie in der primären Region.

Überlegungen:

- Wenn Sie Ihr IAM Identity Center noch nicht in diese Region repliziert haben, empfehlen wir, dass Sie dies zuerst tun, damit die Anwendungsbereitstellung sofort abgeschlossen werden kann.
- AWS verwaltete Anwendungen stellen in vielen Fällen automatisch eine Region-local Verbindung her, wenn Sie IAM Identity Center bereits in die Region repliziert haben.
- Wenn eine AWS verwaltete Anwendung eine regionsübergreifende Verbindung zum IAM Identity Center anbietet, empfehlen wir, eine Region-local Verbindung auszuwählen, sofern die [Voraussetzungen erfüllt sind](#).
- Wenn die Anwendung die Bereitstellung in weiteren Regionen nicht unterstützt, können Sie sie in der primären Region bereitstellen, sofern die Anwendung dort verfügbar ist.

 Important

Wenn Ihre IAM Identity Center-Instanz multiregional ist, müssen alle AWS verwalteten Anwendungen, die von Ihrem Unternehmen verwendet werden, unabhängig von der Region, in der die Anwendung bereitgestellt wird, IAM Identity Center unterstützen, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Bestätigen Sie dies vor der Bereitstellung einer Anwendung und [the section called “Anwendungen, die Sie mit IAM Identity Center verwenden können”](#) vor der Konfiguration eines vom Kunden verwalteten KMS-Schlüssels in Ihrem IAM Identity Center.

Die Verwaltungsregion einer Anwendung

Nachdem Sie eine AWS verwaltete Anwendung mithilfe einer Region-local Verbindung in einer weiteren Region von IAM Identity Center bereitgestellt haben, verwalten Sie die Anwendung und ihre Zuweisungen an Benutzer und Gruppen in derselben Region. IAM Identity Center repliziert die Anwendungsmetadaten, einschließlich Zuweisungen an Benutzer und Gruppen, in andere aktivierte Regionen, sodass Ihre Mitarbeiter Anwendungen von jeder aktivierten Region aus starten können.

Wenn Ihre AWS verwaltete Anwendung eine regionsübergreifende Verbindung zum IAM Identity Center verwendet, können Sie die Anwendungsdetails wie Name und Beschreibung sowie die

Anwendungszuweisungen an Benutzer und Gruppen über die IAM Identity Center-Konsole und die API in der verbundenen Region verwalten. Unabhängig vom Verbindungstyp können Sie die Anwendung über ihre Konsole in ihrer Bereitstellungsregion verwalten.

Weitergabe von vertrauenswürdigen Identitäten

Sie können die vertrauenswürdige Identitätsverbreitung mit AWS verwalteten Anwendungen, die sie unterstützen, in jeder aktivierten Region Ihrer IAM Identity Center-Instance verwenden.

Alle Anwendungen, die den Identitätskontext untereinander weitergeben, müssen sich in derselben Region befinden.

Die Abhängigkeit einer Anwendung von ihrer verbundenen IAM Identity Center-Region

Jede AWS verwaltete Anwendung stellt während der Bereitstellung eine Verbindung zu einer bestimmten IAM Identity Center-Region her. Die Anwendung ist dann für die Benutzeranmeldung von dieser Region abhängig, auch wenn Ihr IAM Identity Center in mehreren Regionen aktiviert ist. Wenn es in Ihrem IAM Identity Center in dieser Region zu einer Störung kommt, können Benutzer möglicherweise nicht auf AWS verwaltete Anwendungen zugreifen, die mit der Region verbunden sind.

Bereitstellung und Verwaltung von kundenverwalteten Anwendungen auf mehreren AWS-Regionen

IAM Identity Center unterstützt vom Kunden verwaltete SAML- und OAuth2-Anwendungen. Sie können wählen, ob Sie sie in jeder aktivierten Region Ihrer IAM Identity Center-Instanz erstellen möchten. Nachdem Sie eine erstellt haben, verwalten Sie die Anwendung und ihre Zuweisungen an Benutzer und Gruppen in derselben Region.

Eine Region aus dem IAM Identity Center entfernen

Gehen Sie folgendermaßen vor, um eine weitere Region aus Ihrer IAM Identity Center-Instanz zu entfernen:

Schritt 1: Aktualisieren Sie die externe IdP-Konfiguration (falls zutreffend)

Wenn Sie einen externen Identitätsanbieter verwenden, können Sie wählen, ob Sie die ACS-URL für diese Region von Ihrem externen IdP entfernen oder sie behalten möchten, falls Sie diese Region später erneut hinzufügen möchten. Wir empfehlen, dass Sie die Lesezeichen-App, die Sie möglicherweise für die AWS-Zugangsportal in dieser Region erstellt haben, entfernen oder

ausblenden. Wenn Sie das Identity Center-Verzeichnis als Ihre Identitätsquelle verwenden, fahren Sie mit Schritt 2 fort.

Schritt 2: Entfernen Sie die Region

Console

Um eine Region zu entfernen

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie den Tab Management.
4. Wählen Sie im Abschnitt Regionen für IAM Identity Center die zusätzliche Region aus, die Sie entfernen möchten.
5. Wählen Sie Remove (Entfernen) aus.
6. Bevor Sie das Entfernen mit der Option Region entfernen bestätigen, beachten Sie die Warnung vor dem potenziellen Verlust des Zugriffs auf Anwendungen, die in dieser IAM Identity Center-Region erstellt wurden. Wenn Sie sich nicht sicher sind, ob Sie über solche Anwendungen verfügen, wählen Sie im Navigationsbereich Anwendungen aus und bestätigen Sie die verbundene Region in der Spalte Erstellt von für jede AWS verwaltete und vom Kunden verwaltete Anwendung.

Note

Möglicherweise fallen weiterhin Gebühren für die Bereitstellung AWS verwalteter Anwendungen an, die immer noch mit der entfernten Region verbunden sind, auch wenn Sie den Zugriff auf diese Anwendungen verlieren. Um dies zu verhindern, müssen Sie diese AWS verwalteten Anwendungsbereitstellungen über die Anwendungskonsole oder API entfernen, bevor Sie die Region im IAM Identity Center entfernen. Wenn Sie die IAM Identity Center-Region bereits entfernt haben, können Sie den Zugriff auf Anwendungen wiederherstellen, indem Sie die Region wieder hinzufügen.

7. Überwachen Sie im Abschnitt Regionen für IAM Identity Center den Status der Region. Verwenden Sie die Schaltfläche „Aktualisieren“ (runder Pfeil), um bei Bedarf den aktuellen Status der Region anzuzeigen. Nachdem die Region entfernt wurde, erscheint sie nicht mehr in der Regionsliste.

AWS CLI

Um eine Region zu entfernen

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Um den aktuellen Status der Region zu überprüfen

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Wenn die Region entfernt ist, fahren Sie mit Schritt 3 fort.

Schritt 3: Löschen Sie den Replikatschlüssel

Sie können den Replikatschlüssel aus dieser Region entfernen, um zu vermeiden, dass KMS-Speichergebühren anfallen. Weitere Informationen finden Sie unter [Löschen eines Schlüssels. AWS KMS](#)

Important

Stellen Sie sicher, dass Sie nur den Replikatschlüssel in dieser bestimmten Region löschen. Die anderen IAM Identity Center-Regionen sind für den normalen Betrieb weiterhin auf den KMS-Schlüssel in den anderen aktivierten Regionen angewiesen.

Die IAM Identity Center-Dienst-APIs werden zusätzlich unterstützt AWS Regionen

API	Funktionalität in weiteren Regionen
Identity Center-API	Unterstützt: <ul style="list-style-type: none">• read/write Abläufe bei der Anwendungsverwaltung• Lesevorgänge für Instanzen

API	Funktionalität in weiteren Regionen
	Nicht unterstützt:
	<ul style="list-style-type: none"> • Alle Schreibvorgänge, die sich nicht auf die Anwendung beziehen • Lesevorgänge für Berechtigungssatz und Kontozuweisung
Identity Store-API	Lesevorgänge
OIDC-API	Alle Operationen werden unterstützt
Zugriff auf die Portal-API	Alle Operationen werden unterstützt
SCIM-API	Keine Operation wird unterstützt

AWS CloudTrail Ereignisse von IAM Identity Center in der primären und zusätzlichen Region

In können Sie die Aktionen überprüfen AWS CloudTrail, die IAM Identity Center-Benutzer und -Administratoren für alle aktivierten AWS-Regionen IAM Identity Center-Instanzen ausführen. Die AWS CloudTrail Ereignisse werden in der Region ausgegeben und protokolliert, in der die Aktion stattfindet. Weitere Informationen finden Sie unter [the section called “Protokollieren und Überwachen”](#).

Verfügbarkeit von IAM Identity Center-Anwendungsfällen in der primären und weiteren Region

Feature	Regionale Verfügbarkeit
Mitarbeiterverzeichnis mit einem Benutzerportal	
Benutzerzugriff auf das Portal AWS-Zugangsporta , einschließlich Portalanmeldung und globalen Sitzungen (eine Anmeldung für alle Regionen)	Alle aktivierten Regionen
Anzeige aller zugewiesenen Konten	Alle aktivierten Regionen

Feature	Regionale Verfügbarkeit
Anzeige aller zugewiesenen Anwendungen (unabhängig davon, wo die Anwendungen erstellt wurden)	Alle aktivierten Regionen
Lesezugriff auf Benutzer, Gruppen und Mitgliedschaften in der AWS Konsole oder über Identity Store-APIs	Alle aktivierten Regionen
Benutzersitzungen widerrufen	Alle aktivierten Regionen
Automatische Synchronisation von Benutzern und Gruppen aus einer externen Identitätsquelle (z. B. externer IdP über SCIM-API oder Identity Store-API). Diese Zeile gilt nur für externe Identitätsanbieter.	Nur primäre Region
Konfigurieren Sie die automatische Identitätsbereitstellung mit SCIM	Nur primäre Region
Konfigurieren Sie SAML SSO mit einem externen IdP	Nur primäre Region — Lesezugriff über die Konsole in allen aktivierten Regionen
Create/update/delete Operationen für Benutzer, Gruppen und Gruppenmitgliedschaften über die Konsole oder Identity Store-APIs.	Nur primäre Region. Wenn Sie das Identity Center-Verzeichnis verwenden, sind diese Operationen über die IAM Identity Center-Konsole und die Identity Store-API in der primären Region verfügbar. Wenn Sie einen externen IdP mit SCIM-Bereitstellung verwenden, werden Schreibvorgänge in der Konsole blockiert (außer disable/enable Benutzerzugriff und Benutzer löschen). Zusätzliche Regionen: schreibgeschützter Zugriff.

Feature	Regionale Verfügbarkeit
Operationen auf Benutzerdatenebene (Kennwort zurücksetzung, MFA-Geräteverwaltung) über das AWS-Zugangsportale (nur Identity Center-Verzeichnis)	Alle aktivierten Regionen (gilt nur, wenn das Identity Center-Verzeichnis als Identitätsquelle verwendet wird)
Multi-account Zugriff	
Greifen Sie über die Verknüpfungen AWS-Zugangsportale AWS CLI, und auf zugewiesene Konten zu	Alle aktivierten Regionen
Verwalten Sie Berechtigungssätze für mehrere Konten und deren Zuweisungen in der Konsole und in den APIs (einschließlich temporärer erweiterter Zugriffe)	Nur primäre Region
Zugriff auf Anwendungen und AWS Dienste	
Stellen Sie AWS verwaltete Anwendungen über die Anwendungskonsole und APIs bereit	Alle aktivierten Regionen — abhängig von der regionalen Verfügbarkeit der Anwendungen und der Unterstützung für die Bereitstellung in weiteren Regionen
Erstellen Sie vom Kunden verwaltete Anwendungen über die Identity Center-Konsole und die APIs	Alle aktivierten Regionen
Verwalten Sie Anwendungsmetadaten und Zuweisungen in der Konsole und in den APIs	Mit der Anwendung verbundene IAM Identity Center-Region
Starten Sie Anwendungen von AWS-Zugangsportale oder direkt über einen Anwendungslink oder ein Lesezeichen	Alle aktivierten Regionen
SSO für Amazon EC2-Instances	Alle aktivierten Regionen
Vertrauenswürdige Identitätsverbreitung	
Erstellen eines vertrauenswürdigen Token-Ausstellers	Nur primäre Region

Feature	Regionale Verfügbarkeit
Vertrauenswürdige Identitätsverbreitung bei AWS verwalteten Anwendungen	Alle aktivierten Regionen — Anwendungen, die den Identitätskontext untereinander weitergeben, müssen sich in derselben Region befinden
Andere Verwaltungsfunktionen	
Alle anderen Verwaltungsfunktionen wie Regionsverwaltung, KMS-Schlüsselverwaltung, Instanzverwaltung und Sitzungsverwaltung (außer Sitzungsperrung)	Nur primäre Region — Lesezugriff ist in allen aktivierten Regionen für einige Daten verfügbar (Zuweisungen von Berechtigungssätzen ausgeschlossen)

Resilienzdesign und regionales Verhalten

Der IAM Identity Center-Service wird vollständig verwaltet und nutzt hochverfügbare und langlebige AWS Dienste wie Amazon S3 und Amazon EC2. Um die Verfügbarkeit im Falle einer Störung der Availability Zone sicherzustellen, arbeitet IAM Identity Center in mehreren Availability Zones. Sie können Ihre IAM Identity Center-Instanz in weitere Regionen replizieren, um im Falle einer regionalen Störung den Kontozugriff mit den bereits bereitgestellten Berechtigungen aufrechtzuerhalten. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

Sie aktivieren IAM Identity Center in Ihrem Verwaltungskonto. AWS Organizations Dies ist erforderlich, damit IAM Identity Center Rollen für alle Benutzer bereitstellen, deprovisionieren und aktualisieren kann. AWS-Konten Wenn Sie IAM Identity Center aktivieren, wird es in der aktuell ausgewählten AWS-Region bereitgestellt, die als „primäre Region“ bezeichnet wird. Wenn Sie die Bereitstellung in einer bestimmten Region durchführen möchten AWS-Region, ändern Sie die Regionsauswahl, bevor Sie IAM Identity Center aktivieren, da die primäre Region nach der Aktivierung von IAM Identity Center nicht mehr geändert werden kann.

IAM Identity Center unterstützt die meisten Verwaltungsfunktionen nur in der primären Region. Dazu gehören die Verbindung zu einem externen Identitätsanbieter, die Synchronisation von Benutzern und Gruppen sowie die Erstellung und Zuweisung von Berechtigungssätzen für Benutzer und Gruppen. Im Gegensatz dazu müssen die Verwaltung von Anwendungen und deren Zuweisungen in der IAM Identity Center-Region erfolgen, in der die Anwendung erstellt wurde.

Note

[Auch wenn Ihr IAM Identity Center in weitere Regionen repliziert wird, empfehlen wir Ihnen, einen bruch sicheren Zugriff einzurichten AWS](#) . Auf diese Weise können Sie AWS den Zugriff für eine kleine Gruppe privilegierter Benutzer bei Ereignissen wie einer Dienstunterbrechung im externen IdP aufrechterhalten. [Der Notfallzugriff](#) ist eine weitere Option, bei der Identitäten von einem externen IdP anstelle von IAM-Benutzern verwendet werden. Er schützt jedoch nicht vor einer Unterbrechung des externen IdP.

Das IAM Identity Center bestimmt zwar den Zugriff von der Region aus, in der Sie den Dienst aktivieren, aber es handelt sich um globale Zugriffe. AWS-Konten Das bedeutet, dass Benutzer, nachdem sie sich bei IAM Identity Center angemeldet haben, in jeder Region operieren können, wenn sie AWS-Konten über IAM Identity Center darauf zugreifen. Die meisten AWS verwalteten

Anwendungen wie Amazon SageMaker AI müssen jedoch in einer Region Ihrer IAM Identity Center-Instance installiert sein, damit Benutzer sich authentifizieren und Zugriff auf diese Anwendungen zuweisen können. Informationen zu regionalen Einschränkungen bei der Verwendung einer Anwendung mit IAM Identity Center finden Sie in der Dokumentation zur Anwendung und [the section called “Bereitstellung und Verwaltung AWS verwalteter Anwendungen auf mehreren AWS-Regionen”](#)

Sie können IAM Identity Center auch verwenden, um den Zugriff auf vom SAML-based Kunden verwaltete Anwendungen zu authentifizieren und zu autorisieren, die über eine öffentliche URL erreichbar sind, unabhängig von der Plattform oder Cloud, auf der die Anwendung erstellt wurde.

Wir raten davon ab, sie [Konto-Instances von IAM Identity Center](#) als Mittel zur Implementierung von Resilienz zu verwenden, da sie den AWS Kontozugriff nicht unterstützen und weil sie einen zweiten, isolierten Kontrollpunkt schaffen, der nicht mit Ihrer Unternehmensinstanz verbunden ist.

Auf Verfügbarkeit ausgelegt

Die folgende Tabelle zeigt die Verfügbarkeit, die IAM Identity Center in einer einzelnen AWS Region erreichen soll. Diese Werte stellen kein Service Level Agreement oder eine Garantie dar, sondern geben vielmehr Aufschluss über die Designziele. Die Prozentsätze der Verfügbarkeit beziehen sich auf den Zugriff auf Daten oder Funktionen und nicht auf die Haltbarkeit (z. B. die langfristige Aufbewahrung von Daten).

Servicekomponente	Verfügbarkeitsdesignziel
Datenebene (einschließlich Anmeldung)	99.95%
Steuerebene	99.90%

Richten Sie den Notfallzugriff auf das ein AWS-Managementkonsole

IAM Identity Center basiert auf einer hochverfügbaren AWS Infrastruktur und verwendet eine Availability Zone-Architektur, um einzelne Fehlerquellen zu eliminieren. Für einen zusätzlichen Schutz im unwahrscheinlichen Fall eines IAM Identity Center oder einer AWS-Region Unterbrechung empfehlen wir Ihnen, eine Konfiguration einzurichten, die Sie für den temporären Zugriff auf das verwenden können. AWS-Managementkonsole

AWS ermöglicht Ihnen:

- [Connect Ihren Drittanbieter-IdP mit dem IAM Identity Center](#).
- Connect Ihren Drittanbieter-IdP mit einer Einzelperson, AWS-Konten indem Sie einen [SAML 2.0-basierten](#) Verbund verwenden.

Wenn Sie IAM Identity Center verwenden, können Sie diese Funktionen verwenden, um die in den folgenden Abschnitten beschriebene Notfallzugriffskonfiguration zu erstellen. Diese Konfiguration ermöglicht es Ihnen, IAM Identity Center als Zugriffsmechanismus zu AWS-Konto verwenden. Wenn das IAM Identity Center unterbrochen wird, können sich Ihre Benutzer für den Notfallbetrieb AWS-Managementkonsole über einen direkten Verbund anmelden, indem sie dieselben Anmeldeinformationen verwenden, die sie für den Zugriff auf ihre Konten verwenden. Diese Konfiguration funktioniert, wenn IAM Identity Center nicht verfügbar ist, die IAM-Datenebene und Ihr externer Identitätsanbieter (IdP) jedoch verfügbar sind. Wenn Sie nicht vom externen IdP abhängig sein möchten, sollten Sie die Einrichtung eines [AWS Break-Glass-Zugriffs](#) in Betracht ziehen

 Important

Wir empfehlen, dass Sie diese Konfiguration bereitstellen, bevor es zu einer Unterbrechung kommt, da Sie die Konfiguration nicht erstellen können, wenn Ihr Zugriff auf die erforderlichen IAM-Rollen ebenfalls unterbrochen ist. Testen Sie diese Konfiguration außerdem regelmäßig, um sicherzustellen, dass Ihr Team weiß, was zu tun ist, wenn IAM Identity Center unterbrochen wird.

Themen

- [Zusammenfassung der Konfiguration des Notfallzugriffs](#)
- [Wie gestalten Sie Ihre kritischen Operations-Rollen](#)
- [Wie planen Sie Ihr Zugriffsmodell](#)
- [Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#)
- [So erstellen Sie Ihre Notfallzugriffskonfiguration](#)
- [Aufgaben zur Notfallvorbereitung](#)
- [Failover-Prozess für Notfälle](#)
- [Kehren Sie zum normalen Betrieb zurück](#)
- [One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta](#)

- [One-time Einrichtung einer direkten IAM-Verbundanwendung mit ADFS](#)

Zusammenfassung der Konfiguration des Notfallzugriffs

Um den Notfallzugriff zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

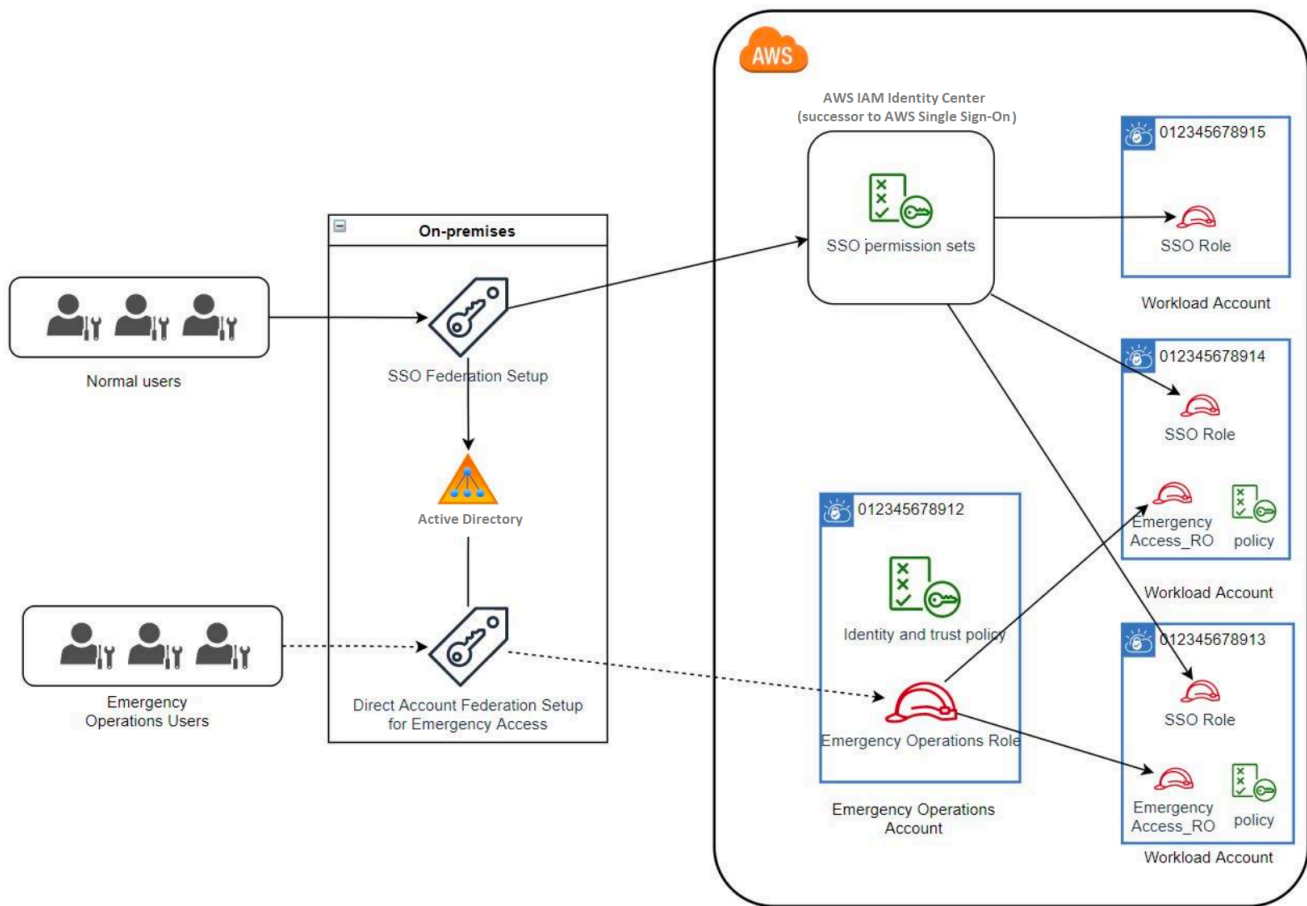
1. [Erstellen Sie in Ihrer Organisation ein Notfallkonto für den Betrieb von Notfällen AWS Organizations](#). Dieses Konto wird zu Ihrem Notfallkonto.
2. Connect Sie Ihren IdP mithilfe eines [SAML 2.0-basierten](#) Verbunds mit dem Notfalleinsatzkonto.
3. [Erstellen Sie im Notfallbetriebskonto eine Rolle für den Verbund von externen Identitätsanbietern](#). Erstellen Sie außerdem in jedem Ihrer Workload-Konten eine Notfalleinsatzrolle mit den erforderlichen Berechtigungen.
4. [Delegieren Sie den Zugriff auf Ihre Workload-Konten für die IAM-Rolle](#), die Sie im Notfallbetriebskonto erstellt haben. Um den Zugriff auf Ihr Notfalleinsatzkonto zu autorisieren, erstellen Sie in Ihrem IdP eine Notfalleinsatzgruppe ohne Mitglieder.
5. Ermöglichen Sie der Notfalleinsatzgruppe in Ihrem IdP, die Notfalleinsatzrolle zu verwenden, indem Sie in Ihrem IdP eine Regel erstellen, die den [SAML 2.0-Verbundzugriff auf die ermöglicht](#). AWS-Managementkonsole

Während des normalen Betriebs hat niemand Zugriff auf das Notfalleinsatzkonto, da die Notfalleinsatzgruppe in Ihrem IdP keine Mitglieder hat. Im Falle einer IAM Identity Center-Störung verwenden Sie Ihren IdP, um vertrauenswürdige Benutzer zur Notfalleinsatzgruppe in Ihrem IdP hinzuzufügen. Diese Benutzer können sich dann bei Ihrem IdP anmelden, zu dem AWS-Managementkonsole navigieren und die Rolle Notfallbetrieb im Notfalleinsatzkonto übernehmen. Von dort aus können diese Benutzer die [Rolle](#) für den Notfallzugriff in Ihren Workload-Konten übernehmen, wo sie Betriebsarbeiten ausführen müssen.

Wie gestalten Sie Ihre kritischen Operations-Rollen

Mit diesem Design konfigurieren Sie eine einzige Lösung, AWS-Konto in der Sie sich über IAM zusammenschließen, sodass Benutzer wichtige Betriebsrollen übernehmen können. Die Rollen für kritische Operationen verfügen über eine Vertrauensrichtlinie, die es Benutzern ermöglicht, eine entsprechende Rolle in Ihren Workload-Konten einzunehmen. Die Rollen in den Workload-Konten stellen die Berechtigungen bereit, die Benutzer benötigen, um wichtige Aufgaben auszuführen.

Das folgende Diagramm bietet einen Überblick über den Entwurf.



Wie planen Sie Ihr Zugriffsmodell

Bevor Sie den Notfallzugriff konfigurieren, erstellen Sie einen Plan, wie das Zugriffsmodell funktionieren soll. Gehen Sie wie folgt vor, um diesen Plan zu erstellen.

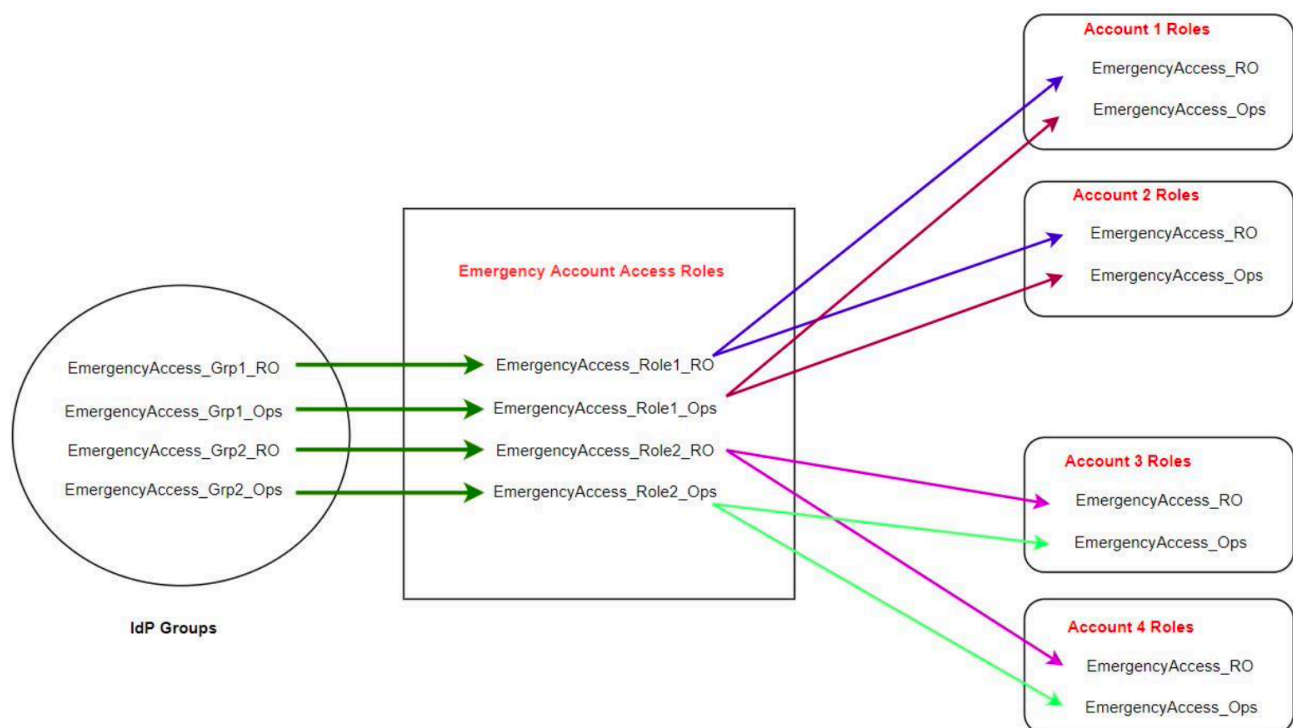
1. Identifizieren Sie die AWS-Konten Bereiche, in denen der Notfalldienst während einer Unterbrechung des IAM Identity Center unbedingt erforderlich ist. Beispielsweise sind Ihre Produktionskonten wahrscheinlich unverzichtbar, Ihre Entwicklungs- und Testkonten jedoch möglicherweise nicht.
2. Identifizieren Sie für diese Sammlung von Konten die spezifischen kritischen Rollen, die Sie in Ihren Konten benötigen. Definieren Sie bei all diesen Konten einheitlich, was die Rollen leisten können. Dies vereinfacht die Arbeit in Ihrem Notfallzugriffskonto, in dem Sie kontoübergreifende Rollen erstellen. Wir empfehlen, dass Sie in diesen Konten mit zwei unterschiedlichen Rollen beginnen: Read Only (RO) und Operations (Ops). Bei Bedarf können Sie weitere Rollen erstellen

und diese Rollen in Ihrem Setup einer eindeutigeren Gruppe von Benutzern mit Notfallzugriff zuordnen.

3. Identifizieren und erstellen Sie Notfallzugriffsgruppen in Ihrem IdP. Die Gruppenmitglieder sind die Benutzer, an die Sie den Zugriff auf Notfallzugriffsrollen delegieren.
4. Definieren Sie, welche Rollen diese Gruppen im Notfallzugriffskonto übernehmen können. Definieren Sie dazu in Ihrem IdP Regeln, die Ansprüche generieren, die auflisten, auf welche Rollen die Gruppe zugreifen kann. Diese Gruppen können dann Ihre Rollen „Nur Lesen“ oder „Operations“ im Notfallzugriffskonto übernehmen. Von diesen Rollen aus können sie die entsprechenden Rollen in Ihren Workload-Konten übernehmen.

Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle

Das folgende Diagramm zeigt, wie Sie Ihre Notfallzugriffsgruppen den Rollen in Ihrem Notfallzugriffskonto zuordnen. Das Diagramm zeigt auch die kontenübergreifenden Rollenvertrauensbeziehungen, die es Kontorollen mit Notfallzugriff ermöglichen, auf die entsprechenden Rollen in Ihren Workload-Konten zuzugreifen. Wir empfehlen, bei der Gestaltung Ihres Notfallplans diese Zuordnungen als Ausgangspunkt zu verwenden.



So erstellen Sie Ihre Notfallzugriffskonfiguration

Verwenden Sie die folgende Zuordnungstabelle, um Ihre Notfallzugriffskonfiguration zu erstellen. Diese Tabelle zeigt einen Plan, der zwei Rollen in den Workload-Konten umfasst: Read Only (RO) und Operations (Ops) mit den entsprechenden Vertrauens- und Berechtigungsrichtlinien. Die Vertrauensrichtlinien ermöglichen es den Notfallzugriffskontrollen, auf die einzelnen Workload-Kontrollen zuzugreifen. Die einzelnen Workload-Kontrollen verfügen auch über Berechtigungsrichtlinien für die Aufgaben, die die Rolle im Konto ausführen kann. Bei den Berechtigungsrichtlinien kann [AWS es sich um verwaltete Richtlinien](#) oder um vom [Kunden verwaltete Richtlinien handeln](#).

Account	Zu erstellende Rollen	Vertrauensrichtlinie	Berechtigungsrichtlinie
Konto 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Konto 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Konto 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Konto 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Konto für Notfallzugriff	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO	IdP	AssumeRole für die Rolle „Ressource“ im Konto

Account	Zu erstellende Rollen	Vertrauensrichtlinie	Berechtigungsrichtlinie
	Emergency Access_Role2_Ops		

In diesem Zuordnungsplan enthält das Notfallzugriffskonto zwei Rollen mit Schreibschutz und zwei Rollen für den Betrieb. Diese Rollen vertrauen darauf, dass Ihr IdP Ihre ausgewählten Gruppen authentifiziert und autorisiert, auf die Rollen zuzugreifen, indem er die Namen der Rollen in Assertionen weitergibt. In Workload Account 1 und Account 2 gibt es entsprechende Nur-Lese-Rollen und Operations-Rollen. Für Workload-Konto 1 vertraut die EmergencyAccess_R0 Rolle der Rolle, die sich im EmergencyAccess_Role1_R0 Notfallzugriffskonto befindet. In der Tabelle sind ähnliche Vertrauensmuster zwischen den Rollen „Schreibgeschützt“ und „Betrieb“ des Workload-Kontos und den entsprechenden Rollen für den Notfallzugriff angegeben.

Aufgaben zur Notfallvorbereitung

Um Ihre Notfallzugriffskonfiguration vorzubereiten, empfehlen wir Ihnen, die folgenden Aufgaben durchzuführen, bevor ein Notfall eintritt.

1. Richten Sie eine direkte IAM-Verbundanwendung in Ihrem IdP ein. Wenn Sie Okta oder eine andere externe Quelle IdPs als Identitätsquelle verwenden, finden Sie weitere Informationen unter [One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta](#). Wenn Sie Active Directory als Identitätsquelle verwenden, finden Sie weitere Informationen unter [One-time Einrichtung einer direkten IAM-Verbundanwendung mit ADFS](#).
2. Erstellen Sie eine IdP-Verbindung im Notfallzugriffskonto, auf die während der Veranstaltung zugegriffen werden kann.
3. Erstellen Sie Notfallzugriffsrollen in den Notfallzugriffskonten, wie in der obigen Zuordnungstabelle beschrieben.
4. Erstellen Sie temporäre Betriebsrollen mit Vertrauens- und Berechtigungsrichtlinien für jedes der Workload-Konten.
5. Erstellen Sie temporäre Betriebsgruppen in Ihrem IdP. Die Gruppennamen hängen von den Namen der temporären Betriebsrollen ab.
6. Testen Sie den direkten IAM-Verbund.
7. Deaktivieren Sie die IdP-Verbundanwendung in Ihrem IdP, um eine regelmäßige Nutzung zu verhindern.

Failover-Prozess für Notfälle

Wenn eine IAM Identity Center-Instanz nicht verfügbar ist und Sie feststellen, dass Sie Notfallzugriff auf die AWS Management Console gewähren müssen, empfehlen wir den folgenden Failover-Prozess.

1. Der IdP-Administrator aktiviert die direkte IAM-Verbundanwendung in Ihrem IdP.
2. Benutzer beantragen Zugriff auf die temporäre Betriebsgruppe über Ihren bestehenden Mechanismus, z. B. eine E-Mail-Anfrage, einen Slack-Channel oder eine andere Form der Kommunikation.
3. Benutzer, die Sie zu Ihren Notfallzugriffsgruppen hinzufügen, melden sich beim IdP an, wählen das Notfallzugriffskonto aus, und Benutzer wählen eine Rolle aus, die im Notfallzugriffskonto verwendet werden soll. Von diesen Rollen aus können sie Rollen in entsprechenden Workload-Konten übernehmen, denen kontenübergreifendes Vertrauen mit der Notfallkontrolle gilt.

Kehren Sie zum normalen Betrieb zurück

Überprüfen Sie im [AWS Health Dashboard](#), wann der Zustand des IAM Identity Center-Dienstes wiederhergestellt ist. Gehen Sie wie folgt vor, um zum normalen Betrieb zurückzukehren.

1. Wenn das Statussymbol für den IAM Identity Center-Dienst anzeigt, dass der Dienst fehlerfrei ist, melden Sie sich bei IAM Identity Center an.
2. Wenn Sie sich erfolgreich beim IAM Identity Center anmelden können, teilen Sie den Benutzern mit Notfallzugriff mit, dass IAM Identity Center verfügbar ist. Weisen Sie diese Benutzer an, sich abzumelden und sich über das AWS Zugriffsportal wieder bei IAM Identity Center anzumelden.
3. Nachdem sich alle Benutzer mit Notfallzugriff abgemeldet haben, deaktivieren Sie im IdP die IdP-Verbundanwendung. Wir empfehlen, dass Sie diese Aufgabe außerhalb der Geschäftszeiten ausführen.
4. Entfernen Sie alle Benutzer aus der Notfallzugriffsgruppe im IdP.

Ihre Rolleninfrastruktur für den Notfallzugriff bleibt als Backup-Zugriffsplan bestehen, ist aber jetzt deaktiviert.

One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta

1. Melden Sie sich als Benutzer mit Administratorrechten bei Ihrem Okta Konto an.

2. Wählen Sie in der Okta Admin-Konsole unter Anwendungen die Option Anwendungen aus.
3. Wählen Sie „App-Katalog durchsuchen“. Suchen Sie nach AWS Account Federation und wählen Sie es aus. Wählen Sie dann Integration hinzufügen.
4. Richten Sie einen direkten IAM-Verbund ein, AWS indem Sie die Schritte unter [So konfigurieren Sie SAML 2.0 für den AWS Kontoverbund](#) befolgen. Um regionale Ausfallszenarien zu bewältigen, empfehlen wir, bei der Konfiguration des Anmeldeendpunkts sowohl den nicht-regionalen Endpunkt als auch mehrere regionale Endpunkte für alle Regionen, in denen Sie tätig sind, zu aktivieren, um die Ausfallsicherheit des Verbunds zu verbessern. Bei der Konfiguration der ACS-URL für diesen Notfallzugriff empfehlen wir, dass Sie den regionalen Endpunkt einer anderen Region als der Region verwenden, in der Ihr IAM Identity Center bereitgestellt wird. Eine Liste der regionalen [Sign-in Endpunkte](#) finden Sie in der AWS Allgemeinen Referenz unter Endpunkte.
5. Wählen Sie auf der Registerkarte Sign-On Optionen die Option SAML 2.0 aus und geben Sie die Einstellungen für Gruppenfilter und Rollenwertmuster ein. Der Name der Gruppe für das Benutzerverzeichnis hängt vom Filter ab, den Sie konfigurieren.

Group Filter

`^aws\#\S+\#(?{role}}[\w\-\+)]\#(?{accountid}}\d+)\$`

Role Value Pattern

`arn:aws:iam::${accountid}:saml-provider/Okta,arn:aws:iam::${accountid}:role/${role}`

In der Abbildung oben bezieht sich die `role` Variable auf die Rolle „Notfallbetrieb“ in Ihrem Notfallzugriffskonto. Wenn Sie beispielsweise die `EmergencyAccess_Role1_R0` Rolle (wie in der Zuordnungstabelle beschrieben) in erstellen und Ihre Gruppenfiltereinstellung so konfiguriert ist AWS-Konto 123456789012, wie in der Abbildung oben gezeigt, sollte Ihr Gruppenname lauten `aws#EmergencyAccess_Role1_R0#123456789012`.

6. Erstellen Sie in Ihrem Verzeichnis (z. B. Ihrem Verzeichnis in Active Directory) die Notfallzugriffsgruppe und geben Sie einen Namen für das Verzeichnis an (z. B. `aws#EmergencyAccess_Role1_R0#123456789012`). Weisen Sie Ihre Benutzer dieser Gruppe zu, indem Sie Ihren vorhandenen Bereitstellungsmechanismus verwenden.
7. [Konfigurieren Sie im Notfallzugriffskonto eine benutzerdefinierte Vertrauensrichtlinie](#), die die erforderlichen Berechtigungen bereitstellt, damit die Notfallzugriffsrolle während einer Störung übernommen werden kann. Im Folgenden finden Sie eine Beispielanweisung für eine benutzerdefinierte Vertrauensrichtlinie, die der `EmergencyAccess_Role1_R0` Rolle zugeordnet ist. Eine Veranschaulichung finden Sie in der Abbildung unten unter dem Notfallkonto [Wie](#)

[gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#). Ersetzen Sie den Muster-ARN für den SAML-Anbieter durch den richtigen, den Sie im Notfallzugriffskonto erstellt haben. Ersetzen Sie die regionalen Endpunkte im Beispiel durch die Regionen Ihrer Wahl.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML PROVIDER NAME]"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": [
            "https://signin.aws.amazon.com/saml",
            "https://us-west-2.signin.aws.amazon.com/saml",
            "https://us-west-1.signin.aws.amazon.com/saml",
            "https://us-east-2.signin.aws.amazon.com/saml"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": "sts:SetSourceIdentity"
    }
  ]
}
```

8. Im Folgenden finden Sie eine Beispielanweisung für eine Berechtigungsrichtlinie, die der EmergencyAccess_Role1_R0 Rolle zugeordnet ist. Eine Veranschaulichung finden Sie in der Abbildung unten unter dem Notfallkonto [Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
        "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
      ]
    }
  ]
}
```

9. Konfigurieren Sie für die Workload-Konten eine benutzerdefinierte Vertrauensrichtlinie. Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie, die der EmergencyAccess_R0 Rolle zugeordnet ist. In diesem Beispiel 123456789012 ist Konto das Notfallzugriffskonto. Eine Veranschaulichung finden Sie in der Abbildung unten unter Workload-Konto [Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```



```
}
```

Note

In den IdPs meisten Fällen können Sie eine Anwendungsintegration so lange deaktivieren, bis sie benötigt wird. Wir empfehlen Ihnen, die direkte IAM-Verbundanwendung in Ihrem IdP so lange deaktiviert zu lassen, bis sie für den Notfallzugriff benötigt wird.

One-time Einrichtung einer direkten IAM-Verbundanwendung mit ADFS

In diesem Handbuch wird der einmalige Einrichtungsprozess für die Konfiguration des direkten IAM-Verbunds beschrieben, um den Notfallzugriff ADFS zu ermöglichen, AWS-Konten wenn das IAM Identity Center nicht verfügbar ist.

Voraussetzungen

Wenn Sie eine Konfiguration ADFS mit AWS Managed Microsoft AD planen, empfehlen wir aus Gründen der Ausfallsicherheit, zunächst die [Multi-Region Replikation zu konfigurieren](#) und mit den folgenden Schritten in der zusätzlichen Region und nicht in der primären Region fortzufahren.

Planen Sie Ihre Active Directory-Gruppenbenennungskonvention

Erstellen Sie AD-Gruppen mithilfe eines bestimmten Benennungsmusters, das einen automatisierten Abgleich zwischen Gruppennamen und AWS IAM-Rollen ermöglicht.

Format der Gruppenbenennung: AWS-<AccountNumber>-<RoleName>

Eine Veranschaulichung finden Sie in der Abbildung unten unter dem Notfallkonto [Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#). Wenn ein Benutzer dieser Gruppe zugewiesen wird, erhält er Zugriff auf die EmergencyAccess_Role1_R0 Rolle im Konto123456789012. Wenn ein Benutzer mehreren Gruppen zugeordnet ist, wird ihm eine Liste der verfügbaren Rollen angezeigt AWS-Konto und er kann auswählen, welche Rolle er annehmen möchte.

AWS configuration

Das komplette Setup umfasst Konfigurationen für ein Notfallzugriffskonto und die Workload-Konten. Eine Veranschaulichung der Gesamtkonfiguration finden Sie unter [Wie gestaltet man die Rollen-, Konto- und Gruppenzuordnungen für Notfälle](#).

1. [Erstellen Sie einen SAML-Identitätsanbieter](#)
2. [Rollen für den Notfallzugriff erstellen](#)
3. [Konfigurieren Sie die Rollen der Workload-Konten](#)

Erstellen Sie einen SAML-Identitätsanbieter

Erstellen Sie im Notfallzugriffskonto einen SAML-Identitätsanbieter in IAM, indem Sie die Schritte unter [SAML-Identitätsanbieter in IAM erstellen](#) ausführen. Laden Sie die erforderlichen Metadaten von Ihrem Server herunter: ADFS

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

Rollen für den Notfallzugriff erstellen

[Erstellen Sie Notfallzugriffsrollen](#) im Notfallkonto, indem Sie den SAML 2.0-Verbund als vertrauenswürdigen Entitätstyp verwenden. Wählen Sie den SAML 2.0-Anbieter aus, den Sie im vorherigen Schritt erstellt haben.

Überlegungen:

- Schließen Sie alle Regionen ein, in denen Sie tätig sind — wählen Sie alle Regionen aus, in denen Sie aktive Workloads haben, um sicherzustellen, dass der Verbund auch während einer regionalen Unterbrechung verfügbar bleibt.
- Konfigurieren Sie mindestens einen zusätzlichen regionalen Endpunkt, auch wenn Sie in einer einzigen Region tätig sind. Wenn Sie beispielsweise nur in einer Region tätig sind us-east-1, fügen Sie ihn us-west-2 als sekundären Endpunkt hinzu. Sie können einen Failover Ihres IdP zum us-west-2 SAML-Anmeldeendpunkt durchführen und trotzdem auf Ihre us-east-1 Ressourcen zugreifen, auch ohne dass Workloads eingehen. us-west-2
- Aktivieren Sie sowohl den nichtregionalen Endpunkt als auch die regionalen Endpunkte — Der überregionale Endpunkt (<https://signin.aws.amazon.com/saml>) ist zwar hochverfügbar, wird aber auf einem einzigen Server gehostet, während regionale Endpunkte (<https://>

<region>.signin.aws.amazon.com/saml) die Ausfallsicherheit verbessern AWS-Regionus-east-1, indem sie die Abhängigkeit von einem einzigen globalen Endpunkt verringern.

Konfigurieren Sie die Vertrauensrichtlinie

Ein Beispiel [One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta](#) für eine Vertrauensrichtlinie mit mehreren regionalen Endpunkten für die Anmeldung finden Sie unter. Ersetzen Sie die Beispiel-Regionalendpunkte und die ARNs der SAML-Anbieter durch Ihre eigenen.

Konfigurieren Sie Berechtigungsrichtlinien

Ein Beispiel [One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta](#) für eine Berechtigungsrichtlinie, die Sie den Notfallzugriffsrollen zuordnen, finden Sie unter.

Konfigurieren Sie die Rollen der Workload-Konten

Konfigurieren Sie für die Workload-Kontrollen eine benutzerdefinierte Vertrauensrichtlinie, die es den Notfallzugriffsrollen im Notfallzugriffskonto ermöglicht, sie zu übernehmen. Ein Beispiel [One-time Einrichtung einer direkten IAM-Verbundanwendung in Okta](#) für eine Vertrauensrichtlinie finden Sie, wobei Konto das Notfallzugriffskonto 123456789012 ist.

Active Directory-Konfiguration

In den folgenden Schritten wird beschrieben, wie Active Directory und ADFS der Notfallzugriff konfiguriert werden.

1. [Gruppen erstellen](#)
2. [Erstellen Sie eine vertrauende Partei](#)
3. [Regeln für Ansprüche erstellen](#)

Gruppen erstellen

Erstellen Sie Notfallgruppen in Active Directory gemäß der zuvor beschriebenen Namenskonvention (z. B. AWS-123456789012-EmergencyAccess_Role1_R0). Weisen Sie diesen Gruppen mithilfe Ihrer vorhandenen Bereitstellungsmechanismen Benutzer zu.

Erstellen Sie eine vertrauende Partei

ADFSFür den Verbund ist eine Konfiguration der vertrauenden Partei erforderlich. Die vertrauende Partei ist AWS -Security-Token-Service (AWS STS), die die Authentifizierung an ADFS den Identitätsanbieter auslagert.

1. Wählen Sie in der ADFS Managementkonsole im Aktionsmenü die Option Vertrauensstellung der vertrauenden Partei hinzufügen aus. Wählen Sie Claims Aware aus, wenn Sie eine vertrauende Partei hinzufügen.
2. Geben Sie für Verbund-Metadaten die Metadaten-URL aus den Metadateninformationen des Identitätsanbieters auf der IAM-Konsole ein. Beispiel:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. Legen Sie den Anzeigenamen für die vertrauende Partei fest (z. B. AWS Kontozugriff) und wählen Sie dann Weiter.
4. Wählen Sie aus, wem Sie Zugriff gewähren möchten AWS. Sie können bestimmte Gruppen auswählen und Anforderungen wie MFA definieren.
5. Wählen Sie auf der Seite „Fertig stellen“ die Option „Schließen“, um den Assistenten zum Hinzufügen vertrauensvoller Parteien abzuschließen. AWS ist jetzt als vertrauende Partei konfiguriert.

Regeln für Ansprüche erstellen

ADFSverwendet die Claims Rule Language, um Ansprüche zwischen Antragstellern und vertrauenden Parteien auszustellen und zu transformieren. Sie müssen vier Anspruchsregeln erstellen:NameId,RoleSessionName, Get AD Groups und Roles for AWS Access.

Right-click klicken Sie auf die vertrauende Partei und wählen Sie dann „Richtlinie zur Ausstellung von Ansprüchen bearbeiten“. Wählen Sie Regel hinzufügen, um Regeln hinzuzufügen.

1NameId.

- a. Wählen Sie „Eingehenden Anspruch umwandeln“ und anschließend „Weiter“.
- b. Verwenden Sie die folgenden Einstellungen:
 - Name der Anspruchsregel: NameId
 - Art des eingehenden Antrags: Windows Account Name

- Art des ausgehenden Antrags: Name ID
- ID-Format für ausgehende Namen: Persistent Identifier
- Alle Antragswerte durchgehen: aktiviert

c. Wählen Sie OK aus.

2. RoleSessionName

- a. Klicken Sie auf Add Rule (Regel hinzufügen).
- b. Wählen Sie in der Liste der Vorlagen für Anspruchsregeln die Option LDAP-Attribute als Ansprüche senden aus.

c. Verwenden Sie die folgenden Einstellungen:

- Name der Anspruchsregel: RoleSessionName
- Attributspeicher: Active Directory
- LDAP-Attribut: E-Mail-Addresses
- Art des ausgehenden Anspruchs: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`

d. Wählen Sie OK aus.

3. Holen Sie sich AD-Gruppen

- a. Klicken Sie auf Add Rule (Regel hinzufügen).
- b. Wählen Sie in der Liste der Vorlagen für Anspruchsregeln die Option Ansprüche mithilfe einer benutzerdefinierten Regel senden aus und klicken Sie dann auf Weiter.
- c. Geben Sie Get AD Groups als Name der Anspruchsregel Folgendes ein und geben Sie dann im Feld Benutzerdefinierte Regel Folgendes ein:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Diese benutzerdefinierte Regel verwendet ein Skript in der Sprache der Anspruchsregeln, das alle Gruppen abrufen, in denen der authentifizierte Benutzer Mitglied ist, und sie in einen temporären Anspruch mit dem Namen einfügt. `http://temp/variable`

 Note

Stellen Sie sicher, dass kein Leerzeichen am Ende steht, um unerwartete Ergebnisse zu vermeiden.

4. Rollenattribute

- a. Klicken Sie auf Add Rule (Regel hinzufügen).
- b. Wählen Sie in der Liste der Vorlagen für Anspruchsregeln die Option Ansprüche mithilfe einer benutzerdefinierten Regel senden aus und klicken Sie dann auf Weiter.
- c. Geben Sie Roles als Name der Anspruchsregel Folgendes ein und geben Sie dann im Feld Benutzerdefinierte Regel Folgendes ein:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]  
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/  
<ADFS>,arn:aws:iam::$1:role/"));
```

Diese benutzerdefinierte Regel verwendet reguläre Ausdrücke, um jede Gruppenmitgliedschaft des Formulars AWS-<Account Number>-<Role Name> in das erwartete ARN-Formular für die IAM-Rolle und ARN ARN-Formular des IAM-Verbundanbieters umzuwandeln. AWS

 Note

Im obigen Beispiel ADFS steht die Regelsprache für den logischen Namen, der dem SAML-Identitätsanbieter im Identitätsanbieter-Setup gegeben wurde. AWS Ändern Sie dies auf der Grundlage des logischen Namens, den Sie in der IAM-Konsole für Ihren Identitätsanbieter ausgewählt haben.

Testen der Konfiguration

Testen Sie, ob die Lösung funktioniert, indem Sie sich unter authentifizieren. `https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx` Wählen Sie den Namen der vertrauenden Partei, die Sie erstellt haben, aus der Dropdownliste der Websites aus.

Aktualisieren Sie den standardmäßigen SAML-Assertion-Endpunkt in ADFS

Important

Bei der Konfiguration des Vertrauens der vertrauenden Partei wird standardmäßig der SAML-Assertion-Endpunkt auf den Endpunkt gesetzt `https://signin.aws.amazon.com/`, der kein globaler Endpunkt ist und sich in befindet. ADFS us-east-1 Wir empfehlen, dass Sie den Standardendpunkt auf einen regionalen Endpunkt ändern, der sich von dem unterscheidet, an dem Ihr IAM Identity Center aus Gründen der Resilienz konfiguriert ist. Wenn Ihr IAM Identity Center beispielsweise in bereitgestellt wird us-east-1 und Sie dort auch arbeiten us-west-2, ändern Sie den standardmäßigen SAML Assertion-Verbraucherendpunkt auf `https://us-west-2.signin.aws.amazon.com/saml`

1. Wählen Sie „Eigenschaften“ für den Trust der vertrauenden Partei aus und wechseln Sie zur Registerkarte „Überwachung“. Deaktivieren Sie das Kontrollkästchen Vertrauende Partei automatisch aktualisieren.
2. Gehen Sie zur Registerkarte Endpunkte, wählen Sie Ihren bevorzugten Anmeldeendpunkt aus und klicken Sie auf Bearbeiten.
3. Aktivieren Sie das Kontrollkästchen Vertrauenswürdige URL als Standard festlegen. Wählen Sie OK und Anwenden, damit die Einstellung wirksam wird.

Note

In den IdPs meisten Fällen können Sie eine Anwendungsintegration so lange deaktivieren, bis sie benötigt wird. Wir empfehlen Ihnen, die direkte IAM-Verbundanwendung in Ihrem IdP so lange deaktiviert zu lassen, bis sie für den Notfallzugriff benötigt wird.

Sicherheit bei AWS IAM Identity Center

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die auf die Anforderungen der sicherheitsrelevantesten Organisationen zugeschnitten sind.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- **Sicherheit der Cloud** — AWS ist für den Schutz der Infrastruktur verantwortlich, auf der AWS Dienste in der AWS Cloud ausgeführt werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Auditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsvorkehrungen im Rahmen der [AWS Compliance-Programme](#). Weitere Informationen zu den Compliance-Programmen, die für Folgendes gelten AWS IAM Identity Center, finden Sie unter [AWS Services im Umfang der einzelnen Compliance-Programme](#).
- **Sicherheit in der Cloud** — Ihre Verantwortung hängt von dem AWS Dienst ab, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von IAM Identity Center anwenden. Die folgenden Themen zeigen Ihnen, wie Sie IAM Identity Center so konfigurieren, dass Ihre Sicherheits- und Compliance-Ziele erreicht werden. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, mit denen Sie Ihre IAM Identity Center-Ressourcen überwachen und sichern können.

Topics

- [Identitäts- und Zugriffsmanagement für IAM Identity Center](#)
- [IAM Identity Center-Konsole und API-Autorisierung](#)
- [AWS STS Bedingungskontextschlüssel für IAM Identity Center](#)
- [Protokollierung und Überwachung im IAM Identity Center](#)
- [Konformitätsüberprüfung für IAM Identity Center](#)
- [Resilienz im IAM Identity Center](#)
- [Infrastruktursicherheit im IAM Identity Center](#)

Identitäts- und Zugriffsmanagement für IAM Identity Center

Für den Zugriff auf IAM Identity Center sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen verfügen, z. B. auf eine AWS verwaltete Anwendung.

Die Authentifizierung für das AWS Zugriffsportal wird durch das Verzeichnis gesteuert, das Sie mit IAM Identity Center verbunden haben. Die Autorisierung für die AWS-Konten, die Benutzern im AWS Access Portal zur Verfügung stehen, wird jedoch von zwei Faktoren bestimmt:

1. Wem wurde der Zugriff auf die Benutzer AWS-Konten in der IAM Identity Center-Konsole zugewiesen. Weitere Informationen finden Sie unter [Single-Sign-On-Zugriff auf AWS-Konten](#).
2. Welche Berechtigungsebenen wurden den Benutzern in der IAM Identity Center-Konsole gewährt, um ihnen den entsprechenden Zugriff auf diese zu gewähren. AWS-Konten Weitere Informationen finden Sie unter [Berechtigungssätze erstellen, verwalten und löschen](#).

In den folgenden Abschnitten wird erläutert, wie Sie als Administrator den Zugriff auf die IAM Identity Center-Konsole kontrollieren oder den Administratorzugriff für alltägliche Aufgaben von der IAM Identity Center-Konsole aus delegieren können.

- [Authentifizierung](#)
- [Zugriffskontrolle](#)

Authentifizierung

Erfahren Sie, wie Sie AWS mithilfe [von IAM-Identitäten darauf zugreifen](#).

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen zu authentifizieren, aber ohne entsprechende Berechtigungen können Sie keine IAM Identity Center-Ressourcen erstellen oder darauf zugreifen. Beispielsweise benötigen Sie Berechtigungen, um ein mit IAM Identity Center verbundenes Verzeichnis zu erstellen.

Note

Wenn Ihre IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist, benötigen Ihre IAM Identity Center-Administratoren und andere Akteure, die

Zugriff auf den KMS-Schlüssel benötigen, zusätzliche Berechtigungen. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).

In den folgenden Abschnitten wird beschrieben, wie Sie Berechtigungen für IAM Identity Center verwalten. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen](#)
- [Identity-based Beispiele für Richtlinien für IAM Identity Center](#)
- [Resource-based Beispiel für eine Richtlinie für IAM Identity Center](#)
- [Verwenden von dienstverknüpften Rollen für IAM Identity Center](#)

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen werden durch Berechtigungsrichtlinien geregelt. Um Zugriff zu gewähren, kann ein Kontoadministrator IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungen hinzufügen. Einige Dienste (z. B. AWS Lambda) unterstützen auch das Hinzufügen von Berechtigungen zu Ressourcen.

Note

Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter [Bewährte Methoden für IAM](#) im IAM-Benutzerhandbuch.

Themen

- [Ressourcen und Abläufe im IAM Identity Center](#)
- [Grundlegendes zum Eigentum an Ressourcen](#)
- [Verwaltung des Zugriffs auf -Ressourcen](#)
- [Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipale](#)
- [Angaben von Bedingungen in einer Richtlinie](#)

Ressourcen und Abläufe im IAM Identity Center

In IAM Identity Center sind die primären Ressourcen Anwendungsinstanzen, Profile und Berechtigungssätze.

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist derjenige AWS-Konto, der eine Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist die AWS-Konto Hauptentität (das Konto, ein Benutzer oder eine IAM-Rolle), die die Anforderung authentifiziert, mit der die Ressource erstellt wird. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn der eine IAM Identity Center-Ressource Root-Benutzer des AWS-Kontos erstellt, z. B. eine Anwendungsinstanz oder einen Berechtigungssatz, sind Sie AWS-Konto der Eigentümer dieser Ressource.
- Wenn Sie einen Benutzer in Ihrem AWS Konto erstellen und diesem Benutzer Berechtigungen zum Erstellen von IAM Identity Center-Ressourcen gewähren, kann der Benutzer dann IAM Identity Center-Ressourcen erstellen. Ihr AWS Konto, zu dem der Benutzer gehört, ist jedoch Eigentümer der Ressourcen.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Erstellen von IAM Identity Center-Ressourcen erstellen, kann jeder, der diese Rolle übernehmen kann, IAM Identity Center-Ressourcen erstellen. Ihr AWS-Konto, zu dem die Rolle gehört, ist Eigentümer der IAM Identity Center-Ressourcen.

Verwaltung des Zugriffs auf -Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

Note

In diesem Abschnitt wird die Verwendung von IAM im Kontext von IAM Identity Center beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter [Was ist IAM?](#) im IAM-Benutzerhandbuch. Informationen über die Syntax und Beschreibungen von IAM-Richtlinien finden Sie in der [AWS -IAM-Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

An eine IAM-Identität angefügte Richtlinien werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. An Ressourcen angehängte Richtlinien werden als ressourcenbasierte Richtlinien bezeichnet. IAM Identity Center unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- [Identity-based Richtlinien \(IAM-Richtlinien\)](#)
- [Resource-based Richtlinien](#)

Identity-based Richtlinien (IAM-Richtlinien)

Sie können IAM-Identitäten Berechtigungen hinzufügen. Sie können z. B. Folgendes tun:

- Hängen Sie eine Berechtigungsrichtlinie an einen Benutzer oder eine Gruppe in Ihrem AWS-Konto — Ein Kontoadministrator kann eine Berechtigungsrichtlinie verwenden, die einem bestimmten Benutzer zugeordnet ist, um diesem Benutzer Berechtigungen zum Hinzufügen einer IAM Identity Center-Ressource, z. B. einer neuen Anwendung, zu erteilen.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen.

Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter [Zugriffsverwaltung](#) im IAM-Benutzerhandbuch.

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit `beginne List` beginnt. Diese Aktionen zeigen Informationen zu einer IAM Identity Center-Ressource an, z. B. zu einer Anwendungsinstanz oder einem Berechtigungssatz. Beachten Sie, dass das Platzhalterzeichen (*) im Resource Element angibt, dass die Aktionen für alle IAM Identity Center-Ressourcen zulässig sind, die dem Konto gehören.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sso:List*",
      "Resource": "*"
    }
  ]
}
```

```
}  
  ]  
}
```

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit IAM Identity Center finden Sie unter [Identity-based Beispiele für Richtlinien für IAM Identity Center](#). Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter [Identitäten \(Benutzer, Gruppen und Rollen\)](#) im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Andere Services, z. B. Amazon-S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. IAM Identity Center unterstützt keine ressourcenbasierten Richtlinien.

Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipale

Für jede IAM Identity Center-Ressource (siehe [Ressourcen und Abläufe im IAM Identity Center](#)) definiert der Service eine Reihe von API-Vorgängen. Um Berechtigungen für diese API-Operationen zu gewähren, definiert IAM Identity Center eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können. Zur Durchführung einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- **Ressource** – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt.
- **Aktion** – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Die `sso:DescribePermissionsPolicies` Berechtigung ermöglicht es den Benutzern beispielsweise, den IAM Identity DescribePermissionsPolicies Center-Vorgang auszuführen.
- **Auswirkung** – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("allow"), ist der Zugriff automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.

- **Prinzipal** – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). IAM Identity Center unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der [AWS -IAM-Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der Sprache der Zugriffsrichtlinie die Bedingungen angeben, die erfüllt werden müssen, damit die Richtlinie in Kraft tritt. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtlinienyntax finden Sie im Thema [Bedingung](#) im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Es gibt keine spezifischen Bedingungsschlüssel für IAM Identity Center. Es gibt jedoch AWS Bedingungsschlüssel, die Sie bei Bedarf verwenden können. Eine vollständige Liste der AWS Schlüssel finden Sie unter [Verfügbare globale Bedingungsschlüssel](#) im IAM-Benutzerhandbuch.

Identity-based Beispiele für Richtlinien für IAM Identity Center

Dieses Thema enthält Beispiele für IAM-Richtlinien, die Sie erstellen können, um Benutzern und Rollen Berechtigungen zur Verwaltung von IAM Identity Center zu gewähren.

Important

Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die grundlegenden Konzepte und Optionen erläutert werden, die Ihnen zur Verwaltung des Zugriffs auf Ihre IAM Identity Center-Ressourcen zur Verfügung stehen. Weitere Informationen finden Sie unter [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen](#).

Dieses Thema besteht aus folgenden Abschnitten:

- [Beispiele für benutzerdefinierte Richtlinien](#)

- [Für die Verwendung der IAM Identity Center-Konsole sind Berechtigungen erforderlich](#)

Beispiele für benutzerdefinierte Richtlinien

Dieser Abschnitt enthält Beispiele für häufige Anwendungsfälle, die eine benutzerdefinierte IAM-Richtlinie erfordern. Bei diesen Beispielrichtlinien handelt es sich um identitätsbasierte Richtlinien, die das Principal-Element nicht angeben. Das liegt daran, dass Sie bei einer identitätsbasierten Richtlinie nicht den Prinzipal angeben, der die Berechtigung erhält. Stattdessen hängen Sie die Richtlinie an den Prinzipal an. Wenn Sie einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuordnen, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen. Sie können identitätsbasierte Richtlinien in IAM erstellen und sie Benutzern, Gruppen und Rollen zuordnen. and/or Sie können diese Richtlinien auch auf IAM Identity Center-Benutzer anwenden, wenn Sie einen Berechtigungssatz in IAM Identity Center erstellen.

Note

Verwenden Sie diese Beispiele, wenn Sie Richtlinien für Ihre Umgebung erstellen, und stellen Sie sicher, dass Sie sowohl positive („Zugriff gewährt“) als auch negative („Zugriff verweigert“) Testfälle testen, bevor Sie diese Richtlinien in Ihrer Produktionsumgebung bereitstellen. Weitere Informationen zum Testen von IAM-Richtlinien finden Sie unter [Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator](#) im IAM-Benutzerhandbuch.

Themen

- [Beispiel 1: Erlauben Sie einem Benutzer, das IAM Identity Center anzuzeigen](#)
- [Beispiel 2: Erlauben Sie einem Benutzer die Verwaltung von Berechtigungen für AWS-Konten im IAM Identity Center](#)
- [Beispiel 3: Erlauben Sie einem Benutzer, Anwendungen im IAM Identity Center zu verwalten](#)
- [Beispiel 4: Erlauben Sie einem Benutzer, Benutzer und Gruppen in Ihrem Identity Center-Verzeichnis zu verwalten](#)

Beispiel 1: Erlauben Sie einem Benutzer, das IAM Identity Center anzuzeigen

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Leseberechtigungen, sodass er alle in IAM Identity Center konfigurierten Einstellungen und Verzeichnisinformationen einsehen kann.

 Note

Diese Richtlinie dient nur zu Beispielzwecken. In einer Produktionsumgebung empfehlen wir, die ViewOnlyAccess AWS verwaltete Richtlinie für IAM Identity Center zu verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListAccountAssignments",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListPermissionSets",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso-directory:DescribeDirectory",
        "sso-directory:SearchUsers",
        "sso-directory:SearchGroups"
      ],
      "Resource": "*"
    }
  ]
}
```



```
}
```

Beispiel 2: Erlauben Sie einem Benutzer die Verwaltung von Berechtigungen für AWS-Konten im IAM Identity Center

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, die es einem Benutzer ermöglichen, Berechtigungssätze für Sie zu erstellen, zu verwalten und bereitzustellen. AWS-Konten

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AttachManagedPolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:CreatePermissionSet",
        "sso>DeleteAccountAssignment",
        "sso>DeleteInlinePolicyFromPermissionSet",
        "sso>DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:UpdatePermissionSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMListPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:ListPolicies"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AccessToSSOProvisionedRoles",
      "Effect": "Allow",
```

```

        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:GetRole",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription"
        ],
        "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:GetSAMLProvider"
        ],
        "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
    }
]
}

```

Note

Die zusätzlichen Berechtigungen "Sid": "IAMListPermissions", die in den "Sid": "AccessToSSOProvisionedRoles" Abschnitten und aufgeführt sind, sind nur erforderlich, damit der Benutzer Aufgaben im AWS Organizations Verwaltungskonto erstellen kann. In bestimmten Fällen müssen Sie diese Abschnitte möglicherweise auch erweitern `iam:UpdateSAMLProvider`.

Beispiel 3: Erlauben Sie einem Benutzer, Anwendungen im IAM Identity Center zu verwalten

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, die es einem Benutzer ermöglichen, Anwendungen in IAM Identity Center anzuzeigen und zu konfigurieren, einschließlich vorintegrierter SaaS-Anwendungen aus dem IAM Identity Center-Katalog.

 Note

Der im folgenden Richtlinienbeispiel verwendete `sso:AssociateProfile` Vorgang ist für die Verwaltung von Benutzer- und Gruppenzuweisungen zu Anwendungen erforderlich. Außerdem kann ein Benutzer Benutzer und Gruppen AWS-Konten mithilfe vorhandener Berechtigungssätze zuweisen. Wenn ein Benutzer den AWS-Konto Zugriff innerhalb von IAM Identity Center verwalten muss und die für die Verwaltung von Berechtigungssätzen erforderlichen Berechtigungen benötigt, finden Sie weitere Informationen unter [Beispiel 2: Erlauben Sie einem Benutzer die Verwaltung von Berechtigungen für AWS-Konten im IAM Identity Center](#).

Seit Oktober 2020 sind viele dieser Operationen nur über die AWS Konsole verfügbar. Diese Beispielrichtlinie umfasst „Lesen“-Aktionen wie Auflisten, Abrufen und Suchen, die für den fehlerfreien Betrieb der Konsole in diesem Fall relevant sind.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AssociateProfile",
        "sso:CreateApplicationInstance",
        "sso:ImportApplicationInstanceServiceProviderMetadata",
        "sso>DeleteApplicationInstance",
        "sso>DeleteProfile",
        "sso:DisassociateProfile",
        "sso:GetApplicationTemplate",
        "sso:UpdateApplicationInstanceServiceProviderConfiguration",
        "sso:UpdateApplicationInstanceDisplayData",
        "sso>DeleteManagedApplicationInstance",
        "sso:UpdateApplicationInstanceStatus",
        "sso:GetManagedApplicationInstance",
        "sso:UpdateManagedApplicationInstanceStatus",
        "sso>CreateManagedApplicationInstance",
        "sso:UpdateApplicationInstanceSecurityConfiguration",
        "sso:UpdateApplicationInstanceResponseConfiguration",

```

```

        "sso:GetApplicationInstance",
        "sso:CreateApplicationInstanceCertificate",
        "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
        "sso:UpdateApplicationInstanceActiveCertificate",
        "sso:DeleteApplicationInstanceCertificate",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationTemplates",
        "sso:ListApplications",
        "sso:ListApplicationInstances",
        "sso:ListDirectoryAssociations",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:ListInstances",
        "sso:GetProfile",
        "sso:GetSSOStatus",
        "sso:GetSsoConfiguration",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}
]
}

```

Beispiel 4: Erlauben Sie einem Benutzer, Benutzer und Gruppen in Ihrem Identity Center-Verzeichnis zu verwalten

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, die es einem Benutzer ermöglichen, Benutzer und Gruppen in IAM Identity Center zu erstellen, anzuzeigen, zu ändern und zu löschen.

In einigen Fällen sind direkte Änderungen an Benutzern und Gruppen in IAM Identity Center eingeschränkt. Zum Beispiel, wenn Active Directory oder ein externer Identitätsanbieter mit aktivierter automatischer Bereitstellung als Identitätsquelle ausgewählt wird.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "sso-directory:ListGroupForUser",
          "sso-directory:DisableUser",
          "sso-directory:EnableUser",
          "sso-directory:SearchGroups",
          "sso-directory>DeleteGroup",
          "sso-directory:AddMemberToGroup",
          "sso-directory:DescribeDirectory",
          "sso-directory:UpdateUser",
          "sso-directory:ListMembersInGroup",
          "sso-directory:CreateUser",
          "sso-directory:DescribeGroups",
          "sso-directory:SearchUsers",
          "sso:ListDirectoryAssociations",
          "sso-directory:RemoveMemberFromGroup",
          "sso-directory>DeleteUser",
          "sso-directory:DescribeUsers",
          "sso-directory:UpdateGroup",
          "sso-directory:CreateGroup"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

Für die Verwendung der IAM Identity Center-Konsole sind Berechtigungen erforderlich

Damit ein Benutzer fehlerfrei mit der IAM Identity Center-Konsole arbeiten kann, sind zusätzliche Berechtigungen erforderlich. Wenn eine IAM-Richtlinie erstellt wurde, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Benutzer mit dieser Richtlinie nicht wie vorgesehen. Im folgenden Beispiel sind die Berechtigungen aufgeführt, die möglicherweise erforderlich sind, um einen fehlerfreien Betrieb innerhalb der IAM Identity Center-Konsole sicherzustellen.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "sso:DescribeAccountAssignmentCreationStatus",
      "sso:DescribeAccountAssignmentDeletionStatus",
      "sso:DescribePermissionSet",
      "sso:DescribePermissionSetProvisioningStatus",
      "sso:DescribeRegisteredRegions",
      "sso:GetApplicationInstance",
      "sso:GetApplicationTemplate",
      "sso:GetInlinePolicyForPermissionSet",
      "sso:GetManagedApplicationInstance",
      "sso:GetMfaDeviceManagementForDirectory",
      "sso:GetPermissionSet",
      "sso:GetProfile",
      "sso:GetSharedSsoConfiguration",
      "sso:GetSsoConfiguration",
      "sso:GetSSOStatus",
      "sso:GetTrust",
      "sso:ListAccountAssignmentCreationStatus",
      "sso:ListAccountAssignmentDeletionStatus",
      "sso:ListAccountAssignments",
      "sso:ListAccountsForProvisionedPermissionSet",
      "sso:ListApplicationInstanceCertificates",
      "sso:ListApplicationInstances",
      "sso:ListApplications",
      "sso:ListApplicationTemplates",
      "sso:ListDirectoryAssociations",
      "sso:ListInstances",
      "sso:ListManagedPoliciesInPermissionSet",
      "sso:ListPermissionSetProvisioningStatus",
      "sso:ListPermissionSets",
      "sso:ListPermissionSetsProvisionedToAccount",
      "sso:ListProfileAssociations",
      "sso:ListProfiles",
      "sso:ListTagsForResource",
      "sso-directory:DescribeDirectory",
      "sso-directory:DescribeGroups",
      "sso-directory:DescribeUsers",
      "sso-directory:ListGroupsForUser",
      "sso-directory:ListMembersInGroup",
      "sso-directory:SearchGroups",

```

```

        "sso-directory:SearchUsers"
      ],
      "Resource": "*"
    }
  ]
}

```

Resource-based Beispiel für eine Richtlinie für IAM Identity Center

Jede Anwendung, die mit IAM Identity Center zusammenarbeitet und [OAuth 2.0 verwendet](#), benötigt eine ressourcenbasierte Richtlinie. Die Anwendung kann vom Kunden oder vom Kunden verwaltet werden. AWS Die erforderliche ressourcenbasierte Richtlinie, die als Anwendungsrichtlinie (oder [ActorPolicy](#) in den APIs) bezeichnet wird, definiert, welche [IAM-Prinzipale berechtigt](#) sind, API-Aktionen für die IAM-Authentifizierungsmethode aufzurufen, z. B. [CreateTokenWithIAM](#) Die IAM-Authentifizierungsmethode ermöglicht es einem IAM-Prinzipal, z. B. einer IAM-Rolle oder einem Dienst, sich beim IAM Identity Center AWS OIDC-Dienst zu authentifizieren, indem er die IAM-Anmeldeinformationen zum Anfordern oder Verwalten von Zugriffstoken unter `/token?` vorlegt. `aws_iam=t`-Endpunkt.

Die Anwendungsrichtlinie regelt die Operationen zur Ausgabe von Tokens ().

`CreateTokenWithIAM` Die Richtlinie regelt auch Aktionen, für die nur Berechtigungen gelten und nur von AWS verwalteten Anwendungen zum Validieren von Token () und zum Widerrufen von Tokens (`IntrospectTokenWithIAM`) verwendet werden. `RevokeTokenWithIAM` Für eine vom Kunden verwaltete Anwendung konfigurieren Sie diese Richtlinie, indem Sie angeben, welche IAM-Prinzipale zum Aufrufen autorisiert sind. `CreateTokenWithIAM` Wenn ein autorisierter Principal diese API-Aktion aufruft, erhält der Principal Zugriffs- und Aktualisierungstoken für die Anwendung.

Wenn Sie die IAM Identity Center-Konsole verwenden, um eine vom Kunden verwaltete Anwendung für die Verbreitung [vertrauenswürdiger Identitäten einzurichten](#), finden Sie unter Schritt 4 unter [Einrichten von kundenverwalteten OAuth 2.0-Anwendungen weitere Informationen](#) zur Konfiguration der Anwendungsrichtlinie. Ein Beispiel für eine Richtlinie finden Sie weiter unten in [Beispielrichtlinie: Erlauben Sie einer IAM-Rolle, Zugriffs- und Aktualisierungstoken zu erstellen](#) diesem Thema.

Politische Anforderungen

Die Richtlinie muss die folgenden Anforderungen erfüllen:

- Die Richtlinie muss ein `Version` Element enthalten, das auf „2012-10-17“ gesetzt ist.
- Die Richtlinie muss mindestens ein Element enthalten. `Statement`

- Jede Richtlinie Statement muss die folgenden Elemente enthalten: `EffectPrincipal`, `Action`, und `Resource`.

Richtlinienelemente

Die Richtlinie muss die folgenden Elemente enthalten:

Version

Gibt die Version des Richtliniendokuments an. Wir empfehlen, die Version auf 2012-10-17 (neueste Version) einzustellen.

Statement

Enthält die RichtlinieStatements. Die Richtlinie muss mindestens eine enthaltenStatement.

Jede Richtlinie Statement besteht aus den folgenden Elementen.

Auswirkung

(Erforderlich) Gibt an, ob die Berechtigungen in der Richtlinienanweisung zugelassen oder verweigert werden. Gültige Werte sind `Allow` oder `Deny`.

Auftraggeber

(Erforderlich) Der [Prinzipal](#) ist die Identität, die die in der Richtlinienanweisung angegebenen Berechtigungen erhält. Sie können IAM-Rollen oder AWS Dienstprinzipale angeben.

Action

(Erforderlich) Die OIDC-Dienst-API-Operationen von IAM Identity Center, die zugelassen oder verweigert werden sollen. Zu den gültigen Aktionen gehören:

- `sso-oauth:CreateTokenWithIAM`: Diese Aktion, die dem [CreateTokenWithIAM](#) API-Vorgang entspricht, gewährt die Erlaubnis, Zugriffs- und Aktualisierungstoken für autorisierte Client-Anwendungen zu erstellen und zurückzugeben, die mithilfe einer beliebigen IAM-Entität, z. B. einer AWS Servic Rolle oder eines Benutzers, authentifiziert werden. Diese Token können definierte Bereiche enthalten, die Berechtigungen wie oder angeben.
`read:profile write:data`
- `sso-oauth:InspectTokenWithIAM` [Nur Erlaubnis]: Erteilt die Erlaubnis, Informationen über aktive OAuth 2.0-Zugriffstoken und Aktualisierungstoken, einschließlich der zugehörigen Bereiche und Berechtigungen, zu validieren und abzurufen. Diese

Berechtigung wird nur von AWS verwalteten Anwendungen verwendet und ist in der OIDC-API-Referenz für IAM Identity Center nicht dokumentiert.

- `RevokeTokenWithIAM` [Nur Erlaubnis]: Erteilt die Erlaubnis, OAuth 2.0-Zugriffstoken zu widerrufen und Tokens zu aktualisieren, sodass sie vor ihrem normalen Ablauf ungültig werden. Diese Berechtigung wird nur von AWS verwalteten Anwendungen verwendet und ist in der OIDC-API-Referenz für IAM Identity Center nicht dokumentiert.

Ressource

(Erforderlich) In dieser Richtlinie lautet der Wert des Resource Elements "*", was „diese Anwendung“ bedeutet.

Weitere Informationen zur AWS Richtlinienyntax finden Sie in der [AWS IAM-Richtlinienreferenz](#) im IAM-Benutzerhandbuch.

Beispielrichtlinie: Erlauben Sie einer IAM-Rolle, Zugriffs- und Aktualisierungstoken zu erstellen

Die folgende Berechtigungsrichtlinie gewährt einer IAM-Rolle `ExampleAppClientRole`, die von einem Workload übernommen wird, Berechtigungen zum Erstellen und Zurückgeben von Zugriffs- und Aktualisierungstoken.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      },
      "Action": "sso-oauth:CreateTokenWithIAM",
      "Resource": "*"
    }
  ]
}
```

AWS verwaltete Richtlinien für IAM Identity Center

Das [Erstellen von vom Kunden verwalteten IAM-Richtlinien](#), die Ihrem Team nur die Berechtigungen gewähren, die es benötigt, erfordert Zeit und Fachwissen. Um schnell loszulegen, können Sie AWS verwaltete Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS -Richtlinien finden Sie unter [Verwaltete AWS -Richtlinien](#) im IAM-Leitfaden.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in [Verwaltete AWS -Richtlinien für Auftragsfunktionen](#) im IAM-Leitfaden.

Neue Aktionen, mit denen Sie Benutzersitzungen auflisten und löschen können, sind unter dem neuen Namespace verfügbar. `identitystore-auth` Alle zusätzlichen Berechtigungen für Aktionen in diesem Namespace werden auf dieser Seite aktualisiert. Vermeiden Sie beim Erstellen Ihrer benutzerdefinierten IAM-Richtlinien die Verwendung von `*` after, `identitystore-auth` da dies für alle Aktionen gilt, die heute oder in Zukunft im Namespace existieren.

AWS verwaltete Richtlinie: `AWSSSOMasterAccountAdministrator`

Die `AWSSSOMasterAccountAdministrator` Richtlinie sieht die erforderlichen Verwaltungsmaßnahmen für Schulleiter vor. Die Richtlinie richtet sich an Schulleiter, die die Rolle eines AWS IAM Identity Center Administrators ausüben. Im Laufe der Zeit wird die Liste der bereitgestellten Aktionen aktualisiert, sodass sie den vorhandenen Funktionen von IAM Identity Center und den Aktionen entspricht, die als Administrator erforderlich sind.

Sie können die `AWSSSOMasterAccountAdministrator`-Richtlinie an Ihre IAM-Identitäten anfügen. Wenn Sie die `AWSSSOMasterAccountAdministrator` Richtlinie an eine Identität anhängen, gewähren Sie AWS IAM Identity Center Administratorberechtigungen. Principals mit dieser Richtlinie können innerhalb des AWS Organizations Verwaltungskontos und aller Mitgliedskonten auf IAM Identity Center zugreifen. Dieser Principal kann alle IAM Identity Center-Operationen vollständig verwalten, einschließlich der Fähigkeit, eine IAM Identity Center-Instanz, Benutzer, Berechtigungssätze und Zuweisungen zu erstellen. Der Principal kann diese Zuweisungen auch in allen Mitgliedskonten der AWS Organisation instanziierten und Verbindungen zwischen AWS Directory Service verwalteten Verzeichnissen und IAM Identity Center herstellen. Sobald neue Verwaltungsfunktionen veröffentlicht werden, werden dem Kontoadministrator diese Berechtigungen automatisch gewährt.

Diese Richtlinie umfasst auch AWS Key Management Service Berechtigungen, die für IAM Identity Center-Instanzen erforderlich sind, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.

Gruppierungen von Berechtigungen

Diese Richtlinie ist in Anweisungen gruppiert, die auf den bereitgestellten Berechtigungen basieren.

- `AWSSSOMasterAccountAdministrator`— Ermöglicht IAM Identity Center, die [benannte Servicerolle `AWSServiceRoleforSSO` an IAM Identity Center](#) weiterzuleiten, sodass es die Rolle später übernehmen und in ihrem Namen Aktionen ausführen kann. Dies ist erforderlich, wenn die Person oder Anwendung versucht, IAM Identity Center zu aktivieren. Weitere Informationen finden Sie unter [Konfigurieren Sie den Zugriff auf AWS-Konten](#).
- `AWSSSOMemberAccountAdministrator`— Ermöglicht IAM Identity Center, Kontoadministratoraktionen in einer Umgebung mit mehreren AWS Konten auszuführen. Weitere Informationen finden Sie unter [AWS verwaltete Richtlinie: `AWSSSOMemberAccountAdministrator`](#).
- `AWSSSOManageDelegatedAdministrator`— Ermöglicht IAM Identity Center die Registrierung und Abmeldung eines delegierten Administrators für Ihre Organisation.
- `AllowKMSKeyUseViaService` und `AllowKMSKeyDiscovery` — Ermöglicht den AWS Key Management Service Betrieb von vom Kunden verwalteten Schlüsseln, die von IAM Identity Center-Instanzen verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSSSOMasterAccountAdministrator](#) AWS Managed Policy Reference.

Zusätzliche Informationen zu dieser Richtlinie

Wenn IAM Identity Center zum ersten Mal aktiviert wird, erstellt der IAM Identity [Center-Dienst eine dienstverknüpfte Rolle](#) im AWS Organizations Verwaltungskonto (früher Hauptkonto), sodass IAM Identity Center die Ressourcen in Ihrem Konto verwalten kann. Die erforderlichen Aktionen sind `iam:CreateServiceLinkedRole` und `iam:PassRole`.

AWS verwaltete Richtlinie: AWSSSOMemberAccountAdministrator

Die `AWSSSOMemberAccountAdministrator` Richtlinie sieht die erforderlichen Verwaltungsmaßnahmen für Schulleiter vor. Die Richtlinie richtet sich an Principals, die die Rolle eines IAM Identity Center-Administrators ausüben. Im Laufe der Zeit wird die Liste der bereitgestellten Aktionen aktualisiert, sodass sie den vorhandenen Funktionen von IAM Identity Center und den Aktionen, die als Administrator erforderlich sind, entspricht.

Sie können die `AWSSSOMemberAccountAdministrator`-Richtlinie an Ihre IAM-Identitäten anfügen. Wenn Sie die `AWSSSOMemberAccountAdministrator` Richtlinie an eine Identität anhängen, gewähren Sie AWS IAM Identity Center Administratorberechtigungen. Principals mit dieser Richtlinie können innerhalb des AWS Organizations Verwaltungskontos und aller Mitgliedskonten auf IAM Identity Center zugreifen. Dieser Principal kann alle IAM Identity Center-Operationen vollständig verwalten, einschließlich der Fähigkeit, Benutzer, Berechtigungssätze und Zuweisungen zu erstellen. Der Principal kann diese Zuweisungen auch in allen Mitgliedskonten der AWS Organisation instanziiieren und Verbindungen zwischen AWS Directory Service verwalteten Verzeichnissen und IAM Identity Center herstellen. Sobald neue Verwaltungsfunktionen veröffentlicht werden, erhält der Kontoadministrator diese Berechtigungen automatisch.

Diese Richtlinie umfasst auch AWS Key Management Service Berechtigungen, die für IAM Identity Center-Instanzen erforderlich sind, die vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz [AWSSSOMemberAccountAdministrator](#) zu AWS verwalteten Richtlinien.

Zusätzliche Informationen zu dieser Richtlinie

IAM Identity Center-Administratoren verwalten Benutzer, Gruppen und Passwörter in ihrem Identity Center-Verzeichnisspeicher (SSO-Verzeichnis). Die Rolle des Kontoadministrators umfasst Berechtigungen für die folgenden Aktionen:

- `"sso:*"`

- "sso-directory:*"

IAM Identity Center-Administratoren benötigen eingeschränkte Berechtigungen für die folgenden Directory Service Aktionen, um tägliche Aufgaben ausführen zu können.

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- "ds:CreateAlias"

Diese Berechtigungen ermöglichen es IAM Identity Center-Administratoren, vorhandene Verzeichnisse zu identifizieren und Anwendungen zu verwalten, sodass sie für die Verwendung mit IAM Identity Center konfiguriert werden können. Weitere Informationen zu jeder dieser Aktionen finden Sie unter [Directory Service API-Berechtigungen: Referenz für Aktionen, Ressourcen und Bedingungen](#).

IAM Identity Center verwendet IAM-Richtlinien, um IAM Identity Center-Benutzern Berechtigungen zu gewähren. IAM Identity Center-Administratoren erstellen Berechtigungssätze und hängen ihnen Richtlinien an. Der IAM Identity Center-Administrator muss über die Berechtigungen zum Auflisten der vorhandenen Richtlinien verfügen, damit er auswählen kann, welche Richtlinien mit dem Berechtigungssatz, den er gerade erstellt oder aktualisiert, verwendet werden sollen. Um sichere und funktionale Berechtigungen einrichten zu können, muss der IAM Identity Center-Administrator über die Berechtigungen zur Ausführung der IAM Access Analyzer-Richtlinienvvalidierung verfügen.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

IAM Identity Center-Administratoren benötigen eingeschränkten Zugriff auf die folgenden AWS Organizations Aktionen, um tägliche Aufgaben ausführen zu können:

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"

- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

Diese Berechtigungen ermöglichen es IAM Identity Center-Administratoren, mit Organisationsressourcen (Konten) für grundlegende IAM Identity Center-Administrationsaufgaben wie die folgenden zu arbeiten:

- Identifizierung des Verwaltungskontos, das zur Organisation gehört
- Identifizierung der Mitgliedskonten, die zur Organisation gehören
- Aktivierung des AWS Servicezugriffs für Konten
- Einrichtung und Verwaltung eines delegierten Administrators

Weitere Informationen zur Verwendung eines delegierten Administrators mit IAM Identity Center finden Sie unter [Delegierte Verwaltung](#). Weitere Informationen zur Verwendung dieser Berechtigungen finden Sie unter [Verwenden AWS Organizations mit AWS Organizations anderen AWS Diensten](#).

AWS verwaltete Richtlinie: AWSSSODirectoryAdministrator

Sie können die AWSSSODirectoryAdministrator-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen für IAM Identity Center-Benutzer und -Gruppen. Principals, denen diese Richtlinie zugeordnet ist, können alle Aktualisierungen an IAM Identity Center-Benutzern und -Gruppen vornehmen. Diese Richtlinie umfasst auch AWS Key Management Service Berechtigungen, die für IAM Identity Center-Instanzen erforderlich sind, die vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden.

Diese Richtlinie umfasst die folgenden Berechtigungen:

- IAM Identity Center-Verzeichnis — Vollständiger Administratorzugriff auf IAM Identity Center-Verzeichnisvorgänge.
- Identity Store — Vollständiger Administratorzugriff auf Vorgänge und Authentifizierung im Identitätsspeicher.
- IAM Identity Center — Berechtigung zum Auflisten von Verzeichniszuordnungen.
- AWS Key Management Service— Berechtigungen zum Entschlüsseln, Beschreiben von Schlüsseln und Generieren von Datenschlüsseln für vom Kunden verwaltete Schlüssel, die von IAM Identity Center-Instanzen verwendet werden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWS Managed Policy [AWSSSODirectoryAdministrator](#) Reference.

AWS verwaltete Richtlinie: AWSSSOReadOnly

Sie können die AWSSSOReadOnly-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen im IAM Identity Center anzuzeigen. Principals, denen diese Richtlinie zugeordnet ist, können die IAM Identity Center-Benutzer oder -Gruppen nicht direkt sehen. Principals, an die diese Richtlinie angehängt ist, können keine Aktualisierungen im IAM Identity Center vornehmen. Principals mit diesen Berechtigungen können beispielsweise die IAM Identity Center-Einstellungen einsehen, aber keinen der Einstellungswerte ändern.

Diese Richtlinie umfasst auch AWS Key Management Service Berechtigungen, die für IAM Identity Center-Instanzen erforderlich sind, die vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz [AWSSSOReadOnly](#) zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSSSODirectoryReadOnly

Sie können die AWSSSODirectoryReadOnly-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Leseberechtigungen, die es Benutzern ermöglichen, Benutzer und Gruppen im IAM Identity Center anzuzeigen. Principals, denen diese Richtlinie zugeordnet ist, können IAM Identity Center-Zuweisungen, Berechtigungssätze, Anwendungen oder Einstellungen nicht anzeigen. Principals, an die diese Richtlinie angehängt ist, können keine Aktualisierungen in IAM Identity

Center vornehmen. Principals mit diesen Berechtigungen können beispielsweise IAM Identity Center-Benutzer sehen, aber sie können keine Benutzerattribute ändern oder MFA-Geräte zuweisen.

Diese Richtlinie umfasst auch AWS Key Management Service Berechtigungen, die für IAM Identity Center-Instanzen erforderlich sind, die vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz [AWSSSODirectoryReadOnly](#) zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSIdentitySyncFullAccess

Sie können die AWSIdentitySyncFullAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Prinzipale, denen diese Richtlinie zugeordnet ist, haben volle Zugriffsberechtigungen, um Synchronisierungsprofile zu erstellen und zu löschen, ein Synchronisierungsprofil mit einem Synchronisierungsziel zu verknüpfen oder zu aktualisieren, Synchronisierungsfilter zu erstellen, aufzulisten und zu löschen sowie die Synchronisierung zu starten oder zu beenden.

Berechtigungsdetails

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz [AWSIdentitySyncFullAccess](#) zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSIdentitySyncReadOnlyAccess

Sie können die AWSIdentitySyncReadOnlyAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen über das Identitätssynchronisierungsprofil, die Filter und die Zieleinstellungen einzusehen.

Prinzipale, an die diese Richtlinie angehängt ist, können keine Aktualisierungen an den Synchronisierungseinstellungen vornehmen. Beispielsweise können Hauptbenutzer mit diesen Berechtigungen die Einstellungen für die Identitätssynchronisierung einsehen, aber keinen der Profil- oder Filterwerte ändern.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSIdentitySyncReadOnlyAccess](#) Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSSOServiceRolePolicy

Sie können die AWSSSOServiceRolePolicy Richtlinie nicht an Ihre IAM-Identitäten anhängen.

Diese Richtlinie ist mit einer dienstverknüpften Rolle verknüpft, die es IAM Identity Center ermöglicht, zu delegieren und durchzusetzen, welche Benutzer Single-Sign-On-Zugriff auf bestimmte Zugangsdaten haben. AWS-Konten AWS Organizations Wenn Sie IAM aktivieren, wird in allen Bereichen Ihrer Organisation eine serviceverknüpfte Rolle erstellt. AWS-Konten IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen. Service-linked Die Rollen, die in den einzelnen Rollen erstellt werden, AWS-Konto sind benannt `AWSServiceRoleForSSO`. Weitere Informationen finden Sie unter [Verwenden von dienstverknüpften Rollen für IAM Identity Center](#).

AWS verwaltete Richtlinie: `AWSIAMIdentityCenterAllowListForIdentityContext`

Wenn AWS -Security-Token-Service (AWS STS) eine Rolle im IAM Identity Center-Identitätskontext übernimmt, hängt die `AWSIAMIdentityCenterAllowListForIdentityContext` Richtlinie automatisch an die Rolle an.

Diese Richtlinie enthält die Liste der Aktionen, die zulässig sind, wenn Sie die Weitergabe vertrauenswürdiger Identitäten mit Rollen verwenden, die im IAM Identity Center-Identitätskontext übernommen werden. Alle anderen Aktionen, die in diesem Kontext aufgerufen werden, sind blockiert. Der Identitätskontext wird als `übergebenProvidedContext`.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie [AWSIAMIdentityCenterAllowListForIdentityContext](#) in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: `AWSIdentityCenterExternalManagementPolicy`

Sie können die `AWSIdentityCenterExternalManagementPolicy`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht den Zugriff auf die Verwaltung von IAM Identity Center-Benutzern von einem externen Anbieter aus.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie [AWSIdentityCenterExternalManagementPolicy](#) in der Referenz zu AWS verwalteten Richtlinien.

IAM Identity Center wird aktualisiert auf AWS Verwaltete Richtlinien

In der folgenden Tabelle werden die Aktualisierungen der AWS verwalteten Richtlinien für IAM Identity Center beschrieben, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen.

Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der IAM Identity Center-Dokumentverlaufsseite.

Änderungen	Beschreibung	Date
AWSIdentityCenterExternalManagementPolicy	Die verwaltete Richtlinie wurde aktualisiert, um den ARN für den Provisioning-Mandanten zu ändern.	5. Dezember 2025
AWSIdentityCenterExternalManagementPolicy	Diese Richtlinie ermöglicht den Zugriff auf die Verwaltung von IAM Identity Center-Benutzern von einem externen Anbieter aus.	21. November 2025
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSOReadOnly , AWSSSODirectoryAdministrator , AWSSSODirectoryReadOnly	Die verwalteten Richtlinien wurden aktualisiert und enthalten AWS KMS nun die erforderlichen Berechtigungen für IAM Identity Center-Instanzen, die vom Kunden verwaltete Schlüssel zur Verschlüsselung verwenden.	17. September 2025
AWSSSOServiceRolePolicy	Diese Richtlinie beinhaltet jetzt auch Anrufberechtigungen <code>identity-sync:DeleteSyncProfile</code> .	11. Februar 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die <code>qapps:ListQAppSessionData</code> und <code>qapps:ExportQAppSessionData</code> Aktionen zur Unterstützung identitätsverbesserter Konsolensitzungen für AWS	2. Oktober 2024

Änderungen	Beschreibung	Date
	verwaltete Anwendungen, die diese Sitzungen unterstützen.	
<u>AWSSSOMasterAccountAdministrator</u>	IAM Identity Center hat eine neue Aktion hinzugefügt, mit der Sie DeleteSyncProfile Berechtigungen erteilen können, damit Sie diese Richtlinie zum Löschen von Synchronisierungsprofilen verwenden können. Diese Aktion ist mit der DeleteInstance API verknüpft.	26. September 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Diese Richtlinie umfasst jetzt die s3:ListCallerAccessGrants Aktion zur Unterstützung identitätsverbesserter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	4. September 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Diese Richtlinie umfasst nun die es:ESHttpPut Aktionen aoss:APIAccessAll „es:ESHttpHead „es:ESHttpPost es:ESHttpGet es:ESHttpPatch es:ESHttpDelete , und zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	12. Juli 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die Aktionen <code>qapps:PredictQApp</code> , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> , <code>qapps:DissociateLibraryItemReview</code> , <code>qapps:GetQAppSession</code> , <code>qapps:UpdateQAppSession</code> , <code>qapps:GetQAppSessionMetadata</code> , <code>qapps:UpdateQAppSessionMetadata</code> , und die <code>qapps:TagResource</code> Aktionen zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	27. Juni 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die elasticmapreduce:ListSteps Aktionen elasticmapreduce:AddJobFlowSteps, elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps elasticmapreduce:DescribeStep, und zur Unterstützung der Verbreitung vertrauenswürdiger Identitäten in Amazon EMR.	17. Mai 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps>DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DisassociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps:CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps:CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps:CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , und <code>qapps:StopQAppSession</code> . Aktionen zur Unterstützung identitätsverbesserter	30. April 2024

Änderungen	Beschreibung	Date
	Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	
AWSSSOMasterAccountAdministrator	Diese Richtlinie umfasst nun die <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> Aktionen zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst nun die <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> Aktionen <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> und zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderungen	Beschreibung	Date
AWSSSOReadOnly	Diese Richtlinie umfasst nun die <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> Aktion zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die <code>qbusiness:PutFeedback</code> Aktion zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderungen	Beschreibung	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die <code>q:UpdateTroubleshootingCommandResult</code> Aktionen <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , und zur Unterstützung identitätsverstärkter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	24. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst nun die <code>sts:SetContext</code> Aktion zur Unterstützung identitätsverbesserter Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	19. April 2024

Änderungen	Beschreibung	Date
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Diese Richtlinie umfasst nun die <code>qbusiness:DeleteConversation</code> Aktionen <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , und zur Unterstützung Identitätsverstärkter Konsolenitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	11. April 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Diese Richtlinie umfasst jetzt die Aktionen <code>s3:GetAccessGrantsInstanceForPrefix</code> und <code>s3:GetDataAccess</code> .	26. November 2023
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Diese Richtlinie enthält die Liste der Aktionen, die zulässig sind, wenn Sie die Weitergabe vertrauenswürdiger Identitäten mit Rollen verwenden, die im IAM Identity Center-Identitätskontext übernommen werden.	15. November 2023
<u>AWSSSODirectoryReadOnly</u>	Diese Richtlinie umfasst jetzt den neuen Namespace <code>identitystore-auth</code> mit neuen Berechtigungen, sodass Benutzer Sitzungen auflisten und abrufen können.	21. Februar 2023

Änderungen	Beschreibung	Date
AWSSSOServiceRolePolicy	Diese Richtlinie ermöglicht jetzt, dass die UpdateSAMLProvider Aktion für das Verwaltungskonto ausgeführt wird.	20. Oktober 2022
AWSSSOMasterAccountAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace <code>identitystore-auth</code> mit neuen Berechtigungen, sodass der Administrator Sitzungen für einen Benutzer auflisten und löschen kann.	20. Oktober 2022
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace <code>identitystore-auth</code> mit neuen Berechtigungen, die es dem Administrator ermöglichen, Sitzungen für einen Benutzer aufzulisten und zu löschen.	20. Oktober 2022
AWSSSODirectoryAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace <code>identitystore-auth</code> mit neuen Berechtigungen, die es dem Administrator ermöglichen, Sitzungen für einen Benutzer aufzulisten und zu löschen.	20. Oktober 2022

Änderungen	Beschreibung	Date
AWSSSOMasterAccountAdministrator	Diese Richtlinie beinhaltet jetzt neue Zugriffsberechtigungen ListDelegatedAdministrators . AWS Organizations Diese Richtlinie umfasst jetzt auch eine Untergruppe von Berechtigungen AWSSSOManageDelegatedAdministrator , einschließlich der Berechtigungen zum Anrufen RegisterDelegatedAdministrator und DeregisterDelegatedAdministrator .	16. August 2022
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt neue ListDelegatedAdministrators _Anruferlaubnisse. AWS Organizations Diese Richtlinie umfasst jetzt auch eine Untergruppe von Berechtigungen AWSSSOManageDelegatedAdministrator , einschließlich der Berechtigungen zum Anrufen RegisterDelegatedAdministrator und DeregisterDelegatedAdministrator .	16. August 2022

Änderungen	Beschreibung	Date
AWSSSOReadOnly	Diese Richtlinie umfasst jetzt neue ListDelegatedAdministrators _Anruferlaubnisse. AWS Organizations	11. August 2022
AWSSSOServiceRolePolicy	Diese Richtlinie enthält jetzt neue Berechtigungen für Anrufe DeleteRolePermissionsBoundary und PutRolePermissionsBoundary .	14. Juli 2022
AWSSSOServiceRolePolicy	Diese Richtlinie enthält jetzt neue Berechtigungen, die das Eingehen von Anrufen ermöglichen ListAWSServiceAccessForOrganization and ListDelegatedAdministrators AWS Organizations.	11. Mai 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Fügen Sie IAM Access Analyzer-Berechtigungen hinzu, die es einem Principal ermöglichen, die Policy-Checks zur Validierung zu verwenden.	28. April 2022

Änderungen	Beschreibung	Date
<u>AWSSSOMasterAccountAdministrator</u>	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen. Informationen zu den Aktionen, die im IAM Identity Center Identity Store-Dienst verfügbar sind, finden Sie in der <u>IAM Identity Center Identity Store API-Referenz</u> .	29. März 2022
<u>AWSSSOMemberAccountAdministrator</u>	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen.	29. März 2022
<u>AWSSSODirectoryAdministrator</u>	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen.	29. März 2022
<u>AWSSSODirectoryReadOnly</u>	Diese Richtlinie gewährt jetzt Zugriff auf die Leseaktionen des IAM Identity Center Identity Store-Dienstes. Dieser Zugriff ist erforderlich, um Benutzer- und Gruppeninformationen aus dem IAM Identity Center Identity Store-Dienst abzurufen.	29. März 2022
<u>AWSIdentitySyncFullAccess</u>	Diese Richtlinie ermöglicht den vollen Zugriff auf Identitätssynchronisierungsberechtigungen.	3. März 2022

Änderungen	Beschreibung	Date
AWSIdentitySyncReadOnlyAccess	Diese Richtlinie gewährt nur Leseberechtigungen, die es einem Prinzipal ermöglichen, Einstellungen für die Identitätssynchronisierung einzusehen.	3. März 2022
AWSSSOReadOnly	Diese Richtlinie gewährt nur Leseberechtigungen, die es einem Principal ermöglichen, die IAM Identity Center-Konfigurationseinstellungen einzusehen.	4. August 2021
IAM Identity Center hat begonnen, Änderungen zu verfolgen	IAM Identity Center hat begonnen, Änderungen für AWS verwaltete Richtlinien zu verfolgen.	4. August 2021

Verwenden von dienstverknüpften Rollen für IAM Identity Center

AWS IAM Identity Center verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte Rollen](#). Eine serviceverknüpfte Rolle ist ein einzigartiger IAM-Rollentyp, der direkt mit IAM Identity Center verknüpft ist. Es ist vom IAM Identity Center vordefiniert und beinhaltet alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Weitere Informationen finden Sie unter [Grundlegendes zu serviceverknüpften Rollen in IAM Identity Center](#).

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von IAM Identity Center, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. IAM Identity Center definiert die Berechtigungen seiner serviceverknüpften Rolle. Sofern nicht anders definiert, kann nur IAM Identity Center diese Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS Dienste, die mit IAM](#) funktionieren. Suchen Sie nach den Diensten, für die in der Spalte Rolle „Ja“ steht. Service-Linked Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für IAM Identity Center

IAM Identity Center verwendet die benannte service-verknüpfte Rolle, `AWSServiceRoleForSSO` um IAM Identity Center Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich IAM-Rollen, Richtlinien und SAML-IdP, in Ihrem Namen zu gewähren.

Die `AWSServiceRoleForSSO` serviceverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- IAM Identity Center (Dienstpräfix:) `sso`

Die Richtlinie für `AWSSSOServiceRolePolicy` dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, die folgenden Aufgaben für Rollen im Pfad `„/aws- reserved/ sso .amazonaws.com/“` und mit dem Namenspräfix `„awsReservedSSO_“` auszuführen:

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePermissionsBoundary`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

Die Berechtigungsrichtlinie für `AWSSSOServiceRolePolicy` serviceverknüpfte Rollen ermöglicht es IAM Identity Center, Folgendes bei SAML-Anbietern mit dem Namenspräfix `„AWSSSO_“` durchzuführen:

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

Die Berechtigungsrichtlinie für `AWSSSOServiceRolePolicy` serviceverknüpfte Rollen ermöglicht es IAM Identity Center, die folgenden Aufgaben für alle Organisationen auszuführen:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Die Berechtigungsrichtlinie für `AWSSSOServiceRolePolicy` serviceverknüpfte Rollen ermöglicht es IAM Identity Center, die folgenden Aufgaben für alle IAM-Rollen auszuführen (*):

- `iam:listRoles`

Die Berechtigungsrichtlinie für `AWSSSOServiceRolePolicy` serviceverknüpfte Rollen ermöglicht es IAM Identity Center, die folgenden Aufgaben auf „`arn:aws:iam: *: -service- .amazonaws`“ auszuführen. `role/aws role/sso com/AWSServiceRoleForSSO`:

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

Die Richtlinie für `AWSSSOServiceRolePolicy` dienstgebundene Rollenberechtigungen ermöglicht es IAM Identity Center, Folgendes auf „`arn:aws:identity-sync: *:profile/*`“ durchzuführen:

- `identity-sync>DeleteSyncProfile`

Weitere Informationen zu Aktualisierungen der Berechtigungsrichtlinie für serviceverknüpfte Rollen finden Sie unter. `AWSSSOServiceRolePolicy` [IAM Identity Center wird aktualisiert auf AWS Verwaltete Richtlinien](#)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMRoleProvisioningActions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "IAMRoleReadActions",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "IAMRoleCleanupActions",
      "Effect": "Allow",
      "Action": [
        "iam>DeleteRole",

```

```

        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    ]
},
{
    "Sid": "IAMSLRCleanupActions",
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
    ]
},
{
    "Sid": "IAMSAMLProviderCreationAction",
    "Effect": "Allow",
    "Action": [
        "iam:CreateSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "IAMSAMLProviderUpdateAction",
    "Effect": "Allow",
    "Action": [
        "iam:UpdateSAMLProvider"
    ],

```

```

    "Resource": [
      "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
  },
  {
    "Sid": "IAMSAMLProviderCleanupActions",
    "Effect": "Allow",
    "Action": [
      "iam:DeleteSAMLProvider",
      "iam:GetSAMLProvider"
    ],
    "Resource": [
      "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganization",
      "organizations:ListAccounts",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowUnauthAppForDirectory",
    "Effect": "Allow",
    "Action": [
      "ds:UnauthorizeApplication"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "AllowDescribeForDirectory",
    "Effect": "Allow",
    "Action": [
      "ds:DescribeDirectories",
      "ds:DescribeTrusts"
    ]
  }

```

```

    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDescribeAndListOperationsOnIdentitySource",
    "Effect": "Allow",
    "Action": [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDeleteSyncProfile",
    "Effect": "Allow",
    "Action": [
        "identity-sync:DeleteSyncProfile"
    ],
    "Resource": [
        "arn:aws:identity-sync:*:*:profile/*"
    ]
}
]
}

```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie [im IAM-Benutzerhandbuch unter](#) Service-linked Rollenberechtigungen.

Erstellen einer dienstverknüpften Rolle für IAM Identity Center

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Nach der Aktivierung erstellt IAM Identity Center eine serviceverknüpfte Rolle in allen Konten innerhalb der Organisation in Organizations. AWS IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem

Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen.

Hinweise

- Wenn Sie beim AWS Organizations Verwaltungskonto angemeldet sind, verwendet es Ihre aktuell angemeldete Rolle und nicht die serviceverknüpfte Rolle. Dies verhindert die Eskalation von Rechten.
- Wenn IAM Identity Center IAM-Vorgänge im AWS Organizations Verwaltungskonto ausführt, werden für alle Vorgänge die Anmeldeinformationen des IAM-Prinzipals verwendet. Auf diese Weise können die Anmeldungen CloudTrail Aufschluss darüber geben, wer alle Rechteänderungen im Verwaltungskonto vorgenommen hat.

Important

Wenn Sie den IAM Identity Center-Dienst vor dem 7. Dezember 2017 verwendet haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat IAM Identity Center die `AWSServiceRoleForSSO` Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem IAM-Konto erschienen](#).

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen.

Bearbeitung einer serviceverknüpften Rolle für IAM Identity Center

Im `AWSServiceRoleForSSO` IAM Identity Center können Sie die serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer dienstverknüpften Rolle für IAM Identity Center

Sie müssen die Rolle nicht manuell löschen. `AWSServiceRoleForSSO` Wenn eine aus einer AWS Organisation entfernt AWS-Konto wird, bereinigt IAM Identity Center automatisch die Ressourcen und löscht die mit dem Dienst verknüpfte Rolle aus der Organisation. AWS-Konto

Sie können auch die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die serviceverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

 Note

Wenn der IAM Identity Center-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um IAM Identity Center-Ressourcen zu löschen, die von AWSServiceRoleForSSO

1. [Entfernen Sie den Benutzer- und Gruppenzugriff auf eine AWS-Konto](#) für alle Benutzer und Gruppen, die Zugriff auf die AWS-Konto haben.
2. [Entfernen Sie Berechtigungssätze im IAM Identity Center](#) die Sie mit dem verknüpft haben AWS-Konto.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die AWSServiceRoleForSSO-serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie [im IAM-Benutzerhandbuch unter Löschen einer Service-Linked Rolle](#).

IAM Identity Center-Konsole und API-Autorisierung

Bestehende IAM Identity Center-Konsolen-APIs unterstützen die doppelte Autorisierung, sodass Sie bestehende API-Operationen auch dann nutzen können, wenn neuere APIs verfügbar sind. Wenn Sie bereits über Instanzen von IAM Identity Center verfügen, die vor dem 15. November 2023 und dem 15. Oktober 2020 erstellt wurden, können Sie anhand der folgenden Tabellen ermitteln, welche API-Operationen jetzt neueren API-Vorgängen zugeordnet werden, die nach diesen Daten veröffentlicht wurden.

Themen

- [API-Aktionen nach November 2023](#)
- [API-Aktionen nach Oktober 2020](#)

API-Aktionen nach November 2023

Instanzen von IAM Identity Center, die vor dem 15. November 2023 erstellt wurden, berücksichtigen sowohl alte als auch neue API-Aktionen, sofern keine der Aktionen explizit verweigert wird. Instanzen, die nach dem 15. November 2023 erstellt wurden, verwenden [neuere API-Aktionen](#) für die Autorisierung in der IAM Identity Center-Konsole.

Name des Konsolenbetriebs, der vor dem 15. November 2023 verwendet wurde	API-Aktion, die nach dem 15. November 2023 verwendet wurde
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Name des Konsolenbetriebs, der vor dem 15. November 2023 verwendet wurde	API-Aktion, die nach dem 15. November 2023 verwendet wurde
UpdateApplicationInstanceDisplayData UpdateApplicationInstanceStatus UpdateManagedApplicationInstanceStatus	UpdateApplication

API-Aktionen nach Oktober 2020

Instanzen von IAM Identity Center, die vor dem 15. Oktober 2020 erstellt wurden, berücksichtigen sowohl alte als auch neue API-Aktionen, sofern keine der Aktionen explizit verweigert wird.

Instanzen, die nach dem 15. Oktober 2020 erstellt wurden, verwenden [neuere API-Aktionen](#) für die Autorisierung in der IAM Identity Center-Konsole.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWSAccount	DeleteApplicationInstance DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile CreateProfile UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust CreateTrust UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS Bedingungskontextschlüssel für IAM Identity Center

Wenn ein [Principal eine Anfrage an](#) stellt AWS, fasst er AWS die Anforderungsinformationen in einem Anforderungskontext zusammen, der zur Auswertung und Autorisierung der Anfrage verwendet wird. Sie können das Condition-Element einer JSON-Richtlinie verwenden, um Schlüssel im Anforderungskontext mit Schlüsselwerten zu vergleichen, die Sie in Ihrer Richtlinie angeben. Die Anforderungsinformationen werden aus verschiedenen Quellen bereitgestellt, einschließlich des Prinzipals, der die Anfrage stellt, der Ressource, der Anfrage, für die sie gestellt wird, und der Metadaten zur Anfrage selbst. Service-specific Bedingungsschlüssel sind für die Verwendung mit einem einzelnen AWS Dienst definiert.

IAM Identity Center umfasst einen AWS STS Kontextanbieter, der AWS es verwalteten Anwendungen und Drittanbieteranwendungen ermöglicht, Werte für Bedingungsschlüssel hinzuzufügen, die von IAM Identity Center definiert werden. Diese Schlüssel sind in [IAM-Rollen enthalten](#). Die Schlüsselwerte werden festgelegt, wenn eine Anwendung ein Token an AWS STS übergibt. Die Anwendung erhält das Token, an das sie übergibt, AWS STS auf eine der folgenden Arten:

- Während der Authentifizierung mit IAM Identity Center.
- Nach dem Tokenaustausch mit einem [vertrauenswürdigen Token-Aussteller](#) zur Weitergabe vertrauenswürdiger Identitäten. In diesem Fall erhält die Anwendung ein Token von einem vertrauenswürdigen Token-Aussteller und tauscht dieses Token gegen ein Token vom IAM Identity Center aus.

Diese Schlüssel werden in der Regel von Anwendungen verwendet, die die Verbreitung vertrauenswürdiger Identitäten integrieren. In einigen Fällen können Sie, wenn Schlüsselwerte vorhanden sind, diese Schlüssel in IAM-Richtlinien verwenden, die Sie erstellen, um Berechtigungen zuzulassen oder zu verweigern.

Beispielsweise möchten Sie möglicherweise bedingten Zugriff auf eine Ressource gewähren, der auf dem Wert von `UserId` basiert. Dieser Wert gibt an, welcher IAM Identity Center-Benutzer die

Rolle verwendet. Das Beispiel ähnelt der Verwendung `SourceId` von. Im `SourceId` Gegensatz dazu `UserId` steht der Wert für jedoch für einen bestimmten, verifizierten Benutzer aus dem Identitätsspeicher. Dieser Wert ist in dem Token enthalten, das die Anwendung erhält und an das sie dann AWS STS weitergibt. Es handelt sich nicht um eine allgemeine Zeichenfolge, die beliebige Werte enthalten kann.

Themen

- [Identitätsspeicher: UserId](#)
- [Identitätsspeicher: IdentityStoreArn](#)
- [Identitätszentrum: ApplicationArn](#)
- [Identitätszentrum: CredentialId](#)
- [Identitätszentrum: InstanceArn](#)

Identitätsspeicher: UserId

Dieser Kontextschlüssel ist der `UserId` des IAM Identity Center-Benutzers, der Gegenstand der von IAM Identity Center ausgegebenen Kontext-Assertion ist. Die Kontext-Assertion wird an übergeben. AWS STS Sie können diesen Schlüssel verwenden, um die ID `UserId` des IAM Identity Center-Benutzers, in dessen Namen die Anfrage gestellt wird, mit der Benutzerkennung zu vergleichen, die Sie in der Richtlinie angeben.

- Verfügbarkeit — Dieser Schlüssel wird in den Anforderungskontext aufgenommen, nachdem eine vom IAM Identity Center ausgegebene Kontext-Assertion festgelegt wurde, wenn eine Rolle mithilfe eines beliebigen AWS STS `assume-role` Befehls im AWS CLI oder AWS STS `AssumeRole` API-Vorgang übernommen wird.
- Datentyp – [Zeichenfolge](#)
- Werttyp — Single-valued

Identitätsspeicher: IdentityStoreArn

Dieser Kontextschlüssel ist der ARN des Identitätsspeichers, der an die Instanz von IAM Identity Center angehängt ist, die die Kontext-Assertion ausgegeben hat. Es ist auch der Identitätsspeicher, in dem Sie nach Attributen suchen können. `identitystore:UserID` Sie können diesen Schlüssel in Richtlinien verwenden, um festzustellen, ob der ARN aus einem erwarteten Identitätsspeicher `identitystore:UserID` stammt.

- **Verfügbarkeit** — Dieser Schlüssel ist im Anforderungskontext enthalten, nachdem eine vom IAM Identity Center ausgegebene Kontext-Assertion festgelegt wurde, wenn eine Rolle mithilfe eines beliebigen AWS STS `assume-role` Befehls in der AWS CLI oder AWS STS `AssumeRole` API-Operation übernommen wird.
- **Datentyp** — [Arn](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html#Conditions_String), String https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html#Conditions_String
- **Werttyp** — Single-valued

Identitätszentrum: ApplicationArn

Dieser Kontextschlüssel ist der ARN der Anwendung, für die IAM Identity Center eine Kontext-Assertion ausgegeben hat. Sie können diesen Schlüssel in Richtlinien verwenden, um festzustellen, ob er von einer erwarteten Anwendung `identitycenter:ApplicationArn` stammt. Mithilfe dieses Schlüssels kann verhindert werden, dass eine unerwartete Anwendung auf eine IAM-Rolle zugreift.

- **Verfügbarkeit** — Dieser Schlüssel ist im Anforderungskontext einer AWS STS `AssumeRole` API-Operation enthalten. Der Anforderungskontext beinhaltet eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- **Datentyp** — [Arn](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html#Conditions_String), String https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html#Conditions_String
- **Werttyp** — Single-valued

Identitätszentrum: CredentialId

Dieser Kontextschlüssel ist eine zufällige ID für die Anmeldeinformationen für die Rolle mit erweiterter Identität und wird nur für die Protokollierung verwendet. Da dieser Schlüsselwert nicht vorhersehbar ist, empfehlen wir, ihn nicht für Kontextzusicherungen in Richtlinien zu verwenden.

- **Verfügbarkeit** — Dieser Schlüssel ist im Anforderungskontext einer AWS STS `AssumeRole` API-Operation enthalten. Der Anforderungskontext beinhaltet eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- **Datentyp** — [Zeichenfolge](#)
- **Werttyp** — Single-valued

Identitätszentrum: InstanceArn

Dieser Kontextschlüssel ist der ARN der Instanz von IAM Identity Center, die die Kontext-Assertion für den ausgegeben hat. `identitystore:UserID` Mit diesem Schlüssel können Sie ermitteln, ob die `identitystore:UserID` UND-Kontext-Assertion von einem erwarteten ARN der IAM Identity Center-Instanz stammt.

- Verfügbarkeit — Dieser Schlüssel ist im Anforderungskontext einer AWS STS `AssumeRole` API-Operation enthalten. Der Anforderungskontext beinhaltet eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- Datentyp — [Arn](#), String https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition_operators.html#Conditions_String
- Werttyp — Single-valued

Protokollierung und Überwachung im IAM Identity Center

Es hat sich bewährt, Ihre Organisation zu überwachen, um sicherzustellen, dass Änderungen protokolliert werden. Mithilfe der Überwachung können Sie sicherstellen, dass Sie jede unerwartete Änderung untersuchen und unerwünschte Änderungen rückgängig machen können. IAM Identity Center unterstützt derzeit zwei AWS Dienste, mit denen Sie Ihr Unternehmen und die darin ablaufenden Aktivitäten überwachen können: AWS CloudTrail und Amazon EventBridge.

Themen

- [Protokollierung von IAM Identity Center-API-Aufrufen mit AWS CloudTrail](#)
- [Protokollierung von IAM Identity Center SCIM-API-Aufrufen mit AWS CloudTrail](#)
- [Verbinden Sie Anwendungskomponenten mit Amazon EventBridge](#)
- [Protokollierung konfigurierbarer AD-Synchronisierungsfehler](#)

Protokollierung von IAM Identity Center-API-Aufrufen mit AWS CloudTrail

AWS IAM Identity Center ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst in IAM Identity Center ausgeführten Aktionen bereitstellt. CloudTrail erfasst API-Aufrufe für IAM Identity Center als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der IAM Identity Center-Konsole und Codeaufrufen an die IAM Identity Center-API-Operationen. Wenn Sie einen [Trail erstellen](#), können Sie die kontinuierliche Übertragung

von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für IAM Identity Center. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der gesammelten Informationen von können Sie ermitteln CloudTrail, welche Anfrage an das IAM Identity Center gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

In der folgenden Tabelle werden die CloudTrail Ereignisse von IAM Identity Center, ihre CloudTrail Ereignisquellen und die entsprechenden APIs zusammengefasst. Weitere Informationen zu den APIs finden Sie in den [IAM Identity Center-API-Referenzen](#).

 Note

Es gibt eine zusätzliche Gruppe von CloudTrail Ereignissen, die als, bezeichnet werden Sign-in, wenn AWS Sie sich AWS als IAM Identity Center-Benutzer anmelden. Für diese Ereignisse gibt es keine passenden öffentlichen APIs und sind daher nicht in den API-Referenzen aufgeführt.

CloudTrail Ereignisse	Öffentliche APIs	Description	CloudTrail Quellen von Ereignissen
IAM Identity Center	IAM Identity Center	Die IAM Identity Center-APIs ermöglichen die Verwaltung von Berechtigungssätzen, Anwendungen, vertrauenswürdigem Token-Ausstellen, Konto- und Anwendungszuweisungen, IAM Identity Center-Instanzen und -Tags.	sso.amazonaws.com

CloudTrail Ereignisse	Öffentliche APIs	Description	CloudTrail Quellen von Ereignissen
Identitätsspeicher	Identitätsspeicher	Die Identity Store-APIs ermöglichen die Verwaltung des Lebenszyklus der Benutzer und Gruppen Ihrer Mitarbeiter sowie der Gruppenmitgliedschaften der Benutzer. Außerdem unterstützen sie die Verwaltung der MFA-Geräte der Benutzer.	sso-directory.amazonaws.com , identitystore.amazonaws.com
OIDC	OIDC	Die OIDC-APIs unterstützen die Verbreitung vertrauenswürdiger Identitäten sowie die Anmeldung bei AWS CLI und IDE-Toolkits als bereits authentifizierter IAM Identity Center-Benutzer.	sso.amazonaws.com , sso-oauth.amazonaws.com
AWS auf das Portal zugreifen	AWS auf das Portal zugreifen	Die AWS Access Portal-APIs unterstützen den Betrieb des AWS Access Portals und Benutzer, die Kontoanmeldinformationen über das erhalten AWS CLI.	sso.amazonaws.com

CloudTrail Ereignisse	Öffentliche APIs	Description	CloudTrail Quellen von Ereignissen
SCIM	ABSCHAUM	Die SCIM-APIs unterstützen die Bereitstellung von Benutzern, Gruppen und Gruppenmitgliedschaften über das SCIM-Protokoll. Weitere Informationen finden Sie unter Protokollierung von IAM Identity Center SCIM-API-Aufrufen mit AWS CloudTrail .	identitystore-scim.amazonaws.com
AWS-Anmeldung	Keine öffentliche API	AWS sendet Sign-in CloudTrail Ereignisse für die Benutzerauthentifizierung aus und der Verbund fließt in das IAM Identity Center.	signin.amazonaws.com

Themen

- [CloudTrail Anwendungsfälle für IAM Identity Center](#)
- [Informationen zum IAM Identity Center in CloudTrail](#)

CloudTrail Anwendungsfälle für IAM Identity Center

Die CloudTrail Ereignisse, die IAM Identity Center ausgibt, können für eine Vielzahl von Anwendungsfällen wertvoll sein. Unternehmen können diese Ereignisprotokolle verwenden, um den Benutzerzugriff und die Benutzeraktivitäten in ihrer AWS Umgebung zu überwachen und zu überprüfen. Dies kann bei der Einhaltung von Vorschriften helfen, da in den Protokollen Details darüber erfasst werden, wer wann auf welche Ressourcen zugreift. Sie können die CloudTrail Daten

auch für die Untersuchung von Vorfällen verwenden, sodass Teams Benutzeraktionen analysieren und verdächtiges Verhalten verfolgen können. Darüber hinaus kann der Ereignisverlauf bei der Problembehebung helfen, da er einen Überblick über Änderungen bietet, die im Laufe der Zeit an Benutzerberechtigungen und Konfigurationen vorgenommen wurden.

In den folgenden Abschnitten werden die grundlegenden Anwendungsfälle beschrieben, die Ihre Arbeitsabläufe beeinflussen, wie z. B. Audit, Untersuchung von Vorfällen und Problembehebung.

Identifizierung des Benutzers in benutzerinitiierten Ereignissen von IAM Identity Center CloudTrail

IAM Identity Center gibt zwei CloudTrail Felder aus, anhand derer Sie den IAM Identity Center-Benutzer identifizieren können, der hinter den CloudTrail Ereignissen steht, z. B. bei der Anmeldung bei IAM Identity Center oder bei der Nutzung des AWS Zugriffsportals AWS CLI, einschließlich der Verwaltung von MFA-Geräten:

- **userId**— Die eindeutige und unveränderliche Benutzerkennung aus dem Identity Store einer IAM Identity Center-Instanz.
- **identityStoreArn**— Der Amazon-Ressourcenname (ARN) des Identity Stores, der den Benutzer enthält.

Die **identityStoreArn** Felder **userId** und werden in dem **onBehalfOf** Element angezeigt, das innerhalb des [userIdentity](#) Elements verschachtelt ist, wie im folgenden Beispiel für ein CloudTrail Ereignisprotokoll dargestellt. Dieses Ereignisprotokoll zeigt diese beiden Felder bei einem Ereignis mit dem **userIdentity** Typ "IdentityCenterUser". Sie finden diese Felder auch bei Ereignissen für authentifizierte IAM Identity Center-Benutzer, deren **userIdentity** Typ "" Unknown ist. Ihre Workflows sollten beide Typwerte akzeptieren.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

 Tip

Wir empfehlen Ihnen, `userId` und `identityStoreArn` zur Identifizierung des Benutzers zu verwenden, der hinter IAM Identity CloudTrail Center-Ereignissen steht. Die `principalId` Felder `userName` und unter dem `userIdentity` Element sind nicht mehr verfügbar. Wenn Ihre Workflows, wie z. B. Audit oder Incident-Response, davon abhängen, dass Sie Zugriff auf die `habenusername`, haben Sie zwei Möglichkeiten:

- Rufen Sie den Benutzernamen aus dem IAM Identity Center-Verzeichnis ab, wie unter [beschrieben Benutzername bei Anmeldeereignissen CloudTrail](#).
- Ruft den Wert `UserName` ab, den IAM Identity Center unter dem `additionalEventData` Element in ausgibt. Sign-in Für diese Option ist kein Zugriff auf das IAM Identity Center-Verzeichnis erforderlich. Weitere Informationen finden Sie unter [Benutzername bei Anmeldeereignissen CloudTrail](#).

Um die Details eines Benutzers einschließlich des `username` Felds abzurufen, fragen Sie den Identity Store mit Benutzer-ID und Identity Store-ID als Parametern ab. Sie können diese Aktion über die [DescribeUser](#) API-Anforderung oder über die CLI ausführen. Im Folgenden finden Sie ein Beispiel für einen CLI-Befehl. Sie können den `region` Parameter weglassen, wenn sich Ihre IAM Identity Center-Instanz in der CLI-Standardregion befindet.

```
aws identitystore describe-user \  
--identity-store-id d-1234567890 \  
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \  
--region your-region-id
```

Um den Identity Store-ID-Wert für den CLI-Befehl im vorherigen Beispiel zu ermitteln, können Sie die Identity Store-ID aus dem `identityStoreArn` Wert extrahieren. Im Beispiel-ARN lautet `arn:aws:identitystore::111122223333:identitystore/d-1234567890` die Identity Store-ID `d-1234567890`. Sie können die Identity Store-ID auch finden, indem Sie in der IAM Identity Center-Konsole im Abschnitt „Einstellungen“ zur Registerkarte „Identitätsspeicher“ navigieren.

Wenn Sie die Suche nach Benutzern im IAM Identity Center-Verzeichnis automatisieren, empfehlen wir Ihnen, die Häufigkeit von Benutzersuchen abzuschätzen und das [IAM Identity Center-Drossellimit für die Identity Store API zu berücksichtigen](#). Durch das Zwischenspeichern von abgerufenen Benutzerattributen können Sie das Drossellimit einhalten.

Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzung

Das bei Anmeldeereignissen ausgegebene [AuthWorkflowID](#) Feld ermöglicht die Verfolgung aller CloudTrail Ereignisse, die mit einer Anmeldesequenz vor Beginn einer IAM Identity Center-Benutzersitzung verknüpft sind.

Für Benutzeraktionen innerhalb des AWS Access Portals wird der `credentialId` Wert auf die ID der Sitzung des IAM Identity Center-Benutzers gesetzt, mit der die Aktion angefordert wurde. Sie können diesen Wert verwenden, um CloudTrail Ereignisse zu identifizieren, die innerhalb derselben authentifizierten IAM Identity Center-Benutzersitzung im AWS Access Portal ausgelöst wurden.

Note

Sie können ihn nicht verwenden `credentialId`, um Anmeldeereignisse mit nachfolgenden Ereignissen zu korrelieren, z. B. der Nutzung des Access Portals. AWS Der Wert des `credentialId` Feldes, der bei Anmeldeereignissen ausgegeben wird, ist von interner Bedeutung, und es wird empfohlen, sich nicht darauf zu verlassen. Der Wert des `credentialId` Feldes, das für [AWS Access Portal-Ereignisse ausgegeben wird, die mit OIDC](#) aufgerufen werden, entspricht der ID des Zugriffstokens.

Identifizierung der Hintergrund Sitzungsdetails von Benutzern in benutzerinitiierten IAM Identity Center-Ereignissen CloudTrail

Das folgende CloudTrail Ereignis erfasst den Prozess des OAuth 2.0-Token austauschs, bei dem ein vorhandenes Zugriffstoken (das `subjectToken`), das die interaktive Sitzung des Benutzers darstellt, gegen ein Aktualisierungstoken (das) ausgetauscht wird. `requestedTokenType` Mit dem Aktualisierungstoken können alle vom Benutzer initiierten Jobs mit langer Laufzeit mit den Benutzerberechtigungen weiterlaufen, auch wenn sich der Benutzer abmeldet.

Bei Hintergrund Sitzungen von IAM Identity [Center-Benutzern enthält das CloudTrail Ereignis ein zusätzliches Element](#), das `resource requestParameters` im Element genannt wird. Der `resource` Parameter enthält den Amazon-Ressourcennamen (ARN) des Jobs, der im Hintergrund ausgeführt wird. Dieses Element ist nur in CloudTrail Ereignisdatensätzen vorhanden und nicht in den [CreateTokenWithIAM](#) API- oder SDK-Antworten von IAM Identity Center enthalten.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
"redirectUri": "https://example.com/callback",
"assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
"subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
"subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
"requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
"resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

Korrelieren von Benutzern zwischen IAM Identity Center und externen Verzeichnissen

IAM Identity Center bietet zwei Benutzerattribute, mit denen Sie einen Benutzer in seinem Verzeichnis mit demselben Benutzer in einem externen Verzeichnis korrelieren können (z. B. und). Microsoft Active Directory Okta Universal Directory

- **externalId**— Die externe ID eines IAM Identity Center-Benutzers. Wir empfehlen, diese Kennung einer unveränderlichen Benutzerkennung im externen Verzeichnis zuzuordnen. Beachten Sie, dass IAM Identity Center diesen Wert nicht ausgibt in. CloudTrail
- **username**— Ein vom Kunden bereitgestellter Wert, mit dem sich Benutzer normalerweise anmelden. Der Wert kann sich ändern (z. B. bei einem SCIM-Update). Beachten Sie, dass bei Angabe der Identitätsquelle der Benutzername Directory Service, den IAM Identity Center ausgibt, mit dem Benutzernamen CloudTrail übereinstimmt, den Sie zur Authentifizierung eingeben. Der Benutzername muss nicht exakt mit dem Benutzernamen im IAM Identity Center-Verzeichnis übereinstimmen.

Wenn Sie Zugriff auf die CloudTrail Ereignisse haben, aber nicht auf das IAM Identity Center-Verzeichnis, können Sie den Benutzernamen verwenden, der bei der Anmeldung unter dem `additionalEventData` Element angegeben wurde. Weitere Informationen zum Benutzernamen in finden Sie `additionalEventData` unter. [Benutzername bei Anmeldeereignissen CloudTrail](#)

Die Zuordnung dieser beiden Benutzerattribute zu den entsprechenden Benutzerattributen in einem externen Verzeichnis wird im IAM Identity Center definiert, wenn die Identitätsquelle der Directory Service ist. Weitere Informationen finden Sie unter. [Attributzuordnungen zwischen dem IAM Identity Center und dem Verzeichnis externer Identitätsanbieter](#) Externe Benutzer IdPs , die Benutzern SCIM zur Verfügung stellen, haben ihre eigene Zuordnung. Auch wenn Sie das IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, können Sie das `externalId` Attribut verwenden, um Sicherheitsprinzipale mit Ihrem externen Verzeichnis abzugleichen.

Im folgenden Abschnitt wird erläutert, wie Sie anhand des Benutzernamens und nach einem IAM Identity Center-Benutzer suchen können. `username` `externalId`

Einen IAM Identity Center-Benutzer anhand seines Benutzernamens und seiner externen ID anzeigen

Sie können Benutzerattribute für einen bekannten Benutzernamen aus dem IAM Identity Center-Verzeichnis abrufen, indem Sie zunächst `userId` mithilfe der [GetUserId](#) API-Anforderung einen entsprechenden Benutzernamen anfordern und dann eine [DescribeUser](#) API-Anfrage stellen, wie im vorherigen Beispiel gezeigt. Das folgende Beispiel zeigt, wie Sie eine `userId` aus dem Identity Store für einen bestimmten Benutzernamen abrufen können. Sie können den `region` Parameter weglassen, wenn sich Ihre IAM Identity Center-Instanz mit der CLI in der Standardregion befindet.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Ebenso können Sie den gleichen Mechanismus verwenden, wenn Sie den `kennenexternalId`. Aktualisieren Sie den Attributpfad im vorherigen Beispiel mit dem `externalId` Wert und den Attributwert mit dem spezifischen `externalId`, nach dem Sie suchen.

Den Secure Identifier (SID) eines Benutzers in Microsoft Active Directory (AD) und die ExternalID anzeigen

In bestimmten Fällen gibt IAM Identity Center die SID eines Benutzers im `principalId` Feld der CloudTrail Ereignisse aus, z. B. bei Ereignissen, die das AWS Zugriffsportal und die OIDC-APIs ausgeben. Diese Fälle werden schrittweise eingestellt. Wir empfehlen, dass Ihre Workflows das AD-Attribut `objectguid` verwenden, wenn Sie eine eindeutige Benutzererkennung von AD benötigen. Sie finden diesen Wert im `externalId` Attribut im IAM Identity Center-Verzeichnis. Wenn Ihre Workflows jedoch die Verwendung von SID erfordern, rufen Sie den Wert aus AD ab, da er nicht über die IAM Identity Center-APIs verfügbar ist.

[Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzung](#) beschreibt, wie Sie mithilfe der `username` Felder `externalId` und einen IAM Identity Center-Benutzer einem entsprechenden Benutzer in einem externen Verzeichnis zuordnen können. Standardmäßig wird IAM Identity Center dem `objectguid` Attribut in AD `externalId` zugeordnet, und diese Zuordnung ist behoben. IAM

Identity Center bietet Administratoren die Flexibilität, andere Zuordnungen username als bei der Standardzuordnung `userprincipalname` in AD vorzunehmen.

Sie können diese Zuordnungen in der IAM Identity Center-Konsole anzeigen. Navigieren Sie in den Einstellungen zur Registerkarte „Identitätsquelle“ und wählen Sie im Menü „Aktionen“ die Option Synchronisierung verwalten aus. Wählen Sie im Abschnitt „Synchronisation verwalten“ die Schaltfläche „Attributzuordnungen anzeigen“.

Sie können zwar jede eindeutige AD-Benutzerkennung verwenden, die im IAM Identity Center verfügbar ist, um einen Benutzer in AD zu suchen, wir empfehlen jedoch, die `objectguid` in Ihren Abfragen zu verwenden, da es sich um eine unveränderliche Kennung handelt. Das folgende Beispiel zeigt, wie Microsoft AD mit Powershell abgefragt wird, um einen Benutzer mithilfe des `objectguid` Benutzerwerts von abzurufen. `16809ecc-7225-4c20-ad98-30094aefdbca` Eine erfolgreiche Antwort auf diese Abfrage beinhaltet die SID des Benutzers.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell

Get-ADUser `
  -Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

Informationen zum IAM Identity Center in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im IAM Identity Center eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Eventverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Eventverlauf [anzeigen](#).

Note

Weitere Informationen zur Entwicklung der Benutzeridentifikation und der Verfolgung von Benutzeraktionen bei CloudTrail Ereignissen finden Sie im AWS Sicherheitsblog unter [Wichtige Änderungen an CloudTrail Ereignissen für IAM Identity Center](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für IAM Identity Center, erstellen Sie einen Trail. Ein Trail ermöglicht die CloudTrail

Übermittlung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Wenn die CloudTrail Protokollierung in Ihrem aktiviert ist AWS-Konto, werden API-Aufrufe an IAM Identity Center-Aktionen in Protokolldateien aufgezeichnet. IAM Identity Center-Datensätze werden zusammen mit anderen AWS Servicedatensätzen in eine Protokolldatei geschrieben. CloudTrail bestimmt anhand eines Zeitraums und einer Dateigröße, wann eine neue Datei erstellt und in sie geschrieben werden muss.

CloudTrail Ereignisse für unterstützte IAM Identity Center-APIs

Die folgenden Abschnitte enthalten Informationen zu den CloudTrail Ereignissen im Zusammenhang mit den folgenden APIs, die IAM Identity Center unterstützt:

- [IAM Identity Center-API](#)
- [Identitätsspeicher-API](#)
- [OIDC-API](#)
- [AWS auf die Portal-API zugreifen](#)
- [SCIM-API](#)

CloudTrail Ereignisse von IAM Identity Center-API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen IAM Identity Center-Operationen zusammen mit der `sso.amazonaws.com` Ereignisquelle auslösen. Weitere Informationen zu den öffentlichen IAM Identity Center-API-Vorgängen finden Sie in der [IAM Identity Center API-Referenz](#).

Möglicherweise finden Sie zusätzliche Ereignisse unter API-Vorgängen der CloudTrail IAM Identity Center-Konsole, auf die die Konsole angewiesen ist. Weitere Informationen zu diesen Konsolen-APIs finden Sie in der [Service Authorization Reference](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
- [DeleteInlinePolicyFromPermissionSet](#)

- [DeleteInstance](#)
- [DeleteInstanceAccessControlAttributeConfiguration](#)
- [DeletePermissionsBoundaryFromPermissionSet](#)
- [DeletePermissionSet](#)
- [DeleteTrustedTokenIssuer](#)
- [DescribeAccountAssignmentCreationStatus](#)
[s](#)
- [DescribeAccountAssignmentDeletionStatus](#)
- [DescribeApplication](#)
- [DescribeApplicationAssignment](#)
- [DescribeApplicationProvider](#)
- [DescribeInstance](#)
- [DescribeInstanceAccessControlAttributeConfiguration](#)
- [DescribePermissionSet](#)
- [DescribePermissionSetProvisioningStatus](#)
- [DescribeTrustedTokenIssuer](#)

- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
- [GetPermissionsBoundaryForPermissionSet](#)
- [ListAccountAssignmentCreationStatus](#)
- [ListAccountAssignmentDeletionStatus](#)
- [ListAccountAssignments](#)
- [ListAccountAssignmentsForPrincipal](#)
- [ListAccountsForProvisionedPermissionSet](#)
- [ListApplicationAccessScopes](#)
- [ListApplicationAssignments](#)
-

[ListApplicationAssignmentsForPrincipal](#)

•

[ListApplicationAuthenticationMethods](#)

•

[ListApplicationGrants](#)

•

[ListApplicationProviders](#)

•

[ListApplications](#)

•

[ListCustomerManagedPolicyReferencesInPermissionSet](#)

•

[ListInstances](#)

•

[ListManagedPoliciesInPermissionSet](#)

•

[ListPermissionSetProvisioningStatus](#)

•

[ListPermissionSets](#)

•

[ListPermissionSetsProvisionedToAccount](#)

•

[ListTagsForResource](#)

•

[ListTrustedTokenIssuers](#)

•

[ProvisionPermissionSet](#)

•

[PutApplicationAccessScope](#)

•

[PutApplicationAssignmentConfiguration](#)

- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

CloudTrail Ereignisse von Identity Store-API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen Identity Store-Operationen zusammen mit der `identitystore.amazonaws.com` Ereignisquelle auslösen. Weitere Informationen zu den öffentlichen Identity Store-API-Vorgängen finden Sie in der [Identity Store-API-Referenz](#).

Möglicherweise finden Sie zusätzliche Ereignisse CloudTrail für die API-Operationen der Identity Store-Konsole mit der `sso-directory.amazonaws.com` Ereignisquelle. Diese APIs unterstützen

die Konsole und das AWS Zugriffsportal. Wenn Sie das Auftreten eines bestimmten Vorgangs erkennen müssen, z. B. das Hinzufügen eines Mitglieds zu einer Gruppe, empfehlen wir, sowohl öffentliche als auch Konsolen-API-Operationen in Betracht zu ziehen. Weitere Informationen zu diesen Konsolen-APIs finden Sie in der [Service Authorization Reference](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

CloudTrail Ereignisse von OIDC-API-Vorgängen

Die folgende Liste enthält die CloudTrail Ereignisse, die die öffentlichen OIDC-Operationen auslösen. Weitere Informationen zu den öffentlichen OIDC-API-Vorgängen finden Sie in der [OIDC-API-Referenz](#).

- [CreateToken](#)(Quelle des Ereignisses) `sso.amazonaws.com`
- [CreateTokenWithIAM](#)(Quelle des Ereignisses) `sso-oauth.amazonaws.com`

CloudTrail Ereignisse von AWS auf den API-Betrieb des Portals zugreifen

Die folgende Liste enthält die CloudTrail Ereignisse, die von den API-Vorgängen des AWS Access Portals zusammen mit der `sso.amazonaws.com` Ereignisquelle ausgelöst werden. Die API-Operationen, bei denen festgestellt wurde, dass sie in der öffentlichen API nicht verfügbar sind, unterstützen den Betrieb des AWS Zugangsportals. Die Verwendung von AWS CLI kann dazu führen, dass CloudTrail Ereignisse sowohl bei den API-Vorgängen des Portals für den öffentlichen AWS Zugriff als auch bei Vorgängen, die in der öffentlichen API nicht verfügbar sind, ausgegeben werden. Weitere Informationen zu den API-Vorgängen für öffentliche AWS Portale finden Sie in der API-Referenz für das [AWS Zugangsportal](#).

- `Authenticate`(In der öffentlichen API nicht verfügbar. Ermöglicht die Anmeldung beim AWS Access-Portal.)
- `Federate`(In der öffentlichen API nicht verfügbar. Ermöglicht den Zusammenschluss von Anwendungen.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- `ListApplications`(In der öffentlichen API nicht verfügbar. Stellt den Benutzern zugewiesene Ressourcen zur Anzeige im AWS Access-Portal bereit.)
- `ListProfilesForApplication`(In der öffentlichen API nicht verfügbar. Stellt Anwendungsmetadaten zur Anzeige im AWS Access-Portal bereit.)
- [GetRoleCredentials](#)
- [Logout](#)

CloudTrail Ereignisse von SCIM-API-Vorgängen

Informationen zu öffentlichen SCIM-API-Vorgängen finden Sie in der API-Referenz für das [AWS Zugriffsportal](#).

Identitätsinformationen in IAM Identity Center-Ereignissen CloudTrail

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root-Benutzer- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.
- Ob die Anfrage von einem IAM Identity Center-Benutzer gestellt wurde. Wenn ja, sind die `identityStoreArn` Felder `userId` und in den CloudTrail Ereignissen verfügbar, um den IAM Identity Center-Benutzer zu identifizieren, der die Anfrage initiiert hat. Weitere Informationen finden Sie unter [Identifizierung des Benutzers in benutzerinitiierten Ereignissen von IAM Identity Center CloudTrail](#).

Weitere Informationen finden Sie unter [CloudTrail -Element `userIdentity`](#).

 Note

Derzeit gibt IAM Identity Center keine CloudTrail Ereignisse für die Benutzeranmeldung bei AWS verwalteten Webanwendungen (z. B. Amazon SageMaker AI Studio) mit der [OIDC-API aus](#). Diese Webanwendungen sind Teil der breiteren Palette von Webanwendungen [the section called "AWS verwaltete Anwendungen"](#), zu denen auch Nicht-Webanwendungen wie Amazon Athena SQL und Amazon S3 Access Grants gehören.

Wissenswertes über CloudTrail Ereignisse für IAM Identity Center

Ein Trail ist eine Konfiguration, durch die Ereignisse an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Ereignisse sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie nicht in einer bestimmten Reihenfolge. Erfahren Sie mehr über den [Inhalt eines CloudTrail Datensatzes](#) im CloudTrail Benutzerhandbuch.

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine `DescribePermissionsPolicies` Aktion aufzeichnet, die von einem IAM-Benutzer (`samadams`) ausgeführt wird, der mit IAM Identity Center interagiert:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
```



```

        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIIJM2K4example",
        "userName": "samadams"
    },
    "eventTime": "2017-11-29T22:39:43Z",
    "eventSource": "sso.amazonaws.com",
    "eventName": "DescribePermissionsPolicies",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
    "requestParameters": {
        "permissionSetId": "ps-79a0dde74b95ed05"
    },
    "responseElements": null,
    "requestID": "319ac6a1-d556-11e7-a34f-69a333106015",
    "eventID": "a93a952b-13dd-4ae5-a156-d3ad6220b071",
    "readOnly": true,
    "resources": [

    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
]
}

```

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine `ListApplications` Aktion aufzeichnet, die von einem IAM Identity Center-Benutzer im Access Portal ausgeführt wurde: AWS

```

{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",

```

```

        "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
      },
      "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
    },
    "eventTime": "2017-11-29T18:48:28Z",
    "eventSource": "sso.amazonaws.com",
    "eventName": "ListApplications",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
    "eventID": "e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
]
}

```

Dieses Beispiel zeigt einen CloudTrail Protokolleintrag, der eine CreateToken Aktion erfasst, die von einem IAM Identity Center-Benutzer ausgeführt wird, der sich beim IAM Identity Center OIDC-Dienst authentifiziert:

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
  },
  "eventTime": "2020-06-16T01:31:15Z",
  "eventSource": "sso.amazonaws.com",
  "eventName": "CreateToken",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",

```

```

    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
    "requestParameters": {
      "clientId": "clientid1234example",
      "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "grantType": "urn:ietf:params:oauth:grant-type:device_code",
      "deviceCode": "devicecode1234example"
    },
    "responseElements": {
      "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "tokenType": "Bearer",
      "expiresIn": 28800,
      "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "IdentityStoreId",
        "ARN": "d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

Grundlegendes zu IAM Identity Center-Anmeldeereignissen

AWS CloudTrail zeichnet erfolgreiche und erfolglose Anmeldeereignisse für alle IAM Identity Center-Identitätsquellen auf. Identitäten aus IAM Identity Center und Active Directory (AD Connector und AWS Managed Microsoft AD) enthalten zusätzliche Anmeldeereignisse, die jedes Mal erfasst werden, wenn ein Benutzer aufgefordert wird, eine bestimmte Herausforderung oder einen bestimmten Faktor zu lösen, zusätzlich zum Status dieser speziellen Anforderung zur Überprüfung der Anmeldeinformationen. Erst wenn ein Benutzer alle erforderlichen Anforderungen an die Anmeldeinformationen abgeschlossen hat, wird er angemeldet, was dazu führt, dass ein Ereignis protokolliert wird. `UserAuthentication`

In der folgenden Tabelle sind die Namen der einzelnen IAM Identity CloudTrail Center-Anmeldeereignisse, ihr Zweck und ihre Anwendbarkeit auf verschiedene Identitätsquellen aufgeführt.

Ereignisname	Zweck des Ereignisses	Anwendbarkeit der Identitätsquelle
CredentialChallenge	Wird verwendet, um zu benachrichtigen, dass IAM Identity Center den Benutzer aufgefordert hat, eine bestimmte Herausforderung bei den Anmeldeinformationen zu lösen, und gibt anCredentialType , welche Anforderung erforderlich war (z. B. PASSWORD oder TOTP).	Systemeigene IAM Identity Center-Benutzer, AD Connector und AWS Managed Microsoft AD
CredentialVerification	Wird verwendet, um zu benachrichtigen, dass der Benutzer versucht hat, eine bestimmte CredentialChallenge Anfrage zu lösen, und gibt an, ob die Anmeldeinformationen erfolgreich waren oder fehlgeschlagen sind.	Systemeigene IAM Identity Center-Benutzer, AD Connector und AWS Managed Microsoft AD
UserAuthentication	Wird verwendet, um zu benachrichtigen, dass alle Authentifizierungsanforderungen, mit denen der Benutzer konfrontiert wurde, erfolgreich erfüllt wurden und dass der Benutzer erfolgreich angemeldet wurde. Wenn Benutzer die erforderlichen Anmeldeinformationen nicht erfolgreich abschließen, wird kein	Alle Identitätsquellen

Ereignisname	Zweck des Ereignisses	Anwendbarkeit der Identitätsquelle
--------------	-----------------------	------------------------------------

UserAuthentication
Ereignis protokolliert.

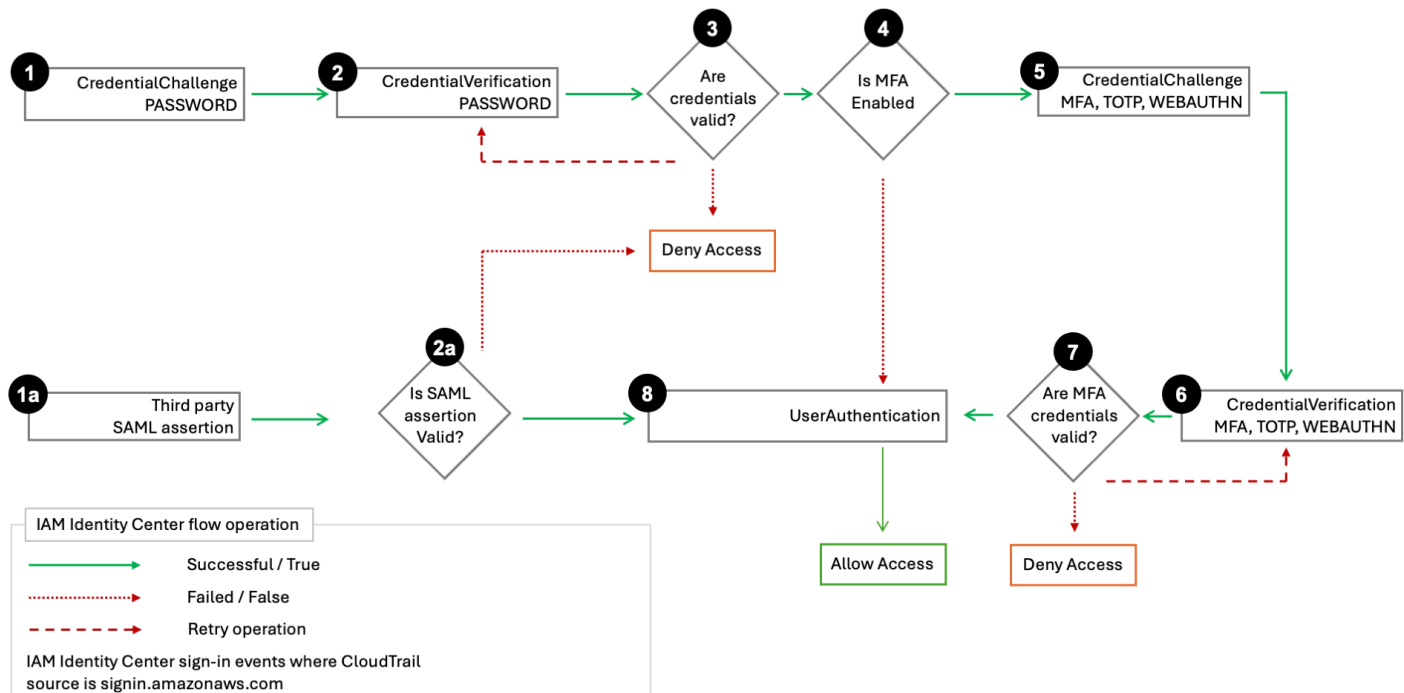
In der folgenden Tabelle sind zusätzliche nützliche Ereignisdatenfelder aufgeführt, die in bestimmten CloudTrail Anmeldeereignissen enthalten sind.

Feld	Zweck des Ereignisses	Sign-in Anwendbarkeit von Ereignissen	Beispielwerte
AuthWorkflowID	Wird verwendet, um alle Ereignisse zu korrelieren, die über eine gesamte Anmeldesequenz ausgegeben wurden. Bei jeder Benutzermeldung können mehrere Ereignisse vom IAM Identity Center ausgelöst werden.	CredentialChallenge, CredentialVerification, UserAuthentication	„AuthWorkflowID“: „9de74b32-8362-4a01-a524-de21df59fd83“
CredentialType	Wird verwendet, um die Anmeldeinformationen oder Faktoren anzugeben, die angefochten wurden. UserAuthentication Ereignisse umfassen alle CredentialType Werte, die in der Anmeldesequenz	CredentialChallenge, CredentialVerification, UserAuthentication	CredentialType: „PASSWORD“ oder „: CredentialType „PASSWORD, TOTP“ (zu den möglichen Werten gehören: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)

Feld	Zweck des Ereignisses	Sign-in Anwendbarkeit von Ereignissen	Beispielwerte
	Sequenz des Benutzers erfolgreich verifiziert wurden.		
DeviceEnrollmentRequired	Wird verwendet, um anzugeben, dass der Benutzer bei der Anmeldung ein MFA-Gerät registrieren musste und dass der Benutzer diese Anfrage erfolgreich abgeschlossen hat.	UserAuthentication	"DeviceEnrollmentRequired": „wahr“
LoginTo	Wird verwendet, um den Ort der Weiterleitung nach einer erfolgreichen Anmeldesequenz anzugeben.	UserAuthentication	"LoginTo": "https://mydirectory.awsapps.com/start/....."

CloudTrail Ereignisse in den Anmeldeabläufen von IAM Identity Center

Das folgende Diagramm beschreibt den Anmeldeablauf und die ausgehenden CloudTrail Ereignisse. Sign-in



Das Diagramm zeigt einen Kennwortanmeldeablauf und einen Verbundanmeldeablauf.

Der Ablauf der Passwortanmeldung, der aus den Schritten 1—8 besteht, veranschaulicht die Schritte bei der Anmeldung mit Benutzername und Passwort. IAM Identity Center wird `userIdentity.additionalEventData.CredentialType` auf "PASSWORD" gesetzt, und IAM Identity Center durchläuft den Abfrage-Antwort-Zyklus für Anmeldeinformationen und versucht es bei Bedarf erneut.

Die Anzahl der Schritte hängt von der Art der [Anmeldung und dem Vorhandensein der Multifaktor-Authentifizierung \(MFA\) ab](#). Der anfängliche Vorgang führt zu drei oder fünf CloudTrail Ereignissen, bei denen die Sequenz für eine erfolgreiche Authentifizierung `UserAuthentication` beendet wird. Erfolgreiche Versuche zur Kennwortauthentifizierung führen zu weiteren CloudTrail Ereignissen, da das IAM Identity Center erneut `CredentialChallenge` eine reguläre Authentifizierung oder, falls aktiviert, eine MFA-Authentifizierung durchführt.

Der Ablauf der Passwortanmeldung deckt auch das Szenario ab, in dem sich ein IAM Identity Center-Benutzer, der mit einem `CreateUser` API-Aufruf neu erstellt wurde, mit einem Einmalkennwort (OTP) anmeldet. Der Anmeldeinformationstyp in diesem Szenario ist „`EMAIL_OTP`“.

Der Verbundanmeldeablauf, der aus den Schritten 1a, 2a und 8 besteht, veranschaulicht die wichtigsten Schritte während des Verbundauthentifizierungsprozesses, bei dem eine [SAML-Assertion von einem Identitätsanbieter bereitgestellt](#), vom IAM Identity Center validiert wird und im Erfolgsfall zu folgenden Ergebnissen führt. `UserAuthentication` IAM Identity Center ruft die interne MFA-Authentifizierungssequenz in den Schritten 3 bis 7 nicht auf, da ein externer, verbundener Identitätsanbieter für die gesamte Authentifizierung der Benutzeranmeldeinformationen verantwortlich ist.

Benutzername bei Anmeldeereignissen CloudTrail

IAM Identity Center gibt das `UserName` Feld unter dem `additionalEventData` Element einmal pro erfolgreicher Anmeldung eines IAM Identity Center-Benutzers aus. In der folgenden Liste werden die beiden Anmeldeereignisse im Geltungsbereich sowie die Bedingungen beschrieben, unter denen diese Ereignisse auftreten. Nur eine der Bedingungen kann zutreffen, wenn sich ein Benutzer anmeldet.

- `CredentialChallenge`
 - Wann `CredentialType` ist "PASSWORD" — gilt für die Passwortauthentifizierung mit Directory Service oder IAM-Identity-Center-Verzeichnis.
 - Wann `CredentialType` ist "EMAIL_OTP" — gilt nur für den IAM-Identity-Center-Verzeichnis Fall, dass ein mit einem `CreateUser` API-Aufruf erstellter Benutzer versucht, sich zum ersten Mal anzumelden, und der Benutzer ein Einmalkennwort erhält, mit dem er sich einmal mit diesem Passwort anmelden kann.
- `UserAuthentication`
 - Wann `CredentialType` ist "EXTERNAL_IDP" — gilt für die Authentifizierung mit einem externen IdP.

Der Wert von `UserName` für erfolgreiche Authentifizierungen lautet wie folgt:

- Wenn die Identitätsquelle ein externer IdP ist, entspricht der Wert dem `nameID` Wert in der eingehenden SAML-Assertion. Dieser Wert entspricht dem `UserName` Feld in der. IAM-Identity-Center-Verzeichnis
- Wenn die Identitätsquelle ein ist IAM-Identity-Center-Verzeichnis, entspricht der ausgegebene Wert dem `UserName` Feld in diesem Verzeichnis.
- Wenn es sich bei der Identitätsquelle um den Wert handelt Directory Service, entspricht der ausgegebene Wert dem Benutzernamen, den der Benutzer bei der Authentifizierung eingibt.

Beispielsweise kann sich ein Benutzer, der den Benutzernamen `hatanyuser@company.com`, `mitanyuser`, oder authentifizieren `anyuser@company.comcompany.com/anyuser`, und in jedem Fall wird der eingegebene Wert CloudTrail entsprechend ausgegeben.

Sicherheitsmaskierung falscher Versuche mit einem Benutzernamen

Das `UserName` Feld enthält die Zeichenfolge, `HIDDEN_DUE_TO_SECURITY_REASONS` wenn es sich bei dem aufgezeichneten Ereignis um einen Fehler bei der Konsolenanmeldung handelt, der durch eine falsche Eingabe des Benutzernamens verursacht wurde. CloudTrail zeichnet den Inhalt in diesem Fall nicht auf, da der Text vertrauliche Informationen enthalten könnte, wie in den folgenden Beispielen beschrieben:

- Ein Benutzer gibt versehentlich ein Passwort im Feld für den Benutzernamen ein.
- Ein Benutzer gibt versehentlich den Kontonamen eines persönlichen E-Mail-Kontos, eine Bank-Anmelde-ID oder eine andere private ID ein.

Tip

Wir empfehlen Ihnen, `userId` und `identityStoreArn` zur Identifizierung des Benutzers zu verwenden, der hinter IAM Identity CloudTrail Center-Ereignissen steht. Wenn Sie das `userName` Feld benötigen, können Sie das Element `userName` unter dem `additionalEventData` Element verwenden, das einmal pro erfolgreicher Anmeldung ausgegeben wird.

Weitere Informationen zur Verwendung des `UserName` Felds finden Sie unter. [Korrelieren von Benutzerereignissen innerhalb derselben Benutzersitzung](#)

Beispielereignisse für Anmeldeszenarien im IAM Identity Center

Die folgenden Beispiele veranschaulichen die typischen CloudTrail Ereignissequenzen, die bei verschiedenen AWS Anmeldeszenarien generiert werden. Diese Beispiele dienen als Referenzmuster, anhand derer Sie Authentifizierungsprotokolle interpretieren, Sicherheitsprobleme identifizieren und überprüfen können, ob Ihre Authentifizierungsrichtlinien ordnungsgemäß funktionieren.

Themen

- [Erfolgreiche Anmeldung, wenn Sie sich nur mit Passwort authentifizieren](#)

- [Erfolgreiche Anmeldung bei der Authentifizierung bei einem externen Identitätsanbieter](#)
- [Erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer TOTP-Authentifikator-App \(Time Based One One Password\)](#)
- [Erfolgreiche Anmeldung, wenn die Authentifizierung mit einem Passwort und eine erzwungene MFA-Registrierung erforderlich sind](#)
- [Die Anmeldung ist aufgrund einer falschen Passwortauthentifizierung fehlgeschlagen](#)

Erfolgreiche Anmeldung, wenn Sie sich nur mit Passwort authentifizieren

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Anmeldung nur mit Passwort.

CredentialChallenge (Passwort)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:33:58Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  }
}
```

```

},
"requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
"eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"serviceEventDetails":{"
  "CredentialChallenge":"Success"
}
}

```

Erfolgreich CredentialVerification (Passwort)

```

{
  "eventVersion":"1.08",
  "userIdentity":{"
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{"
    "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
    "CredentialType":"PASSWORD"
  },
  "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",

```

```

    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{"
      "CredentialVerification":"Success"
    }
  }
}

```

Erfolgreich UserAuthentication (nur Passwort)

```

{
  "eventVersion":"1.08",
  "userIdentity":{"
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{"
    "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo":"https://d-1234567890.awsapps.com/start/?state=QVLbQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBsh1Ic50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType":"PASSWORD"
  }
}

```

```

},
"requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
"eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{"
  "UserAuthentication":"Success"
}
}

```

Erfolgreiche Anmeldung bei der Authentifizierung bei einem externen Identitätsanbieter

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Anmeldung bei der Authentifizierung über das SAML-Protokoll unter Verwendung eines externen Identitätsdienstleisters.

Erfolgreich UserAuthentication (externer Identitätsanbieter)

```

{
  "eventVersion":"1.08",
  "userIdentity":{"
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-07T20:34:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,

```

```

"additionalEventData":{
  "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
  "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
Bsh1Ic50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx
east-1",
  "CredentialType":"EXTERNAL_IDP",
  "UserName":"bobsmith@example.com"
},
"requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
"eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "UserAuthentication":"Success"
}
}

```

Erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer TOTP-Authentifikator-App (Time Based One One Password)

Die folgende Abfolge von Ereignissen zeigt ein Beispiel, bei dem bei der Anmeldung eine mehrstufige Authentifizierung erforderlich war und der Benutzer sich erfolgreich mit einem Passwort und einer TOTP-Authentifikator-App angemeldet hat.

CredentialChallenge (Passwort)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },

```

```

    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:13Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialChallenge",
  "awsRegion":"us-east-1",
  "sourceIpAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
    "CredentialType":"PASSWORD",
    "UserName":"bobsmith@example.com"
  },
  "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
  "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "recipientAccountId":"111122223333",
  "serviceEventDetails":{
    "CredentialChallenge":"Success"
  }
}

```

Erfolgreich CredentialVerification (Passwort)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  }
}

```

```

},
"eventTime":"2020-12-08T20:40:20Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialVerification",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
  "CredentialType":"PASSWORD"
},
"requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
"eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialVerification":"Success"
}
}

```

CredentialChallenge (TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:20Z",

```



```

    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType": "TOTP"
    },
    "requestID": "92c4ac90-0d9b-452d-95d5-728487612f5e",
    "eventID": "29202f08-f240-40cc-b789-c0cea8a27847",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "CredentialChallenge": "Success"
    }
  }
}

```

Erfolgreich CredentialVerification (TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:27Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",

```

```

    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType": "TOTP"
    },
    "requestID": "c40a691f-eeb1-4352-b286-5e909f96f318",
    "eventID": "e889ff1d-fcaf-454f-805d-7132cf2362a4",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "CredentialVerification": "Success"
    }
  }
}

```

Erfolgreich UserAuthentication (Passwort + TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:27Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",

```

```

    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
        "LoginTo": "https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMLui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
        "CredentialType": "PASSWORD,TOTP"
    },
    "requestID": "c40a691f-eeb1-4352-b286-5e909f96f318",
    "eventID": "7a8c8725-db2f-488d-a43e-788dc6c73a4a",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "UserAuthentication": "Success"
    }
}

```

Erfolgreiche Anmeldung, wenn die Authentifizierung mit einem Passwort und eine erzwungene MFA-Registrierung erforderlich sind

Die folgende Abfolge von Ereignissen zeigt eine erfolgreiche Kennwortauthentifizierung, bei der sich der Benutzer registrieren und die Multifaktor-Authentifizierung (MFA) erfolgreich abschließen musste, bevor der Anmeldevorgang abgeschlossen werden konnte.

CredentialChallenge (Passwort)

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",

```

```

    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-09T01:24:02Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIpAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "CredentialType": "PASSWORD",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "321f4b13-42b5-4005-a0f7-826cad26d159",
  "eventID": "8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}

```

Erfolgreich CredentialVerification (Passwort)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",

```

```

    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-09T01:24:09Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,
  "additionalEventData":{
    "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "CredentialType":"PASSWORD"
  },
  "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
  "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
  "readOnly":false,
  "eventType":"AwsServiceEvent",
  "managementEvent":true,
  "eventCategory":"Management",
  "recipientAccountId":"111122223333",
  "serviceEventDetails":{
    "CredentialVerification":"Success"
  }
}

```

Erfolgreich UserAuthentication (Passwort und MFA-Registrierung erforderlich)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",

```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-09T01:24:14Z",
"eventSource":"signin.amazonaws.com",
"eventName":"UserAuthentication",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
  "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrggrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
  "CredentialType":"PASSWORD",
  "DeviceEnrollmentRequired":"true"
},
"requestID":"74d24604-a365-4237-8c4a-350795494b92",
"eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "UserAuthentication":"Success"
}
}

```

Die Anmeldung ist aufgrund einer falschen Passwortauthentifizierung fehlgeschlagen

Die folgende Abfolge von Ereignissen zeigt einen Authentifizierungsversuch, bei dem der Benutzer seinen Benutzernamen erfolgreich eingegeben hat, aber den Schritt zur Kennwortüberprüfung nicht bestanden hat, was zu einer erfolglosen Anmeldung führte.

CredentialChallenge (Passwort)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
  },
  "eventTime": "2020-12-08T18:56:15Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "adbf67c4-8188-4e2b-8527-fe539e328fa7",
    "CredentialType": "PASSWORD",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
  "eventID": "d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

CredentialVerification Fehlgeschlagen (Passwort)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
  },
  "eventTime": "2020-12-08T18:56:21Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "adbf67c4-8188-4e2b-8527-fe539e328fa7",
    "CredentialType": "PASSWORD"
  },
  "requestID": "04528c82-a678-4a1f-a56d-ea2c6445a72a",
  "eventID": "9160fe06-fc2a-474f-9b78-000ee067a09d",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialVerification": "Failure"
  }
}
```

Protokollierung von IAM Identity Center SCIM-API-Aufrufen mit AWS CloudTrail

[IAM Identity Center SCIM](#) ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem Benutzer ausgeführten Aktionen bereitstellt. AWS-Service CloudTrail erfasst API-Aufrufe für SCIM als Ereignisse. Anhand der von CloudTrail gesammelten Informationen können Sie die Informationen über die angeforderte Aktion, Datum und

Uhrzeit der Aktion, Anforderungsparameter usw. ermitteln. Weitere Informationen finden CloudTrail Sie im [AWS CloudTrail Benutzerhandbuch](#).

 Note

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Möglicherweise müssen Sie Ihr Zugriffstoken jedoch rotieren, um Ereignisse von SCIM zu sehen, wenn Ihr Token vor September 2024 erstellt wurde.

Weitere Informationen finden Sie unter [Ein Zugriffstoken rotieren](#).

SCIM unterstützt die Protokollierung der folgenden Operationen als Ereignisse in: CloudTrail

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroup](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

Beispiele für Ereignisse CloudTrail

Die folgenden Beispiele zeigen typische CloudTrail Ereignisprotokolle, die bei SCIM-Vorgängen mit IAM Identity Center generiert werden. Diese Beispiele zeigen die Struktur und den Inhalt von Ereignissen für erfolgreiche Operationen und allgemeine Fehlerszenarien. Sie helfen Ihnen dabei,

zu verstehen, wie CloudTrail Protokolle bei der Behebung von SCIM-Bereitstellungsproblemen zu interpretieren sind.

Erfolgreicher Vorgang **CreateUser**

Dieses CloudTrail Ereignis zeigt einen erfolgreichen CreateUser Vorgang an, der über die SCIM-API ausgeführt wurde. Das Ereignis erfasst sowohl die Anforderungsparameter (mit maskierten vertraulichen Informationen) als auch die Antwortelemente, einschließlich der neu erstellten Benutzer-ID. Dieser Ereignistyp wird generiert, wenn ein Identitätsanbieter mithilfe des SCIM-Protokolls erfolgreich einen neuen Benutzer für IAM Identity Center bereitstellt.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
```

```

    "resourceType" : "User"
  },
  "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
  "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "name": {
    "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "active": true,
  "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
  "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Fehlgeschlagener **PatchGroup** Vorgang: Fehlendes erforderliches Pfadattribut

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen PatchGroup Vorgang an, der zu ValidationException einer Fehlermeldung geführt hat "Missing path in PATCH request". Der Fehler ist aufgetreten, weil für den PATCH Vorgang ein Pfadattribut erforderlich ist, um anzugeben, welches Gruppenattribut geändert werden soll, dieses Attribut jedoch in der Anforderung fehlte.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",

```

```

"eventName": "PatchGroup",
"awsRegion": "us-east-1",
"sourceIPAddress": "xxx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"errorCode": "ValidationException",
"errorMessage": "Missing path in PATCH request",
"requestParameters": {
  "httpBody": {
    "operations": [
      {
        "op": "REMOVE",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Fehlgeschlagener **CreateGroup** Vorgang: Der Gruppenname ist bereits vorhanden

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen CreateGroup Vorgang an, der zu ConflictException einer Fehlermeldung geführt hat "Duplicate GroupDisplayName". Dieser Fehler tritt auf, wenn versucht wird, eine Gruppe mit einem Anzeigenamen zu erstellen, der bereits in IAM Identity Center vorhanden ist. Der Identitätsanbieter muss einen eindeutigen Gruppennamen verwenden oder die vorhandene Gruppe aktualisieren, anstatt eine neue zu erstellen.

```
{
```

```

"eventVersion": "1.10",
"userIdentity": {
  "type": "Unknown",
  "accountId": "123456789012",
  "accessKeyId": "xxxx"
},
"eventTime": "xxxx",
"eventSource": "identitystore-scim.amazonaws.com",
"eventName": "CreateGroup",
"awsRegion": "us-east-1",
"sourceIPAddress": "xxx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"errorCode": "ConflictException",
"errorMessage": "Duplicate GroupDisplayName",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Fehlgeschlagener **PatchUser** Vorgang: Mehrere E-Mail-Adressen werden nicht unterstützt

Dieses CloudTrail Ereignis zeigt einen fehlgeschlagenen PatchUser Vorgang an, der zu `ValidationException` einer Fehlermeldung geführt hat `"List attribute emails exceeds allowed limit of 1"`. Dieser Fehler tritt auf, wenn versucht wird, einem Benutzer mehrere E-Mail-Adressen zuzuweisen, da IAM Identity Center nur eine E-Mail-Adresse pro Benutzer unterstützt. Der Identitätsanbieter muss die SCIM-Zuordnung so konfigurieren, dass nur eine einzige E-Mail-Adresse für jeden Benutzer gesendet wird.

```
{
```

```

"eventVersion": "1.10",
"userIdentity": {
  "type": "Unknown",
  "accountId": "123456789012",
  "accessKeyId": "xxxx"
},
"eventTime": "xxxx",
"eventSource": "identitystore-scim.amazonaws.com",
"eventName": "PatchUser",
"awsRegion": "us-east-1",
"sourceIPAddress": "xxx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"errorCode": "ValidationException",
"errorMessage": "List attribute emails exceeds allowed limit of 1",
"requestParameters": {
  "httpBody": {
    "operations": [
      {
        "op": "REPLACE",
        "path": "emails",
        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Häufige SCIM-API-Validierungsfehler im IAM Identity Center

Die folgenden Validierungsfehlermeldungen treten häufig bei CloudTrail Ereignissen auf, wenn die SCIM-API mit IAM Identity Center verwendet wird. Diese Validierungsfehler treten in der Regel bei der Benutzer- und Gruppenbereitstellung auf.

Eine ausführliche Anleitung zur Behebung dieser Fehler und zur ordnungsgemäßen Konfiguration der SCIM-Bereitstellung finden Sie in diesem Artikel. [AWS re:Post](#)

- Das Listenattribut E-Mail überschreitet das zulässige Limit von 1
- Zulässige Attributadressen auflisten (Limit von 1)
- 1 Überprüfungsfehler erkannt: Der Wert unter '*Name.FamilyName*' erfüllte die Einschränkung nicht: Das Mitglied muss das Muster des regulären Ausdrucks erfüllen: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`
- Es wurden 2 Überprüfungsfehler erkannt: Der Wert unter 'Name.FamilyName' erfüllte die Einschränkung nicht: Das Mitglied muss eine Länge von mindestens 1 haben; der Wert unter 'Name.FamilyName' erfüllte die Einschränkung nicht: Das Mitglied muss das Muster des regulären Ausdrucks erfüllen: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`
- Es wurden 2 Überprüfungsfehler erkannt: Der Wert auf 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' konnte die Einschränkung nicht erfüllen: Das Element muss eine Länge größer oder gleich 1 haben; Wert auf 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' erfüllt die Einschränkung nicht: Das Mitglied muss das Muster des regulären Ausdrucks erfüllen: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`,
- Ungültiges JSON von RequestBody
- Ungültiges Filterformat

Verbinden Sie Anwendungskomponenten mit Amazon EventBridge

Sie können IAM Identity Center mit [Amazon integrieren, EventBridge](#) um Ereignisse auszulösen, die administrative Benachrichtigungen auslösen oder automatisierte Workflows als Reaktion auf bestimmte, in Ereignissen aufgezeichnete IAM Identity Center-Aktionen aufrufen. CloudTrail

Sie können beispielsweise [EventBridge Regeln konfigurieren](#), um zu erkennen, wenn ein Benutzer eine Anwendung löscht oder wenn IAM Identity Center eine neue Gruppe erstellt. Je nach Anwendungsfall können Sie diese Ereignisse an ein Amazon SNS-Thema weiterleiten, um

Administratoren zu benachrichtigen oder zusätzliche Automatisierungsfunktionen mithilfe von [Step Functions](#) oder AWS Lambda anderen Diensten aufzurufen. [EventBridge-supported](#)

Protokollierung konfigurierbarer AD-Synchronisierungsfehler

Sie können die Protokollierung in Ihren konfigurierbaren Active Directory-Synchronisationskonfigurationen (AD) aktivieren, um Protokolle mit Informationen zu Fehlern zu erhalten, die während des Synchronisierungsvorgangs auftreten können. Anhand dieser Protokolle können Sie überwachen, ob ein Problem mit Ihrer konfigurierbaren AD-Synchronisierung vorliegt, und gegebenenfalls Maßnahmen ergreifen. Sie können Ihre Protokolle an eine Amazon CloudWatch Logs-Protokollgruppe, einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose senden, dessen kontoübergreifende Zustellung für Amazon S3-Buckets und Firehose unterstützt wird.

Weitere Informationen zu Einschränkungen, Berechtigungen und versendeten Protokollen finden Sie unter [Protokollierung von aktivieren. AWS-Services](#)

Note

Die Protokollierung wird Ihnen in Rechnung gestellt. Weitere Informationen finden Sie unter [Venced Logs](#) auf der [CloudWatch](#) Amazon-Preisseite.

So aktivieren Sie konfigurierbare AD-Sync-Fehlerprotokolle

1. Melden Sie sich bei der [IAM Identity Center-Konsole](#) an.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, wählen Sie „Aktionen“ und anschließend „Protokolle verwalten“.
4. Wählen Sie Protokollzustellung hinzufügen und einen der folgenden Zieltypen aus.
 - a. Wählen Sie Zu Amazon CloudWatch Logs. Wählen Sie dann die Ziel-Log-Gruppe aus oder geben Sie sie ein.
 - b. Wählen Sie Zu Amazon S3. Wählen Sie dann den Ziel-Bucket aus oder geben Sie ihn ein.
 - c. Wählen Sie To Firehose. Wählen Sie dann den Ziel-Lieferstrom aus oder geben Sie ihn ein.
5. Wählen Sie Absenden aus.

Um konfigurierbare AD-Sync-Fehlerprotokolle zu deaktivieren

1. Melden Sie sich bei der [IAM Identity Center-Konsole](#) an.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, wählen Sie „Aktionen“ und anschließend „Protokolle verwalten“.
4. Wählen Sie Entfernen für das Ziel, das Sie entfernen möchten.
5. Wählen Sie Absenden aus.

Konfigurierbare AD-Sync-Fehlerprotokollfelder

Mögliche Fehlerprotokollfelder finden Sie in der folgenden Liste.

`sync_profile_name`

Der Name des Synchronisierungsprofils.

`error_code`

Der Fehlercode, der angibt, welche Art von Fehler aufgetreten ist.

`error_message`

Eine Meldung, die detaillierte Informationen über den aufgetretenen Fehler enthält.

`sync_source`

Die Synchronisierungsquelle ist der Ort, von dem aus Entitäten synchronisiert werden. Für IAM Identity Center ist dies ein Active Directory (AD), das von verwaltet wird. Directory Service Die Synchronisierungsquelle enthält die Domain und den ARN des betroffenen Verzeichnisses.

`sync_target`

Das Synchronisierungsziel ist das Ziel, an dem Entitäten gespeichert werden. Für IAM Identity Center ist dies ein Identitätsspeicher. Das Synchronisierungsziel enthält den betroffenen Identity Store-ARN.

`source_entity_id`

Eine eindeutige Kennung für die Entität, die den Fehler verursacht. Für IAM Identity Center ist dies die SID der Entität.

source_entity_type

Der Entitätstyp, der den Fehler verursacht. Dabei kann es sich um den Wert USER oder GROUP handeln.

eventTimestamp

Der Zeitstempel, zu dem der Fehler aufgetreten ist.

Beispiele für konfigurierbare AD-Synchronisierungsfehlerprotokolle

Beispiel 1: Ein Fehlerprotokoll für ein abgelaufenes Passwort für ein AD-Verzeichnis

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "InvalidDirectoryCredentials",
    "error_message": "The password for your AD directory has expired. Please reset the password to allow Identity Sync to access the directory."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "eventTimestamp": "1683355579981"
}
```

Beispiel 2: Ein Fehlerprotokoll für einen Benutzer mit einem nicht eindeutigen Benutzernamen

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "ConflictError",
    "error_message": "The source entity has a username conflict with the sync target. Please verify that the source identity has a unique username in the target."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "sync_target": {
    "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
  }
}
```

```
},  
  "source_entity_id": "SID-1234",  
  "source_entity_type": "USER",  
  "eventTimestamp": "1683355579981"  
}
```

Konformitätsüberprüfung für IAM Identity Center

Third-party Auditoren bewerten die Sicherheit und Konformität AWS-Services solcher Programme beispielsweise im AWS IAM Identity Center Rahmen mehrerer AWS Compliance-Programme.

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Arbeitslasten konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen [für AWS Ihre Umgebung anmelden oder](#) diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm](#) und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme](#).

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte [herunterladen im Abschnitt Berichte AWS Artifact](#).

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

Unterstützte Compliance-Standards

IAM Identity Center wurde nach den folgenden Standards geprüft und kann als Teil von Lösungen verwendet werden, für die Sie eine Konformitätszertifizierung benötigen.



AWS hat sein Compliance-Programm nach dem Health Insurance Portability and Accountability Act (HIPAA) erweitert, um IAM Identity Center als HIPAA-fähigen Service aufzunehmen. <https://aws.amazon.com/compliance/hipaa-eligible-services-reference/>

AWS bietet ein [HIPAA-focused Whitepaper](#) für Kunden, die mehr darüber erfahren möchten, wie sie Gesundheitsinformationen verarbeiten und speichern können AWS-Services. Weitere Informationen finden Sie unter [HIPAA-Compliance](#).



Das Information Security Registered Assessors Program (IRAP) ermöglicht es Kunden der australischen Regierung, sicherzustellen, dass angemessene Compliance-Kontrollen vorhanden sind, und das angemessene Verantwortungsmodell für die Erfüllung der Anforderungen des vom Australian Cyber Security Centre (ACSC) herausgegebenen Informationssicherheitshandbuchs (ISM) der australischen Regierung festzulegen. Weitere Informationen finden Sie unter IRAP-Ressourcen. <https://aws.amazon.com/compliance/irap/>



Das IAM Identity Center verfügt über eine Konformitätsbescheinigung für den PCI (Payment Card Industry) Data Security Standard (DSS), Version 3.2, auf Service Provider Level 1.

Kunden, die AWS Produkte und Dienste zum Speichern, Verarbeiten oder Übertragen von Karteninhaberdaten verwenden, können die folgenden Identitätsquellen in IAM Identity Center verwenden, um ihre eigene PCI-DSS-Konformitätszertifizierung zu verwalten:

- Active Directory
- Externer Identitätsanbieter

Die IAM Identity Center-Identitätsquelle ist derzeit nicht mit PCI DSS kompatibel.

Weitere Informationen zu PCI DSS, einschließlich der Möglichkeit, eine Kopie des AWS PCI Compliance Package anzufordern, finden Sie unter [PCI DSS Level 1](#).



System & Organization Control (SOC) -Berichte sind unabhängige Prüfungsberichte von Drittanbietern, die belegen, wie IAM Identity Center wichtige Compliance-Kontrollen und -Ziele erreicht. Diese Berichte helfen Ihnen und Ihren Auditoren zu verstehen, wie Kontrollen den Betrieb und die Einhaltung von Vorschriften unterstützen. Es gibt drei Arten von SOC-Berichten:

- AWS SOC 1-Bericht — Mit Artifact [herunterladen AWS](#)
- AWS SOC 2: Sicherheits-, Verfügbarkeits- und Vertraulichkeitsbericht — [Mit Artifact herunterladen AWS](#)
- [AWS SOC 3: Bericht über Sicherheit, Verfügbarkeit und Vertraulichkeit](#)

IAM Identity Center ist für AWS SOC 1-, SOC 2- und SOC 3-Berichte vorgesehen. Weitere Informationen finden Sie unter [SOC-Compliance](#).

Resilienz im IAM Identity Center

Die AWS globale Infrastruktur basiert auf AWS Regionen und Verfügbarkeitszonen. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hochredundanten Netzwerken miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Weitere Informationen zur AWS IAM Identity Center Resilienz finden Sie unter [Resilienzdesign und regionales Verhalten](#).

Infrastruktursicherheit im IAM Identity Center

Als verwalteter Dienst AWS IAM Identity Center ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung anhand der Best Practices für die Infrastruktursicherheit finden Sie unter [Infrastrukturschutz](#) im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf IAM Identity Center zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungssammlungen mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Datenschutz im IAM Identity Center

Das Modell der AWS [gemeinsamen Verantwortung](#) gilt für den Datenschutz in AWS IAM Identity Center. Wie in diesem Modell beschrieben, AWS ist es für den Schutz der globalen Infrastruktur verantwortlich, auf der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS Dienste verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS-Modell der geteilten Verantwortung und die GDPRAWS im Blog zur -Sicherheit](#).

Wir empfehlen Ihnen, Ihre Daten auf folgende Weise zu sichern:

- Verwenden Sie die Multifaktor-Authentifizierung (MFA) mit IAM Identity Center.
- Verwenden Sie TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten findest du unter [Arbeiten mit CloudTrail Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.

Wir empfehlen dringend, niemals vertrauliche oder vertrauliche Informationen, wie z. B. die E-Mail-Adressen Ihrer Kunden, in Tags oder Freiform-Textfelder wie ein Namensfeld einzugeben. Dies gilt auch, wenn Sie mit der Konsole AWS IAM Identity Center, der API oder den AWS SDKs arbeiten oder andere AWS Dienste verwenden. AWS CLI Alle Daten, die Sie in Tags oder Freiform-Textfelder eingeben, die für Namen verwendet werden, können für Diagnoseprotokolle verwendet werden.

Verschlüsselung während der Übertragung

IAM Identity Center schützt Daten bei der Übertragung zum und vom Service, indem es automatisch alle Netzwerkdaten mithilfe des Transport Layer Security (TLS) 1.2- oder TLS 1.3-Verschlüsselungsprotokolls verschlüsselt. Direkte HTTPS-Anfragen, die mit IAM authentifiziert und an die IAM Identity Center APIs, Identity Store API oder OIDC API gesendet werden, werden mithilfe des [AWS Signature Version 4-Algorithmus signiert, um eine sichere Verbindung herzustellen](#).

Datenschutz

Mit IAM Identity Center behalten Sie die Kontrolle über die Daten Ihres Unternehmens. Ihre in IAM Identity Center gespeicherten Benutzer- und Gruppenidentitäten werden [nur dann mit anderen AWS Diensten wie](#) AWS verwalteten Anwendungen geteilt, wenn Sie sie für IAM Identity Center aktivieren und wenn diese Dienste dies benötigen.

Weitere Informationen finden Sie in den häufig gestellten Fragen zum [AWS Datenschutz](#).

Datenaufbewahrung

IAM Identity Center speichert Ihre Daten wie Benutzer- und Gruppenidentitäten sowie Metadaten, bis Sie sie aus dem Service löschen. Wenn Sie eine IAM Identity Center-Instanz löschen, werden die darin enthaltenen Daten ebenfalls gelöscht.

Verschlüsselung im Ruhezustand

IAM Identity Center bietet Verschlüsselung zum Schutz von Kundendaten im Ruhezustand mithilfe der folgenden Schlüsseltypen:

- **AWS-eigene Schlüssel (Standardschlüsseltyp)** — IAM Identity Center verwendet diese Schlüssel standardmäßig, um Ihre Daten automatisch zu verschlüsseln. Sie können ihre Verwendung nicht einsehen, verwalten, überprüfen oder AWS eigene Schlüssel für andere Zwecke verwenden. IAM Identity Center kümmert sich vollständig um die Schlüsselverwaltung, um die Sicherheit Ihrer Daten zu gewährleisten, ohne dass Sie Maßnahmen ergreifen müssen. Weitere Informationen finden Sie unter [AWS -eigene Schlüssel](#) im [AWS Key Management Service -Entwicklerhandbuch](#).
- **Vom Kunden verwaltete Schlüssel** — In Organisationsinstanzen von IAM Identity Center können Sie einen symmetrischen, vom Kunden verwalteten Schlüssel für die Verschlüsselung der übrigen Personalitätsdaten wie Benutzer- und Gruppenattribute wählen. Sie erstellen, besitzen und verwalten diese Verschlüsselungsschlüssel. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:
 - Einrichtung und Verwaltung von Schlüsselrichtlinien, um den Zugriff auf den Schlüssel nur auf IAM-Prinzipale zu beschränken, die Zugriff benötigen, z. B. IAM Identity Center, und [AWS verwaltete Anwendungen](#) deren Administratoren AWS Organizations .
 - Einrichtung und Pflege von IAM-Richtlinien für den Zugriff auf den Schlüssel, einschließlich des kontoübergreifenden Zugriffs
 - Aktivieren und Deaktivieren wichtiger Richtlinien
 - Kryptographisches Material mit rotierendem Schlüssel

- Überprüfung des Zugriffs auf Ihre Daten, für den ein Schlüsselzugriff erforderlich ist
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Informationen zur Implementierung eines vom Kunden verwalteten KMS-Schlüssels im IAM Identity Center finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#). Weitere Informationen zu vom Kunden verwalteten Schlüsseln finden Sie [im AWS Key Management Service Entwicklerhandbuch unter vom](#) Kunden verwaltete Schlüssel.

 Note

IAM Identity Center aktiviert automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener KMS-Schlüssel, um Kundendaten kostenlos zu schützen. Bei Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie in der [AWS Key Management Service Preisgestaltung](#).

Überlegungen zur Implementierung von vom Kunden verwalteten Schlüsseln:

- **Dedizierte Schlüssel:** Wir empfehlen, für jede IAM Identity Center-Instanz einen neuen dedizierten, vom Kunden verwalteten KMS-Schlüssel zu erstellen, anstatt einen vorhandenen Schlüssel wiederzuverwenden. Dieser Ansatz sorgt für eine klarere Aufgabentrennung, vereinfacht die Verwaltung der Zugriffskontrolle und vereinfacht die Sicherheitsüberprüfung. Ein dedizierter Schlüssel reduziert auch das Risiko, da die Auswirkungen wichtiger Änderungen auf eine einzelne IAM Identity Center-Instanz begrenzt werden.
- **Verwendung von IAM Identity Center für mehrere Instanzen AWS-Regionen:** Wenn Sie Ihre IAM Identity Center-Instanz auf weitere replizieren möchten AWS-Regionen, müssen Sie einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand verwenden. Der standardmäßige AWS eigene KMS-Schlüsseltyp wird in einem multiregionalen IAM Identity Center nicht unterstützt. Weitere Informationen finden Sie unter [Verwenden von IAM Identity Center auf mehreren AWS-Regionen](#).

 Note

IAM Identity Center verwendet bei der Verschlüsselung [Ihrer Personalidentitätsdaten eine](#) Umschlagverschlüsselung. Ihr KMS-Schlüssel spielt die Rolle eines Wrapping-Schlüssels, der

den Datenschlüssel verschlüsselt, der tatsächlich zum Verschlüsseln der Daten verwendet wird.

Weitere Informationen zu AWS KMS finden Sie unter [Was ist der AWS Schlüsselverwaltungsdienst?](#)

IAM Identity Center-Verschlüsselungskontext

Ein [Verschlüsselungskontext](#) ist ein optionaler Satz nicht geheimer Schlüssel-Wert-Paare, die zusätzliche Kontextinformationen zu den Daten enthalten. AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zum Verschlüsseln von Daten einbeziehen, wird der Verschlüsselungskontext AWS KMS an die verschlüsselten Daten gebunden. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben. Weitere Informationen zum Verschlüsselungskontext finden Sie im [AWS KMS Entwicklerhandbuch](#).

IAM Identity Center verwendet die folgenden Verschlüsselungskontextschlüssel: `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn` und `tenant-key-id`. Beispielsweise kann der AWS KMS folgende Verschlüsselungskontext in API-Vorgängen vorkommen, die von der IAM Identity Center [API aufgerufen werden](#).

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

Der folgende Verschlüsselungskontext kann in AWS KMS API-Vorgängen vorkommen, die von der [Identity Store API aufgerufen werden](#).

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
  "arn:aws:identitystore:::123456789012:identitystore/d-1234567890"
}
```

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf den kundenseitig verwalteten Schlüssel

Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen verwenden, um den Zugriff auf Ihren symmetrischen, kundenseitig verwalteten Schlüssel zu kontrollieren. Einige der wichtigsten Richtlinienvorlagen in der [Erweiterte KMS-Grundsatzserklärungen](#) enthalten solche Bedingungen, um sicherzustellen, dass der Schlüssel nur mit einer bestimmten IAM Identity Center-Instanz verwendet wird.

Überwachung Ihrer Verschlüsselungsschlüssel für IAM Identity Center

Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel mit Ihrer IAM Identity Center-Instanz verwenden, können Sie [Amazon CloudWatch Logs verwenden AWS CloudTrail, um Anfragen](#) zu verfolgen, an die IAM Identity Center sendet. AWS KMS Die KMS-API-Operationen, die IAM Identity Center aufruft, sind unter aufgeführt. [Schritt 2: Bereiten Sie die wichtigsten KMS-Richtlinienerklärungen vor](#) CloudTrail Ereignisse für diese API-Operationen enthalten den Verschlüsselungskontext, mit dem Sie AWS KMS API-Operationen überwachen können, die von Ihrer IAM Identity Center-Instanz aufgerufen werden, um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.

Beispiel für einen Verschlüsselungskontext bei einem CloudTrail Ereignis eines AWS KMS API-Vorgangs:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS Speicherung, Verschlüsselung und Löschung von IAM Identity Center-Identitätsattributen durch verwaltete Anwendungen

Einige AWS verwaltete Anwendungen, die Sie mit bereitstellen AWS IAM Identity Center, wie AWS Systems Manager und Amazon CodeCatalyst, speichern bestimmte Benutzer- und

Gruppenattribute aus IAM Identity Center in ihrem eigenen Datenspeicher. Die Verschlüsselung im Ruhezustand mit einem vom Kunden verwalteten KMS-Schlüssel in IAM Identity Center erstreckt sich nicht auf die Benutzer- und Gruppenattribute von IAM Identity Center, die in AWS verwalteten Anwendungen gespeichert sind. AWS verwaltete Anwendungen unterstützen verschiedene Verschlüsselungsmethoden für die von ihnen gespeicherten Daten. Wenn Sie außerdem Benutzer- und Gruppenattribute in IAM Identity Center löschen, speichern diese AWS verwalteten Anwendungen diese Informationen möglicherweise auch nach dem Löschen im IAM Identity Center weiter. Informationen zur Verschlüsselung und Sicherheit der in den Anwendungen gespeicherten Daten finden Sie im Benutzerhandbuch Ihrer AWS verwalteten Anwendungen.

Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center

Vom Kunden verwaltete Schlüssel sind AWS Schlüssel des Schlüsselverwaltungsdienstes, die Sie erstellen, besitzen und verwalten. Gehen Sie folgendermaßen vor, um einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung im Ruhezustand im AWS IAM Identity Center zu implementieren:

Important

Einige AWS verwaltete Anwendungen können nicht verwendet werden, wenn das AWS IAM Identity Center mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Siehe [AWS verwaltete Anwendungen, die Sie mit IAM Identity Center verwenden können](#).

1. [Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen](#)— Um die richtigen Berechtigungen für die Verwendung des KMS-Schlüssels zu definieren, müssen Sie die relevanten Anwendungsfälle in Ihrem Unternehmen identifizieren. Die KMS-Schlüsselberechtigungen bestehen aus KMS-Schlüsselrichtlinienanweisungen und identitätsbasierten Richtlinien, die zusammenarbeiten, um es den entsprechenden IAM-Prinzipalen zu ermöglichen, den KMS-Schlüssel für ihre spezifischen Anwendungsfälle zu verwenden.
2. [Schritt 2: Bereiten Sie die wichtigsten KMS-Richtlinienerklärungen vor](#)— Wählen Sie auf der Grundlage der in Schritt 1 identifizierten Anwendungsfälle die entsprechenden Vorlagen für wichtige KMS-Richtlinien aus und geben Sie die erforderlichen Kennungen und IAM-Prinzipalnamen ein. Beginnen Sie mit den grundlegenden KMS-Grundsatzserklärungen, und falls Ihre Sicherheitsrichtlinien dies erfordern, verfeinern Sie sie, wie unter Erweiterte KMS-Grundsatzserklärungen beschrieben.

3. [Schritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel](#)— Erstellen Sie in KMS einen AWS KMS-Schlüssel, der die Anforderungen von IAM Identity Center erfüllt, und fügen Sie die in Schritt 2 vorbereiteten KMS-Schlüsselrichtlinien zur KMS-Schlüsselrichtlinie hinzu.
4. [Schritt 4: Konfigurieren Sie die IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](#)- Wählen Sie die entsprechenden Vorlagen für IAM-Richtlinienerklärungen auf der Grundlage der in Schritt 1 identifizierten Anwendungsfälle aus und bereiten Sie sie für die Verwendung vor, indem Sie den wichtigsten ARN eingeben. Erlauben Sie dann den IAM-Principals für jeden spezifischen Anwendungsfall, den KMS-Schlüssel kontoübergreifend zu verwenden, indem Sie die vorbereiteten IAM-Policy-Statements zu den IAM-Richtlinien der Principals hinzufügen.
5. [Schritt 5: Konfigurieren Sie den KMS-Schlüssel im IAM Identity Center](#)— Aktivieren Sie den vom Kunden verwalteten KMS-Schlüssel in Ihrer IAM Identity Center-Instanz, um ihn für die Verschlüsselung im Ruhezustand zu verwenden.

Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen

Bevor Sie Ihren vom Kunden verwalteten KMS-Schlüssel erstellen und konfigurieren, identifizieren Sie Ihre Anwendungsfälle und bereiten Sie die erforderlichen KMS-Schlüsselberechtigungen vor. Weitere Informationen zur [AWS KMS-Schlüsselrichtlinie finden Sie im KMS-Entwicklerhandbuch](#).

IAM-Prinzipale, die die IAM Identity Center Service-APIs aufrufen, benötigen Berechtigungen. Beispielsweise kann ein delegierter Administrator über eine Berechtigungssatzrichtlinie autorisiert werden, diese APIs zu verwenden. Wenn IAM Identity Center mit einem vom Kunden verwalteten Schlüssel konfiguriert wird, müssen IAM-Prinzipale auch über Berechtigungen verfügen, um die KMS-API über die IAM Identity Center-Service-APIs zu verwenden. Sie definieren diese KMS-API-Berechtigungen an zwei Stellen: in der KMS-Schlüsselrichtlinie und in den IAM-Richtlinien, die den IAM-Prinzipalen zugeordnet sind.

Die KMS-Schlüsselberechtigungen bestehen aus:

1. Richtlinienanweisungen für KMS-Schlüssel, die Sie bei der Erstellung des KMS-Schlüssels angeben [Schritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel](#).
2. IAM-Richtlinienanweisungen für IAM-Prinzipale, die Sie [Schritt 4: Konfigurieren Sie die IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](#) nach der Erstellung des KMS-Schlüssels angeben.

In der folgenden Tabelle sind die relevanten Anwendungsfälle und IAM-Prinzipale aufgeführt, für die Berechtigungen zur Verwendung Ihres KMS-Schlüssels erforderlich sind.

Anwendungsfall	IAM-Prinzipale, die Berechtigungen zur Verwendung des KMS-Schlüssels benötigen	Required/ Optional
Verwendung von AWS IAM Identity Center	<ul style="list-style-type: none"> Administratoren von AWS IAM Identity Center Der IAM Identity Center-Dienst und der zugehörige Identity Store-Dienst 	Erforderlich
Verwendung AWS verwalteter Anwendungen mit IAM Identity Center	<ul style="list-style-type: none"> Administratoren AWS verwalteter Anwendungen AWS verwaltete Anwendungen Dienstrollen, von denen AWS verwaltete Anwendungen annehmen, dass sie die IAM Identity Center Service-APIs aufrufen 	Optional
Verwendung von AWS Control Tower auf der AWS IAM Identity Center-Instanz, die es aktiviert hat	<ul style="list-style-type: none"> AWS Control Tower Administratoren 	Optional
SSO für Amazon EC2-Instanzen mit AWS IAM Identity Center	<ul style="list-style-type: none"> IAM-Prinzipale sind autorisiert, SSO für Amazon EC2-Instances durchzuführen 	Optional
Jeder andere Anwendungsfall, bei dem IAM Identity Center Service-APIs mit IAM-Prinzipalen aufgerufen werden, z. B. vom Kunden verwaltete Anwendungen, Workflows zur Bereitstellung von Berechtig	<ul style="list-style-type: none"> IAM-Prinzipale, die von diesen Workflows zum Aufrufen der IAM Identity Center-Service-APIs verwendet werden 	Optional

Anwendungsfall	IAM-Prinzipale, die Berechtigungen zur Verwendung des KMS-Schlüssels benötigen	Required/ Optional
ungssätzen oder Funktionen AWS Lambda		

Note

Für mehrere in der Tabelle aufgeführte IAM-Prinzipale sind KMS-API-Berechtigungen erforderlich. AWS Um Ihre Benutzer- und Gruppendaten in IAM Identity Center zu schützen, rufen jedoch nur die IAM Identity Center- und Identity Store-Dienste die KMS-API direkt auf. AWS

Schritt 2: Bereiten Sie die wichtigsten KMS-Richtlinienerklärungen vor

Beginnen Sie mit dem [Grundlegende KMS-Schlüsselrichtlinie](#) und passen Sie es an Ihre Organisation an. Wenn Sie auf der Grundlage Ihrer Sicherheitsanforderungen spezifischere Richtlinien benötigen, können Sie die Richtlinienaussagen anhand der Beispiele unter [ändernErweiterte KMS-Grundsatzserklärungen](#). Hinweise zu dieser Entscheidung finden Sie unter [Überlegungen zur Auswahl grundlegender und erweiterter KMS-Schlüsselrichtlinien](#).

1. Kopieren Sie die Basisrichtlinie in einen Editor und fügen Sie die erforderlichen Identifikatoren und IAM-Prinzipalnamen in die wichtigsten KMS-Richtlinienanweisungen ein. Hilfe bei der Suche nach den Werten der Identifikatoren, auf die verwiesen wird, finden Sie unter [Wo finde ich die erforderlichen Identifikatoren](#)
2. Wenn Ihre Sicherheitsanforderungen dies erfordern, verfeinern Sie die Richtlinienaussagen anhand der Beispiele unter [Erweiterte KMS-Grundsatzserklärungen](#).

Important

Seien Sie vorsichtig, wenn Sie die KMS-Schlüsselrichtlinien für Schlüssel ändern, die bereits von IAM Identity Center verwendet werden. IAM Identity Center überprüft zwar die Verschlüsselungs- und Entschlüsselungsberechtigungen, wenn Sie einen KMS-Schlüssel zum ersten Mal konfigurieren, es kann jedoch keine nachfolgenden Richtlinienänderungen

überprüfen. Das versehentliche Entfernen der erforderlichen Berechtigungen kann den normalen Betrieb Ihres IAM Identity Center stören. Anleitungen zur Behebung häufiger Fehler im Zusammenhang mit vom Kunden verwalteten Schlüsseln im IAM Identity Center finden Sie unter [Beheben Sie Probleme mit vom Kunden verwalteten Schlüsseln in AWS IAM Identity Center](#)

 Note

IAM Identity Center und der zugehörige Identity Store benötigen Service-Level-Berechtigungen, um Ihren vom Kunden verwalteten KMS-Schlüssel verwenden zu können. Diese Anforderung gilt auch für AWS verwaltete Anwendungen, die IAM Identity Center Service-APIs mithilfe von Dienstanmeldedaten aufrufen. In anderen Anwendungsfällen, in denen IAM Identity Center Service-APIs mit [Forward-Access-Sitzungen aufgerufen werden](#), benötigt nur der initiiierende IAM-Prinzipal (z. B. ein Administrator) KMS-Schlüsselberechtigungen. Insbesondere Endbenutzer, die das AWS Zugriffsportal und AWS verwaltete Anwendungen verwenden, benötigen keine direkten KMS-Schlüsselberechtigungen, da diese über die jeweiligen Dienste erteilt werden.

Schritt 3: Erstellen Sie einen vom Kunden verwalteten KMS-Schlüssel

Sie können einen vom Kunden verwalteten Schlüssel mithilfe der AWS Managementkonsole oder der AWS KMS-APIs erstellen. Fügen Sie beim Erstellen des Schlüssels die KMS-Schlüsselrichtlinien, die Sie in Schritt 2 vorbereitet haben, zur KMS-Schlüsselrichtlinie hinzu. Detaillierte Anweisungen, einschließlich Anleitungen zur standardmäßigen KMS-Schlüsselrichtlinie, finden Sie im [AWS Key Management Service Developer Guide](#).

Der Schlüssel muss die folgenden Anforderungen erfüllen:

- Der KMS-Schlüssel muss sich in derselben AWS Region wie die IAM Identity Center-Instanz befinden
- Sie können entweder einen Schlüssel für mehrere Regionen oder einen Schlüssel für eine einzelne Region wählen. Wenn Sie IAM Identity Center jedoch in mehreren Fällen verwenden möchten, müssen AWS-Regionen Sie einen KMS-Schlüssel für mehrere Regionen erstellen. Sie können einen KMS-Schlüssel für eine einzelne Region nicht in einen KMS-Schlüssel für mehrere Regionen konvertieren. Wir empfehlen daher, mit einem KMS-Schlüssel für mehrere Regionen zu beginnen,

es sei denn, Sie haben spezielle Anforderungen zur Verwendung eines KMS-Schlüssels für eine einzelne Region.

- Der KMS-Schlüssel muss ein symmetrischer Schlüssel sein, der für die Verwendung „Verschlüsseln und Entschlüsseln“ konfiguriert ist
- Der KMS-Schlüssel muss sich im selben AWS Organizations Verwaltungskonto wie die Organisationsinstanz von IAM Identity Center befinden

Note

Wenn Sie vorhaben, diesen KMS-Schlüssel in Regionen zu replizieren, in denen Sie Ihr IAM Identity Center replizieren möchten, empfehlen wir Ihnen, zuerst die Einrichtung in diesem Abschnitt abzuschließen und dann den Anweisungen unter [the section called “Replizieren Sie IAM Identity Center in eine zusätzliche Region”](#)

Schritt 4: Konfigurieren Sie die IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels

Jeder IAM-Principal, der die IAM Identity Center-Service-APIs von einem anderen AWS Konto aus verwendet, z. B. delegierte IAM Identity Center-Administratoren, benötigt ebenfalls eine IAM-Richtlinienerklärung, die die Verwendung des KMS-Schlüssels über diese APIs ermöglicht.

Für jeden in Schritt 1 identifizierten Anwendungsfall:

1. Suchen Sie die entsprechenden Vorlagen für IAM-Richtlinienerklärungen unter Baseline-KMS-Schlüssel und IAM-Policy-Statements.
2. Kopieren Sie die Vorlagen in einen Editor und geben Sie den Schlüssel-ARN ein, der nun nach der Erstellung des KMS-Schlüssels in Schritt 3 verfügbar ist. Hilfe bei der Suche nach dem ARN-Schlüsselwert finden Sie unter [Wo finde ich die erforderlichen Identifikatoren](#).
3. Suchen Sie in der AWS-Managementkonsole nach der IAM-Richtlinie des IAM-Prinzips, der dem Anwendungsfall zugeordnet ist. Der Speicherort dieser Richtlinie hängt vom Anwendungsfall ab und davon, wie der Zugriff gewährt wird.
 - Für den Zugriff, der direkt in IAM gewährt wird, können Sie in der IAM-Konsole nach IAM-Prinzipalen suchen, z. B. nach IAM-Rollen.
 - Für den Zugriff, der über IAM Identity Center gewährt wird, finden Sie den entsprechenden Berechtigungssatz in der IAM Identity Center-Konsole.

4. Fügen Sie der IAM-Rolle die anwendungsfallspezifischen IAM-Policy-Statements hinzu und speichern Sie die Änderung.

 Note

Die hier beschriebenen IAM-Richtlinien sind identitätsbasierte Richtlinien. Solche Richtlinien können zwar IAM-Benutzern, -Gruppen und -Rollen zugewiesen werden, wir empfehlen jedoch, wenn möglich, IAM-Rollen zu verwenden. Weitere Informationen zu IAM-Rollen und IAM-Benutzern finden Sie im IAM-Benutzerhandbuch.

In einigen Fällen zusätzliche Konfigurationen AWS verwaltete Anwendungen

Bei einigen AWS verwalteten Anwendungen müssen Sie eine Servicerolle konfigurieren, damit die Anwendungen die IAM Identity Center Service-APIs verwenden können. Wenn Ihre Organisation AWS verwaltete Anwendungen mit IAM Identity Center verwendet, führen Sie die folgenden Schritte für jede bereitgestellte Anwendung aus:

1. Lesen Sie im Benutzerhandbuch der Anwendung nach, ob die Berechtigungen aktualisiert wurden und nun auch KMS-Schlüsselberechtigungen für die Verwendung der Anwendung mit IAM Identity Center enthalten.
2. Wenn ja, aktualisieren Sie die Berechtigungen gemäß den Anweisungen im Benutzerhandbuch der Anwendung, um eine Unterbrechung des Anwendungsbetriebs zu vermeiden.

 Note

Wenn Sie sich nicht sicher sind, ob eine AWS verwaltete Anwendung diese Berechtigungen verwendet, empfehlen wir Ihnen, die Benutzerhandbücher aller bereitgestellten AWS verwalteten Anwendungen zu lesen. Sie müssen diese Konfiguration nur einmal für jede Anwendung durchführen, für die die Konfiguration erforderlich ist.

Schritt 5: Konfigurieren Sie den KMS-Schlüssel im IAM Identity Center

 Important

Bevor Sie mit diesem Schritt fortfahren:

- Stellen Sie sicher, dass Ihre AWS verwalteten Anwendungen mit vom Kunden verwalteten KMS-Schlüsseln kompatibel sind. Eine Liste kompatibler Anwendungen finden Sie unter [AWS Verwaltete Anwendungen, die Sie mit IAM Identity Center](#) verwenden können. Wenn Sie inkompatible Anwendungen haben, fahren Sie nicht fort.
- Konfigurieren Sie die erforderlichen Berechtigungen für die Verwendung des KMS-Schlüssels. Ohne die richtigen Berechtigungen kann dieser Schritt fehlschlagen oder die Verwaltung von IAM Identity Center, die Verwendung AWS verwalteter Anwendungen und andere Anwendungsfälle, für die KMS-Schlüsselberechtigungen erforderlich sind, unterbrechen. Weitere Informationen finden Sie unter [Schritt 1: Identifizieren Sie Anwendungsfälle für Ihr Unternehmen](#).
- Stellen Sie sicher, dass Berechtigungen für AWS verwaltete Anwendungen und vom Kunden verwaltete Anwendungen, die IAM Identity Center Service-APIs mit IAM-Rollen aufrufen, auch die Verwendung des KMS-Schlüssels über IAM Identity Center Service-APIs ermöglichen. Bei einigen AWS verwalteten Anwendungen müssen Sie Berechtigungen für die Verwendung dieser APIs konfigurieren, z. B. eine Servicerolle. Vergewissern Sie sich im Benutzerhandbuch jeder bereitgestellten AWS verwalteten Anwendung, ob Sie bestimmte KMS-Schlüsselberechtigungen hinzufügen müssen.

Geben Sie einen KMS-Schlüssel an, wenn Sie eine neue Organisationsinstanz von IAM Identity Center aktivieren

 Note

Wenn AWS-Regionen diese standardmäßig aktiviert sind, können Sie im Rahmen der Instanzerstellung einen vom Kunden verwalteten Schlüssel konfigurieren. Weitere Informationen finden Sie unter [IAM Identity Center aktivieren](#).

Wenn Sie eine neue Organisationsinstanz von IAM Identity Center in einer Region aktivieren, in der keine Instanzkonfigurationsoptionen verfügbar sind, können Sie bei der Einrichtung einen vom Kunden verwalteten KMS-Schlüssel angeben. Dadurch wird sichergestellt, dass die Instanz Ihren Schlüssel von Anfang an für die Verschlüsselung im Ruhezustand verwendet. Bevor Sie beginnen, lesen Sie unter [Überlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien](#).

1. Erweitern Sie auf der Seite „IAM Identity Center aktivieren“ den Abschnitt Verschlüsselung im Ruhezustand.
2. Wählen Sie Manage Encryption (Verschlüsselung verwalten).
3. Wählen Sie vom Kunden verwalteter Schlüssel aus.
4. Führen Sie für den KMS-Schlüssel einen der folgenden Schritte aus:
 - a. Wählen Sie Aus Ihren KMS-Schlüsseln auswählen und wählen Sie den Schlüssel, den Sie erstellt haben, aus der Dropdownliste aus.
 - b. Wählen Sie KMS-Schlüssel-ARN eingeben und geben Sie den vollständigen ARN Ihres Schlüssels ein.
5. Wählen Sie Speichern.
6. Wählen Sie Aktivieren, um die Einrichtung abzuschließen.

Weitere Informationen finden Sie unter IAM Identity Center <https://docs.aws.amazon.com/singlesignon/latest/userguide/enable-identity-center.html> aktivieren.

Ändern Sie die Schlüsselkonfiguration für eine vorhandene Organisationsinstanz von IAM Identity Center

Sie können Ihren vom Kunden verwalteten KMS-Schlüssel jederzeit in einen anderen Schlüssel ändern oder AWS zu einem eigenen Schlüssel wechseln.

Console

Um Ihre KMS-Schlüsselkonfiguration zu ändern

1. Öffnen Sie die IAM Identity Center-Konsole unter <https://console.aws.amazon.com/singlesignon/>.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie die Registerkarte Zusätzliche Einstellungen aus.
4. Wählen Sie Verschlüsselung verwalten.
5. Wählen Sie eine der folgenden Optionen:
 - a. Kundenverwalteter Schlüssel — Wählen Sie einen anderen vom Kunden verwalteten Schlüssel aus der Dropdownliste aus oder geben Sie einen neuen Schlüssel-ARN ein.
 - b. AWS Eigener Schlüssel — Wechseln Sie zur Standardverschlüsselungsoption.

6. Wählen Sie Speichern.

AWS CLI

Um eine bestehende Organisationsinstanz von IAM Identity Center so zu ändern, dass sie den vom Kunden verwalteten KMS-Schlüssel verwendet

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Um eine bestehende Organisationsinstanz von IAM Identity Center so zu ändern, dass sie einen eigenen Schlüssel verwendet AWS

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Wichtige Überlegungen zur Verwaltung durch den Kunden

- Die Aktualisierung des KMS-Schlüssels, der für den Betrieb des IAM Identity Center konfiguriert ist, hat keine Auswirkungen auf aktive Benutzersitzungen in Ihrem IAM Identity Center. Während dieses Vorgangs können Sie das AWS Zugriffsportal, die IAM Identity Center-Konsole und die IAM Identity Center Service-APIs weiterhin verwenden.
- Wenn Sie zu einem neuen KMS-Schlüssel wechseln, überprüft IAM Identity Center, ob der Schlüssel erfolgreich für die Verschlüsselung und Entschlüsselung verwendet werden kann. Wenn Sie bei der Einrichtung der Schlüssel- oder IAM-Richtlinie einen Fehler gemacht haben, zeigt die Konsole eine erläuternde Fehlermeldung an, und der vorherige KMS-Schlüssel wird weiterhin verwendet.
- Die standardmäßige jährliche KMS-Schlüsselrotation findet automatisch statt. Informationen zu Themen wie der [Schlüsselrotation](#), der [Überwachung von AWS KMS Schlüsseln](#) und der [Zugriffskontrolle bei der Schlüssellöschung finden Sie im AWS KMS Entwicklerhandbuch](#).

Important

Wenn der vom Kunden verwaltete KMS-Schlüssel, der von Ihrer IAM Identity Center-Instanz verwendet wird, gelöscht, deaktiviert oder aufgrund einer falschen KMS-Schlüsselrichtlinie nicht mehr darauf zugegriffen werden kann, können Ihre Mitarbeiter und IAM Identity Center-Administratoren IAM Identity Center nicht verwenden. Der Verlust des Zugriffs kann je nach den Umständen vorübergehend (eine Schlüsselrichtlinie kann korrigiert werden) oder dauerhaft (ein gelöschter Schlüssel kann nicht wiederhergestellt werden) sein. Wir empfehlen, [den](#) Zugriff auf wichtige Vorgänge wie das Löschen oder Deaktivieren des KMS-Schlüssels zu beschränken. Wir empfehlen außerdem, dass Ihr Unternehmen [AWS glasklare Zugriffsverfahren einrichtet](#), um sicherzustellen, dass Ihre privilegierten Benutzer Zugriff haben, falls auf AWS das IAM Identity Center nicht zugegriffen werden kann.

Wo finde ich die erforderlichen Identifikatoren

Wenn Sie die Berechtigungen für Ihren vom Kunden verwalteten KMS-Schlüssel konfigurieren, benötigen Sie bestimmte AWS Ressourcen-Identifikatoren, um die Vorlagen für wichtige Richtlinien und IAM-Richtlinienerklärungen auszufüllen. Fügen Sie die erforderlichen Kennungen (z. B. die Organisations-ID) und die IAM-Prinzipalnamen in die wichtigsten KMS-Richtlinienerklärungen ein.

Im Folgenden finden Sie eine Anleitung zum Auffinden dieser Identifikatoren in der AWS Managementkonsole.

IAM Identity Center, Amazon-Ressourcenname (ARN) und Identity Store-ARN

Eine IAM Identity Center-Instanz ist eine AWS Ressource mit einer eigenen eindeutigen ARN, z. B. `arn:aws:sso:::1234567890abcdef.instance/ssoins`. Der ARN folgt dem Muster, das im Abschnitt „IAM Identity Center-Ressourcentypen“ der Service Authorization Reference dokumentiert ist.

Jeder IAM Identity Center-Instanz ist ein Identity Store zugeordnet, der die Benutzer- und Gruppenidentitäten speichert. Ein Identitätsspeicher hat eine eindeutige Kennung namens Identity Store ID (z. B. `d-123456789a`). Der ARN folgt dem Muster, das im Abschnitt Identity Store-Ressourcentypen der Service Authorization Reference dokumentiert ist. https://docs.aws.amazon.com/service-authorization/latest/reference/list_awsiamidentitycenterdirectory.html

Sie finden sowohl die ARN- als auch die Identity Store-ID-Werte auf der Einstellungsseite Ihres IAM Identity Center. Die Identity Store-ID befindet sich auf der Registerkarte „Identitätsquelle“.

AWS Organizations ID (ID)

Wenn Sie eine Organisations-ID (z. B. o-example.org1) in Ihrer Schlüsselrichtlinie angeben möchten, finden Sie ihren Wert auf der Seite „Einstellungen“ Ihrer IAM Identity Center- und Organisationskonsolen. Der ARN folgt dem Muster, das im Abschnitt Organisations Resource Types in der Service Authorization Reference dokumentiert ist.

KMS-Schlüssel (ARN)

Den ARN eines KMS-Schlüssels finden Sie in der AWS KMS Konsole. Wählen Sie links vom Kunden verwaltete Schlüssel aus, klicken Sie auf den Schlüssel, dessen ARN Sie nachschlagen möchten, und Sie sehen ihn im Abschnitt Allgemeine Konfiguration. Der ARN folgt dem Muster, das im Abschnitt AWS KMS Ressourcentypen der Service Authorization Reference dokumentiert ist.

Weitere Informationen zu den wichtigsten Richtlinien AWS KMS und zur Problembehandlung bei AWS KMS Berechtigungen finden Sie im AWS Key Management Service Entwicklerhandbuch. Weitere Informationen zu IAM-Richtlinien und ihrer JSON-Darstellung finden Sie im IAM-Benutzerhandbuch.

Grundlegende KMS-Schlüsselrichtlinie

Die folgende KMS-Schlüsselrichtlinie deckt das gängigste Bereitstellungsszenario ab: eine IAM Identity Center-Instance mit delegierten Administratoren und AWS verwalteten Anwendungen AWS Control Tower, einschließlich SSO für Amazon EC2-Instances, und benutzerdefinierte Workflows. Verwenden Sie diese Richtlinie als Ausgangspunkt, wenn Sie einen vom Kunden verwalteten KMS-Schlüssel für IAM Identity Center erstellen. Wenn Sie detailliertere Zugriffskontrollen benötigen, z. B. die Beschränkung des Schlüssels auf eine bestimmte IAM Identity Center-Instanz oder -Anwendung, finden Sie unter [Erweiterte KMS-Grundsatzserklärungen](#). Bitte beachten Sie, dass bei Verwendung eines Mehrregionenschlüssels dieselbe Richtlinie für alle Replikate verwendet werden sollte, um eine konsistente Autorisierung sicherzustellen.

Um diese Richtlinie zu verwenden, ersetzen Sie die folgenden Platzhalterwerte durch Ihre eigenen:

- **111122223333**— Die AWS Konto-ID Ihrer IAM Identity Center-Instanz (das AWS Organizations Verwaltungskonto).
- **444455556666**— Die AWS Konto-ID Ihres Kontos für delegierte Administratoren. Wenn Sie die delegierte Administration nicht verwenden, entfernen Sie diesen Prinzipal.

Da AWS IAM Identity Center erfordert, dass sich der KMS-Schlüssel im selben AWS Konto wie der Dienst befindet, verwenden die folgenden Anweisungen die `${aws:ResourceAccount}` Variablen

`${aws:ResourceOrgID}` und anstelle von Literalwerten. Sie können diese Variablen durch Ihre AWS Organisations- und AWS Konto-ID ersetzen, wenn Sie dies bevorzugen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIdentityCenterAdminAccounts",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToDescribeKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToUseKey",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "identitystore.amazonaws.com",
          "sso.amazonaws.com"
        ]
      }
    }
  ]
}
```



```

    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "${aws:ResourceAccount}"
        },
        "ForAnyValue:StringEquals": {
            "kms:EncryptionContextKeys": [
                "aws:sso:instance-arn",
                "aws:identitystore:identitystore-arn"
            ]
        }
    }
},
{
    "Sid": "AllowOrgPrincipalsViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        },
        "StringLike": {
            "kms:ViaService": [
                "sso.*.amazonaws.com",
                "identitystore.*.amazonaws.com"
            ]
        },
        "ForAnyValue:StringEquals": {
            "kms:EncryptionContextKeys": [
                "aws:sso:instance-arn",
                "aws:identitystore:identitystore-arn"
            ]
        }
    }
}
},

```

```
{
  "Sid": "AllowManagedApps",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    },
    "StringEquals": {
      "aws:SourceOrgID": "${aws:ResourceOrgID}"
    },
    "StringLike": {
      "kms:ViaService": [
        "identitystore.*.amazonaws.com",
        "sso.*.amazonaws.com"
      ]
    },
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": [
        "aws:sso:instance-arn",
        "aws:identitystore:identitystore-arn"
      ]
    }
  }
}
```

Diese Richtlinie enthält fünf Aussagen. In der folgenden Tabelle wird beschrieben, was die einzelnen Anweisungen bewirken.

Statement	Zweck
AllowIdentityCenterAdminAccounts	Gewährt dem IAM Identity Center-Verwaltungskonto und dem delegierten Administratorkonto vollständige KMS-Schlüsselberechtigungen. Dazu gehören wichtige Verwaltungsmaßnahmen wie das Ändern der Schlüsselrichtlinie und das Planen der Schlüssellöschung. Administratoren dieser Konten können den Schlüssel verwalten und verwenden, sofern sie

Statement	Zweck
	in ihren identitätsbasierten Richtlinien über die erforderlichen Berechtigungen verfügen.
<code>AllowIdentityCenterAndIdentityStoreToDescribeKey</code>	Ermöglicht den IAM Identity Center- und Identity Store-Dienstprinzipalen das Abrufen wichtiger Metadaten. Dies ist für Dienstvorgänge erforderlich, bei denen der Schlüssel überprüft wird, ohne eine Verschlüsselung oder Entschlüsselung durchzuführen. Diese <code>aws:SourceAccount</code> Bedingung stellt sicher, dass nur Ihre IAM Identity Center-Instanz Ihren KMS-Schlüssel verwenden kann.
<code>AllowIdentityCenterAndIdentityStoreToUseKey</code>	Ermöglicht den IAM Identity Center- und Identity Store-Dienstprinzipalen, den Schlüssel für Verschlüsselungsvorgänge wie das Verschlüsseln, Entschlüsseln und erneute Verschlüsseln von Daten zu verwenden. Diese <code>aws:SourceAccount</code> Bedingung stellt sicher, dass nur Ihre IAM Identity Center-Instanz Ihren KMS-Schlüssel verwenden kann.
<code>AllowOrgPrincipalsViaIdentityCenterAndIdentityStore</code>	Ermöglicht IAM-Prinzipalen in Ihrem AWS Unternehmen, Daten über die IAM Identity Center- und Identity Store-Dienste zu entschlüsseln. Dies gilt für Anwendungsadministratoren, die mithilfe von Forward Access Sessions (FAS) mit IAM Center-integrierten AWS Identity-Diensten interagieren.
<code>AllowManagedApps</code>	Ermöglicht AWS verwalteten Anwendungen das Entschlüsseln von Daten, die durch Ihren KMS-Schlüssel geschützt sind, über IAM Identity Center und Identity Store.

Verwenden Sie die folgende IAM-Richtlinienerklärung in, [Schritt 4: Konfigurieren Sie die IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](#) um delegierten Administratoren die Verwendung des KMS-Schlüssels über die IAM Identity Center Service-APIs zu ermöglichen. Ersetzen Sie den Beispielschlüssel-ARN durch Ihren tatsächlichen KMS-Schlüssel-ARN. Die Platzhalterregion im Beispiel enthält alle Replikate eines KMS-Schlüssels mit mehreren Regionen.

Bei kontoübergreifenden Anwendungsfällen, bei denen es sich nicht um die Verwaltung von IAM Identity Center handelt, wie SSO für Amazon EC2-Instances oder Verwaltung AWS verwalteter Anwendungen, beschränken Sie den Bereich AllowCrossAccountKMSKeyUse auf nur die Anweisung und entfernen Sie sie. kms:Decrypt AllowListKMSKeyAliases

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountKMSKeyUse",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/mrk-1234abcd-12ab-34cd-56ef-1234567890ab"
      ]
    },
    {
      "Sid": "AllowListKMSKeyAliases",
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

Erweiterte KMS-Grundsatzserklärungen

Verwenden Sie erweiterte KMS-Schlüsselrichtlinien, um detailliertere Zugriffskontrollen für Ihren vom Kunden verwalteten KMS-Schlüssel zu implementieren. Diese Richtlinien bauen darauf auf, [Grundlegende KMS-Schlüsselrichtlinie](#) indem sie Verschlüsselungskontextbedingungen und dienstspezifische Einschränkungen hinzufügen. Bevor Sie entscheiden, ob Sie erweiterte KMS-Schlüsselrichtlinien verwenden möchten, sollten Sie unbedingt die entsprechenden Überlegungen überprüfen.

Verwenden Sie den Verschlüsselungskontext, um den Zugriff einzuschränken

Sie können die Verwendung von KMS-Schlüsseln auf eine bestimmte IAM Identity Center-Instanz einschränken, indem Sie den AllowManagedApps Anweisungen AllowOrgPrincipalsViaIdentityCenterAndIdentityStore und in Ihrem [Grundlegende KMS-Schlüsselrichtlinie](#) Verschlüsselungskontext hinzufügen. Fügen Sie die folgenden Bedingungen mit Ihrem spezifischen Identity Center-Instanz-ARN und Identity Store-ARN hinzu. Sie können der IAM-Richtlinie, die für die kontoübergreifende Verwendung des KMS-Schlüssels konfiguriert ist, auch dieselben Bedingungen für den Verschlüsselungskontext hinzufügen.

Identity Center

```
"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn":
    "arn:aws:sso::instance/ssoins-1234567890abcdef"
}
```

Identitätsspeicher

```
"StringEquals": {
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":
    "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
}
```

Wenn Sie Hilfe bei der Suche nach diesen Identifikatoren benötigen, finden Sie weitere Informationen unter [Wo finde ich die erforderlichen Identifikatoren](#).

Note

Sie können einen vom Kunden verwalteten KMS-Schlüssel nur mit einer Organisationsinstanz von IAM Identity Center verwenden. Der vom Kunden verwaltete Schlüssel muss sich im Verwaltungskonto der AWS Organisation befinden. Dadurch wird sichergestellt, dass der Schlüssel mit einer einzelnen IAM Identity Center-Instanz verwendet wird. Der Verschlüsselungskontextmechanismus bietet jedoch einen unabhängigen technischen Schutz bei der Verwendung einer einzelnen Instanz. Sie können den `aws:SourceArn` Bedingungsschlüssel auch in den KMS-Schlüsselrichtlinienanweisungen verwenden, die für die Identity Center- und Identity Store-Dienstprinzipale bestimmt sind.

Überlegungen zur Implementierung der Bedingungen für den Verschlüsselungskontext

Bevor Sie die Bedingungen für den Verschlüsselungskontext implementieren, sollten Sie die folgenden Anforderungen überprüfen:

- **DescribeKey Aktion.** Der Verschlüsselungskontext kann nicht auf die Aktion „kms:DescribeKey“ angewendet werden, die von IAM Identity Center-Administratoren verwendet werden kann. Schließen Sie bei der Konfiguration Ihrer KMS-Schlüsselrichtlinie den Verschlüsselungskontext für diese spezielle Aktion aus, um den ordnungsgemäßen Betrieb Ihrer IAM Identity Center-Instanz sicherzustellen.
- **Neue Instanzeinrichtung.** Wenn Sie eine neue IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel aktivieren, finden Sie weitere Informationen unter [Überlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien](#).
- **Änderungen an der Identitätsquelle.** Wenn Sie Ihre Identitätsquelle zu oder von Active Directory ändern, muss der Verschlüsselungskontext besonders beachtet werden. Siehe [Überlegungen zum Ändern Ihrer Identitätsquelle](#).

Vorlagen für Richtlinien

Wählen Sie je nach Ihren Sicherheitsanforderungen aus diesen erweiterten Richtlinienvorlagen. Sorgen Sie für ein ausgewogenes Verhältnis zwischen granularen Zugriffskontrollen und dem damit verbundenen Verwaltungsaufwand.

Hier behandelte Themen:

- [KMS-Richtlinienanweisungen für die schreibgeschützte Verwendung einer bestimmten IAM Identity Center-Instanz](#). In diesem Abschnitt wird die Verwendung des Verschlüsselungskontexts für den schreibgeschützten Zugriff auf das IAM Identity Center veranschaulicht.
- [Verfeinerte KMS-Grundsatzserklärungen für die Verwendung von AWS verwaltete Anwendungen](#). In diesem Abschnitt wird gezeigt, wie Sie die KMS-Schlüsselrichtlinien für AWS verwaltete Anwendungen mithilfe des Verschlüsselungskontextes und der Anwendungsinformationen wie Anwendungsdienstprinzipal, Anwendungs-ARN und AWS Konto-ID verfeinern.

KMS-Richtlinienanweisungen für die schreibgeschützte Verwendung einer bestimmten IAM Identity Center-Instanz

Diese Richtlinie ermöglicht es [Sicherheitsprüfern](#) und anderem Personal, das nur Lesezugriff auf das IAM Identity Center benötigt, den KMS-Schlüssel zu verwenden.

Um diese Richtlinie zu verwenden:

1. Ersetzen Sie das Beispiel für schreibgeschützte Administrator-IAM-Prinzipale durch Ihre tatsächlichen Administrator-IAM-Prinzipale
2. Ersetzen Sie den Beispiel-ARN der IAM Identity Center-Instanz durch Ihren tatsächlichen Instanz-ARN
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Wenn Sie die [delegierte Administration verwenden](#), finden Sie weitere Informationen unter [Schritt 4: Konfigurieren Sie die IAM-Richtlinien für die kontoübergreifende Verwendung des KMS-Schlüssels](#)

Wenn Sie Hilfe bei der Suche nach den Werten dieser Identifikatoren benötigen, finden Sie unter [Wo finde ich die erforderlichen Identifikatoren](#)

Nachdem Sie die Vorlage mit Ihren Werten aktualisiert haben, kehren Sie zu zurück, [Schritt 2: Bereiten Sie die wichtigsten KMS-Richtlinienerklärungen vor](#) um bei Bedarf weitere wichtige KMS-Richtlinienerklärungen vorzubereiten.

Die Aktion `kms:Decrypt` allein schränkt den Zugriff nicht auf schreibgeschützte Operationen ein. Die IAM-Richtlinie muss den schreibgeschützten Zugriff auf die IAM Identity Center-Service-APIs erzwingen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
    }
  ]
}
```

```

    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn":
"arn:aws:sso::instance/ssoins-1234567890abcdef"
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
  ]
}

```

Verfeinerte KMS-Grundsatzserklärungen für die Verwendung von AWS verwaltete Anwendungen

Diese Richtlinienvorlagen bieten eine detailliertere Kontrolle darüber, welche AWS verwalteten Anwendungen Ihren KMS-Schlüssel verwenden können.

Note

Einige AWS verwaltete Anwendungen können nicht mit IAM Identity Center verwendet werden, das mit einem vom Kunden verwalteten KMS-Schlüssel konfiguriert ist. Sehen Sie sich [AWS verwaltete Anwendungen an, die Sie mit IAM Identity Center verwenden können.](#)

[Grundlegende KMS-Schlüsselrichtlinie](#) Mit dem kann jede AWS verwaltete Anwendung von jedem Konto in derselben AWS Organisation aus den KMS-Schlüssel verwenden. Verwenden Sie diese verfeinerten Richtlinien, um den Zugriff einzuschränken, indem Sie:

- Principal des Anwendungsdienstes
- ARNs der Anwendungsinstanz
- AWS Konto-IDs
- Verschlüsselungskontext für bestimmte IAM Identity Center-Instanzen

 Note

Ein Service Principal ist eine eindeutige Kennung für einen AWS Service, die in der Regel als `servicename.amazonaws.com` formatiert ist (z. B. `elasticmapreduce.amazonaws.com` für Amazon EMR).

Nach Konto einschränken

Diese Vorlage für eine KMS-Schlüsselrichtlinie ermöglicht es einer AWS verwalteten Anwendung in bestimmten AWS Konten, den KMS-Schlüssel mithilfe einer bestimmten IAM Identity Center-Instanz zu verwenden.

Um diese Richtlinie zu verwenden:

1. Ersetzen Sie den Beispiel-Serviceprinzipal durch Ihren tatsächlichen Anwendungs-Serviceprinzipal
2. Ersetzen Sie die Beispielkonto-IDs durch die tatsächlichen Konto-IDs, auf denen Ihre AWS verwalteten Anwendungen bereitgestellt werden
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Ersetzen Sie den ARN einer IAM Identity Center-Beispielinstanz durch Ihren tatsächlichen Instanz-ARN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
```

```

    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  },
  {
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
}

```

```

    }
  }
}
]
}

```

Nach Anwendungsinstanz einschränken

Diese Vorlage für KMS-Schlüsselrichtlinien ermöglicht es einer bestimmten AWS verwalteten Anwendungsinstanz, den KMS-Schlüssel mithilfe einer bestimmten IAM Identity Center-Instanz zu verwenden.

Um diese Richtlinie zu verwenden:

1. Ersetzen Sie den Beispiel-Serviceprinzipal durch Ihren tatsächlichen Anwendungs-Serviceprinzipal
2. Ersetzen Sie den ARN der Beispielanwendung durch den ARN Ihrer tatsächlichen Anwendungsinstanz
3. Ersetzen Sie den Beispiel-Identity Store-ARN durch Ihren tatsächlichen Identity Store-ARN
4. Ersetzen Sie den ARN einer IAM Identity Center-Beispielinstanz durch Ihren tatsächlichen Instanz-ARN

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        }
      }
    }
  ]
}

```

```

    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    }
  },
  {
    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

Überlegungen zu vom Kunden verwalteten KMS-Schlüsseln und erweiterten KMS-Schlüsselrichtlinien

Wenn Sie vom Kunden verwaltete KMS-Schlüssel mit IAM Identity Center implementieren, sollten Sie diese Faktoren berücksichtigen, die sich auf die Einrichtung, Sicherheit und laufende Wartung Ihrer Verschlüsselungskonfiguration auswirken.

Überlegungen zur Auswahl grundlegender und erweiterter KMS-Schlüsselrichtlinien

Bei der Entscheidung, ob Sie die KMS-Schlüsselberechtigungen spezifischer verwenden möchten [Erweiterte KMS-Grundsatzserklärungen](#), sollten Sie den Verwaltungsaufwand und die

Sicherheitsanforderungen Ihrer Organisation berücksichtigen. Spezifischere Policy-Statements ermöglichen eine genauere Kontrolle darüber, wer den Schlüssel für welche Zwecke verwenden kann. Sie müssen jedoch fortlaufend gewartet werden, da sich Ihre IAM Identity Center-Konfiguration weiterentwickelt. Wenn Sie beispielsweise die Verwendung des KMS-Schlüssels auf bestimmte AWS verwaltete Anwendungsbereitstellungen beschränken, müssen Sie die Schlüsselrichtlinie jedes Mal aktualisieren, wenn Ihre Organisation eine Anwendung bereitstellen oder deren Bereitstellung aufheben möchte. Weniger restriktive Richtlinien reduzieren den Verwaltungsaufwand, gewähren jedoch möglicherweise umfassendere Berechtigungen, als für Ihre Sicherheitsanforderungen erforderlich sind.

Überlegungen zur Aktivierung einer neuen IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel

Die hier aufgeführten Überlegungen gelten, wenn Sie den Verschlüsselungskontext verwenden, wie unter [Erweiterte KMS-Grundsatzzerklärungen](#). Um die Verwendung des KMS-Schlüssels auf eine bestimmte IAM Identity Center-Instanz zu beschränken, beschrieben.

Wenn Sie eine neue IAM Identity Center-Instanz mit einem vom Kunden verwalteten KMS-Schlüssel aktivieren, sind die IAM Identity Center- und Identity Store-ARNs erst nach der Einrichtung verfügbar. Ihnen stehen folgende Optionen zur Verfügung:

- Verwenden Sie vorübergehend generische ARN-Muster und ersetzen Sie sie nach der Aktivierung der Instanz durch vollständige ARNs. Denken Sie daran, bei Bedarf zwischen den StringLike Operatoren StringEquals und zu wechseln.
 - Für IAM Identity Center SPN: „arn: \$ {Partition} :sso: ::instance/*“.
 - Für Identitätsspeicher-SPN: „arn: \$ {Partition} :identitystore: :\$ {Account} :identitystore/*“.
- Verwenden Sie vorübergehend „purpose:KEY_CONFIGURATION“ im ARN. Dies funktioniert nur für die Instanzaktivierung und muss durch den tatsächlichen ARN ersetzt werden, damit Ihre IAM Identity Center-Instanz normal funktioniert. Der Vorteil dieses Ansatzes besteht darin, dass Sie nicht vergessen können, ihn zu ersetzen, nachdem die Instanz aktiviert wurde.
 - Verwenden Sie für IAM Identity Center SPN: „arn: \$ {Partition} :sso: ::KEY_CONFIGURATION“ instance/purpose
 - Verwenden Sie für Identity Store SPN: „arn: \$ {Partition} :identitystore: :\$ {Account} ::KEY_CONFIGURATION“ identitystore/purpose

 Important

Wenden Sie diese Konfiguration nicht auf einen KMS-Schlüssel an, der bereits in einer vorhandenen IAM Identity Center-Instanz verwendet wird, da dies den normalen Betrieb stören kann.

- Lassen Sie die Bedingung für den Verschlüsselungskontext in der KMS-Schlüsselrichtlinie aus, bis die Instanz aktiviert ist.

Ressourcen taggen AWS IAM Identity Center

Ein Tag ist eine benutzerdefinierte Attributbezeichnung, die Sie einer AWS Ressource hinzufügen, um die Identifizierung, Organisation und Suche nach Ressourcen zu erleichtern. Jedes -Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Tag-Schlüssel können bis zu 128 Zeichen lang sein und berücksichtigen die Groß-/Kleinschreibung.
- Einem Tag-Wert (z. B. `111122223333` oder `Production`). Tag-Werte können bis zu 256 Zeichen lang sein und wie bei Tag-Schlüsseln muss die Groß-/Kleinschreibung beachtet werden. Sie können den Wert eines Tags auf eine leere Zeichenfolge festlegen, aber Sie können den Wert eines Tags nicht auf Null setzen. Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge.

Mithilfe von Tags können Sie Ihre AWS Ressourcen identifizieren und organisieren. Viele AWS Dienste unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind. Sie können beispielsweise dasselbe Tag einem bestimmten Berechtigungssatz in Ihrer Instanz von IAM Identity Center zuweisen. Weitere Informationen zu Tagging-Strategien finden Sie unter [Tagging AWS Resources](#) im Allgemeine AWS-Referenz Guide und Best Practices für [Tagging](#).

Neben der Identifizierung, Organisation und Nachverfolgung Ihrer AWS Ressourcen mithilfe von Tags können Sie mithilfe von Tags in IAM-Richtlinien steuern, wer Ihre Ressourcen einsehen und mit ihnen interagieren kann. Weitere Informationen zur Verwendung von Tags zur Zugriffskontrolle finden Sie im IAM-Benutzerhandbuch unter [Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags](#). Sie können einem Benutzer beispielsweise erlauben, einen IAM Identity Center-Berechtigungssatz zu aktualisieren, aber nur, wenn der IAM Identity Center-Berechtigungssatz ein `owner` Tag mit dem Wert des Benutzernamens enthält.

Sie können Tags nur auf Berechtigungssätze anwenden. Sie können keine Tags auf die entsprechenden Rollen anwenden, in AWS-Konten denen IAM Identity Center erstellt. Sie können die IAM Identity Center-Konsole AWS CLI oder das IAM Identity Center verwenden, APIs um Tags für einen Berechtigungssatz hinzuzufügen, zu bearbeiten oder zu löschen.

In den folgenden Abschnitten finden Sie weitere Informationen zu Tags für IAM Identity Center.

Themen

- [Tag-Einschränkungen](#)
- [Verwalten Sie Tags mithilfe der IAM Identity Center-Konsole](#)
- [AWS CLI Beispiele](#)
- [Verwalten Sie Tags mithilfe der IAM Identity Center-API](#)

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags auf IAM Identity Center-Ressourcen:

- Die maximale Anzahl von Tags, die Sie einer Ressource zuweisen können, beträgt 50.
- Die maximale Schlüssellänge beträgt 128 Unicode-Zeichen.
- Die maximale Wertlänge beträgt 256 Unicode-Zeichen.
- Gültige Zeichen für einen Tag-Schlüssel und -Wert sind:

a-z, A-Z, 0-9, Leerzeichen und die folgenden Zeichen: _ . / = + - und @

- Bei Schlüssel und Werten wird die Groß-/Kleinschreibung berücksichtigt.
- Nicht `aws:` als Präfix für Schlüssel verwenden; es ist für die Verwendung reserviert AWS

Verwalten Sie Tags mithilfe der IAM Identity Center-Konsole

Sie können die IAM Identity Center-Konsole verwenden, um Tags hinzuzufügen, zu bearbeiten und zu entfernen, die Ihrer Instanz oder Ihren Berechtigungssätzen zugeordnet sind.

Um Berechtigungssätze und Tags für eine IAM Identity Center-Konsole zu verwalten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Berechtigungssätze.
3. Wählen Sie den Namen des Berechtigungssatzes, der die Tags enthält, die Sie verwalten möchten.
4. Führen Sie auf der Registerkarte Berechtigungen unter Tags eine der folgenden Aktionen aus, und fahren Sie dann mit dem nächsten Schritt fort:
 - a. Wenn diesem Berechtigungssatz bereits Tags zugewiesen wurden, wählen Sie Tags bearbeiten aus.

- b. Wenn diesem Berechtigungssatz keine Tags zugewiesen sind, wählen Sie Tags hinzufügen aus.
5. Geben Sie für jedes neue Tag die Werte in die Spalten Schlüssel und Wert (optional) ein. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

Um ein Tag zu entfernen, wählen Sie das X in der Spalte Entfernen neben dem Tag, das Sie entfernen möchten.

Um Tags für eine Instanz von IAM Identity Center zu verwalten

1. Öffnen Sie die [IAM-Identity-Center-Konsole](#).
2. Wählen Sie Einstellungen aus.
3. Wählen Sie die Registerkarte Tags aus.
4. Geben Sie für jedes Tag die Werte in die Felder Schlüssel und Wert (optional) ein. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Neues Tag hinzufügen.

Um ein Tag zu entfernen, klicken Sie auf die Schaltfläche Entfernen neben dem Tag, das Sie entfernen möchten.

AWS CLI Beispiele

Das AWS CLI stellt Befehle bereit, mit denen Sie die Tags verwalten können, die Sie Ihrem Berechtigungssatz zuweisen.

Zuweisen von Tags

Verwenden Sie die folgenden Befehle, um Ihrem Berechtigungssatz Tags zuzuweisen.

Example **tag-resource**Befehl für einen Berechtigungssatz

Weisen Sie einem Berechtigungssatz Tags zu, indem Sie [tag-resource](#) innerhalb des sso Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test
```

Dieser Befehl enthält die folgenden Parameter:

- **instance-arn**— Der Amazon-Ressourcenname (ARN) der IAM Identity Center-Instance, unter der der Vorgang ausgeführt wird.
- **resource-arn**— Der ARN der Ressource mit den aufgelisteten Tags.
- **tags** – Die Schlüssel-Wert-Paare der Tags.

Wenn Sie mehrere Tags auf einmal zuweisen möchten, geben Sie sie in eine durch Kommata getrennte Liste ein:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

Anzeigen von Tags

Verwenden Sie die folgenden Befehle, um die Tags anzuzeigen, die Sie Ihrem Berechtigungssatz zugewiesen haben.

Example **list-tags-for-resource** Befehl für einen Berechtigungssatz

Zeigen Sie die Tags an, die einem Berechtigungssatz zugewiesen sind, indem Sie [list-tags-for-resource](#) innerhalb des sso Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Entfernen von Tags

Verwenden Sie die folgenden Befehle, um Tags aus einem Berechtigungssatz zu entfernen.

Example **untag-resource** Befehl für einen Berechtigungssatz

Entfernen Sie Tags aus einem Berechtigungssatz, indem Sie [untag-resource](#) innerhalb des sso Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin untag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
>
```

```
> --tag-keys Stage CostCenter Owner
```

Geben Sie für den `--tag-keys`-Parameter einen oder mehrere Tag-Schlüssel ohne Tag-Werte an.

Anwenden von Tags beim Erstellen eines Berechtigungssatzes

Verwenden Sie die folgenden Befehle, um Tags zuzuweisen, sobald Sie einen Berechtigungssatz erstellen.

Example **create-permission-set**-Befehl mit Tags

Wenn Sie mithilfe des [create-permission-set](#)-Befehls einen Berechtigungssatz erstellen, können Sie Tags mit dem `--tags` Parameter angeben:

```
$ aws sso-admin create-permission-set \  
> --instance-arn sso-instance-arn \  
> --name permission=set-name \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

Verwalten Sie Tags mithilfe der IAM Identity Center-API

Verwenden Sie die folgenden API-Aktionen, um Tags für einen Berechtigungssatz oder eine Instanz von IAM Identity Center zuzuweisen, anzuzeigen und zu entfernen.

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

Integration von AWS CLI mit IAM Identity Center

AWS Die Integration von Command Line Interface (CLI) Version 2 mit IAM Identity Center vereinfacht den Anmeldevorgang. Entwickler können sich direkt AWS CLI mit den gleichen Active Directory- oder IAM Identity Center-Anmeldeinformationen anmelden, die sie normalerweise für die Anmeldung bei IAM Identity Center verwenden, und auf die ihnen zugewiesenen Konten und Rollen zugreifen. Wenn ein Administrator beispielsweise IAM Identity Center für die Verwendung von Active Directory für die Authentifizierung konfiguriert hat, kann sich ein Entwickler AWS CLI direkt mit seinen Active Directory-Anmeldeinformationen anmelden.

AWS Die CLI-Integration mit IAM Identity Center bietet die folgenden Vorteile:

- Unternehmen können es ihren Entwicklern ermöglichen, sich mit Anmeldeinformationen von IAM Identity Center oder Active Directory anzumelden, indem sie IAM Identity Center über ihr Active Directory verbinden. Directory Service
- Entwickler können sich für einen schnelleren Zugriff über die CLI anmelden.
- Entwickler können Konten und Rollen, denen sie Zugriff zugewiesen haben, auflisten und zwischen ihnen wechseln.
- Entwickler können automatisch benannte Rollenprofile in ihrer CLI-Konfiguration generieren und speichern und sie in der CLI referenzieren, um Befehle in den gewünschten Konten und Rollen auszuführen.
- Die CLI verwaltet kurzfristige Anmeldeinformationen automatisch, sodass Entwickler sicher und ohne Unterbrechung in der CLI beginnen und dort bleiben und Skripts mit langer Laufzeit ausführen können.

So integrieren Sie AWS CLI in IAM Identity Center

Um die AWS CLI-Integration mit IAM Identity Center zu verwenden, laden Sie AWS Command Line Interface Version 2 herunter, installieren und konfigurieren Sie sie. Ausführliche Schritte zum Herunterladen und zur Integration AWS CLI mit IAM Identity Center finden Sie unter [Konfiguration der AWS CLI für die Verwendung von IAM Identity Center](#) im AWS Command Line Interface Benutzerhandbuch.

Überlegungen zum AWS-Managementkonsole privaten Zugriff

Wenn Ihr Unternehmen die AWS-Managementkonsole Private Access-Funktion verwendet, sollten Sie sich überlegen, wie sich Ihre Benutzer bei IAM Identity Center anmelden.

Eine VPC-Endpunktrichtlinie schränkt die Anmeldung an der Verwaltungskonsole ein, wodurch verhindert wird, dass sich Ihre Benutzer dort anmelden, zu deren Zugriff AWS-Konten sie nicht berechtigt sind. Weitere Informationen finden Sie unter [AWS-Managementkonsole Private Access im Handbuch AWS-Managementkonsole](#) Erste Schritte.

VPC-Endpunkte blockieren die Anmeldung beim IAM Identity Center

Es ist wichtig zu beachten, dass die Verwendung von VPC-Endpunkten die Anmeldung beim IAM Identity Center blockiert. Dies passiert, wenn ein Benutzer bereits über den VPC-Endpunkt bei der Managementkonsole angemeldet ist. Um sicherzustellen, dass sich Ihre Benutzer weiterhin bei IAM Identity Center anmelden können, müssen sie den öffentlichen Endpunkt für die AWS Anmeldung verwenden und nicht den VPC-Endpunkt.

Kontingente und Grenzwerte in IAM Identity Center

In den folgenden Tabellen werden Kontingente in IAM Identity Center beschrieben. Anfragen zur Erhöhung des Kontingents müssen von einem Verwaltungskonto oder einem delegierten Administratorkonto stammen. Informationen zur Erhöhung eines Kontingents finden Sie unter Eine Kontingenterhöhung <https://docs.aws.amazon.com/servicequotas/latest/userguide/request-quota-increase.html> beantragen.

Note

Wir empfehlen, IAM Identity Center mithilfe der AWS CLI und der APIs zentral zu verwalten, wenn Sie mehr als 50.000 Benutzer, 10.000 Gruppen, 500 Berechtigungssätze oder 3.000 Anwendungen haben. Weitere Informationen zur CLI finden Sie unter [Integration von AWS CLI mit IAM Identity Center](#). Weitere Informationen zu APIs finden Sie unter [Willkommen bei der IAM Identity Center API-Referenz](#).

Kontingente für Anwendungen

Ressource	Standardkontingent	Kann erhöht werden
Dateigröße der SAML-Zertifikate vom Service-Anbieter (im PEM-Format)	2 KB	Nein
SAML-Assertion-Limit	50.000 Zeichen	Nein
Dateigrößenbeschränkung des IdP-Zertifikats, das in das IAM Identity Center hochgeladen wurde	2500 () Zeichen UTF-8	Nein
Zugriffsbereiche pro Anwendung	25	Nein

AWS-Konto Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl der in IAM Identity Center zulässigen Berechtigungssätze	3500	Ja
Anzahl zulässiger bereitgestellter Berechtigungssätze pro AWS-Konto	500	Ja
Anzahl der eingebundenen Richtlinien pro Berechtigungssatz	1	Nein
Anzahl der AWS verwalteten und vom Kunden verwalteten Richtlinien pro Berechtigungssatz	25 ¹	Nein
Maximale Größe der eingebundenen Richtlinie pro Berechtigungssatz	32.768 Byte. Die maximale Größe von Zeichen ohne Leerzeichen in der Inline-Richtlinie pro Berechtigungssatz beträgt 10.240 Byte.	Nein
Anzahl der IAM-Rollen (Berechtigungssätze) in der AWS-Konto , die gleichzeitig aktualisiert werden können	1	Nein

¹ AWS Identity and Access Management (IAM) legt ein Kontingent von 10 verwalteten Richtlinien pro Rolle fest. Um dieses Kontingent nutzen zu können, fordern Sie eine Erhöhung des IAM-Kontingents an. Verwaltete Richtlinien, die einer IAM-Rolle zugeordnet sind, können Sie in

der Dienstkontingents-Konsole für jede AWS-Konto Richtlinie beantragen, für die Sie den Berechtigungssatz bereitstellen möchten.

Note

[Verwalten AWS-Konten mit Berechtigungssätzen](#) werden AWS-Konten als IAM-Rollen bereitgestellt oder verwenden vorhandene IAM-Rollen in und halten sich daher an AWS-Konten IAM-Kontingente. Weitere Informationen zu Kontingenten, die IAM-Rollen zugeordnet sind, finden Sie unter [IAM- und STS-Kontingente](#).

Active Directory-Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl der gleichzeitig möglichen verbundenen Verzeichnisse	1	Nein

Kontingente für den IAM Identity Center-Identitätsspeicher

Ressource	Standardkontingent	Kann erhöht werden
Anzahl unterstützter Benutzer in IAM Identity Center	200000	Ja
Anzahl unterstützter Gruppen in IAM Identity Center	100000	Ja

Drosselungsgrenzen für IAM Identity Center

Ressource	Standardkontingent
IAM Identity Center-APIs	Für IAM Identity Center-APIs gilt ein kollektives Drossellimit von 20 Transaktionen pro Sekunde

Ressource	Standardkontingent
	<p>(TPS). Für Read-APIs können Sie eine Support-Anfrage stellen, um eine Erhöhung des Limits zu beantragen. Die CreateAccountAssignment Schreib-API hat ein Limit von 15 ausstehenden asynchronen Aufrufen. Dieses Limit kann nicht erhöht werden.</p>
Identity Store-APIs	<p>Für Identity Store-APIs gilt ein Drossellimit von 20 Transaktionen pro Sekunde (TPS) pro API. Dieses Limit gilt pro Identity Store-Instanz. Sie können einen Support-Fall eröffnen, um eine Erhöhung des Limits zu beantragen.</p>
SCIM-APIs	<p>SCIM-APIs haben Drosselungsgrenzen pro API von 25 Transaktionen pro Sekunde (TPS) für Schreib-APIs und 40 TPS für Lese-APIs. Diese Grenzwerte gelten pro Identity Store-Instanz. Sie können einen Support-Fall eröffnen, um eine Erhöhung des Limits zu beantragen.</p> <p>Jeder einzelne Mitgliedschaftsvorgang in <code>CreateGroup</code> oder an unseren <code>PatchGroup</code> Aufrufen zählt als Transaktion und führt zu einem separaten Drossellimit für Mitgliedschaftsvorgänge pro Identity Store.</p>

Wenn Ihre IAM Identity Center-Instance in mehreren Fällen aktiviert ist AWS-Regionen, gelten die Drossellimits gleichermaßen für jede aktivierte Region. Zum Beispiel hätten Sie das Drossellimit von 20 TPS für die Identity Store-APIs in jeder aktivierten Region. Weitere Informationen darüber, welche API-Operationen in weiteren Regionen verfügbar sind, finden Sie in der entsprechenden [Tabelle](#).

Kontingente für OIDC-Dienstanfragen

Ressource	Standardwert (Anforderungen pro Sekunde)	Kann erhöht werden
<p>Anforderungsrate von einer Remote-Adresse zur Registrierung eines öffentlichen OAuth-Clients</p> <p>Gilt für: RegisterClient</p>	20	Ja
<p>Anforderungsrate von einem öffentlichen Kunden, der beim OIDC-Dienst registriert ist</p> <p>Gilt für: CreateToken StartDeviceAuthorization</p>	80	Ja
<p>Anforderungsrate von allen öffentlichen Clients, die bei derselben IAM Identity Center-Instanz registriert sind</p> <p>Gilt für: CreateToken</p>	250	Ja
<p>Anforderungsrate von einer IAM Identity Center-Anwendung, die bei der IAM Identity Center-Instanz mit Token-Exchange- und Refresh-Token-Zuweisungen registriert ist.</p> <p>Gilt für: CreateTokenWithIAM</p>	80	Ja
<p>Token-Generierungsrate aus allen IAM Identity Center-Anwendungen, die bei derselben</p>	10	AWS Support kontaktieren

Ressource	Standardwert (Anforderungen pro Sekunde)	Kann erhöht werden
IAM Identity Center-Instanz mit JWT Bearer-Grant registriert sind		
Gilt für: CreateTokenWithIAM		

Wenn Ihre IAM Identity Center-Instance mehrfach aktiviert ist AWS-Regionen, gelten die oben genannten Anforderungsraten für jede aktivierte Region gleichermaßen. Wenn Ihre zulässige Anforderungsrate zum Registrieren eines öffentlichen OAuth-Clients von einer Remote-Adresse aus beispielsweise 20 Anfragen pro Sekunde beträgt, ist dieser Durchsatz in jeder aktivierten Region verfügbar. Weitere Informationen darüber, welche API-Operationen in weiteren Regionen verfügbar sind, finden Sie in der entsprechenden [Tabelle](#).

Zusätzliche Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Gesamtzahl der AWS-Konten Anwendungen, die konfiguriert werden können* **	7000	Ja
Gesamtzahl der IAM Identity Center-Instanzen pro Konto	1	Nein
Gesamtzahl der vertrauenswürdig Token-Aussteller	10	Nein
Gesamtzahl der Gruppen, die einem Berechtigungssatz pro oder einer AWS-Konto Anwendung zugewiesen werden können	100	Nein

Ressource	Standardkontingent	Kann erhöht werden
Gesamtzahl der für eine einzelne IAM Identity Center-Instanz AWS-Regionen aktivierten	6	Ja

* Dieses Kontingent gilt separat für AWS-Konten und für Anwendungen. Sie können bis zu 7000 Konten und bis zu 7000 Anwendungen konfigurieren.

** Der [ProvisionPermissionSet](#) API-Vorgang kann mithilfe der Option `ALL_PROVISIONED_ACCOUNTS` maximal 3500 einen Berechtigungssatz bereitstellen AWS-Konten. Wenn Sie einen Berechtigungssatz von mehr als 3500 bereitstellen müssen AWS-Konten, können Sie den `ProvisionPermissionSet` API-Vorgang mit der `AWS_ACCOUNT` Option verwenden, die den Berechtigungssatz in einem einzigen Vorgang bereitstellt AWS-Konto. Sie können bis zu drei gleichzeitige Anrufe an `ProvisionPermissionSet` tätigen.

Problembehandlung bei IAM Identity Center-Problemen

Die folgenden Informationen können Ihnen bei der Behebung einiger häufig auftretender Probleme helfen, die bei der Einrichtung oder Verwendung der IAM Identity Center-Konsole auftreten können.

Probleme beim Erstellen einer Kontoinstanz von IAM Identity Center

Beim Erstellen einer Kontoinstanz von IAM Identity Center gelten möglicherweise mehrere Einschränkungen. Wenn Sie keine Kontoinstanz über die IAM Identity Center-Konsole oder die Einrichtung einer unterstützten AWS verwalteten Anwendung erstellen können, überprüfen Sie die folgenden Anwendungsfälle:

- Wählen Sie das andere AWS-Regionen Feld aus, AWS-Konto in dem Sie versuchen, die Kontoinstanz zu erstellen. Sie sind auf eine IAM Identity Center-Instanz pro AWS-Konto Instanz beschränkt. Um die Anwendung zu aktivieren, wechseln Sie entweder zu der AWS-Region mit der Instanz von IAM Identity Center oder wechseln Sie zu einem Konto ohne eine Instanz von IAM Identity Center.
- Wenn Ihre Organisation IAM Identity Center vor dem 14. September 2023 aktiviert hat, muss sich Ihr Administrator möglicherweise für die Erstellung einer Kontoinstanz anmelden. Arbeiten Sie mit Ihrem Administrator zusammen, um die Erstellung von Kontoinstanzen über die IAM Identity Center-Konsole im Verwaltungskonto zu ermöglichen.
- Ihr Administrator hat möglicherweise eine Service Control Policy erstellt, um die Erstellung von Kontoinstanzen von IAM Identity Center einzuschränken. Arbeiten Sie mit Ihrem Administrator zusammen und fügen Sie Ihr Konto zur Zulassungsliste hinzu.

Sie erhalten eine Fehlermeldung, wenn Sie versuchen, die Liste der Cloud-Anwendungen anzuzeigen, die für die Verwendung mit IAM Identity Center vorkonfiguriert sind

Der folgende Fehler tritt auf, wenn Sie eine Richtlinie haben, die andere IAM Identity Center-APIs zulässt, `sso:ListApplications` aber nicht. Aktualisieren Sie Ihre Richtlinie, um diesen Fehler zu beheben.

Die `ListApplications` Genehmigung autorisiert mehrere APIs:

- Die ListApplications API.
- Eine interne API, die der in der IAM Identity Center-Konsole verwendeten ListApplicationProviders API ähnelt.

Um Duplikate zu vermeiden, autorisiert die interne API jetzt auch die Verwendung der Aktion. ListApplicationProviders Um die öffentliche ListApplications API zuzulassen, aber die interne API zu verweigern, muss Ihre Richtlinie eine Erklärung enthalten, die die Aktion ablehnt: ListApplicationProviders

```

    "Statement": [
    {
        "Effect": "Deny",
        "Action": "sso:ListApplicationProviders",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "sso:ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
    ]

```

Um die interne API zuzulassen, aber abzulehnen ListApplications, muss die Richtlinie nur ListApplicationProviders zulassen. Die ListApplications API wird verweigert, wenn sie nicht ausdrücklich erlaubt ist.

```

    "Statement": [
    {
        "Effect": "Allow",
        "Action": "sso:ListApplicationProviders",
        "Resource": "*"
    }
    ]

```

Wenn Ihre Richtlinien aktualisiert werden, wenden Sie sich an uns, Support um diese proaktive Maßnahme aufzuheben.

Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden

IAM Identity Center bietet eine webbasierte Debug-Umgebung für die SAML-Assertionen, die von IAM Identity Center erstellt und gesendet wurden, einschließlich der Attribute in diesen Assertionen, wenn auf SAML-Anwendungen vom Access-Portal aus zugegriffen AWS-Konten wird. AWS Gehen Sie wie folgt vor, um die Details einer SAML-Assertion anzuzeigen, die IAM Identity Center generiert.

1. Melden Sie sich beim Access-Portal an AWS .
2. Halten Sie die **UMSCHALTTASTE** gedrückt, während Sie im Portal angemeldet sind, wählen Sie die Anwendungskachel aus, und lassen Sie dann die **UMSCHALTTASTE** los.
3. Überprüfen Sie die Informationen auf der Seite mit dem Titel **You are now in administrator mode** (Sie befinden sich jetzt im Administratormodus). Um diese Informationen zum späteren Nachschlagen aufzubewahren, wählen Sie „XML kopieren“ und fügen Sie den Inhalt an einer anderen Stelle ein.
4. Wählen Sie **Senden**, `<application>`um fortzufahren. Diese Option sendet die Assertion an den Dienstanbieter.

Note

Einige Browserkonfigurationen und Betriebssysteme unterstützen dieses Verfahren möglicherweise nicht. Dieses Verfahren wurde unter Windows 10 mit den Browsern Firefox, Chrome und Edge getestet.

Bestimmte Benutzer können von einem externen SCIM-Anbieter nicht mit IAM Identity Center synchronisiert werden

Wenn Ihr Identity Provider (IdP) so konfiguriert ist, dass Benutzer mithilfe der SCIM-Synchronisierung für IAM Identity Center bereitgestellt werden, kann es bei der Benutzerbereitstellung zu Synchronisierungsfehlern kommen. Dies kann darauf hindeuten, dass die Benutzerkonfiguration in Ihrem IdP nicht mit den IAM Identity Center-Anforderungen kompatibel ist. In diesem Fall geben die SCIM-APIs von IAM Identity Center Fehlermeldungen zurück, die Aufschluss über die Ursache des Problems geben. Sie finden diese Fehlermeldungen in den Protokollen oder in der

Benutzeroberfläche Ihres IdP. Alternativ finden Sie möglicherweise detailliertere Informationen zu den Bereitstellungsfehlern in den [AWS CloudTrail Protokollen](#).

Weitere Informationen zu den SCIM-Implementierungen von IAM Identity Center, einschließlich der Spezifikationen der erforderlichen, optionalen und nicht unterstützten Parameter und Operationen für Benutzerobjekte, finden Sie im [IAM Identity Center SCIM Implementation Developer Guide im SCIM-Entwicklerhandbuch](#)

Im Folgenden sind einige häufige Gründe für diesen Fehler aufgeführt:

1. Dem Benutzerobjekt im IdP fehlt ein Vor- (Vor-) Name, ein Nachname (Familiennamen) und and/ or ein Anzeigename.

Fehlermeldung: „*'name.givenName'* Es wurden 2 Validierungsfehler erkannt: Der Wert at hat die Einschränkung nicht erfüllt: Das Element muss das Muster des regulären Ausdrucks erfüllen: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`; Wert at *'name.givenName'* konnte die Einschränkung nicht erfüllen: Das Element muss eine Länge von größer oder gleich 1" haben

- Lösung: Fügen Sie einen Vor- (bestimmten), Nachnamen- (Familien-) und Anzeigenamen für das Benutzerobjekt hinzu. Stellen Sie außerdem sicher, dass die SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP so konfiguriert sind, dass für all diese Attribute nicht leere Werte gesendet werden.
2. Es wird mehr als ein Wert für ein einzelnes Attribut an den Benutzer gesendet (auch bekannt als „Attribute mit mehreren Werten“). Beispielsweise kann der Benutzer sowohl eine geschäftliche als auch eine private Telefonnummer im IdP oder mehrere E-Mails oder physische Adressen haben, und Ihr IdP ist so konfiguriert, dass er versucht, mehrere oder alle Werte für dieses Attribut zu synchronisieren.

Fehlermeldung: „Das Listenattribut *emails* überschreitet das zulässige Limit von 1“

- Lösungsoptionen:
 - i. Aktualisieren Sie Ihre SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP, sodass nur ein einziger Wert für ein bestimmtes Attribut gesendet wird. Konfigurieren Sie beispielsweise ein Mapping, das nur die geschäftliche Telefonnummer für jeden Benutzer sendet.
 - ii. Wenn die zusätzlichen Attribute problemlos aus dem Benutzerobjekt beim IdP entfernt werden können, können Sie die zusätzlichen Werte entfernen, sodass für dieses Attribut entweder ein Wert oder Null für den Benutzer festgelegt bleibt.

- iii. Wenn das Attribut für keine Aktionen in benötigt wird AWS, entfernen Sie die Zuordnung für dieses Attribut aus den SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP.
3. Ihr IdP versucht, anhand mehrerer Attribute die Benutzer im Ziel (in diesem Fall IAM Identity Center) abzugleichen. Da Benutzernamen innerhalb einer bestimmten IAM Identity Center-Instanz garantiert eindeutig sind, müssen Sie nur das Attribut angeben, das für den username Abgleich verwendet wird.
 - Lösung: Stellen Sie sicher, dass Ihre SCIM-Konfiguration in Ihrem IdP nur ein einziges Attribut für den Abgleich mit Benutzern in IAM Identity Center verwendet. Beispielsweise ist die Zuordnung von `username` oder `userPrincipalName` im IdP zu dem `userName` Attribut in SCIM für die Bereitstellung im IAM Identity Center korrekt und für die meisten Implementierungen ausreichend.

Fehler beim Bereitstellen von Benutzern oder Gruppen bei der Bereitstellung von Benutzern oder Gruppen über einen externen Identitätsanbieter

Wenn bei der Bereitstellung von Benutzern oder Gruppen in einem externen Identitätsanbieter (IdP) Probleme mit der IAM Identity Center-Synchronisierung auftreten, kann dies daran liegen, dass Ihre externen IdP-Benutzer oder -Gruppen keine eindeutigen Attributwerte haben. In Ihrem externen IdP erhalten Sie möglicherweise die folgenden Fehlermeldungen:

Weigerte sich, eine neue, doppelte Ressource zu erstellen

Dieses Problem kann in den folgenden Szenarien auftreten:

- Szenario 1
 - Sie verwenden benutzerdefinierte, nicht eindeutige Attribute in Ihrem externen IdP für Attribute, die in IAM Identity Center eindeutig sein müssen. Bestehende IAM Identity Center-Benutzer oder -Gruppen können nicht mit Ihrem IdP synchronisiert werden.
- Szenario 2
 - Sie versuchen, Benutzer mit doppelten Attributen für Attribute zu erstellen, die in IAM Identity Center eindeutig sein müssen.

- Beispiel: Sie erstellen einen IAM Identity Center-Benutzer mit den folgenden Attributen oder haben einen vorhandenen:
 - Benutzername: Jane Doe
 - Primäre E-Mail-Adresse: jane_doe@example.com
- Dann versuchen Sie, in Ihrem externen IdP einen weiteren Benutzer mit den folgenden Attributen zu erstellen:
 - Benutzername: Richard Doe
 - Primäre E-Mail-Adresse: jane_doe@example.com
 - Der externe IdP versucht, den Benutzer im IAM Identity Center zu synchronisieren und zu erstellen. Diese Aktionen schlagen jedoch fehl, da beide Benutzer doppelte Werte für eine primäre E-Mail-Adresse haben, die eindeutig sein muss.

Der Benutzername, die primäre E-Mail-Adresse und die ExternalID müssen eindeutig sein, damit Ihre externen IdP-Benutzer erfolgreich mit IAM Identity Center synchronisiert werden können. Ebenso muss der Gruppenname für Ihre externen IdP-Gruppen eindeutig sein, damit eine erfolgreiche Synchronisierung mit IAM Identity Center möglich ist.

Die Lösung besteht darin, die Attribute Ihrer Identitätsquelle zu überprüfen und sicherzustellen, dass sie eindeutig sind.

Benutzer können sich nicht anmelden, wenn ihr Benutzername im UPN-Format ist

Benutzer können sich aufgrund des Formats, das sie zur Eingabe ihres Benutzernamens auf der Anmeldeseite verwenden, möglicherweise nicht beim AWS Access-Portal anmelden. In den meisten Fällen können sich Benutzer entweder mit ihrem einfachen Benutzernamen, ihrem untergeordneten Anmeldename (DOMAIN\UserName) oder ihrem UPN-Anmeldename () am Benutzerportal anmelden. `UserName@Corp.Example.com` Die Ausnahme ist, wenn IAM Identity Center ein verbundenes Verzeichnis verwendet, das mit MFA aktiviert wurde und der Bestätigungsmodus auf `Context-aware` oder `Always-on` gesetzt wurde. In diesem Szenario müssen sich Benutzer mit ihrem untergeordneten Anmeldename (DOMAIN\) anmelden. `UserName` Weitere Informationen finden Sie unter [MFA für Identity Center-Verzeichnisbenutzer](#). Allgemeine Informationen zu Benutzernamenformaten, die für die Anmeldung bei Active Directory verwendet werden, finden Sie unter [Benutzernamenformate](#) auf der Microsoft-Dokumentationswebsite.

Beim Ändern einer IAM-Rolle erhalte ich die Fehlermeldung „Der Vorgang kann für die geschützte Rolle nicht ausgeführt werden“

Bei der Überprüfung der IAM-Rollen in einem Konto fallen Ihnen möglicherweise Rollennamen auf, die mit 'awsReservedSSO_' beginnen. Dies sind die Rollen, die der IAM Identity Center-Dienst in dem Konto erstellt hat. Sie stammen aus der Zuweisung eines Berechtigungssatzes zu dem Konto. Der Versuch, diese Rollen von der IAM-Konsole aus zu ändern, führt zu dem folgenden Fehler:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -  
this role is only modifiable by AWS'
```

Diese Rollen können nur über die IAM Identity Center-Administratorkonsole geändert werden, die sich im Verwaltungskonto von befindet. AWS Organizations Nach der Änderung können Sie die Änderungen auf die AWS Konten übertragen, denen sie zugewiesen sind.

Verzeichnisbenutzer können ihr Passwort nicht zurücksetzen

Wenn ein Verzeichnisbenutzer sein Passwort mit der Option Passwort vergessen zurücksetzt? Bei der Anmeldung im AWS Access Portal muss das neue Passwort der Standard-Passwortrichtlinie entsprechen, wie unter beschrieben. [Kennwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center](#)

Wenn ein Benutzer ein Passwort eingibt, das der Richtlinie entspricht, und dann die Fehlermeldung erhält `We couldn't update your password`, überprüfen Sie, ob der Fehler AWS CloudTrail aufgezeichnet wurde. Suchen Sie dazu in der Event-History-Konsole oder CloudTrail verwenden Sie den folgenden Filter:

```
"UpdatePassword"
```

Wenn in der Nachricht Folgendes steht, müssen Sie sich möglicherweise an den Support wenden:

```
"errorCode": "InternalFailure",  
  "errorMessage": "An unknown error occurred"
```

Eine weitere mögliche Ursache für dieses Problem liegt in der Namenskonvention, die auf den Benutzernamenwert angewendet wurde. Benennungskonventionen müssen bestimmten Mustern

wie „Surname.GivenName“ folgen. Einige Benutzernamen können jedoch ziemlich lang sein oder Sonderzeichen enthalten. Dies kann dazu führen, dass Zeichen im API-Aufruf weggelassen werden, was zu einem Fehler führt. Möglicherweise möchten Sie versuchen, das Passwort mit einem Testbenutzer auf die gleiche Weise zurückzusetzen, um zu überprüfen, ob dies der Fall ist.

Wenn das Problem weiterhin besteht, wenden Sie sich an das [AWS Support Center](#).

Auf meinen Benutzer wird in einem Berechtigungssatz verwiesen, er kann jedoch nicht auf die zugewiesenen Konten oder Anwendungen zugreifen

Dieses Problem kann auftreten, wenn Sie System for Cross-domain Identity Management (SCIM) für die automatische Bereitstellung mit einem externen Identitätsanbieter verwenden. Insbesondere wenn ein Benutzer oder die Gruppe, der der Benutzer angehörte, gelöscht und dann mit demselben Benutzernamen (für Benutzer) oder Namen (für Gruppen) im Identitätsanbieter neu erstellt wird, wird eine neue eindeutige interne ID für den neuen Benutzer oder die neue Gruppe in IAM Identity Center erstellt. IAM Identity Center hat jedoch immer noch einen Verweis auf den alten Bezeichner in seiner Berechtigungsdatenbank, sodass der Name des Benutzers oder der Gruppe weiterhin in der Benutzeroberfläche angezeigt wird, der Zugriff jedoch fehlschlägt. Dies liegt daran, dass die zugrunde liegende Benutzer- oder Gruppen-ID, auf die sich die Benutzeroberfläche bezieht, nicht mehr existiert.

Um den AWS-Konto Zugriff in diesem Fall wiederherzustellen, können Sie den Zugriff für den alten Benutzer oder die alte Gruppe von dem/den AWS-Konto Benutzern oder den alten Gruppen entfernen, denen er ursprünglich zugewiesen wurde, und den Zugriff dann wieder dem Benutzer oder der Gruppe zuweisen. Dadurch wird der Berechtigungssatz mit der richtigen Kennung für den neuen Benutzer oder die neue Gruppe aktualisiert. Ebenso können Sie zur Wiederherstellung des Anwendungszugriffs den Zugriff für den Benutzer oder die Gruppe aus der Liste der zugewiesenen Benutzer für diese Anwendung entfernen und den Benutzer oder die Gruppe dann wieder hinzufügen.

Sie können auch überprüfen, ob der Fehler AWS CloudTrail aufgezeichnet wurde, indem Sie Ihre CloudTrail Protokolle nach SCIM-Synchronisierungsereignissen durchsuchen, die auf den Namen des betreffenden Benutzers oder der betreffenden Gruppe verweisen.

Ich kann meine Anwendung aus dem Anwendungskatalog nicht korrekt konfigurieren

Wenn Sie eine Anwendung aus dem Anwendungskatalog in IAM Identity Center hinzugefügt haben, beachten Sie, dass jeder Dienstanbieter seine eigene ausführliche Dokumentation bereitstellt. Sie können auf diese Informationen über die Registerkarte „Konfiguration“ für die Anwendung in der IAM Identity Center-Konsole zugreifen.

Wenn das Problem mit der Einrichtung der Vertrauensstellung zwischen der Anwendung des Dienstanbieters und dem IAM Identity Center zusammenhängt, lesen Sie in der Bedienungsanleitung nach, welche Schritte zur Fehlerbehebung erforderlich sind.

Fehler „Ein unerwarteter Fehler ist aufgetreten“, wenn ein Benutzer versucht, sich mit einem externen Identitätsanbieter anzumelden

Dieser Fehler kann aus mehreren Gründen auftreten, aber ein häufiger Grund ist eine Diskrepanz zwischen den Benutzerinformationen, die in der SAML-Anfrage enthalten sind, und den Informationen für den Benutzer im IAM Identity Center.

Damit sich ein IAM Identity Center-Benutzer erfolgreich anmelden kann, wenn er einen externen IdP als Identitätsquelle verwendet, muss Folgendes zutreffen:

- Das SAML-NameID-Format (bei Ihrem Identitätsanbieter konfiguriert) muss „E-Mail“ lauten
- Der NameID-Wert muss eine ordnungsgemäß (RFC2822) formatierte Zeichenfolge sein (user@domain.com)
- Der NameID-Wert muss exakt mit dem Benutzernamen eines vorhandenen Benutzers in IAM Identity Center übereinstimmen (es spielt keine Rolle, ob die E-Mail-Adresse im IAM Identity Center übereinstimmt oder nicht — der eingehende Treffer basiert auf dem Benutzernamen)
- Die IAM Identity Center-Implementierung des SAML 2.0-Verbunds unterstützt nur eine Assertion in der SAML-Antwort zwischen dem Identitätsanbieter und IAM Identity Center. Verschlüsselte SAML-Assertionen werden nicht unterstützt.
- Die folgenden Anweisungen gelten, wenn sie [Attribute für Zugriffskontrolle](#) in Ihrem IAM Identity Center-Konto aktiviert sind:
 - Die Anzahl der Attribute, die in der SAML-Anfrage zugeordnet sind, muss 50 oder weniger betragen.

- Die SAML-Anfrage darf keine mehrwertigen Attribute enthalten.
- Die SAML-Anfrage darf nicht mehrere Attribute mit demselben Namen enthalten.
- Das Attribut darf kein strukturiertes XML als Wert enthalten.
- Das Namensformat muss ein von SAML spezifiziertes Format sein, kein generisches Format.

Note

IAM Identity Center erstellt Benutzer oder Gruppen für neue Benutzer oder Gruppen nicht „Just-in-Time“ über den SAML-Verbund. Das bedeutet, dass der Benutzer in IAM Identity Center vorab erstellt werden muss, entweder manuell oder über automatische Bereitstellung, um sich bei IAM Identity Center anmelden zu können.

Dieser Fehler kann auch auftreten, wenn der in Ihrem Identitätsanbieter konfigurierte Assertion Consumer Service (ACS) -Endpunkt nicht mit der von Ihrer IAM Identity Center-Instance bereitgestellten ACS-URL übereinstimmt. Stellen Sie sicher, dass diese beiden Werte exakt übereinstimmen.

Darüber hinaus können Sie Anmeldefehler bei externen Identitätsanbietern weiter beheben, indem Sie zum Namen `ExternalIdPDDirectoryLogin` des Ereignisses wechseln AWS CloudTrail und nach diesem filtern.

Fehler 'Die Attribute für die Zugriffskontrolle konnten nicht aktiviert werden'

Dieser Fehler kann auftreten, wenn der Benutzer, der ABAC aktiviert, nicht über die für die Aktivierung `iam:UpdateAssumeRolePolicy` erforderlichen Berechtigungen verfügt. [Attribute für Zugriffskontrolle](#)

Ich erhalte die Meldung „Browser wird nicht unterstützt“, wenn ich versuche, ein Gerät für MFA zu registrieren

WebAuthn wird derzeit in den Webbrowsern Google Chrome, Mozilla Firefox, Microsoft Edge und Apple Safari sowie in Windows 10- und Android-Plattformen unterstützt. Einige

Komponenten der WebAuthn Unterstützung können unterschiedlich sein, z. B. die Unterstützung der Plattformauthentifizierung in macOS- und iOS-Browsern. Wenn Benutzer versuchen, WebAuthn Geräte in einem Browser oder auf einer Plattform zu registrieren, die nicht unterstützt wird, werden bestimmte Optionen ausgegraut, die nicht unterstützt werden, oder sie erhalten eine Fehlermeldung, dass nicht alle unterstützten Methoden unterstützt werden. In diesen Fällen finden Sie weitere Informationen zum [Support unter FIDO2: Webauthentifizierung \(WebAuthn\)](#). browser/platform Weitere Informationen zu WebAuthn IAM Identity Center finden Sie unter. [FIDO2 Authentifikatoren](#)

Die Active Directory-Gruppe „Domänenbenutzer“ wird nicht ordnungsgemäß mit dem IAM Identity Center synchronisiert

Die Gruppe der Active Directory-Domänenbenutzer ist die standardmäßige „primäre Gruppe“ für AD-Benutzerobjekte. Primäre Active Directory-Gruppen und ihre Mitgliedschaften können vom IAM Identity Center nicht gelesen werden. Verwenden Sie beim Zuweisen des Zugriffs auf IAM Identity Center-Ressourcen oder -Anwendungen andere Gruppen als die Gruppe Domänenbenutzer (oder andere Gruppen, die als primäre Gruppen zugewiesen sind), damit die Gruppenmitgliedschaft im IAM Identity Center-Identitätsspeicher korrekt wiedergegeben wird.

Fehler bei den ungültigen MFA-Anmeldeinformationen

Dieser Fehler kann auftreten, wenn ein Benutzer versucht, sich mit einem Konto eines externen Identitätsanbieters (z. B. Okta oder Microsoft Entra ID) bei IAM Identity Center anzumelden, bevor sein Konto mithilfe des SCIM-Protokolls vollständig für IAM Identity Center bereitgestellt wurde. Nachdem das Benutzerkonto für IAM Identity Center bereitgestellt wurde, sollte dieses Problem behoben sein. Vergewissern Sie sich, dass das Konto für IAM Identity Center bereitgestellt wurde. Wenn nicht, überprüfen Sie die Bereitstellungsprotokolle im externen Identitätsanbieter.

Ich erhalte die Meldung „Ein unerwarteter Fehler ist aufgetreten“, wenn ich versuche, mich mit einer Authenticator-App zu registrieren oder anzumelden

Time-based Systeme mit Einmalkennwörtern (TOTP), wie sie beispielsweise von IAM Identity Center in Kombination mit codebasierten Authentifikator-Apps verwendet werden, sind auf die Zeitsynchronisierung zwischen dem Client und dem Server angewiesen. Stellen Sie sicher, dass das Gerät, auf dem Ihre Authenticator-App installiert ist, korrekt mit einer zuverlässigen Zeitquelle

synchronisiert ist, oder stellen Sie die Uhrzeit auf Ihrem Gerät manuell so ein, dass sie einer zuverlässigen Quelle wie NIST () oder anderen Äquivalenten entspricht. <https://www.time.gov/> local/regional

Ich erhalte die Fehlermeldung „Du bist es nicht, das sind wir“, wenn ich versuche, mich im IAM Identity Center anzumelden

Dieser Fehler weist auf ein Einrichtungsproblem mit Ihrer IAM Identity Center-Instanz oder dem externen Identitätsanbieter (IdP) hin, den IAM Identity Center als Identitätsquelle verwendet. Wir empfehlen Ihnen, Folgendes zu überprüfen:

- Überprüfen Sie die Datums- und Uhrzeiteinstellungen auf dem Gerät, mit dem Sie sich anmelden. Wir empfehlen, Datum und Uhrzeit so einzustellen, dass sie automatisch eingestellt werden. Wenn dies nicht verfügbar ist, empfehlen wir, Datum und Uhrzeit mit einem bekannten NTP-Server (Network Time Protocol) zu synchronisieren.
- Stellen Sie sicher, dass das in das IAM Identity Center hochgeladene IdP-Zertifikat mit dem von Ihrem IdP bereitgestellten übereinstimmt. Sie können das Zertifikat von der IAM Identity Center-Konsole aus überprüfen, indem Sie zu Einstellungen navigieren. Wählen Sie auf der Registerkarte „Identitätsquelle“ die Option „Aktion“ und dann „Authentifizierung verwalten“ aus. Wenn die IdP- und IAM Identity Center-Zertifikate nicht übereinstimmen, importieren Sie ein neues Zertifikat in IAM Identity Center.
- Stellen Sie sicher, dass das NameID-Format in der Metadatendatei Ihres Identitätsanbieters wie folgt lautet:
 - `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Wenn Sie AD Connector von AWS Directory Service als Identitätsanbieter verwenden, stellen Sie sicher, dass die Anmeldeinformationen für das Dienstkonto korrekt und nicht abgelaufen sind. Weitere Informationen finden Sie unter [Aktualisieren der Anmeldeinformationen AWS Directory Service](#) für Ihr AD Connector-Dienstkonto in.

Meine Benutzer erhalten keine E-Mails vom IAM Identity Center

Alle vom IAM Identity Center-Dienst gesendeten E-Mails stammen entweder von der Adresse `no-reply@signin.aws` oder `no-reply@login.awsapps.com`. Ihr E-Mail-System muss so konfiguriert sein, dass es E-Mails von diesen Absender-E-Mail-Adressen akzeptiert und sie nicht als Junk oder Spam behandelt.

Fehler: Sie können nicht delete/modify auf die im Verwaltungskonto bereitgestellten Berechtigungssätze remove/assign zugreifen

Diese Meldung weist darauf hin, dass die [Delegierte Verwaltung](#) Funktion aktiviert wurde und dass der Vorgang, den Sie zuvor versucht haben, nur von jemandem erfolgreich ausgeführt werden kann, der über Verwaltungskontoberechtigungen verfügt. AWS Organizations Um dieses Problem zu beheben, melden Sie sich als Benutzer an, der über diese Berechtigungen verfügt, und versuchen Sie erneut, die Aufgabe auszuführen, oder weisen Sie diese Aufgabe einer Person zu, die über die richtigen Berechtigungen verfügt. Weitere Informationen finden Sie unter [Registrieren Sie ein Mitgliedskonto](#).

Fehler: Das Sitzungstoken wurde nicht gefunden oder ist ungültig

Dieser Fehler kann auftreten, wenn ein Client, z. B. ein Webbrowser, versucht AWS Toolkit AWS CLI, eine Sitzung zu verwenden, die serverseitig widerrufen oder für ungültig erklärt wurde. Um dieses Problem zu beheben, kehren Sie zur Client-Anwendung oder Website zurück und versuchen Sie es erneut. Melden Sie sich auch erneut an, wenn Sie dazu aufgefordert werden. In diesem Fall müssen Sie manchmal auch ausstehende Anfragen stornieren, z. B. einen ausstehenden Verbindungsversuch von Ihrer IDE aus. AWS Toolkit

Gruppenmitglieder aus vertrauenswürdigen Domänen werden nicht mit IAM Identity Center synchronisiert

Wenn eine Sicherheitsgruppe erfolgreich mit dem IAM Identity Center synchronisiert wird, ihre Mitglieder aus einer vertrauenswürdigen lokalen Domäne jedoch nicht im IAM Identity Center angezeigt werden, kann dies daran liegen, dass sich die Gruppe in einer vertrauenswürdigen Domäne befindet AWS Managed Microsoft AD und dort Foreign Security Principal (FSPs) enthält, die Benutzer aus einer vertrauenswürdigen Domäne repräsentieren.

Versuchen Sie die folgenden Schritte zur Fehlerbehebung:

- Gruppen direkt aus der vertrauenswürdigen Domäne synchronisieren: Anstatt eine Gruppe zu synchronisieren, die domänenübergreifende Mitglieder enthält AWS Managed Microsoft AD , erstellen und synchronisieren Sie die Gruppe direkt von der vertrauenswürdigen lokalen Domäne aus. Dieser Ansatz funktioniert, weil IAM Identity Center auf tatsächliche Benutzerobjekte in der Quelldomäne zugreifen kann.

- **Dienstkontoberechtigungen überprüfen:** Stellen Sie sicher, dass das IAM Identity Center-Dienstkonto über die erforderlichen Berechtigungen für Benutzerobjekte in der vertrauenswürdigen Domäne verfügt: `ReadProperties` und `ListContents` über die erforderlichen Berechtigungen.

Beheben Sie Probleme mit vom Kunden verwalteten Schlüsseln in AWS IAM Identity Center

In diesem Thema werden häufig auftretende Fehler im Zusammenhang mit vom Kunden verwalteten Schlüsseln beschrieben, die bei der Verwendung auftreten können, AWS IAM Identity Center und es werden Schritte zur Problembehebung beschrieben.

Zugriff verweigert: Problem mit der KMS-Entschlüsselungsberechtigung

Fehler: „Der Benutzer xxxxx ist nicht berechtigt, `kms:Decrypt` für die Ressource auszuführen, die diesem Chiffretext zugeordnet ist, da keine identitätsbasierte Richtlinie die Aktion `kms:Decrypt` zulässt“

Dem Benutzer oder IAM-Prinzipal fehlt die erforderliche Berechtigung in der IAM-Richtlinie oder der KMS-Schlüsselrichtlinie. `kms:Decrypt`

Problembehandlung mit: AWS CloudTrail

1. Suchen Sie nach `kms.amazonaws.com` Ereignissen in CloudTrail
2. Suchen Sie nach dem Namen der Veranstaltung `Decrypt`
3. Überprüfen Sie die `errorMessage` Felder `errorCode` und
4. Prüfen Sie `userIdentity`, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder dem IAM-Prinzipal in seiner IAM-Richtlinie und KMS-Schlüsselrichtlinie `kms:Decrypt` Zugriffsberechtigungen. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).

AWS Fehler bei der Anmeldung verwalteter Anwendungen mit einem vom Kunden verwalteten Schlüssel, der im IAM Identity Center aktiviert ist

Wenn sich keine Identity Center-Benutzer bei AWS verwalteten Anwendungen anmelden können und Sie einen vom Kunden verwalteten Schlüssel in Ihrer IAM Identity Center-Instanz aktiviert

haben, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie den AWS verwalteten Anwendungen Berechtigungen zur Verwendung des vom Kunden verwalteten Schlüssels gewährt. Weitere Informationen finden Sie unter [Grundlegende KMS-Schlüsselrichtlinie](#).

AWS Fehler bei der and/or Benutzerzuweisung bei der Installation verwalteter Anwendungen, wenn ein vom Kunden verwalteter Schlüssel im IAM Identity Center aktiviert ist

Fehler: „Der Benutzer xxxxx ist nicht berechtigt, kms:Decrypt für die Ressource auszuführen, die diesem Chiffretext zugeordnet ist, da keine identitätsbasierte Richtlinie die Aktion kms:Decrypt zulässt“

Dem Benutzer oder IAM-Prinzipal fehlt die erforderliche Berechtigung in der IAM-Richtlinie oder der KMS-Schlüsselrichtlinie. kms : Decrypt

Problembehandlung mit: CloudTrail

1. Suchen Sie nach dem Namen der Veranstaltung Decrypt
2. Überprüfen Sie die errorMessage Felder errorCode und
3. Prüfen SieuserIdentity, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder dem IAM-Prinzipal in seiner IAM-Richtlinie und KMS-Schlüsselrichtlinie kms : Decrypt Zugriffsberechtigungen. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).

KMS-Berechtigungsproblem: Konfiguration des vom Kunden verwalteten Schlüssels mit AWS IAM Identity Center

Dem Benutzer oder IAM-Prinzipal fehlen bei der Aktivierung des vom Kunden verwalteten Schlüssels eine oder mehrere erforderliche KMS-Berechtigungen (kms:Decryptkms:Encryptkms:GenerateDataKey,,,kms:DescribeKey).

Problembehandlung mit CloudTrail:

1. Suchen Sie nach DecryptEncrypt,GenerateDataKey, oder DescribeKey Ereignissen
2. Überprüfen Sie die errorMessage Felder errorCode und
3. Prüfen SieuserIdentity, welcher Principal den Vorgang versucht hat

Um dieses Problem zu beheben, gewähren Sie dem Benutzer oder IAM-Prinzipal alle erforderlichen KMS-Berechtigungen in seiner identitätsbasierten Richtlinie oder KMS-Schlüsselrichtlinie. Weitere Informationen finden Sie unter [Implementierung von kundenverwalteten KMS-Schlüsseln in AWS IAM Identity Center](#).

AWS auf Anmeldefehler im Portal zugreifen, wenn ein vom Kunden verwalteter Schlüssel im IAM Identity Center aktiviert ist

Fehler: „FEHLERCODE: 0001 — IdentityCenter Der Servicezugriff ist gesperrt. Wenden Sie sich für weitere Schritte an Ihren IdentityCenter Administrator.“

Wenn sich Benutzer nicht beim AWS Zugriffsportal anmelden können und Sie einen vom Kunden verwalteten Schlüssel in Ihrer IAM Identity Center-Instanz aktiviert haben, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie die erforderlichen Berechtigungen für Identity Center und Identity Store gewährt. Weitere Informationen finden Sie unter [Grundlegende KMS-Schlüsselrichtlinie](#).

Beheben Sie Probleme bei der Einrichtung mehrerer Regionen in AWS IAM Identity Center

In diesem Thema werden häufig auftretende Fehler im Zusammenhang mit der Einrichtung mehrerer Regionen beschrieben, die bei der Verwendung auftreten können, AWS IAM Identity Center und es werden Schritte zur Problembehebung beschrieben.

Die Region, in die ich meine IAM Identity Center-Instance replizieren möchte, ist in der IAM Identity Center-Konsole nicht verfügbar

Sie müssen zunächst einen Replikatschlüssel für Ihren vom Kunden verwalteten Schlüssel in der Region erstellen, in die Sie Ihre IAM Identity Center-Instance replizieren möchten. Sobald der Replikatschlüssel erstellt wurde, wird die Region in der Liste der Regionen angezeigt, die für Replizierungen verfügbar sind. Weitere Informationen finden Sie unter [the section called “Schritt 1: Erstellen Sie einen Replikatschlüssel”](#).

AWS Fehler bei der Anmeldung verwalteter Anwendungen in einer weiteren Region

Wenn sich keine IAM Identity Center-Benutzer bei AWS verwalteten Anwendungen in einer weiteren Region anmelden können, nachdem Sie die Region im IAM Identity Center hinzugefügt haben,

stellen Sie sicher, dass Sie die ACS-URL (Assertion Consumer Service) der zusätzlichen Region im externen Identitätsanbieter konfiguriert haben, wie unter beschrieben. [the section called “Schritt 3 \(nur externe Identitätsanbieter\): Aktualisieren Sie das externe IdP-Setup”](#) Stellen Sie außerdem sicher, dass Ihre Benutzer mit der Region verbunden sind.

Probleme beim Aktivieren einer Instanz von IAM Identity Center mit mehreren Regionen

Wenn Sie bei der Aktivierung von IAM Identity Center Multi-Region Instance ausgewählt haben, erstellt der Einrichtungsvorgang einen vom Kunden verwalteten Schlüssel, repliziert ihn in die zusätzliche Region, aktiviert Ihre Instance und fügt die zusätzliche Region hinzu. Wenn einer dieser Schritte fehlschlägt, wird möglicherweise einer der folgenden Fehler angezeigt.

Die Schlüsselerstellung ist fehlgeschlagen

Ein vom Kunden verwalteter Schlüssel konnte in Ihrem Konto nicht erstellt werden. Ihre Instanz wurde nicht aktiviert.

Wenn es sich um einen Berechtigungsfehler handelt, überprüfen Sie, ob Ihre Rolle über die `kms:TagResource` Berechtigungen `kms:CreateKey` und verfügt, und wählen Sie dann „Aktivieren“, um es erneut zu versuchen.

Die Schlüsselreplikation ist fehlgeschlagen

In Ihrem Konto wurde ein vom Kunden verwalteter Schlüssel erstellt, der Replikatschlüssel konnte jedoch nicht in der zusätzlichen Region erstellt werden. Ihre Instanz wurde nicht aktiviert.

Wenn es sich um einen Berechtigungsfehler handelt, stellen Sie sicher, dass Ihre Rolle über die `kms:ReplicateKey` entsprechende Berechtigung verfügt.

Wählen Sie **Aktivieren**, um es erneut zu versuchen. Derselbe Schlüssel wird verwendet.

Wenn Sie später zurückkehren, suchen Sie den Schlüssel in der AWS KMS Konsole, indem Sie nach dem Tag `filternCreatedBy: IAM Identity Center`. Kopieren Sie die Schlüssel-ID, wählen Sie dann **Benutzerdefinierte Instanz** und wählen Sie den Schlüssel aus.

Um neu zu beginnen, löschen Sie den Schlüssel in der AWS KMS Konsole und wählen Sie **Multi-Region Instanz**, um einen neuen zu erstellen.

Die Instanzerstellung ist fehlgeschlagen

Ein vom Kunden verwalteter Schlüssel wurde erstellt und in die zusätzliche Region repliziert, aber Ihre Instanz konnte nicht aktiviert werden.

Wenn es sich um einen Berechtigungsfehler handelt, stellen Sie sicher, dass Ihre Rolle über die erforderlichen [Berechtigungen zum Erstellen einer IAM Identity Center-Instanz verfügt](#).

Wählen Sie **Aktivieren**, um es erneut zu versuchen. Derselbe Schlüssel wird verwendet.

Wenn Sie später zurückkehren, suchen Sie den Schlüssel in der AWS KMS Konsole, indem Sie nach dem Tag `CreatedBy: IAM Identity Center` filtern. Kopieren Sie die Schlüssel-ID, wählen Sie dann **Benutzerdefinierte Instanz** und wählen Sie den Schlüssel aus.

Um neu zu beginnen, löschen Sie den Schlüssel und sein Replikat in der AWS KMS Konsole und wählen Sie **Multi-Region Instanz** aus, um ein neues zu erstellen.

Note

Diese Fehler können auch auftreten, wenn Sie eine **benutzerdefinierte Instanz** verwenden, wenn die Instanzerstellung oder die Regionsreplikation fehlschlägt. Wenn Sie Ihren eigenen, vom Kunden verwalteten Schlüssel angegeben haben, gelten die Schritte zur Schlüsselerstellung und -replikation nicht.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Ergänzungen der AWS IAM Identity Center Dokumentation beschrieben. Wir aktualisieren die Dokumentation regelmäßig, um das Feedback, das Sie uns senden, einzuarbeiten.

- Letzte wichtige Aktualisierung der Dokumentation: 21. Oktober 2025

Änderung	Beschreibung	Datum
One-click Erstellung von Instanzen mit mehreren Regionen	Wenn Sie eine neue Organisationsinstanz in unterstützten Regionen aktivieren, können Sie zwischen Single-Region Multi-Region, oder benutzerdefinierten Instanzkonfigurationen wählen. Die Multi-Region Option ermöglicht die Resilienz mehrerer Regionen mit einem Klick, indem automatisch ein vom Kunden verwalteter KMS-Schlüssel erstellt und Ihre Instanz in eine weitere Region repliziert wird.	6. August 2026
Multi-account Berechtigungen sind jetzt für neue Instanzen optional	Beim Erstellen einer Organisationsinstanz können Sie jetzt wählen, ob Sie Berechtigungen für mehrere Konten aktivieren möchten. Standardmäßig sind Berechtigungen für mehrere Konten aktiviert. Sie können die Berechtigungen für mehrere Konten später in den Instanzei	4. August 2026

nstellungen oder mithilfe der UpdateInstance API aktivieren.

[Multi-Region Die Unterstützung wurde auf das Identity Center-Verzeichnis ausgedehnt](#)

Multi-Region Die Unterstützung funktioniert jetzt zusätzlich zu externen Identitätsanbietern mit dem Identity Center-Verzeichnis als Identitätsquelle.

28. Juli 2026

[Separate Kontingente für AWS Konten und Anträge](#)

AWS IAM Identity Center erzwingt jetzt separate Kontingente für AWS Konten und Anträge. Bisher teilten sich diese Ressourcen ein einziges kombiniertes Kontingent. Das neue Standardkontingent für jedes Kontingent beträgt 7.000.

22. Juni 2026

[Aktivieren Sie den AWS Kontozugriff für vom Kunden verwaltete Anwendungen](#)

Sie können jetzt den `sso:account:access` Geltungsbereich für vom Kunden verwaltete Anwendungen mit vertrauenswürdigen Token-Ausstellern aktivieren, sodass diese im Namen von Endbenutzern programmgesteuert auf AWS Kontoanmeldeinformationen zugreifen können.

19. Juni 2026

[Der Zeitpunkt der Authentifizierungssitzung für Änderungen der Gruppenmitgliedschaft wurde aktualisiert](#)

Die Tabelle mit dem Sitzungsv erhalten der Gruppenmitgliedschaft wurde aktualisiert, um zu berücksichtigen, dass Änderungen an Berechtigungen und Anwendungszugriff jetzt sofort wirksam werden, wenn neue Sitzungen erstellt werden.

28. Mai 2026

[Vereinfachte grundlegende KMS-Schlüsselrichtlinie](#)

Die grundlegenden KMS-Schlüsselrichtlinien wurden in einer einzigen vereinfachten Richtlinie zusammengefasst, die die Konfiguration des vom Kunden verwalteten KMS-Schlüssels für die Verschlüsselung im Ruhezustand optimiert.

30. April 2026

[Multi-Region Unterstützung](#)

Unterstützung mehrerer Regionen hinzugefügt, einschließlich Replikation in zusätzliche Regionen, AWS-Konto Zugriff auf und Nutzung AWS verwalteter Anwendungen in weiteren Regionen.

2. Februar 2026

[Aktualisierte AWS verwaltete Richtlinie](#)

Die AWSIdentityCenterExternalManagementPolicy AWS verwaltete Richtlinie wurde aktualisiert, um den ARN für die Bereitstellung von Mandanten zu ändern.

5. Dezember 2025

[Neues Thema für AWS verwaltete Richtlinien](#)

Es wurden Details für die `AWSIdentityCenterExternalManagementPolicy` AWS verwaltete Richtlinie hinzugefügt.

21. November 2025

[Auto-provisioning Beratung bei Audits und Abstimmungen](#)

Es wurden Anleitungen für die Prüfung und den Abgleich von Benutzern, Gruppen und Gruppenmitgliedschaften mit SCIM mithilfe von Identity Store-APIs und -Befehlen hinzugefügt. AWS CLI

17. Oktober 2025

[Kontingente für OIDC-Dienstanfragen](#)

Kontingente für OIDC-Serviceanfragen hinzugefügt, einschließlich Ratenbeschränkungen für die OAuth-Clientregistrierung, Token-Erstellung und andere OIDC-Operationen.

13. Oktober 2025

[Aktualisierungen für AWS verwaltete Richtlinien](#)

IAM Identity Center hat die verwalteten Richtlinien `AWSSSOMasterAccountAdministrator`, `AWSSSOMemberAccountAdministrator`, `AWSSSODirectoryAdministrator`, und `AWSSSODirectoryReadOnly` um die erforderlichen AWS KMS Berechtigungen für IAM Identity Center-Instanzen erweitert, die vom Kunden verwaltete Schlüssel für die Verschlüsselung verwenden.

17. September 2025

[Vom Kunden verwaltete Schlüssel für die Verschlüsselung im Ruhezustand](#)

Unterstützung für vom Kunden verwaltete KMS-Schlüssel zur Verschlüsselung ruhender Personaldaten wurde hinzugefügt.

17. September 2025

[Beispiel für eine ressourcenbasierte Richtlinie, die die Token-Erstellung ermöglicht](#)

Es wurde ein Beispiel für eine ressourcenbasierte Richtlinie hinzugefügt, die die Token-Erstellung für autorisierte Client-Anwendungen ermöglicht.

16. September 2025

[Unterstützung für Benutzersitzungen im Hintergrund](#)

Inhalt für Benutzersitzungen im Hintergrund hinzugefügt.

11. August 2025

[Identity-enhanced Konsolensitzungen](#)

Aktualisierte Terminologie für Konsolensitzungen mit erweiterter Identität (früher bekannt als identitätsbewusste Sitzungen).

12. Mai 2025

Erste Schritte mit der Reorganisation	Der Inhalt für die ersten Schritte wurde neu organisiert, um die Übersichtlichkeit und das Benutzererlebnis zu verbessern.	6. Mai 2025
Verwerfen Sie IAM Identity Center AD Sync	Sie können IAM Identity Center AD Sync nicht mehr für Active Directory-Benutzer bereitstellen. Stattdessen können Sie das konfigurierbare IAM Identity Center AD Sync verwenden.	17. April 2025
Der Inhalt für die authentifizierte Sitzung wurde aktualisiert	Aktualisierung der IAM Identity Center-Sitzungsdauer, wenn die Benutzersitzung gelöscht wird.	2. April 2025
Aktualisierungen für verwaltete Richtlinien AWS	Die Berechtigungen für die <code>AWSSS0ServiceRolePolicy</code> AWS verwaltete Richtlinie wurden aktualisiert.	11. Februar 2025
Der Workflow zur Aktivierung von IAM Identity Center wurde verbessert	Der Arbeitsablauf zur Aktivierung von Organisations- und Kontoinstanzen von IAM Identity Center wurde aktualisiert.	11. Februar 2025
Aktualisierungen für die Aktivierung von IAM Identity Center	Aktualisierte Inhalte und Verfahren zur Aktivierung von Organisations- und Kontoinstanzen von IAM Identity Center.	10. Oktober 2024

[Aktualisierungen für AWS verwaltete Richtlinien](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

2. Oktober 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSSSOMasterAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.

26. September 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

4. September 2024

[Aktualisierungen für „Was ist IAM Identity Center?“ Thema](#)

Der Inhalt, der die Vorteile und Funktionen von IAM Identity Center beschreibt, wurde aktualisiert.

19. August 2024

[Aktualisierungen für AWS verwaltete Richtlinien](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

12. Juli 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

27. Juni 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

17. Mai 2024

[Aktualisierungen für AWS verwaltete Richtlinien](#)

Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.

30. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSSSOMasterAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.

26. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSSSOMemberAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.

26. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die `AWSSS0ReadOnly` AWS verwaltete Richtlinie wurden aktualisiert.

26. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die AWSIAMIdentityCenterAllowListForIdentityContext AWS verwaltete Richtlinie wurden aktualisiert.

26. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die AWSIAMIdentityCenterAllowListForIdentityContext AWS verwaltete Richtlinie wurden aktualisiert.

24. April 2024

[Aktualisierungen für AWS verwaltete Richtlinien](#)

Die Berechtigungen für die AWSIAMIdentityCenterAllowListForIdentityContext AWS verwaltete Richtlinie wurden aktualisiert.

19. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die AWSIAMIdentityCenterAllowListForIdentityContext AWS verwaltete Richtlinie wurden aktualisiert.

11. April 2024

[Aktualisierungen für die AWS verwaltete Richtlinie](#)

Die Berechtigungen für die AWSIAMIdentityCenterAllowListForIdentityContext AWS verwaltete Richtlinie wurden aktualisiert.

26. November 2023

[Neues Thema für AWS verwaltete Richtlinien](#)

Es wurden Details für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie hinzugefügt.

15. November 2023

[Verbesserte Anleitung für die ersten Schritte mit IAM Identity Center](#)

Neue Inhalte für die ersten Schritte mit IAM Identity Center und zum Erstellen eines Administratorbenutzers hinzugefügt

23. September 2022

[Benutzer und Gruppen in der Identity Center API-Referenz wurden aktualisiert](#)

Dieses Update enthält Verweise auf die neuen APIs zum Erstellen, Aktualisieren und Löschen im Identity Center API-Referenzhandbuch.

31. August 2022

[AWS Single Sign-On \(AWS SSO\) wurde in AWS IAM Identity Center umbenannt](#)

AWS führt ein AWS IAM Identity Center. IAM Identity Center erweitert die Funktionen von AWS Identity and Access Management (IAM), sodass Sie Konten und den Zugriff auf Anwendungen für Ihre Mitarbeiter zentral verwalten können. Zu den Funktionen von IAM Identity Center gehören Anwendungszuweisungen, Berechtigungen für mehrere Konten und ein Zugriffsportal. AWS

26. Juli 2022

<u>Unterstützung für Berechtigungsgrenzen und vom Kunden verwaltete Richtlinien in Berechtigungssätzen</u>	Inhalt für die Verwendung von AWS verwalteten und vom Kunden verwalteten AWS Identity and Access Management (IAM) Richtlinien mit Berechtigungssätzen hinzugefügt.	14. Juli 2022
<u>Unterstützung für manuell aktivierte Regionen AWS</u>	Inhalt für die Verwendung von IAM Identity Center in manuell aktivierten Regionen hinzugefügt.	15. Juni 2022
<u>Aktualisierungen für AWS verwaltete Richtlinien</u>	Die Berechtigungen für die <code>AWSSS0ServiceRolePolicy</code> AWS verwaltete Richtlinie wurden aktualisiert.	11. Mai 2022
<u>Unterstützung für delegierte Administration</u>	Inhalt für die Funktion zur delegierten Administration hinzugefügt.	11. Mai 2022
<u>Aktualisierungen für AWS verwaltete Richtlinien</u>	Die Berechtigungen für die <code>AWSSS0MasterAccountAdministrator</code> die <code>AWSSS0MemberAccountAdministrator</code> <code>AWSSS0ReadOnly</code> AWS verwalteten Richtlinien wurden aktualisiert.	28. April 2022
<u>Unterstützung für konfigurierbare AD-Synchronisierung</u>	Inhalt für die konfigurierbare AD-Synchronisierungsfunktion hinzugefügt.	14. April 2022

<u>Neues Thema für AWS verwaltete Richtlinien</u>	Es wurden Details für die AWSSSOMasterAccountAdministrator AWS verwaltete Richtlinie hinzugefügt.	4. August 2021
<u>Aktualisierungen für Kontingente</u>	Anpassungen der Kontingenttabellen.	21. Dezember 2020
<u>Neue Beispielrichtlinien</u>	Es wurden neue Beispiele für vom Kunden verwaltete Richtlinien hinzugefügt und der Abschnitt „Erforderliche Berechtigungen“ wurde aktualisiert.	21. Dezember 2020
<u>Unterstützung für attributbasierte Zugriffskontrolle (ABAC)</u>	Inhalt für die ABAC-Funktion hinzugefügt.	24. November 2020
<u>Unterstützung für die erzwungene MFA-Registrierung</u>	Updates, sodass Benutzer bei der Anmeldung ein MFA-Gerät registrieren müssen.	23. November 2020
<u>Unterstützung für WebAuthn</u>	Inhalt für neue WebAuthn Funktion hinzugefügt.	20. November 2020
<u>Unterstützung für Ping Identity</u>	Als unterstützter externer Identitätsanbieter wurden Inhalte hinzugefügt, die in Ping Identity Produkte integriert werden können.	26. Oktober 2020
<u>Unterstützung für OneLogin</u>	Inhalt zur Integration OneLogin als unterstützter externer Identitätsanbieter hinzugefügt.	31. Juli 2020

<u>Unterstützung für Okta</u>	Es wurden Inhalte hinzugefügt, die Okta als unterstützter externer Identitätsanbieter integriert werden können.	28. Mai 2020
<u>Unterstützung für externe Identitätsanbieter</u>	Die Verweise vom Verzeichnis zur Identitätsquelle wurden geändert, Inhalte wurden hinzugefügt, um externe Identitätsanbieter zu unterstützen.	26. November 2019
<u>Neue MFA-Einstellungen</u>	Das Thema zur zweistufigen Überprüfung wurde entfernt und stattdessen ein neues MFA-Thema hinzugefügt.	24. Oktober 2019
<u>Neue Einstellung zum Hinzufügen der zweistufigen Überprüfung</u>	Es wurden Inhalte zur Aktivierung der zweistufigen Überprüfung für Benutzer hinzugefügt.	16. Januar 2019
<u>Unterstützung für die Sitzungsdauer auf Konten AWS</u>	Es wurden Inhalte zur Festlegung der Sitzungsdauer für ein AWS Konto hinzugefügt.	30. Oktober 2018
<u>Neue Option zur Verwendung des Identity Center-Verzeichnisses</u>	Inhalt hinzugefügt, um entweder das Identity Center-Verzeichnis auszuwählen oder eine Verbindung zu einem vorhandenen Verzeichnis in Active Directory herzustellen.	17. Oktober 2018
<u>Unterstützung für den Relay-Status und die Sitzungsdauer von Anwendungen</u>	Inhalt zum Relay-Status und zur Sitzungsdauer für Anwendungen hinzugefügt.	10. Oktober 2018

[Zusätzliche Unterstützung für neue Anwendungen](#)

4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, Und UserEcho zum Anwendungskatalog hinzugefügt.

3. August 2018

[Unterstützung für den Zugriff mehrerer Konten auf Verwaltungskonten](#)

Es wurden Inhalte darüber hinzugefügt, wie der Zugriff auf mehrere Konten an Benutzer in einem Verwaltungskonto delegiert werden kann.

9. Juli 2018

[Unterstützung für neue Anwendungen](#)

DocuSign, Keeper Security, Und SugarCRM zum Anwendungskatalog hinzugefügt.

16. März 2018

[Holen Sie sich temporäre Anmeldeinformationen für den CLI-Zugriff](#)

Es wurden Informationen darüber hinzugefügt, wie temporäre Anmeldeinformationen für die Ausführung von AWS CLI Befehlen abgerufen werden.

22. Februar 2018

[Neues Handbuch](#)

Dies ist die erste Version
des IAM Identity Center-Be
nutzerhandbuchs.

7. Dezember 2017

AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.