Benutzerhandbuch

Forschungs- und Ingenieurstudio

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Forschungs- und Ingenieurstudio: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und 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

Übersicht ... 1
Features und Vorteile ... 2
Konzepte und Definitionen ... 3
Übersicht über die Architektur ... 5
Architekturdiagramm ... 5
AWS Dienstleistungen in diesem Produkt ... 7
Demo-Umgebung ... 10
Erstellen Sie einen Demo-Stack mit einem Klick ... 10
Voraussetzungen ... 10
Erstellen Sie Ressourcen und Eingabeparameter ... 11
Schritte nach der Bereitstellung ... 13
Planen Sie Ihren Einsatz ... 14
Kosten ... 14
Sicherheit ... 14
IAM-Rollen ... 14
Sicherheitsgruppen ... 15
Datenverschlüsselung ... 15
Kontingente ... 15
Kontingente für AWS Dienstleistungen in diesem Produkt ... 15
AWS CloudFormation Kontingente ... 16
Planung für Resilienz ... 16
Unterstützt AWS-Regionen ... 16
Stellen Sie das Produkt bereit ... 19
Voraussetzungen ... 19
Erstellen Sie eine AWS-Konto mit einem Administratorbenutzer ... 20
Erstellen Sie ein Amazon EC2 SSH-Schlüsselpaar ... 20
Erhöhen Sie die Servicequoten ... 20
Erstellen Sie eine öffentliche Domain (optional) ... 21
Domain erstellen (GovCloud nur) ... 21
Stellen Sie externe Ressourcen bereit ... 22
Konfigurieren Sie LDAPS in Ihrer Umgebung (optional) ... 23
Konfigurieren Sie eine private VPC (optional) ... 24
Erstellen Sie externe Ressourcen ... 36
Schritt 1: Starten Sie das Produkt ... 42

Schritt 2: Melden Sie sich zum ersten Mal an ... 52
Aktualisieren Sie das Produkt ... 54
Wichtige Versionsupdates ... 54
Kleinere Versionsupdates ... 54
Deinstalliere das Produkt ... 56
Mit dem AWS Management Console ... 56
Benutzen AWS Command Line Interface ... 56
Löschen des shared-storage-security-group ... 56
Löschen der Amazon S3 S3-Buckets ... 57
Leitfaden zur Konfiguration ... 58
Benutzer und Gruppen verwalten ... 58
SSO mit IAM Identity Center einrichten ... 58
Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO) ... 62
Passwörter für Benutzer einrichten ... 73
Subdomains erstellen ... 73
Erstellen Sie ein ACM-Zertifikat ... 74
CloudWatch Amazon-Protokolle ... 75
Festlegung benutzerdefinierter Berechtigungsgrenzen ... 76
RES-Ready konfigurieren AMIs ... 80
Bereiten Sie die IAM-Rolle für den Zugriff auf die RES-Umgebung vor ... 81
EC2 Image Builder Builder-Komponente erstellen ... 83
Bereiten Sie Ihr EC2 Image Builder Builder-Rezept vor ... 87
EC2 Image Builder Builder-Infrastruktur konfigurieren ... 89
Image Builder Builder-Image-Pipeline konfigurieren ... 89
Image Builder Builder-Image-Pipeline ausführen ... 91
Registrieren Sie einen neuen Software-Stack in RES ... 91
Leitfaden für Administratoren ... 92
Sitzungsverwaltung ... 92
Dashboard ... 93
Sitzungen ... 94
Software-Stacks () AMIs ... 97
Debugging ... 101
Desktop-Einstellungen ... 102
Umweltmanagement ... 103
Projekte ... 104
Benutzer ... 110

Gruppen ... 111
Berechtigungsprofile ... 112
Dateisysteme ... 121
Umgebungsstatus ... 126
Snapshot-Verwaltung ... 127
Umgebungseinstellungen ... 133
Amazon-S3-Buckets ... 134
Verwaltung von Secrets ... 149
Überwachung und Kontrolle der Kosten ... 152
Benutze das Produkt ... 158
Virtuelle Desktops ... 158
Unterstützte Betriebssysteme ... 159
Starten Sie einen neuen Desktop ... 159
Greifen Sie auf Ihren Desktop zu ... 159
Kontrollieren Sie Ihren Desktop-Status ... 161
Ändern Sie einen virtuellen Desktop ... 162
Sitzungsinformationen abrufen ... 163
Planen Sie virtuelle Desktops ... 163
Gemeinsam genutzte Desktops ... 165
Teilen Sie einen Desktop ... 165
Greifen Sie auf einen gemeinsam genutzten Desktop zu ... 166
Dateibrowser ... 166
Datei (en) hochladen ... 167
Datei (en) löschen ... 167
Favoriten verwalten ... 167
Dateien bearbeiten ... 168
Übertragen von Dateien ... 168
SSH-Zugang ... 169
Fehlerbehebung ... 171
Allgemeines Debuggen und Überwachen ... 174
Nützliche Quellen für Protokoll- und Ereignisinformationen ... 175
Typisches Erscheinungsbild der EC2 Amazon-Konsole ... 179
Windows-DCV-Debuggen ... 182
Finden Sie Informationen zur NICE DCV DCV-Version ... 182
Problem RunBooks ... 182
Probleme bei der Installation ... 185

Probleme mit dem Identitätsmanagement 192
Speicher 196
Snapshots 201
Infrastruktur 202
Virtuelle Desktops werden gestartet 203
Virtuelle Desktop-Komponente 208
Löschen von Umgebungen 215
Demo-Umgebung 222
Bekannte Probleme 223
Bekannte Probleme 2024.x 224
Hinweise 240
Überarbeitungen 241
..... ccxliii

Übersicht

> **Important**
>
> Diese Version des Benutzerhandbuchs bezieht sich auf Version 2024.08 von Research and Engineering Studio am. AWS Die aktuelle Version finden Sie im Research and Engineering Studio im AWS Benutzerhandbuch.

Research and Engineering Studio (RES) ist ein AWS unterstütztes Open-Source-Produkt, mit dem IT-Administratoren ein Webportal bereitstellen können, auf AWS dem Wissenschaftler und Ingenieure technische Rechenlasten ausführen können. RES bietet Benutzern eine zentrale Oberfläche, über die sie sichere virtuelle Desktops starten können, um wissenschaftliche Forschung, Produktdesign, technische Simulationen oder Datenanalyse-Workloads durchzuführen. Benutzer können mit ihren vorhandenen Unternehmensanmeldedaten eine Verbindung zum RES-Portal herstellen und an individuellen oder kollaborativen Projekten arbeiten.

Administratoren können virtuelle Bereiche für die Zusammenarbeit, sogenannte Projekte, einrichten, in denen eine bestimmte Gruppe von Benutzern auf gemeinsam genutzte Ressourcen zugreifen und zusammenarbeiten kann. Administratoren können ihre eigenen Anwendungssoftware-Stacks (AMIs) erstellen und es RES-Benutzern ermöglichen, virtuelle Windows- oder Linux-Desktops zu starten und den Zugriff auf Projektdaten über gemeinsam genutzte Dateisysteme zu ermöglichen. Administratoren können Software-Stacks und Dateisysteme zuweisen und den Zugriff nur auf diese Projektbenutzer beschränken. Administratoren können die integrierte Telemetrie verwenden, um die Nutzung der Umgebung zu überwachen und Benutzerprobleme zu beheben. Sie können auch Budgets für einzelne Projekte festlegen, um einen übermäßigen Ressourcenverbrauch zu verhindern. Da es sich bei dem Produkt um ein Open-Source-Produkt handelt, können Kunden auch die Benutzererfahrung des RES-Portals an ihre eigenen Bedürfnisse anpassen.

RES ist ohne zusätzliche Kosten erhältlich, und Sie zahlen nur für die AWS Ressourcen, die Sie für die Ausführung Ihrer Anwendungen benötigen.

Dieses Handbuch bietet einen Überblick über Research and Engineering Studio on AWS, seine Referenzarchitektur und Komponenten, Überlegungen zur Planung der Bereitstellung und Konfigurationsschritte für die Bereitstellung von RES in der Amazon Web Services (AWS) Cloud.

Features und Vorteile

Research and Engineering Studio on AWS bietet die folgenden Funktionen:

Webbasierte Benutzerschnittstelle

RES bietet ein webbasiertes Portal, über das Administratoren, Forscher und Ingenieure auf ihre Forschungs- und Entwicklungsarbeitsplätze zugreifen und diese verwalten können. Wissenschaftler und Ingenieure benötigen kein Fachwissen AWS-Konto oder Cloud-Fachwissen, um RES nutzen zu können.

Projektbasierte Konfiguration

Verwenden Sie Projekte, um Zugriffsberechtigungen zu definieren, Ressourcen zuzuweisen und Budgets für eine Reihe von Aufgaben oder Aktivitäten zu verwalten. Weisen Sie einem Projekt bestimmte Software-Stacks (Betriebssysteme und genehmigte Anwendungen) und Speicherressourcen zu, um Konsistenz und Compliance zu gewährleisten. Überwachen und verwalten Sie die Ausgaben pro Projekt.

Tools für die Zusammenarbeit

Wissenschaftler und Ingenieure können andere Mitglieder ihres Projekts zur Zusammenarbeit einladen und dabei die Berechtigungsstufen festlegen, die diese Kollegen haben sollen. Diese Personen können sich bei RES anmelden, um eine Verbindung zu diesen Desktops herzustellen.

Integration in die bestehende Identitätsmanagement-Infrastruktur

Integrieren Sie es in Ihre bestehende Infrastruktur für Identitätsmanagement und Verzeichnisdienste, um mit der vorhandenen Unternehmensidentität eines Benutzers eine Verbindung zum RES-Portal herzustellen und Projekten mithilfe vorhandener Benutzer- und Gruppenmitgliedschaften Berechtigungen zuzuweisen.

Dauerhafter Speicher und Zugriff auf gemeinsam genutzte Daten

Um Benutzern den Zugriff auf gemeinsam genutzte Daten in virtuellen Desktop-Sitzungen zu ermöglichen, stellen Sie eine Verbindung zu Ihren vorhandenen Dateisystemen her oder erstellen Sie neue Dateisysteme in RES. Zu den unterstützten Speicherservices gehören Amazon Elastic File System für Linux-Desktops und Amazon FSx for NetApp ONTAP für Windows- und Linux-Desktops.

Überwachung und Berichterstattung

Verwenden Sie das Analyse-Dashboard, um die Ressourcennutzung für Instanztypen, Software-Stacks und Betriebssystemtypen zu überwachen. Das Dashboard bietet auch eine Aufschlüsselung der Ressourcennutzung nach Projekten für die Berichterstattung.

Budget- und Kostenmanagement

Verlinken Sie AWS Budgets auf Ihre RES-Projekte, um die Kosten für jedes Projekt zu überwachen. Wenn Sie Ihr Budget überschreiten, können Sie den Start von VDI-Sitzungen einschränken.

Konzepte und Definitionen

In diesem Abschnitt werden die wichtigsten Konzepte beschrieben und die für dieses Produkt spezifische Terminologie definiert:

Dateibrowser

Ein Dateibrowser ist ein Teil der RES-Benutzeroberfläche, über den aktuell angemeldete Benutzer ihr Dateisystem einsehen können.

Dateisystem

Das Dateisystem fungiert als Container für Projektdaten (oft als Datensätze bezeichnet). Es bietet eine Speicherlösung innerhalb der Projektgrenzen und verbessert die Zusammenarbeit und die Datenzugriffskontrolle.

Globaler Administrator

Ein administrativer Delegierter mit Zugriff auf RES-Ressourcen, die in einer RES-Umgebung gemeinsam genutzt werden. Umfang und Berechtigungen erstrecken sich über mehrere Projekte. Sie können Projekte erstellen oder ändern und ihnen Projekteigentümer zuweisen. Sie können Projektinhabern und Projektmitgliedern Berechtigungen delegieren oder ihnen zuweisen. Je nach Größe der Organisation fungiert manchmal dieselbe Person als RES-Administrator.

Projekt

Ein Projekt ist eine logische Partition innerhalb der Anwendung, die als klare Grenze für Daten- und Rechenressourcen dient, die Steuerung des Datenflusses sicherstellt und verhindert, dass Daten und VDI-Hosts projektübergreifend gemeinsam genutzt werden.

Projektbasierte Berechtigungen

Projektbasierte Berechtigungen beschreiben eine logische Partition von Daten- und VDI-Hosts in einem System, in dem mehrere Projekte existieren können. Der Zugriff eines Benutzers auf Daten und VDI-Hosts innerhalb eines Projekts wird durch die ihm zugeordnete (n) Rolle (n) bestimmt. Einem Benutzer muss für jedes Projekt, auf das er Zugriff benötigt, Zugriff (oder Projektmitgliedschaft) zugewiesen werden. Andernfalls kann ein Benutzer nicht auf Projektdaten zugreifen und VDIs wenn ihm keine Mitgliedschaft gewährt wurde.

Mitglied des Projekts

Ein Endbenutzer von RES-Ressourcen (VDI, Speicher usw.). Umfang und Berechtigungen sind auf Projekte beschränkt, denen sie zugewiesen sind. Sie können keine Berechtigungen delegieren oder zuweisen.

Projekteigentümer

Ein administrativer Delegierter mit Zugriff auf und Eigentümerschaft für ein bestimmtes Projekt. Umfang und Berechtigungen sind auf die Projekte beschränkt, deren Eigentümer sie sind. Sie können Projektmitgliedern in den Projekten, deren Eigentümer sie sind, Berechtigungen zuweisen.

Software-Stack

Software-Stacks sind Amazon Machine Images (AMI) mit RES-spezifischen Metadaten, die auf einem beliebigen Betriebssystem basieren, das ein Benutzer für die Bereitstellung für seinen VDI-Host ausgewählt hat.

VDI-Hosts

VDI-Hosts (Virtual Desktop Instance) ermöglichen Projektmitgliedern den Zugriff auf projektspezifische Daten- und Rechenumgebungen und sorgen so für sichere und isolierte Arbeitsbereiche.

Eine allgemeine Begriffsübersicht finden Sie im AWS Glossar in der AWS Allgemeinen Referenz.AWS

Übersicht über die Architektur

Dieser Abschnitt enthält ein Architekturdiagramm für die Komponenten, die mit diesem Produkt eingesetzt werden.

Architekturdiagramm

Durch die Bereitstellung dieses Produkts mit den Standardparametern werden die folgenden Komponenten in Ihrem AWS-Konto bereitgestellt.

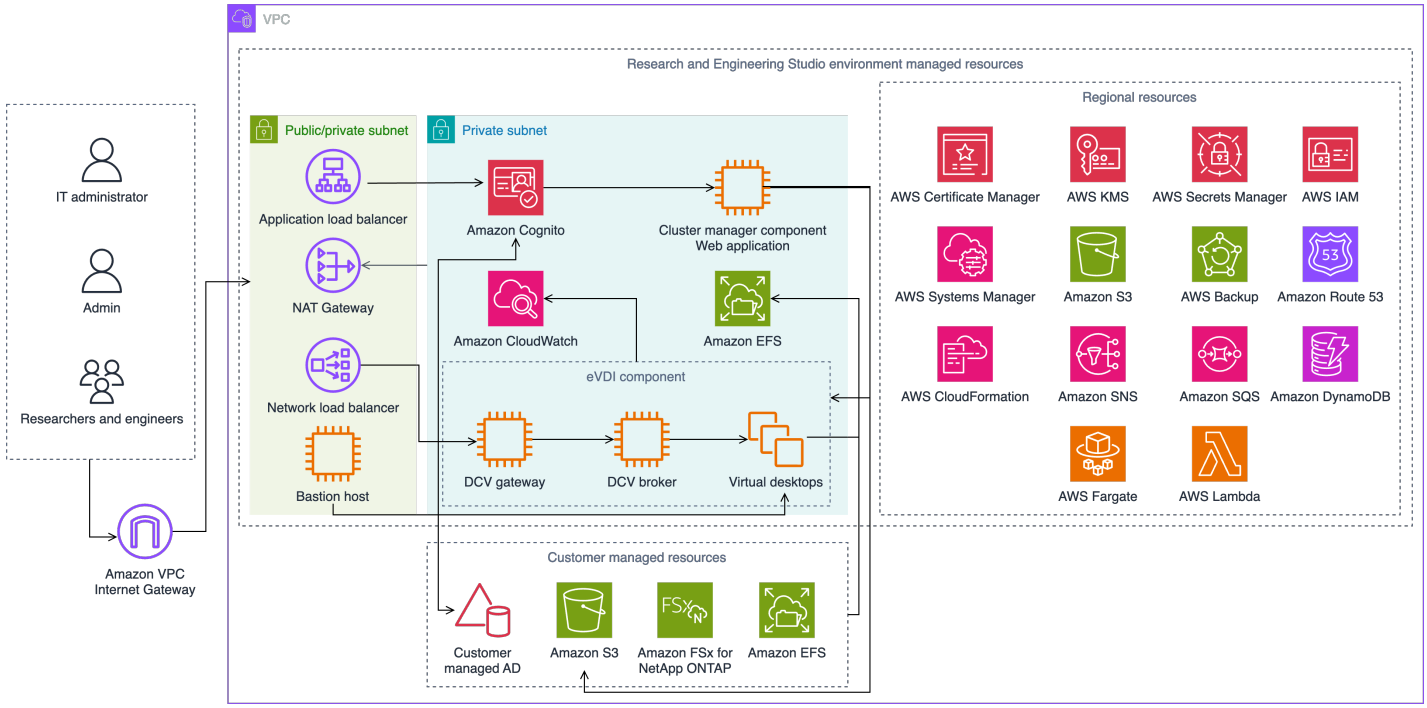


Abbildung 1: Forschungs- und Ingenieurstudio für AWS Architektur

> **Note**
>
> AWS CloudFormation Ressourcen werden aus AWS Cloud Development Kit (AWS CDK) Konstrukten erstellt.

Der allgemeine Prozessablauf für die Produktkomponenten, die mit der AWS CloudFormation Vorlage bereitgestellt werden, sieht wie folgt aus:

1. RES installiert Komponenten für das Webportal sowie:

a. Komponente Engineering Virtual Desktop (eVDI) für interaktive Workloads

b. Komponente „Kennzahlen“

   Amazon CloudWatch erhält Metriken von den eVDI-Komponenten.

c. Bastion Host-Komponente

   Administratoren können über SSH eine Verbindung zur Bastion-Host-Komponente herstellen, um die zugrunde liegende Infrastruktur zu verwalten.

2. RES installiert Komponenten in privaten Subnetzen hinter einem NAT-Gateway. Administratoren greifen über den Application Load Balancer (ALB) oder die Bastion Host-Komponente auf die privaten Subnetze zu.
3. Amazon DynamoDB speichert die Umgebungskonfiguration.
4. AWS Certificate Manager (ACM) generiert und speichert ein öffentliches Zertifikat für den Application Load Balancer (ALB).

   > **Note**
   >
   > Wir empfehlen, es AWS Certificate Manager zu verwenden, um ein vertrauenswürdiges Zertifikat für Ihre Domain zu generieren.

5. Amazon Elastic File System (EFS) hostet das `/home` Standarddateisystem, das auf allen entsprechenden Infrastruktur-Hosts und eVDI-Linux-Sitzungen installiert ist.
6. RES verwendet Amazon Cognito, um darin einen ersten Bootstrap-Benutzer namens clusteradmin zu erstellen, und sendet temporäre Anmeldeinformationen an die bei der Installation angegebene E-Mail-Adresse. Der Clusteradmin muss das Passwort bei der ersten Anmeldung ändern.
7. Amazon Cognito lässt sich für die Rechteverwaltung in das Active Directory und die Benutzeridentitäten Ihres Unternehmens integrieren.
8. Sicherheitszonen ermöglichen es Administratoren, den Zugriff auf bestimmte Komponenten innerhalb des Produkts auf der Grundlage von Berechtigungen einzuschränken.

AWS Dienste in diesem Produkt

AWS Service	Beschreibung
Amazon Elastic Compute Cloud	Kern. Stellt die zugrunde liegenden Rechendienste bereit, um virtuelle Desktops mit dem von ihnen ausgewählten Betriebssystem und Software-Stack zu erstellen.
Elastic Load Balancing	Kern. Bastion-, Cluster-Manager- und VDI-Hosts werden in Auto Scaling Scaling-Gruppen hinter dem Load Balancer erstellt. ELB verteilt den Datenverkehr vom Webportal auf die RES-Hosts.
Amazon Virtual Private Cloud	Kern. Alle Kernproduktkomponenten werden in Ihrer VPC erstellt.
Amazon Cognito	Kern. Verwaltet Benutzeridentitäten und Authentifizierung. Active Directory-Benutzer werden Amazon Cognito Cognito-Benutzern und -Gruppen zugeordnet, um Zugriffsebenen zu authentifizieren.
Amazon Elastic File System	Kern. Stellt das `/home` Dateisystem für den Dateibrowser und die VDI-Hosts sowie gemeinsam genutzte externe Dateisysteme bereit.
Amazon-DynamoDB	Kern. Speichert Konfigurationsdaten wie Benutzer, Gruppen, Projekte, Dateisysteme und Komponenteneinstellungen.
AWS Systems Manager	Kern. Speichert Dokumente zur Ausführung von Befehlen für die VDI-Sitzungsverwaltung.
AWS Lambda	Kern. Unterstützt Produktfunktionen wie das Aktualisieren von Einstellungen in der

AWS Service	Beschreibung
	DynamoDB-Tabelle, das Starten von Active Directory-Synchronisierungsworkflows und das Aktualisieren der Präfixliste.
Amazon CloudWatch	Unterstützend. Stellt Metriken und Aktivität sprotokolle für alle EC2 Amazon-Hosts und Lambda-Funktionen bereit.
Amazon Simple Storage Service	Unterstützend. Speichert Anwendungsbinärdat eien für Host-Bootstrapping und Konfiguration.
AWS Key Management Service	Unterstützend. Wird für die Verschlüsselung im Ruhezustand mit Amazon SQS SQS-Warte schlangen, DynamoDB-Tabellen und Amazon SNS SNS-Themen verwendet.
AWS Secrets Manager	Unterstützend. Speichert Anmeldeinformation en für Dienstkonten in Active Directory und selbstsignierte Zertifikate für VDIs.
AWS CloudFormation	Unterstützend. Stellt einen Bereitstellungsmec hanismus für das Produkt bereit.
AWS Identity and Access Management	Unterstützend. Schränkt die Zugriffsebene für Hosts ein.
Amazon Route 53	Unterstützend. Erstellt eine private gehostete Zone zur Auflösung des internen Load Balancers und des Bastion-Host-Domän ennamens.
Amazon Simple Queue Service	Unterstützend. Erstellt Aufgabenwarteschla ngen zur Unterstützung asynchroner Ausführun gen.

AWS Service	Beschreibung
Amazon Simple Notification Service	Unterstützend. Unterstützt das Publication-Subscriber-Modell zwischen VDI-Komponenten wie dem Controller und den Hosts.
AWS Fargate	Unterstützend. Installiert, aktualisiert und löscht Umgebungen mithilfe von Fargate-Aufgaben.
Amazon FSx File Gateway	Optional. Stellt ein externes gemeinsam genutztes Dateisystem bereit.
Amazon FSx für NetApp ONTAP	Optional. Stellt ein externes gemeinsam genutztes Dateisystem bereit.
AWS Certificate Manager	Optional. Generiert ein vertrauenswürdiges Zertifikat für Ihre benutzerdefinierte Domain.
AWS Backup	Optional. Bietet Backup-Funktionen für EC2 Amazon-Hosts, Dateisysteme und DynamoDB.

Erstellen Sie eine Demo-Umgebung

Folgen Sie den Schritten in diesem Abschnitt, um Research and Engineering Studio auszuprobieren. AWS In dieser Demo wird eine Nicht-Produktionsumgebung mit einem minimalen Satz von Parametern bereitgestellt. Dabei wird die Stack-Vorlage Research and Engineering Studio on AWS Demo-Umgebung verwendet. Es verwendet einen Keycloak-Server für SSO.

Beachten Sie, dass Sie nach der Bereitstellung des Stacks die folgenden Schritte ausführen müssen, um Benutzer in Schritte nach der Bereitstellung der Umgebung einzurichten, bevor Sie sich anmelden.

Erstellen Sie einen Demo-Stack mit einem Klick

Dieser AWS CloudFormation Stack erstellt alle Komponenten, die von Research and Engineering Studio benötigt werden.

Zeit bis zur Bereitstellung: ~90 Minuten

Voraussetzungen

Themen

- Erstellen Sie eine AWS-Konto mit einem Administratorbenutzer
- Erstellen Sie ein Amazon EC2 SSH-Schlüsselpaar
- Erhöhen Sie die Servicequoten

Erstellen Sie eine AWS-Konto mit einem Administratorbenutzer

Sie müssen über ein Konto AWS-Konto mit einem Administratorkonto verfügen:

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und

verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Erstellen Sie ein Amazon EC2 SSH-Schlüsselpaar

Wenn Sie kein Amazon EC2 SSH-Schlüsselpaar haben, müssen Sie eines erstellen. Weitere Informationen finden Sie unter Erstellen eines key pair mithilfe von Amazon EC2 im EC2 Amazon-Benutzerhandbuch.

Erhöhen Sie die Servicequoten

Wir empfehlen, die Servicekontingenten zu erhöhen für:

- Amazon VPC
  - Erhöhen Sie das Elastic IP-Adresskontingent pro NAT-Gateway von fünf auf acht
  - Erhöhen Sie die Anzahl der NAT-Gateways pro Availability Zone von fünf auf zehn
- Amazon EC2
  - Erhöhen Sie EC2 den VPC Elastic IPs von fünf auf zehn

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden. Weitere Informationen finden Sie unter the section called “Kontingente für AWS Dienstleistungen in diesem Produkt”.

Erstellen Sie Ressourcen und Eingabeparameter

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie sich in Ihrem Administratorkonto befinden.

2. Starten Sie die Vorlage in der Konsole.
3. Überprüfen Sie unter Parameter die Parameter für diese Produktvorlage und ändern Sie sie nach Bedarf.

Parameter	Standard	Beschreibung
EnvironmentName	`<res-demo>`	Ein eindeutiger Name für Ihre RES-Umgebung, der mit res- beginnt und nicht länger als 11 Zeichen ist.
AdministratorEmail		Die E-Mail-Adresse des Benutzers, der die Installat ion des Produkts abschließ t. Dieser Benutzer fungiert außerdem als Sicherhei tsbenutzer, falls die Active Directory-Single-Sign-On-In tegration fehlschlägt.
KeyPair		Das key pair, das für die Verbindung zu Infrastru kturhosts verwendet wird.
Klient IPCidr	<0.0.0.0/0>	IP-Adressfilter, der die Verbindung zum System einschränkt. Sie können den ClientIpCidr nach der Bereitstellung aktualisieren.
InboundPrefixList		(Optional) Stellen Sie eine verwaltete Präfixliste für IPs den direkten Zugriff auf die Weboberfläche und SSH auf den Bastion-Host bereit.

Schritte nach der Bereitstellung

1. Benutzerkennwörter zurücksetzen in `AWS Directory Service` — Der Demo-Stack erstellt vier Benutzer mit Benutzernamen, die Sie verwenden können:`admin1`, `user1admin2`, und`user2`.

   a. Rufen Sie die Directory Service Service-Konsole auf.

   b. Wählen Sie die Verzeichnis-ID für Ihre Umgebung aus. Sie können die Verzeichnis-ID aus der Ausgabe von `<StackName>*DirectoryService*` Stack abrufen.

   c. Wählen Sie im Dropdownmenü Aktion oben rechts die Option Benutzerpasswort zurücksetzen aus.

   d. Geben Sie für alle Benutzer, die Sie verwenden möchten, den Benutzernamen und das gewünschte Passwort ein und wählen Sie Passwort zurücksetzen aus.

2. Nachdem Sie die Benutzerkennwörter zurückgesetzt haben, müssen Sie warten, bis Research and Engineering Studio die Benutzer in der Umgebung synchronisiert hat. Research and Engineering Studio synchronisiert die Benutzer stündlich um xx.00 Uhr. Sie können entweder warten, bis das passiert, oder die unter aufgeführten Schritte ausführen, um die Benutzer sofort Der Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES zu synchronisieren.

Ihr Deployment ist jetzt fertig. Verwenden EnvironmentUrl Sie die URL, die Sie in Ihrer E-Mail erhalten haben, um auf die Benutzeroberfläche zuzugreifen, oder Sie können dieselbe URL auch aus der Ausgabe des bereitgestellten Stacks abrufen. Sie können sich jetzt mit dem Benutzer und dem Passwort, für das Sie das Passwort in Active Directory zurückgesetzt haben, bei der Research and Engineering Studio-Umgebung anmelden.

Planen Sie Ihren Einsatz

Kosten

Research and Engineering Studio on AWS ist ohne zusätzliche Kosten verfügbar, und Sie zahlen nur für die Ressourcen, die Sie für die Ausführung Ihrer Anwendungen benötigen. AWS Weitere Informationen finden Sie unter AWS Dienste in diesem Produkt.

> **Note**
>
> Sie sind für die Kosten der AWS Dienste verantwortlich, die Sie beim Betrieb dieses Produkts in Anspruch nehmen.
> Wir empfehlen, ein Budget zu erstellen AWS Cost Explorer, um die Kosten im Griff zu behalten. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Webseite mit den Preisen für jeden AWS Service, der in diesem Produkt verwendet wird.

Sicherheit

Wenn Sie Systeme auf der AWS Infrastruktur aufbauen, teilen Sie sich die Sicherheitsverantwortung zwischen Ihnen und AWS. Dieses Modell der geteilten Verantwortung reduziert Ihren betrieblichen Aufwand, da AWS die Komponenten wie das Host-Betriebssystem, die Virtualisierungsebene und die physische Sicherheit der Einrichtungen, in denen die Services ausgeführt werden, betrieben, verwaltet und kontrolliert werden. Weitere Informationen zur AWS Sicherheit finden Sie unter AWS Cloud Sicherheit.

IAM-Rollen

AWS Identity and Access Management (IAM) -Rollen ermöglichen es Kunden, Diensten und Benutzern auf der Website detaillierte Zugriffsrichtlinien und -berechtigungen zuzuweisen. AWS Cloud Dieses Produkt erstellt IAM-Rollen, die den AWS Lambda Funktionen des Produkts und EC2 Amazon-Instances Zugriff gewähren, um regionale Ressourcen zu erstellen.

RES unterstützt identitätsbasierte Richtlinien innerhalb von IAM. Bei der Bereitstellung erstellt RES Richtlinien zur Definition der Administratorrechte und des Administratorzugriffs. Der Administrator, der das Produkt implementiert, erstellt und verwaltet Endbenutzer und Projektleiter innerhalb des bestehenden Kunden-Active-Directory-Netzwerks, das in RES integriert ist. Weitere Informationen

finden Sie unter Erstellen von IAM-Richtlinien im AWS Identity and Access Management-Benutzerhandbuch.

Der Administrator Ihrer Organisation kann den Benutzerzugriff mit einem Active Directory verwalten. Wenn Endbenutzer auf die RES-Benutzeroberfläche zugreifen, authentifiziert sich RES bei Amazon Cognito.

Sicherheitsgruppen

Die in diesem Produkt erstellten Sicherheitsgruppen dienen dazu, den Netzwerkverkehr zwischen den Lambda-Funktionen, EC2 -Instanzen, Dateisystem-CSR-Instanzen und Remote-VPN-Endpunkten zu kontrollieren und zu isolieren. Wir empfehlen Ihnen, die Sicherheitsgruppen zu überprüfen und den Zugriff nach Bedarf weiter einzuschränken, sobald das Produkt bereitgestellt ist.

Datenverschlüsselung

Standardmäßig verschlüsselt Research and Engineering Studio on AWS (RES) Kundendaten im Speicher und bei der Übertragung mithilfe eines RES-eigenen Schlüssels. Bei der Bereitstellung von RES können Sie einen AWS KMS key angeben. RES verwendet Ihre Anmeldeinformationen, um den Schlüsselzugriff zu gewähren. Wenn Sie einen Kunden angeben, der Eigentümer und verwalteter Kunde ist AWS KMS key, werden die gespeicherten Kundendaten mit diesem Schlüssel verschlüsselt.

RES verschlüsselt Kundendaten während der Übertragung mit SSL/TLS. Wir benötigen TLS 1.2, empfehlen aber TLS 1.3.

Kontingente

Service Quotas, auch als Limits bezeichnet, sind die maximale Anzahl von Serviceressourcen oder -vorgängen für Ihr AWS-Konto.

Kontingente für AWS Dienste in diesem Produkt

Stellen Sie sicher, dass Sie über ein ausreichendes Kontingent für jeden der in diesem Produkt implementierten Dienste verfügen. Weitere Informationen finden Sie unter AWS -Servicekontingente.

Für dieses Produkt empfehlen wir, die Kontingente für die folgenden Dienste zu erhöhen:

- Amazon Virtual Private Cloud

- Amazon EC2

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch zu Service Quotas. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

AWS CloudFormation Kontingente

Ihr AWS-Konto hat AWS CloudFormation Kontingente, die Sie beachten sollten, wenn Sie den Stack in diesem Produkt auf den Markt bringen. Wenn Sie diese Kontingente verstehen, können Sie Limitationsfehler vermeiden, die Sie daran hindern würden, dieses Produkt erfolgreich einzusetzen. Weitere Informationen finden Sie unter AWS CloudFormation Kontingente im AWS CloudFormation Benutzerhandbuch.

Planung für Resilienz

Das Produkt stellt eine Standardinfrastruktur mit der Mindestanzahl und Größe von EC2 Amazon-Instances für den Betrieb des Systems bereit. Um die Ausfallsicherheit in großen Produktionsumgebungen zu verbessern, empfehlen wir, die standardmäßigen Mindestkapazitätseinstellungen innerhalb der Auto Scaling Scaling-Gruppen (ASG) der Infrastruktur zu erhöhen. Die Erhöhung des Werts von einer Instanz auf zwei Instanzen bietet den Vorteil mehrerer Availability Zones (AZ) und reduziert die Zeit für die Wiederherstellung der Systemfunktionalität bei unerwartetem Datenverlust.

Die ASG-Einstellungen können in der EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/angepasst werden. Das Produkt erstellt ASGs standardmäßig vier, wobei jeder Name mit `-asg` endet. Sie können die Mindest- und die gewünschten Werte auf einen Wert ändern, der für Ihre Produktionsumgebung geeignet ist. Wählen Sie die Gruppe aus, die Sie ändern möchten, und klicken Sie dann auf Aktionen und Bearbeiten. Weitere Informationen finden Sie unter Skalieren der Größe Ihrer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. ASGs

Unterstützt AWS-Regionen

Dieses Produkt verwendet Dienste, die derzeit nicht in allen verfügbar sind AWS-Regionen. Sie müssen dieses Produkt an einem Ort auf den Markt bringen AWS-Region , an dem alle Dienste verfügbar sind. Die aktuelle Verfügbarkeit von AWS Diensten nach Regionen finden Sie in der Liste AWS-Region aller Dienste.

Research and Engineering Studio on AWS wird in folgenden Bereichen unterstützt AWS-Regionen:

Name der Region	Region	Version 2024.06 und früher	Version 2024.08
USA Ost (Nord-Virginia)	us-east-1	Ja	Ja
USA Ost (Ohio)	us-east-2	Ja	Ja
USA West (Nordkalifornien)	us-west-1	Ja	Ja
USA West (Oregon)	us-west-2	Ja	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja	Ja
Kanada (Zentral)	ca-central-1	Ja	Ja
Europa (Frankfurt)	eu-central-1	Ja	Ja
Europa (Mailand)	eu-south-1	Ja	Ja
Europa (Ireland)	eu-west-1	Ja	Ja
Europa (London)	eu-west-2	Ja	Ja
Europa (Paris)	eu-west-3	Ja	Ja
Europa (Stockholm)	eu-north-1	Nein	Ja

Name der Region	Region	Version 2024.06 und früher	Version 2024.08
Israel (Tel Aviv)	il-central-1	Ja	Ja
AWS GovCloud (US-West)	us-gov-west-1	Ja	Nein

Stellen Sie das Produkt bereit

> **Note**
>
> Dieses Produkt verwendet AWS CloudFormation Vorlagen und Stacks, um die Bereitstellung zu automatisieren. Die CloudFormation Vorlagen beschreiben die in diesem Produkt enthaltenen AWS Ressourcen und ihre Eigenschaften. Der CloudFormation Stack stellt die Ressourcen bereit, die in den Vorlagen beschrieben sind.

Bevor Sie das Produkt auf den Markt bringen, sollten Sie sich mit den Kosten, der Architektur, der Netzwerksicherheit und anderen Überlegungen befassen, die weiter oben in diesem Handbuch erörtert wurden.

Themen

- Voraussetzungen
- Externe Ressourcen erstellen
- Schritt 1: Starten Sie das Produkt
- Schritt 2: Melden Sie sich zum ersten Mal an

Voraussetzungen

Themen

- Erstellen Sie eine AWS-Konto mit einem Administratorbenutzer
- Erstellen Sie ein Amazon EC2 SSH-Schlüsselpaar
- Erhöhen Sie die Servicequoten
- Erstellen Sie eine öffentliche Domain (optional)
- Domain erstellen (GovCloud nur)
- Stellen Sie externe Ressourcen bereit
- Konfigurieren Sie LDAPS in Ihrer Umgebung (optional)
- Konfigurieren Sie eine private VPC (optional)

Erstellen Sie eine AWS-Konto mit einem Administratorbenutzer

Sie benötigen ein Konto AWS-Konto mit einem Administratorkonto:

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Erstellen Sie ein Amazon EC2 SSH-Schlüsselpaar

Wenn Sie kein Amazon EC2 SSH-Schlüsselpaar haben, müssen Sie eines erstellen. Weitere Informationen finden Sie unter Erstellen eines key pair mithilfe von Amazon EC2 im EC2 Amazon-Benutzerhandbuch.

Erhöhen Sie die Servicequoten

Wir empfehlen, die Servicekontingenten zu erhöhen für:

- Amazon VPC
  - Erhöhen Sie das Elastic IP-Adresskontingent pro NAT-Gateway von fünf auf acht
  - Erhöhen Sie die Anzahl der NAT-Gateways pro Availability Zone von fünf auf zehn
- Amazon EC2
  - Erhöhen Sie EC2 den VPC Elastic IPs von fünf auf zehn

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden. Weitere Informationen finden Sie unter the section called “Kontingente für AWS Dienstleistungen in diesem Produkt”.

Erstellen Sie eine öffentliche Domain (optional)

Wir empfehlen, eine benutzerdefinierte Domain für das Produkt zu verwenden, um eine benutzerfreundliche URL zu erhalten. Sie müssen eine Domain mit Amazon Route 53 oder einem anderen Anbieter registrieren und ein Zertifikat für die verwendete Domain importieren AWS Certificate Manager. Wenn Sie bereits über eine öffentliche Domain und ein Zertifikat verfügen, können Sie diesen Schritt überspringen.

1. Folgen Sie den Anweisungen, um eine Domain bei Route53 zu registrieren. Sie sollten eine Bestätigungs-E-Mail erhalten.
2. Rufen Sie die gehostete Zone für Ihre Domain ab. Diese wird automatisch von Route53 erstellt.
   a. Öffnen Sie die Route53-Konsole.
   b. Wählen Sie im linken Navigationsbereich die Option Gehostete Zonen aus.
   c. Öffnen Sie die Hosting-Zone, die für Ihren Domainnamen erstellt wurde, und kopieren Sie die Hosting-Zone-ID.
3. Öffnen Sie AWS Certificate Manager und folgen Sie diesen Schritten, um ein Domainzertifikat anzufordern. Stellen Sie sicher, dass Sie sich in der Region befinden, in der Sie die Lösung bereitstellen möchten.
4. Wählen Sie in der Navigation die Option Zertifikate auflisten aus und suchen Sie nach Ihrer Zertifikatsanforderung. Die Anfrage sollte ausstehend sein.
5. Wählen Sie Ihre Zertifikat-ID, um die Anfrage zu öffnen.
6. Wählen Sie im Bereich Domains die Option Create Records in Route53 aus. Die Bearbeitung der Anfrage dauert ungefähr zehn Minuten.
7. Sobald das Zertifikat ausgestellt wurde, kopieren Sie den ARN aus dem Abschnitt Zertifikatsstatus.

Domain erstellen (GovCloud nur)

Wenn Sie in der Region AWS GovCloud (USA West) bereitstellen, müssen Sie diese erforderlichen Schritte ausführen.

1. Stellen Sie den AWS CloudFormation Zertifikatsstapel in dem AWS Konto mit kommerzieller Partition bereit, in dem die öffentlich gehostete Domain erstellt wurde.
2. Suchen und notieren Sie in den CloudFormation Zertifikatsausgaben das `CertificateARN` und. `PrivateKeySecretARN`

3. Erstellen Sie im GovCloud Partitionskonto ein Geheimnis mit dem Wert der `CertificateARN` Ausgabe. Notieren Sie sich den neuen geheimen ARN und fügen Sie dem Secret zwei Tags hinzu, damit `vdc-gateway` Sie auf den geheimen Wert zugreifen können:

   a. res: ModuleName = virtual-desktop-controller

   b. res: EnvironmentName = [Umgebungsname] (Das könnte res-demo sein.)

4. Erstellen Sie im GovCloud Partitionskonto ein Geheimnis mit dem Wert der `PrivateKeySecretArn` Ausgabe. Notieren Sie sich den neuen geheimen ARN und fügen Sie dem Secret zwei Tags hinzu, damit `vdc-gateway` Sie auf den geheimen Wert zugreifen können:

   a. res: ModuleName = virtual-desktop-controller

   b. res: EnvironmentName = [Umgebungsname] (Das könnte res-demo sein.)

Stellen Sie externe Ressourcen bereit

Research and Engineering Studio on AWS geht davon aus, dass die folgenden externen Ressourcen vorhanden sind, wenn es bereitgestellt wird.

- Netzwerke (VPC, öffentliche Subnetze und private Subnetze)

  Hier werden Sie die EC2 Instanzen ausführen, die zum Hosten der RES-Umgebung, des Active Directory (AD) und des gemeinsam genutzten Speichers verwendet werden.

- Speicher (Amazon EFS)

  Die Speichervolumes enthalten Dateien und Daten, die für die virtuelle Desktop-Infrastruktur (VDI) benötigt werden.

- Verzeichnisdienst ()AWS Directory Service for Microsoft Active Directory

  Der Verzeichnisdienst authentifiziert Benutzer gegenüber der RES-Umgebung.

- Ein Geheimnis, das das Passwort für das Dienstkonto enthält

  Research and Engineering Studio greift auf Geheimnisse zu, die Sie uns zur Verfügung stellen, einschließlich des Kennworts für das Dienstkonto, mithilfe von AWS Secrets Manager.

> **Tip**
>
> Wenn Sie eine Demoumgebung bereitstellen und diese externen Ressourcen nicht verfügbar sind, können Sie die externen Ressourcen mithilfe von AWS High Performance Compute-Rezepten generieren. Informationen zur Bereitstellung von Ressourcen in Ihrem Konto finden Sie im folgenden Abschnitt. Externe Ressourcen erstellen
> Für Demo-Bereitstellungen in der Region AWS GovCloud (USA West) müssen Sie die erforderlichen Schritte unter ausführen. Domain erstellen (GovCloud nur)

Konfigurieren Sie LDAPS in Ihrer Umgebung (optional)

Wenn Sie die LDAPS-Kommunikation in Ihrer Umgebung verwenden möchten, müssen Sie diese Schritte ausführen, um Zertifikate zu erstellen und an den AWS Managed Microsoft AD (AD) - Domänencontroller anzuhängen, um die Kommunikation zwischen AD und RES bereitzustellen.

1. Folgen Sie den Schritten unter So aktivieren Sie serverseitiges LDAPS für Ihre. AWS Managed Microsoft AD Sie können diesen Schritt überspringen, wenn Sie LDAPS bereits aktiviert haben.
2. Nachdem Sie bestätigt haben, dass LDAPS auf dem AD konfiguriert ist, exportieren Sie das AD-Zertifikat:
   a. Gehen Sie zu Ihrem Active Directory-Server.
   b. PowerShell Als Administrator öffnen.
   c. Ausführen`certmgr.msc`, um die Zertifikatsliste zu öffnen.
   d. Öffnen Sie die Zertifikatsliste, indem Sie zuerst die vertrauenswürdigen Stammzertifizierungsstellen und dann Zertifikate öffnen.
   e. Wählen Sie das Zertifikat mit demselben Namen wie Ihr AD-Server aus und halten Sie es gedrückt (oder klicken Sie mit der rechten Maustaste darauf). Wählen Sie Alle Aufgaben und dann Exportieren aus.
   f. Wählen Sie Base-64 encoded X.509 (.CER) und dann Weiter.
   g. Wählen Sie ein Verzeichnis aus und wählen Sie dann Weiter.
3. Erstellen Sie ein Geheimnis in AWS Secrets Manager:

   Wenn Sie Ihr Geheimnis im Secrets Manager erstellen, wählen Sie Andere Art von Geheimnissen unter Geheimnistyp und fügen Sie Ihr PEM-codiertes Zertifikat in das Klartext-Feld ein.

4. Notieren Sie sich den erstellten ARN und geben Sie ihn als `DomainTLSCertificateSecretARN` Parameter einthe section called “Schritt 1: Starten Sie das Produkt”.

Konfigurieren Sie eine private VPC (optional)

Die Bereitstellung von Research and Engineering Studio in einer isolierten VPC bietet verbesserte Sicherheit, um die Compliance- und Governance-Anforderungen Ihres Unternehmens zu erfüllen. Die standardmäßige RES-Bereitstellung ist jedoch für die Installation von Abhängigkeiten auf den Internetzugang angewiesen. Um RES in einer privaten VPC zu installieren, müssen Sie die folgenden Voraussetzungen erfüllen:

Themen

- Bereiten Sie Amazon Machine Images vor (AMIs)
- VPC-Endpunkte einrichten
- Connect zu Diensten ohne VPC-Endpunkte her
- Stellen Sie private VPC-Bereitstellungsparameter ein

Bereiten Sie Amazon Machine Images vor (AMIs)

1. Laden Sie Abhängigkeiten herunter. Für die Bereitstellung in einer isolierten VPC erfordert die RES-Infrastruktur die Verfügbarkeit von Abhängigkeiten ohne öffentlichen Internetzugang.
2. Erstellen Sie eine IAM-Rolle mit schreibgeschütztem Amazon S3 S3-Zugriff und vertrauenswürdiger Identität als Amazon. EC2

   a. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.

   b. Wählen Sie unter Rollen die Option Rolle erstellen aus.

   c. Gehen Sie auf der Seite Vertrauenswürdige Entität auswählen wie folgt vor:

      - Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS-Service.
      - Wählen Sie für Anwendungsfall unter Service oder Anwendungsfall die Option EC2Weiter aus.

   d. Wählen Sie unter Berechtigungen hinzufügen die folgenden Berechtigungsrichtlinien aus und klicken Sie dann auf Weiter:

      - Amazon S3 ReadOnlyAccess

- Amazon SSMManaged InstanceCore
- EC2InstanceProfileForImageBuilder

e. Fügen Sie einen Rollennamen und eine Beschreibung hinzu und wählen Sie dann Rolle erstellen aus.

3. Erstellen Sie die EC2 Image Builder-Komponente:

a. Öffnen Sie die EC2 Image Builder Builder-Konsole unterhttps://console.aws.amazon.com/imagebuilder.

b. Wählen Sie unter Gespeicherte Ressourcen die Option Komponenten und anschließend Komponente erstellen aus.

c. Geben Sie auf der Seite Komponente erstellen die folgenden Details ein:

- Wählen Sie als Komponententyp die Option Build aus.
- Wählen Sie für Komponentendetails Folgendes aus:

Parameter	Benutzereintrag
Image-Betriebssystem (OS)	Linux
Kompatible Betriebssystemversionen	Amazon Linux 2
Name der Komponente	Wählen Sie einen Namen wie: `<research-and-engineering-studio-infrastructure>`
Version der Komponente	Wir empfehlen, mit 1.0.0 zu beginnen.
Beschreibung	Optionaler Benutzereintrag.

d. Wählen Sie auf der Seite Komponente erstellen die Option Dokumentinhalt definieren aus.

i. Bevor Sie den Inhalt des Definitionsdokuments eingeben können, benötigen Sie einen Datei-URI für die Datei tar.gz. Laden Sie die von RES bereitgestellte Datei tar.gz in einen Amazon S3 S3-Bucket hoch und kopieren Sie den URI der Datei aus den Bucket-Eigenschaften.

ii. Geben Sie Folgendes ein:

> **Note**
>
> `AddEnvironmentVariables`ist optional, und Sie können sie entfernen, wenn Sie keine benutzerdefinierten Umgebungsvariablen in Ihren Infrastruktur-Hosts benötigen.
>
> Wenn Sie `https_proxy` Umgebungsvariablen einrichten`http_proxy`, sind die `no_proxy` Parameter erforderlich, um zu verhindern, dass die Instanz einen Proxy verwendet, um Localhost, IP-Adressen von Instanzmetadaten und die Dienste, die VPC-Endpunkte unterstützen, abzufragen.

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may
 not use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
```

```
          action: S3Download
          onFailure: Abort
          maxAttempts: 3
          inputs:
             - source: '<s3 tar.gz file uri>'
               destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
               expectedBucketOwner: '{{ AWSAccountID }}'
        - name: RunInstallScript
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - 'cd /root/bootstrap/res_dependencies'
                 - 'tar -xf res_dependencies.tar.gz'
                 - 'cd all_dependencies'
                 - '/bin/bash install.sh'
        - name: AddEnvironmentVariables
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - |
                   echo -e "
                   http_proxy=http://<ip>:<port>
                   https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
```

```
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com
                  " > /etc/environment
```

e. Wählen Sie Komponente erstellen aus.

4. Erstellen Sie ein Image Builder Builder-Image-Rezept.

   a. Geben Sie auf der Seite Rezept erstellen Folgendes ein:

Abschnitt	Parameter	Benutzereintrag
Einzelheiten zum Rezept	Name	Geben Sie einen passenden Namen ein, z. B. res-recipe-linux-x 86.
	Version	Geben Sie eine Version ein, die normalerweise mit 1.0.0 beginnt.
	Beschreibung	Fügen Sie eine optionale Beschreibung hinzu.
Basisbild	Wählen Sie ein Bild	Wählen Sie verwaltete Bilder aus.
	OS	Amazon Linux
	Herkunft des Bildes	Schnellstart (von Amazon verwaltet)
	Name des Bildes	Amazon Linux 2 x86

Abschnitt	Parameter	Benutzereintrag
	Optionen für die automatische Versionierung	Verwenden Sie die neueste verfügbare Betriebssystemversion.
Konfiguration der Instanz	–	Behalten Sie die Standardeinstellungen bei und stellen Sie sicher, dass die Option SSM-Agent nach der Pipeline-Ausführung entfernen nicht ausgewählt ist.
Arbeitsverzeichnis	Pfad zum Arbeitsverzeichnis	/root/bootstrap/res_Abhängigkeiten
Komponenten	Komponenten erstellen	Suchen Sie nach den folgenden Optionen und wählen Sie sie aus: • Von Amazon verwaltet: -2-linux aws-cli-version • Von Amazon verwaltet : amazon-cloudwatch-agent-linux • Gehört Ihnen: EC2 Amazon-Komponente, die zuvor erstellt wurde. Geben Sie Ihre AWS-Konto ID und Ihren aktuellen AWS-Region Status in die Felder ein.

Abschnitt	Parameter	Benutzereintrag
	Komponenten testen	Suchen Sie nach und wählen Sie: • Von Amazon verwaltet: simple-boot-test-linux

b. Wählen Sie Create Recipe (Rezept erstellen) aus.

5. Erstellen Sie die Image Builder Builder-Infrastrukturkonfiguration.

a. Wählen Sie unter Gespeicherte Ressourcen die Option Infrastrukturkonfigurationen aus.

b. Wählen Sie Infrastrukturkonfiguration erstellen aus.

c. Geben Sie auf der Seite „Infrastrukturkonfiguration erstellen“ Folgendes ein:

Abschnitt	Parameter	Benutzereintrag
Allgemeines	Name	Geben Sie einen passenden Namen ein, z. B. res-infra-linux-x 86.
	Beschreibung	Fügen Sie eine optionale Beschreibung hinzu.
	IAM role (IAM-Rolle)	Wählen Sie die zuvor erstellte IAM-Rolle aus.
AWS Infrastruktur	Instance-Typ	Wählen Sie t3.medium.
	VPC, Subnetz und Sicherheitsgruppen	Wählen Sie eine Option aus, die den Internetz ugang und den Zugriff auf den Amazon S3 S3-Bucket ermöglicht. Wenn Sie eine Sicherheitsgruppe erstellen müssen, können Sie eine über die EC2 Amazon-Ko

Abschnitt	Parameter	Benutzereintrag

		nsole mit den folgenden Eingaben erstellen:
		• VPC: Wählen Sie dieselbe VPC aus, die für die Infrastrukturkonfiguration verwendet wird. Diese VPC muss über einen Internetzugang verfügen.
		• Regel für eingehenden Datenverkehr:
		  • Typ: SSH
		  • Quelle: Benutzerdefiniert
		  • CIDR-Block: 0.0.0.0/0

d. Wählen Sie Infrastrukturkonfiguration erstellen.

6. Erstellen Sie eine neue EC2 Image Builder Builder-Pipeline:

   a. Gehen Sie zu Image-Pipelines und wählen Sie Image-Pipeline erstellen aus.

   b. Geben Sie auf der Seite „Pipeline-Details angeben“ Folgendes ein und wählen Sie Weiter aus:

      - Name der Pipeline und optionale Beschreibung
      - Legen Sie für Build schedule einen Zeitplan fest oder wählen Sie Manuell, wenn Sie den AMI-Backvorgang manuell starten möchten.

   c. Wählen Sie auf der Seite „Rezept auswählen“ die Option Bestehendes Rezept verwenden und geben Sie den zuvor erstellten Rezeptnamen ein. Wählen Sie Weiter aus.

   d. Wählen Sie auf der Seite „Image-Prozess definieren“ die Standard-Workflows aus und klicken Sie auf Weiter.

   e. Wählen Sie auf der Seite „Infrastrukturkonfiguration definieren“ die Option Bestehende Infrastrukturkonfiguration verwenden aus und geben Sie den Namen der zuvor erstellten Infrastrukturkonfiguration ein. Wählen Sie Weiter aus.

f. Beachten Sie bei Ihrer Auswahl auf der Seite „Verteilungseinstellungen definieren“ Folgendes:

- Das Ausgabe-Image muss sich in derselben Region wie die bereitgestellte RES-Umgebung befinden, damit RES die Infrastruktur-Host-Instances von dort aus ordnungsgemäß starten kann. Unter Verwendung der Dienststandardwerte wird das Ausgabebild in der Region erstellt, in der der EC2 Image Builder Builder-Dienst verwendet wird.
- Wenn Sie RES in mehreren Regionen bereitstellen möchten, können Sie Neue Distributionseinstellungen erstellen auswählen und dort weitere Regionen hinzufügen.

g. Überprüfen Sie Ihre Auswahl und wählen Sie Pipeline erstellen.

7. Führen Sie die EC2 Image Builder Builder-Pipeline aus:

   a. Suchen Sie unter Image-Pipelines die Pipeline, die Sie erstellt haben, und wählen Sie sie aus.

   b. Wählen Sie Aktionen und anschließend Pipeline ausführen aus.

   Es kann etwa 45 Minuten bis eine Stunde dauern, bis die Pipeline ein AMI-Image erstellt.

8. Notieren Sie sich die AMI-ID für das generierte AMI und verwenden Sie sie als Eingabe für den InfrastructureHost AMI-Parameter inthe section called “Schritt 1: Starten Sie das Produkt”.

VPC-Endpunkte einrichten

Um RES bereitzustellen und virtuelle Desktops zu starten, AWS-Services benötigen Sie Zugriff auf Ihr privates Subnetz. Sie müssen VPC-Endpoints einrichten, um den erforderlichen Zugriff bereitzustellen, und Sie müssen diese Schritte für jeden Endpunkt wiederholen.

1. Wenn Endpunkte noch nicht konfiguriert wurden, folgen Sie den Anweisungen unter Zugriff und AWS-Service Verwenden eines VPC-Schnittstellen-Endpunkts.
2. Wählen Sie in jeder der beiden Availability Zones ein privates Subnetz aus.

AWS-Service	Service-Name
Application Auto Scaling	com.amazonaws. *region*.automatische Skalierung von Anwendungen

AWS-Service	Service-Name
AWS CloudFormation	com.amazonaws. *region*. Wolkenbildung
Amazon CloudWatch	com.amazonaws. *region*. Überwachung
CloudWatch Amazon-Protokolle	com.amazonaws. *region*.protokolle
Amazon-DynamoDB	com.amazonaws. *region*.dynamodb (Erfordert einen Gateway-Endpunkt)
Amazon EC2	com.amazonaws. *region*.ec2
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon Elastic File System	com.amazonaws. *region*.elastisches Dateisystem
Elastic Load Balancing	com.amazonaws. *region*.elastischer Lastenausgleich
Amazon EventBridge	com.amazonaws. *region*.veranstaltungen
Amazon FSx	com.amazonaws. *region*.fsx
AWS Key Management Service	com.amazonaws. *region*. km
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-Streams
Amazon S3	com.amazonaws. *region*.s3 (Erfordert einen Gateway-Endpunkt, der standardmäßig in RES erstellt wird.)
AWS Secrets Manager	com.amazonaws. *region*. Geheimnismanager
Amazon SES	com.amazonaws. *region*.email-smtp (In den folgenden Availability Zones nicht unterstützt: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 und cac1-az4.)
AWS Security Token Service	com.amazonaws. *region*.sts

AWS-Service	Service-Name
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
AWS Systems Manager	com.amazonaws. *region*.ec2-Nachrichten
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-Nachrichten

Connect zu Diensten ohne VPC-Endpunkte her

Für die Integration mit Diensten, die keine VPC-Endpunkte unterstützen, können Sie einen Proxyserver in einem öffentlichen Subnetz Ihrer VPC einrichten. Gehen Sie wie folgt vor, um mit AWS Identity Center als Identitätsanbieter einen Proxyserver mit dem für eine Research and Engineering Studio-Bereitstellung erforderlichen Mindestzugriff zu erstellen.

1. Starten Sie eine Linux-Instance im öffentlichen Subnetz der VPC, die Sie für Ihre RES-Bereitstellung verwenden werden.
   - Linux-Familie — Amazon Linux 2 oder Amazon Linux 3
   - Architektur — x86
   - Instanztyp — t2.micro oder höher
   - Sicherheitsgruppe — TCP auf Port 3128 von 0.0.0.0/0
2. Stellen Sie eine Verbindung mit der Instanz her, um einen Proxyserver einzurichten.
   a. Öffnen Sie die HTTP-Verbindung.
   b. Erlauben Sie die Verbindung zu den folgenden Domänen von allen relevanten Subnetzen aus:
      - .amazonaws.com (für allgemeine Dienste) AWS
      - .amazoncognito.com (für Amazon Cognito)
      - .awsapps.com (für Identity Center)
      - .signin.aws (für Identity Center)
      - . amazonaws-us-gov.com (für Gov Cloud)

   c. Lehnen Sie alle anderen Verbindungen ab.
   d. Aktivieren und starten Sie den Proxyserver.
   e. Notieren Sie sich den PORT, auf dem der Proxy-Server lauscht.
3. Konfigurieren Sie Ihre Routing-Tabelle so, dass der Zugriff auf den Proxyserver möglich ist.
   a. Rufen Sie Ihre VPC-Konsole auf und identifizieren Sie die Routing-Tabellen für die Subnetze, die Sie für Infrastruktur-Hosts und VDI-Hosts verwenden werden.
   b. Bearbeiten Sie die Routentabelle, damit alle eingehenden Verbindungen zu der in den vorherigen Schritten erstellten Proxy-Server-Instanz weitergeleitet werden können.
   c. Tun Sie dies für Routing-Tabellen für alle Subnetze (ohne Internetzugang), die Sie für VDIs Infrastructure/ verwenden werden.
4. Ändern Sie die Sicherheitsgruppe der EC2 Proxy-Server-Instanz und stellen Sie sicher, dass sie eingehende TCP-Verbindungen an dem PORT zulässt, den der Proxyserver überwacht.

Stellen Sie private VPC-Bereitstellungsparameter ein

In wird von Ihnen erwartetthe section called “Schritt 1: Starten Sie das Produkt”, dass Sie bestimmte Parameter in die AWS CloudFormation Vorlage eingeben. Stellen Sie sicher, dass Sie die folgenden Parameter wie angegeben festlegen, um die Bereitstellung in der privaten VPC, die Sie gerade konfiguriert haben, erfolgreich durchzuführen.

Parameter	Eingabe
InfrastructureHostAMI	Verwenden Sie die in erstellte Infrastruktur-AMI-IDthe section called “Bereiten Sie Amazon Machine Images vor (AMIs)”.
IsLoadBalancerInternetFacing	Auf „Falsch“ gesetzt.
LoadBalancerSubnets	Wählen Sie private Subnetze ohne Internetz ugang.
InfrastructureHostSubnets	Wählen Sie private Subnetze ohne Internetz ugang.
VdiSubnets	Wählen Sie private Subnetze ohne Internetz ugang.

Parameter	Eingabe
ClientIP	Sie können Ihre VPC-CIDR auswählen, um den Zugriff für alle VPC-IP-Adressen zu ermöglich en.

Externe Ressourcen erstellen

Dieser CloudFormation Stapel erstellt Netzwerk-, Speicher-, Active Directory- und Domänenzertifikate (falls PortalDomainName vorhanden). Sie müssen über diese externen Ressourcen verfügen, um das Produkt bereitstellen zu können.

Sie können die Rezeptvorlage vor der Bereitstellung herunterladen.

Zeit für die Bereitstellung: Ungefähr 40-90 Minuten

1. Melden Sie sich bei https://console.aws.amazon.com/cloudformation an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie sich in Ihrem Administratorkonto befinden.

2. Starten Sie die Vorlage in der Konsole.

   Wenn Sie in der Region AWS GovCloud (USA West) bereitstellen, starten Sie die Vorlage im GovCloud Partitionskonto.

3. Geben Sie die Vorlagenparameter ein:

Parameter	Standard	Beschreibung
DomainName	`corp.res.com`	Domäne, die für das Active Directory verwendet wird. Der Standardwert ist in der `LDIF` Datei enthalten, mit der Bootstrap-Benutzer eingerichtet werden. Wenn Sie die Standardbenutzer

Parameter	Standard	Beschreibung
		verwenden möchten, belassen Sie den Wert als Standard. Um den Wert zu ändern, aktualisieren Sie ihn und stellen Sie eine separate `LDIF` Datei bereit. Dies muss nicht mit der für Active Directory verwendeten Domäne übereinstimmen.
SubDomain (GovCloud nur)		Dieser Parameter ist für kommerzielle Regionen optional, für GovCloud Regionen jedoch erforderl ich. Wenn Sie einen angeben SubDomain, wird der Parameter dem DomainNam e angegebenen vorangest ellt. Der angegebene Active Directory-Domänenname wird zu einer Unterdomäne.

Parameter	Standard	Beschreibung
AdminPassword		Das Passwort für den Active Directory-Administrator (BenutzernameAdmin). Dieser Benutzer wird im Active Directory für die erste Bootstrapping-Phase erstellt und danach nicht mehr verwendet. Wichtig: Das Format dieses Felds kann entweder (1) ein Klartext-Passwort oder (2) der ARN eines als key/value Paar `{"password":"somepassword"}` formatierten AWS Secrets sein. Hinweis: Das Passwort für diesen Benutzer muss die Anforderungen an die Passwortkomplexität für Active Directory erfüllen.

Parameter	Standard	Beschreibung
ServiceAccountPassword		Passwort, das zum Erstellen eines Dienstkontos verwendet wurde (`ReadOnlyUser`). Dieses Konto wird für die Synchronisation verwendet. Wichtig: Das Format dieses Felds kann entweder (1) ein Klartext-Passwort oder (2) der ARN eines als key/value Paar `{"password":"somepassword"}` formatierten AWS Secrets sein. Hinweis: Das Passwort für diesen Benutzer muss die Anforderungen an die Passwortkomplexität für Active Directory erfüllen.
Schlüsselpaar		Verbindet die administrativen Instanzen mithilfe eines SSH-Clients. Hinweis:AWS Systems Manager Session Manager kann auch verwendet werden, um eine Verbindung zu Instanzen herzustellen.

Parameter	Standard	Beschreibung
LDIFS3Pfad	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	Der Amazon S3 S3-Pfad zu einer LDIF-Datei, die während der Bootstrapping-Phase des Active Directory -Setups importiert wurde. Weitere Informationen finden Sie unter LDIF-Unterstützung . Der Parameter wird vorab mit einer Datei gefüllt, die eine Reihe von Benutzern im Active Directory erstellt. Die Datei finden Sie in der Datei res.ldif, die unter verfügbar ist. GitHub
ClientIpCidr		Die IP-Adresse, von der aus Sie auf die Site zugreifen . Sie können beispiels weise Ihre IP-Adresse auswählen und verwenden, `[IPADDRESS]/32` um nur den Zugriff von Ihrem Host aus zuzulassen. Sie können dies nach der Bereitstellung aktualisieren.
ClientPrefixList		Geben Sie eine Präfixliste ein, um Zugriff auf die Active Directory-Verwaltungsknoten zu gewähren. Informationen zum Erstellen einer verwaltet en Präfixliste finden Sie unter Arbeiten mit kundenver walteten Präfixlisten.

Parameter	Standard	Beschreibung
EnvironmentName	`res-[environment name]`	Wenn der angegeben `PortalDomainName` ist, wird dieser Parameter verwendet, um den generierten Geheimnissen Tags hinzuzufügen, sodass sie in der Umgebung verwendet werden können. Dies muss mit dem `EnvironmentName` Parameter übereinstimmen, der bei der Erstellung des RES-Stacks verwendet wurde. Wenn Sie mehrere Umgebungen in Ihrem Konto bereitstellen, muss dies eindeutig sein.

Parameter	Standard	Beschreibung
PortalDomainName		Geben Sie diesen Parameter für GovCloud Bereitste llungen nicht ein. Die Zertifikate und Geheimnis se wurden während der Voraussetzungen manuell erstellt. Der Domainname in Amazon Route 53 für das Konto. Wenn dies angegeben ist, werden ein öffentlic hes Zertifikat und eine Schlüsseldatei generiert und in diese hochgeladen AWS Secrets Manager. Wenn Sie über eine eigene Domain und Zertifikate verfügen, `EnvironmentName` kann dieser Parameter leer gelassen werden.

4. Bestätigen Sie alle Checkboxen unter Capabilities und wählen Sie Create Stack aus.

Schritt 1: Starten Sie das Produkt

Folgen Sie den step-by-step Anweisungen in diesem Abschnitt, um das Produkt zu konfigurieren und in Ihrem Konto bereitzustellen.

Zeit bis zur Bereitstellung: Ungefähr 60 Minuten

Sie können die CloudFormation Vorlage für dieses Produkt herunterladen, bevor Sie es bereitstellen.

Wenn Sie in AWS GovCloud (USA West) bereitstellen, verwenden Sie diese Vorlage.

res-stack — Verwenden Sie diese Vorlage, um das Produkt und alle zugehörigen Komponenten zu starten. Die Standardkonfiguration stellt den RES-Hauptstapel sowie die Authentifizierungs-, Frontend- und Backend-Ressourcen bereit.

> **Note**
>
> AWS CloudFormation Ressourcen werden aus AWS Cloud Development Kit (AWS CDK) ()AWS CDK-Konstrukten erstellt.

Die AWS CloudFormation Vorlage stellt Research and Engineering Studio auf der AWS bereit. AWS Cloud Sie müssen die Voraussetzungen erfüllen, bevor Sie den Stack starten können.

1. Melden Sie sich bei https://console.aws.amazon.com/cloudformation an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole.
2. Starten Sie die Vorlage.

   Für die Bereitstellung in AWS GovCloud (US-West) starten Sie diese Vorlage.
3. Die Vorlage wird standardmäßig in der Region USA Ost (Nord-Virginia) gestartet. Um die Lösung in einer anderen Version zu starten AWS-Region, verwenden Sie die Regionsauswahl in der Navigationsleiste der Konsole.

   > **Note**
   >
   > Dieses Produkt verwendet den Amazon Cognito-Service, der derzeit nicht in allen AWS-Regionen verfügbar ist. Sie müssen dieses Produkt an einem Ort auf den Markt bringen AWS-Region , an dem Amazon Cognito verfügbar ist. Die aktuelle Verfügbarkeit nach Regionen finden Sie in der Liste AWS-Region aller Services.
4. Überprüfen Sie unter Parameter die Parameter für diese Produktvorlage und ändern Sie sie nach Bedarf. Wenn Sie die automatisierten externen Ressourcen bereitgestellt haben, finden Sie diese Parameter auf der Registerkarte Ausgaben des Stacks für externe Ressourcen.

Parameter	Standard	Beschreibung
EnvironmentName	`<res-demo>`	Ein eindeutiger Name für Ihre RES-Umgebung, der mit

Parameter	Standard	Beschreibung
		res- beginnt und nicht länger als 11 Zeichen ist.
AdministratorEmail		Die E-Mail-Adresse des Benutzers, der die Installation des Produkts abschließt. Dieser Benutzer fungiert außerdem als Sicherheitsbenutzer, falls die Active Directory-Single-Sign-On-Integration fehlschlägt.
InfrastructureHostAMI	ami- *[numbers or letters only]*	(Optional) Sie können eine benutzerdefinierte AMI-ID angeben, die für alle Infrastruktur-Hosts verwendet werden soll. Das derzeit unterstützte Basisbetriebssystem ist Amazon Linux 2. Weitere Informationen finden Sie unter RES-Ready konfigurieren AMIs.
SSHKeyPaar		Das key pair, das für die Verbindung zu Infrastrukturhosts verwendet wird.
ClientIP	*x.x.x*.0/24 oder .0/32 *x.x.x*	IP-Adressfilter, der die Verbindung zum System einschränkt. Sie können den ClientIpCidr nach der Bereitstellung aktualisieren.

Parameter	Standard	Beschreibung
ClientPrefixList		(Optional) Stellen Sie eine verwaltete Präfixliste für IPs den direkten Zugriff auf die Weboberfläche und SSH auf den Bastion-Host bereit.
IAMPermissionGrenze		(Optional) Sie können einen ARN für verwaltete Richtlinien angeben, der als Berechtigungsgrenze an alle in RES erstellten Rollen angehängt wird. Weitere Informationen finden Sie unter Benutzerdefinierte Berechtigungsgrenzen festlegen.
VpcId		IP für die VPC, auf der Instances gestartet werden.
IsLoadBalancerInternetFacing		Wählen Sie „True“, um einen mit dem Internet verbundenen Load Balancer bereitzustellen (erfordert öffentliche Subnetze für den Load Balancer). Wählen Sie für Bereitstellungen, die einen eingeschränkten Internetzugang benötigen, Falsch aus.

Parameter	Standard	Beschreibung
LoadBalancerSubnets		Wählen Sie mindestens zwei Subnetze in verschiedenen Availability Zones aus, in denen Load Balancer gestartet werden. Wählen Sie für Bereitstellungen, die einen eingeschränkten Internetzugang benötigen, private Subnetze. Wählen Sie für Bereitstellungen, die Internetzugang benötigen, öffentliche Subnetze. Wenn mehr als zwei vom externen Netzwerkstapel erstellt wurden, wählen Sie alle aus, die erstellt wurden.
InfrastructureHostSubnets		Wählen Sie mindestens zwei private Subnetze in verschiedenen Availability Zones aus, in denen Infrastruktur-Hosts gestartet werden. Wenn mehr als zwei vom externen Netzwerkstapel erstellt wurden, wählen Sie alle aus, die erstellt wurden.

Parameter	Standard	Beschreibung
VdiSubnets		Wählen Sie mindestens zwei private Subnetze in verschiedenen Availability Zones aus, in denen VDI-Instanzen gestartet werden. Wenn mehr als zwei vom externen Netzwerkstapel erstellt wurden, wählen Sie alle aus, die erstellt wurden.
ActiveDirectoryName	`corp.res.com`	Domäne für das Active Directory. Er muss nicht mit dem Domainnamen des Portals übereinstimmen.
ADShortName	`corp`	Der Kurzname für das Active Directory. Dies wird auch als NetBIOS-Name bezeichnet.
LDAP-Basis	***DC=corp,DC=res,DC=com***	Ein LDAP-Pfad zur Basis innerhalb der LDAP-Hier archie.
LDAPConnectionURI		Ein einzelner Ldap://-P fad, der vom Hostserve r des Active Directory erreicht werden kann. Wenn Sie die automatisierten externen Ressourcen mit der Standard-AD-Domäne bereitgestellt haben, können Sie ldap: //corp.res.com verwenden.

Parameter	Standard	Beschreibung
ServiceAccountUserName	ServiceAccount	Benutzername für ein Dienstkonto, das für die Verbindung mit AD verwendet wird. Dieses Konto muss Zugriff haben, um Computer innerhalb der ComputerSOU zu erstellen.
ServiceAccountPass wordSecretArn		Geben Sie einen geheimen ARN an, der das Klartext-Passwort für enthält. ServiceAccount
Benutzer SOU		Organisationseinheit innerhalb von AD für Benutzer, die synchronisiert werden.
Gruppen, OU		Organisationseinheit innerhalb von AD für Gruppen, die synchronisiert werden.
SudoerSou		Organisationseinheit innerhalb von AD für globale Sudoer.
SudoersGroupName	RESAdministrators	Gruppenname, der alle Benutzer mit Sudoer-Zu griff auf Instanzen bei der Installation und Administr atorzugriff auf RES enthält.
Computer SOU		Organisationseinheit innerhalb von AD, der Instanzen beitreten werden.

Parameter	Standard	Beschreibung
TLSCertificateDomain-SekretarN		(Optional) Stellen Sie einen geheimen ARN für ein Domain-TLS-Zertifikat bereit, um die TLS-Kommunikation mit AD zu ermöglichen.
EnableLdapIDMapping		Ermittelt, ob UID- und GID-Nummern von SSSD generiert werden oder ob die vom AD bereitgestellten Nummern verwendet werden. Auf True setzen, um SSSD-generierte UID und GID zu verwenden, oder auf False, um die vom AD bereitgestellte UID und GID zu verwenden. In den meisten Fällen sollte dieser Parameter auf True gesetzt werden.
Deaktivieren ADJoin	False	Um zu verhindern, dass Linux-Hosts der Verzeichnisdomäne beitreten, ändern Sie zu True. Andernfalls behalten Sie die Standardeinstellung False bei.
ServiceAccountUserDN		Geben Sie den eindeutigen Namen (DN) des Dienstkontobenutzers im Verzeichnis an.

Parameter	Standard	Beschreibung
SharedHomeFilesystemID		Eine EFS-ID, die für das Shared Home-Date isystem für Linux-VDI-Hosts verwendet werden soll.
CustomDomainNamefo rWebApp		(Optional) Subdomain, die vom Webportal verwendet wird, um Links für den Webteil des Systems bereitzustellen.
CustomDomainNameforVDI		(Optional) Subdomain, die vom Webportal verwendet wird, um Links für den VDI-Teil des Systems bereitzus tellen.

Parameter	Standard	Beschreibung
ACMCertificateARNforWebApp		(Optional) Bei Verwendung der Standardkonfiguration hostet das Produkt die Webanwendung unter der Domain amazonaws.com. Sie können die Produktservices unter Ihrer Domain hosten. Wenn Sie die automatisierten externen Ressourcen bereitgestellt haben, wurden diese für Sie generiert. Die Informationen finden Sie in den Ausgaben des Res-Bi-Stacks. Informationen zum Generieren eines Zertifikats für Ihre Webanwendung finden Sie unter. Leitfaden zur Konfiguration
CertificateSecretARNforVDI		(Optional) Dieses ARN-Geheimnis speichert das öffentliche Zertifikat für das öffentliche Zertifikat Ihres Webportals. Wenn Sie einen Portaldomänennamen für Ihre automatisierten externen Ressourcen festlegen, finden Sie diesen Wert auf der Registerkarte Ausgaben des Res-Bi-Stacks.

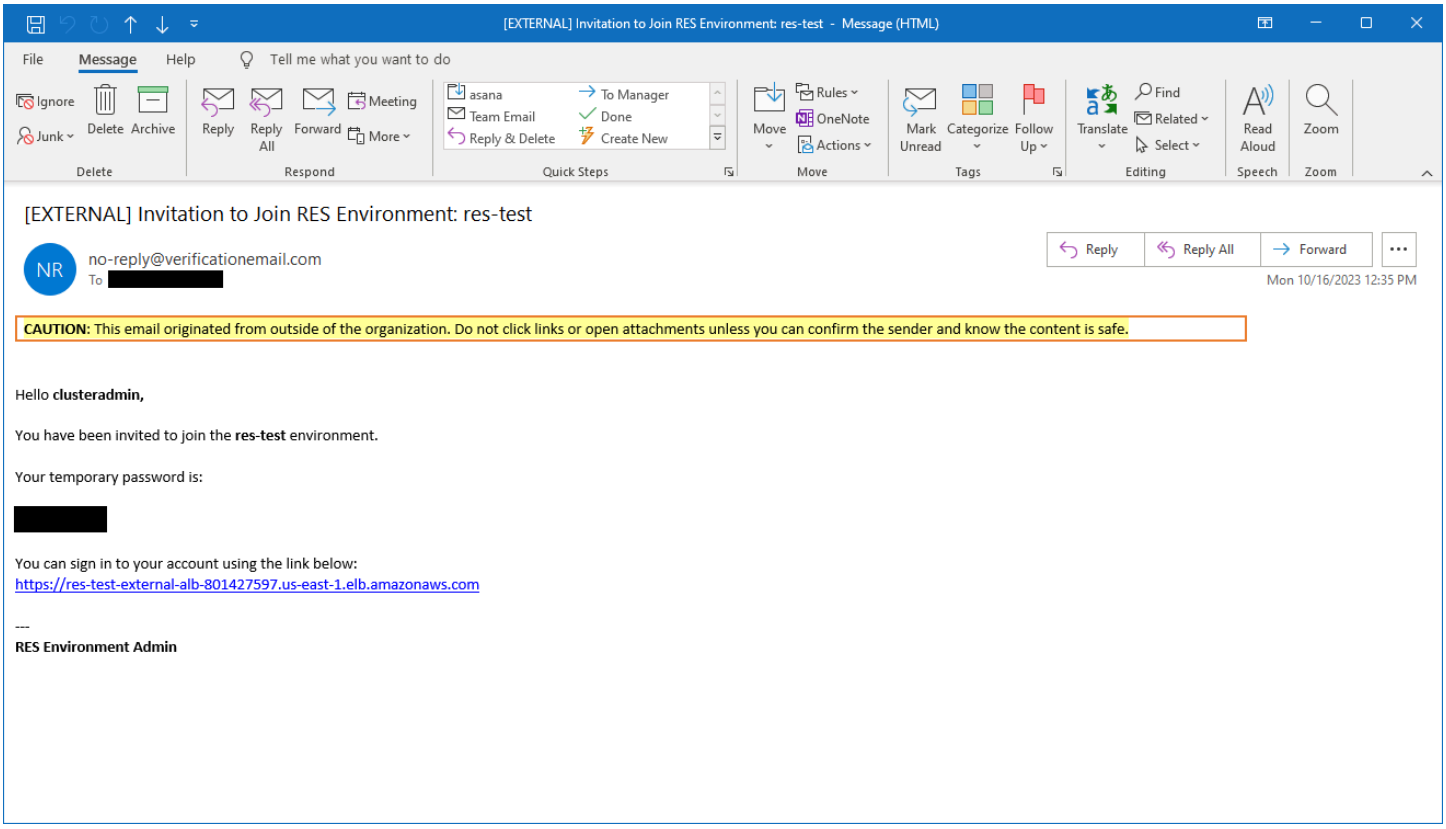
Parameter	Standard	Beschreibung
PrivateKeySecretARNforVDI		(Optional) Dieses ARN-Geheimnis speichert den privaten Schlüssel für das Zertifikat Ihres Webportals. Wenn Sie einen Portaldomänennamen für Ihre automatisierten externen Ressourcen festlegen, finden Sie diesen Wert auf der Registerkarte Ausgaben des Res-Bi-Stacks.

5. Wählen Sie Stack erstellen aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation Konsole in der Spalte Status einsehen. Sie sollten in etwa 60 Minuten den Status CREATE_COMPLETE erhalten.

Schritt 2: Melden Sie sich zum ersten Mal an

Sobald der Produkt-Stack in Ihrem Konto bereitgestellt wurde, erhalten Sie eine E-Mail mit Ihren Anmeldeinformationen. Verwenden Sie die URL, um sich bei Ihrem Konto anzumelden und den Workspace für andere Benutzer zu konfigurieren.



Nachdem Sie sich zum ersten Mal angemeldet haben, können Sie im Webportal Einstellungen konfigurieren, um eine Verbindung zum SSO-Anbieter herzustellen. Informationen zur Konfiguration nach der Bereitstellung finden Sie unterLeitfaden zur Konfiguration. Beachten Sie, dass es `clusteradmin` sich um ein erstklassiges Konto handelt. Sie können es verwenden, um Projekte zu erstellen und diesen Projekten Benutzer- oder Gruppenmitgliedschaften zuzuweisen. Es kann keine Software-Stacks zuweisen oder einen Desktop für sich selbst bereitstellen.

Aktualisiere das Produkt

Research and Engineering Studio (RES) bietet zwei Methoden zur Aktualisierung des Produkts, die davon abhängen, ob es sich um ein größeres oder ein kleines Versionsupdate handelt.

RES verwendet ein datumsbasiertes Versionsschema. Eine Hauptversion verwendet das Jahr und den Monat, und eine Nebenversion fügt bei Bedarf eine Sequenznummer hinzu. Beispielsweise wurde Version 2024.01 im Januar 2024 als Hauptversion veröffentlicht; Version 2024.01.01 war ein Nebenversionsupdate dieser Version.

Themen

- Aktualisierungen der Hauptversionen
- Kleinere Versionsupdates

Aktualisierungen der Hauptversionen

Research and Engineering Studio verwendet Snapshots, um die Migration von einer früheren RES-Umgebung zur neuesten zu unterstützen, ohne dass Ihre Umgebungseinstellungen verloren gehen. Sie können diesen Prozess auch verwenden, um Updates für Ihre Umgebung zu testen und zu verifizieren, bevor Sie Benutzer einbinden.

So aktualisieren Sie Ihre Umgebung mit der neuesten Version von RES:

1. Erstellen Sie einen Snapshot Ihrer aktuellen Umgebung. Siehe the section called “Snapshot erstellen”.
2. Stellen Sie RES mit der neuen Version erneut bereit. Siehe the section called “Schritt 1: Starten Sie das Produkt”.
3. Wenden Sie den Snapshot auf Ihre aktualisierte Umgebung an. Siehe the section called “Wenden Sie einen Snapshot an”.
4. Stellen Sie sicher, dass alle Daten erfolgreich in die neue Umgebung migriert wurden.

Kleinere Versionsupdates

Für kleinere Versionsupdates von RES ist keine Neuinstallation erforderlich. Sie können den vorhandenen RES-Stack aktualisieren, indem Sie seine AWS CloudFormation Vorlage aktualisieren.

Überprüfen Sie die Version Ihrer aktuellen RES-Umgebung, AWS CloudFormation bevor Sie das Update bereitstellen. Die Versionsnummer finden Sie am Anfang der Vorlage.

Beispiel: `"Description": "RES_2024.1"`

Um ein kleines Versionsupdate durchzuführen:

1. Laden Sie die neueste AWS CloudFormation Vorlage unter herunterthe section called “Schritt 1: Starten Sie das Produkt”.
2. Öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
3. Suchen Sie unter Stacks den primären Stack und wählen Sie ihn aus. Er sollte als *<stack-name>* erscheinen.
4. Wählen Sie Aktualisieren.
5. Wählen Sie Aktuelle Vorlage ersetzen.
6. Wählen Sie unter Templete source (Vorlagenquelle) den Wert Upload a template file (Vorlagendatei hochladen) aus.
7. Wählen Sie Datei auswählen und laden Sie die Vorlage hoch, die Sie heruntergeladen haben.
8. Wählen Sie unter Stackdetails angeben die Option Weiter aus. Sie müssen die Parameter nicht aktualisieren.
9. Wählen Sie unter Stack-Optionen konfigurieren die Option Weiter aus.
10. Wählen Sie unter Überprüfen <stack-name>die Option Senden aus.

Deinstalliere das Produkt

Sie können das Research and Engineering Studio auf dem Produkt von oder mit dem deinstallieren. AWS AWS Management Console AWS Command Line Interface Sie müssen die mit diesem Produkt erstellten Amazon Simple Storage Service (Amazon S3) -Buckets manuell löschen. Dieses Produkt löscht < EnvironmentName >- nicht automatisch, shared-storage-security-group falls Sie Daten zur Aufbewahrung gespeichert haben.

Mit dem AWS Management Console

1. Melden Sie sich an der AWS CloudFormation -Konsole an.
2. Wählen Sie auf der Seite Stacks den Installations-Stack dieses Produkts aus.
3. Wählen Sie Löschen aus.

Verwenden AWS Command Line Interface

Ermitteln Sie, ob AWS Command Line Interface (AWS CLI) in Ihrer Umgebung verfügbar ist. Installationsanweisungen finden Sie unter Was ist das AWS Command Line Interface im AWS CLI Benutzerhandbuch. Nachdem Sie AWS CLI sich vergewissert haben, dass das für das Administratorkonto in der Region, in der das Produkt bereitgestellt wurde, verfügbar und konfiguriert ist, führen Sie den folgenden Befehl aus.

```
$ aws cloudformation delete-stack --stack-name
<RES-stack-name>
```

Löschen des shared-storage-security-group

> **Warning**
>
> Das Produkt behält dieses Dateisystem standardmäßig bei, um vor unbeabsichtigtem Datenverlust zu schützen. Wenn Sie sich dafür entscheiden, die Sicherheitsgruppe und die zugehörigen Dateisysteme zu löschen, werden alle in diesen Systemen gespeicherten Daten dauerhaft gelöscht. Wir empfehlen, Daten zu sichern oder die Daten einer neuen Sicherheitsgruppe zuzuweisen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon EFS-Konsole unter https://console.aws.amazon.com/efs/.
2. Löschen Sie alle Dateisysteme, die mit `<RES-stack-name>` - verknüpft sindshared-storage-security-group. Alternativ können Sie diese Dateisysteme einer anderen Sicherheitsgruppe zuweisen, um die Daten zu verwalten.
3. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
4. Löschen Sie das `<RES-stack-name>` -shared-storage-security-group.

Löschen der Amazon S3 S3-Buckets

Dieses Produkt ist so konfiguriert, dass der vom Produkt erstellte Amazon S3 S3-Bucket (für die Bereitstellung in einer Opt-in-Region) beibehalten wird, falls Sie sich entscheiden, den AWS CloudFormation Stack zu löschen, um versehentlichen Datenverlust zu verhindern. Nach der Deinstallation des Produkts können Sie diesen S3-Bucket manuell löschen, wenn Sie die Daten nicht behalten müssen. Gehen Sie wie folgt vor, um den Amazon S3 S3-Bucket zu löschen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich Buckets aus.
3. Suchen Sie die `stack-name` S3-Buckets.
4. Wählen Sie jeden Amazon S3 S3-Bucket aus und wählen Sie dann Leer. Sie müssen jeden Bucket leeren.
5. Wählen Sie den S3-Bucket aus und wählen Sie Löschen.

Um S3-Buckets mit zu löschen AWS CLI, führen Sie den folgenden Befehl aus:

```
$ aws s3 rb s3://<bucket-name> --force
```

> **Note**
>
> Der `--force` Befehl leert den Inhalt des Buckets.

Leitfaden zur Konfiguration

Dieser Konfigurationshandbuch enthält nach der Bereitstellung Anleitungen für technische Anwender zur weiteren Anpassung und Integration mit dem Research and Engineering Studio auf dem Produkt. AWS

Themen

- Benutzer und Gruppen verwalten
- Subdomains erstellen
- Erstellen Sie ein ACM-Zertifikat
- CloudWatch Amazon-Protokolle
- Benutzerdefinierte Berechtigungsgrenzen festlegen
- RES-Ready konfigurieren AMIs

Benutzer und Gruppen verwalten

Research and Engineering Studio kann jeden SAML 2.0-kompatiblen Identitätsanbieter verwenden. Wenn Sie RES mithilfe der externen Ressourcen bereitgestellt haben oder planen, IAM Identity Center zu verwenden, finden Sie weitere Informationen unter. Single Sign-On (SSO) mit IAM Identity Center einrichten Wenn Sie über einen eigenen SAML 2.0-kompatiblen Identitätsanbieter verfügen, finden Sie weitere Informationen unter. Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)

Themen

- Single Sign-On (SSO) mit IAM Identity Center einrichten
- Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)
- Passwörter für Benutzer einrichten

Single Sign-On (SSO) mit IAM Identity Center einrichten

Wenn Sie noch kein Identity Center haben, das mit dem verwalteten Active Directory verbunden ist, beginnen Sie mitSchritt 1: Richten Sie ein Identitätscenter ein. Wenn Sie bereits ein Identity Center haben, das mit dem verwalteten Active Directory verbunden ist, beginnen Sie mitSchritt 2: Connect zu einem Identitätscenter her.

> **Note**
>
> Wenn Sie in der Region AWS GovCloud (USA West) bereitstellen, richten Sie SSO in dem AWS GovCloud (US) Partitionskonto ein, in dem Sie Research and Engineering Studio bereitgestellt haben.

Schritt 1: Richten Sie ein Identitätscenter ein

IAM Identity Center aktivieren

1. Melden Sie sich an der AWS Identity and Access Management -Konsole an.
2. Öffnen Sie das Identity Center.
3. Wählen Sie Enable (Aktivieren).
4. Wählen Sie Aktivieren mit AWS Organizations.
5. Wählen Sie Weiter aus.

> **Note**
>
> Stellen Sie sicher, dass Sie sich in derselben Region befinden, in der Sie Ihr verwaltetes Active Directory haben.

IAM Identity Center mit einem verwalteten Active Directory verbinden

Nachdem Sie IAM Identity Center aktiviert haben, führen Sie die folgenden empfohlenen Einrichtungsschritte durch:

1. Wählen Sie im Navigationsbereich Einstellungen aus.
2. Wählen Sie unter Identitätsquelle die Option Aktionen und dann Identitätsquelle ändern aus.
3. Wählen Sie unter Bestehende Verzeichnisse Ihr Verzeichnis aus.
4. Klicken Sie auf Weiter.
5. Überprüfen Sie Ihre Änderungen und geben Sie sie **`ACCEPT`** in das Bestätigungsfeld ein.
6. Wählen Sie Identitätsquelle ändern aus.

Benutzer und Gruppen mit Identity Center synchronisieren

Sobald die vorgenommenen Änderungen abgeschlossen IAM Identity Center mit einem verwalteten Active Directory verbinden sind, erscheint ein grünes Bestätigungsbanner.

1. Wählen Sie im Bestätigungsbanner die Option Geführte Einrichtung starten aus.
2. Wählen Sie unter Attributzuordnungen konfigurieren die Option Weiter aus.
3. Geben Sie im Abschnitt Benutzer die Benutzer ein, die Sie synchronisieren möchten.
4. Wählen Sie Hinzufügen aus.
5. Klicken Sie auf Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie dann Konfiguration speichern aus.
7. Der Synchronisierungsvorgang kann einige Minuten dauern. Wenn Sie eine Warnmeldung darüber erhalten, dass Benutzer nicht synchronisieren, wählen Sie Synchronisierung fortsetzen aus.

Aktivieren von Benutzern

1. Wählen Sie im Menü Benutzer aus.
2. Wählen Sie die Benutzer aus, für die Sie den Zugriff aktivieren möchten.
3. Wählen Sie Benutzerzugriff aktivieren aus.

Schritt 2: Connect zu einem Identitätscenter her

Einrichtung der Anwendung im IAM Identity Center

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Anwendungen aus.
3. Wählen Sie Anwendung hinzufügen aus.
4. Wählen Sie unter Setup-Einstellungen die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
5. Wählen Sie unter Anwendungstyp die Option SAML 2.0 aus.
6. Klicken Sie auf Weiter.
7. Geben Sie den Anzeigenamen und die Beschreibung ein, die Sie verwenden möchten.

8. Kopieren Sie unter IAM Identity Center-Metadaten den Link für die SAML-Metadatendatei von IAM Identity Center. Sie benötigen dies, wenn Sie IAM Identity Center mit dem RES-Portal konfigurieren.
9. Geben Sie unter Anwendungseigenschaften die Start-URL Ihrer Anwendung ein. Beispiel, `<your-portal-domain>/sso`.
10. Geben Sie unter ACS-URL der Anwendung die Umleitungs-URL aus dem RES-Portal ein. Um das zu finden:
    a. Wählen Sie unter Umgebungsmanagement die Option Allgemeine Einstellungen aus.
    b. Wählen Sie die Registerkarte Identity provider.
    c. Unter Single Sign-On finden Sie die SAML-Umleitungs-URL.
11. Geben Sie unter Anwendungs-SAML-Zielgruppe die Amazon Cognito Cognito-URN ein.

    Um die Urne zu erstellen:

    a. Öffnen Sie im RES-Portal die Allgemeinen Einstellungen.
    b. Suchen Sie auf der Registerkarte Identitätsanbieter nach der Benutzerpool-ID.
    c. Fügen Sie die Benutzerpool-ID zu dieser Zeichenfolge hinzu:

    ```
    urn:amazon:cognito:sp:<user_pool_id>
    ```

12. Nachdem Sie die Amazon Cognito Cognito-URN eingegeben haben, wählen Sie Senden aus.

Konfiguration von Attributzuordnungen für die Anwendung

1. Öffnen Sie im Identity Center die Details für Ihre erstellte Anwendung.
2. Wählen Sie Aktionen und dann Attributzuordnungen bearbeiten aus.
3. Geben Sie unter Betreff ein. **`${user:email}`**
4. Wählen Sie unter Format die Option E-Mail-Adresse aus.
5. Wählen Sie Neue Attributzuordnung hinzufügen aus.
6. Geben Sie in der Anwendung unter Benutzerattribut „E-Mail“ ein.
7. Geben Sie unter Zuordnungen zu diesem Zeichenkettenwert oder Benutzerattribut in IAM Identity Center den folgenden Wert ein. **`${user:email}`**
8. Geben Sie unter Format den Wert „nicht spezifiziert“ ein.
9. Wählen Sie Änderungen speichern aus.

Benutzer zur Anwendung in IAM Identity Center hinzufügen

1. Öffnen Sie im Identity Center die Option Zugewiesene Benutzer für Ihre erstellte Anwendung und wählen Sie Benutzer zuweisen aus.
2. Wählen Sie die Benutzer aus, denen Sie Anwendungszugriff zuweisen möchten.
3. Wählen Sie Benutzer zuweisen aus.

IAM Identity Center in der RES-Umgebung einrichten

1. Öffnen Sie in der Research and Engineering Studio-Umgebung unter Umgebungsmanagement die Option Allgemeine Einstellungen.
2. Öffnen Sie die Registerkarte Identitätsanbieter.
3. Wählen Sie unter Single Sign-On die Option Bearbeiten (neben Status) aus.
4. Füllen Sie das Formular mit den folgenden Informationen aus:
   a. Wählen Sie SAML.
   b. Geben Sie unter Anbietername einen benutzerfreundlichen Namen ein.
   c. Wählen Sie Endpunkt-URL für das Metadaten-Dokument eingeben aus.
   d. Geben Sie die URL ein, die Sie währenddessen kopiert habenEinrichtung der Anwendung im IAM Identity Center.
   e. Geben Sie unter E-Mail-Attribut des Anbieters „E-Mail“ ein.
   f. Wählen Sie Absenden aus.
5. Aktualisieren Sie die Seite und überprüfen Sie, ob der Status als aktiviert angezeigt wird.

Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)

Research and Engineering Studio lässt sich in jeden SAML 2.0-Identitätsanbieter integrieren, um den Benutzerzugriff auf das RES-Portal zu authentifizieren. Diese Schritte enthalten Anweisungen zur Integration mit dem von Ihnen ausgewählten SAML 2.0-Identitätsanbieter. Wenn Sie beabsichtigen, IAM Identity Center zu verwenden, finden Sie weitere Informationen unter. the section called “SSO mit IAM Identity Center einrichten”

> **Note**
>
> Die E-Mail-Adresse des Benutzers muss in der IDP-SAML-Assertion und in Active Directory übereinstimmen. Sie müssen Ihren Identitätsanbieter mit Ihrem Active Directory verbinden und Benutzer regelmäßig synchronisieren.

Themen

- Konfigurieren Sie Ihren Identitätsanbieter
- Konfigurieren Sie RES für die Verwendung Ihres Identitätsanbieters
- Konfiguration Ihres Identitätsanbieters in einer Umgebung außerhalb der Produktionsumgebung
- Debuggen von SAML-IdP-Problemen

Konfigurieren Sie Ihren Identitätsanbieter

Dieser Abschnitt enthält die Schritte zur Konfiguration Ihres Identitätsanbieters mit Informationen aus dem RES Amazon Cognito Cognito-Benutzerpool.

1. RES geht davon aus, dass Sie über ein AD (AWS Managed AD oder ein selbst bereitgestelltes AD) mit den Benutzeridentitäten verfügen, die Zugriff auf das RES-Portal und die Projekte haben. Connect Sie Ihr AD mit Ihrem Identitätsdienstanbieter und synchronisieren Sie die Benutzeridentitäten. In der Dokumentation Ihres Identitätsanbieters erfahren Sie, wie Sie Ihr AD verbinden und Benutzeridentitäten synchronisieren. Weitere Informationen finden Sie beispielsweise unter Verwenden von Active Directory als Identitätsquelle im AWS IAM Identity Center Benutzerhandbuch.
2. Konfigurieren Sie eine SAML 2.0-Anwendung für RES in Ihrem Identity Provider (IdP). Für diese Konfiguration sind die folgenden Parameter erforderlich:
   - SAML-Umleitungs-URL — Die URL, die Ihr IdP verwendet, um die SAML 2.0-Antwort an den Dienstanbieter zu senden.

     > **Note**
     >
     > Je nach IdP kann die SAML-Umleitungs-URL einen anderen Namen haben:
     >
     > - URL der Anwendung
     > - URL des Assertion Consumer Service (ACS)

- ACS-POST-Bindungs-URL

Um die URL zu erhalten

1. Melden Sie sich bei RES als Administrator oder Clusteradmin an.
2. Navigieren Sie zu Environment Management ⇒ Allgemeine Einstellungen ⇒ Identity Provider.
3. Wählen Sie SAML-Umleitungs-URL.

- SAML-Zielgruppen-URI — Die eindeutige ID der SAML-Zielgruppenentität auf der Seite des Dienstanbieters.

> **Note**
>
> Je nach IdP kann die SAML-Zielgruppen-URI einen anderen Namen haben:
>
> - ClientID
> - SAML-Zielgruppe der Anwendung
> - SP-Entitäts-ID

Geben Sie die Eingabe im folgenden Format an.

```
urn:amazon:cognito:sp:user-pool-id
```

Um Ihre SAML-Zielgruppen-URI zu finden

1. Melden Sie sich bei RES als Administrator oder Clusteradmin an.
2. Navigieren Sie zu Environment Management ⇒ Allgemeine Einstellungen ⇒ Identity Provider.
3. Wählen Sie Benutzerpool-ID.

3. Für die SAML-Assertion, die an RES gesendet wird, muss die E-Mail-Adresse des Benutzers wie folgt fields/claims festgelegt sein:

- SAML-Betreff oder NameID

- SAML-E-Mail

4. Ihr IdP trägt je fields/claims nach Konfiguration zur SAML-Assertion bei. RES benötigt diese Felder. Die meisten Anbieter füllen diese Felder standardmäßig automatisch aus. Beachten Sie die folgenden Feldeingaben und Werte, wenn Sie sie konfigurieren müssen.

   - AudienceRestriction— Eingestellt auf`urn:amazon:cognito:sp:`*`user-pool-id`*. *`user-pool-id`*Ersetzen Sie es durch die ID Ihres Amazon Cognito Cognito-Benutzerpools.

     ```
     <saml:AudienceRestriction>
         <saml:Audience> urn:amazon:cognito:sp:user-pool-id
     </saml:AudienceRestriction>
     ```

   - Antwort — Eingestellt `InResponseTo` auf. `https://`*`user-pool-domain`*`/saml2/idpresponse` *`user-pool-domain`*Ersetzen Sie es durch den Domainnamen Ihres Amazon Cognito Cognito-Benutzerpools.

     ```
     <saml2p:Response
       Destination="http://user-pool-domain/saml2/idpresponse"
       ID="id123"
       InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
       IssueInstant="Date-time stamp"
       Version="2.0"
       xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:xs="http://www.w3.org/2001/XMLSchema">
     ```

   - SubjectConfirmationData— Stellen Sie `Recipient` Ihren `saml2/idpresponse` Benutzerpool-Endpunkt und `InResponseTo` die ursprüngliche SAML-Anforderungs-ID ein.

     ```
     <saml2:SubjectConfirmationData
       InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
       NotOnOrAfter="Date-time stamp"
       Recipient="https://user-pool-domain/saml2/idpresponse"/>
     ```

   - AuthnStatement— Konfigurieren Sie wie folgt:

     ```
     <saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
       SessionIndex="32413b2e54db89c764fb96ya2k"
      SessionNotOnOrAfter="2016-10-30T13:13:28">
         <saml2:SubjectLocality />
         <saml2:AuthnContext>
     ```

```
 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
```

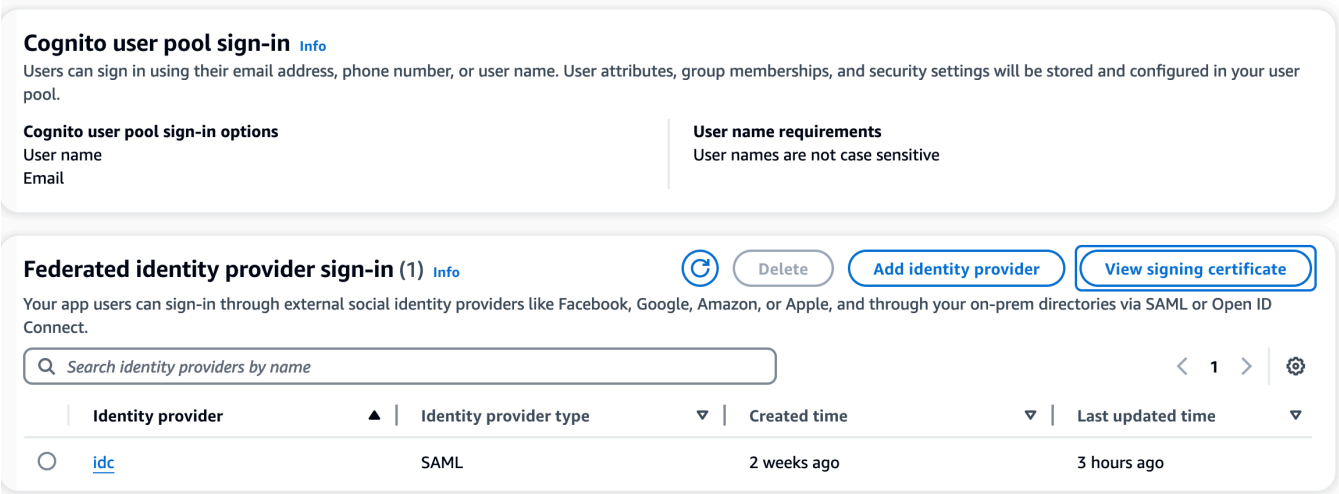
5. Wenn Ihre SAML-Anwendung über ein Abmelde-URL-Feld verfügt, setzen Sie es auf:. `<domain-url>/saml2/logout`

   Um die Domain-URL zu erhalten

   1. Melden Sie sich bei RES als Admin oder Clusteradmin an.
   2. Navigieren Sie zu Environment Management ⇒ Allgemeine Einstellungen ⇒ Identity Provider.
   3. Wählen Sie Domain-URL.
6. Wenn Ihr IdP ein Signaturzertifikat akzeptiert, um Vertrauen mit Amazon Cognito aufzubauen, laden Sie das Amazon Cognito-Signaturzertifikat herunter und laden Sie es in Ihren IdP hoch.

   Um das Signaturzertifikat zu erhalten

   1. Öffnen Sie die Amazon Cognito Cognito-Konsole in den Getting Started mit dem AWS Management Console
   2. Wählen Sie Ihren Benutzerpool aus. Ihr Benutzerpool sollte es sein`res-<environment name>-user-pool`.
   3. Wählen Sie die Registerkarte Sign-in experience (Anmeldeerlebnis) aus.
   4. Wählen Sie im Abschnitt Anmeldung mit dem Federated Identity Provider die Option Signaturzertifikat anzeigen aus.



Sie können dieses Zertifikat verwenden, um Active Directory-IDP einzurichten`relying party trust`, einen hinzuzufügen und die SAML-Unterstützung für diese vertrauende Partei zu aktivieren.

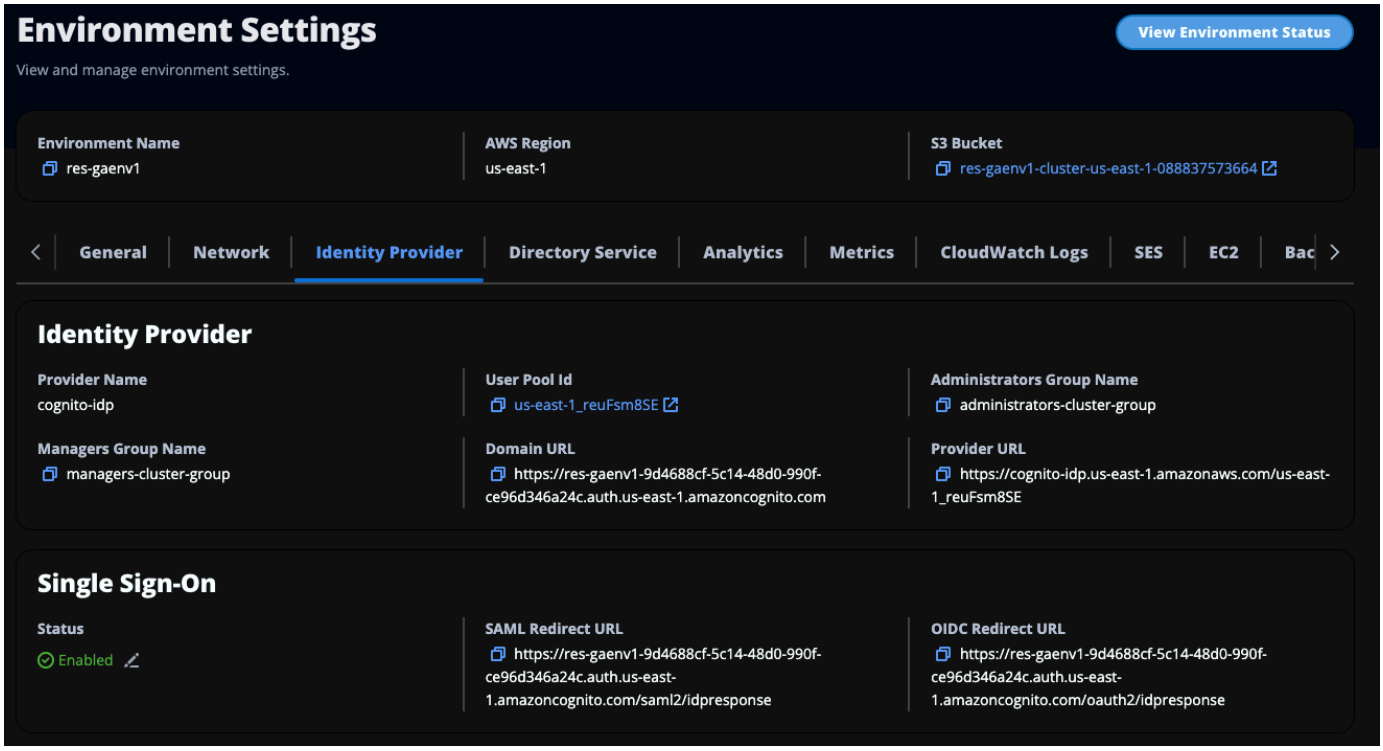
> **Note**
>
> Dies gilt nicht für Keycloak und IDC.

5. Nachdem die Einrichtung der Anwendung abgeschlossen ist, laden Sie die SAML 2.0-Anwendungsmetadaten (XML oder URL) herunter. Sie verwenden es im nächsten Abschnitt.

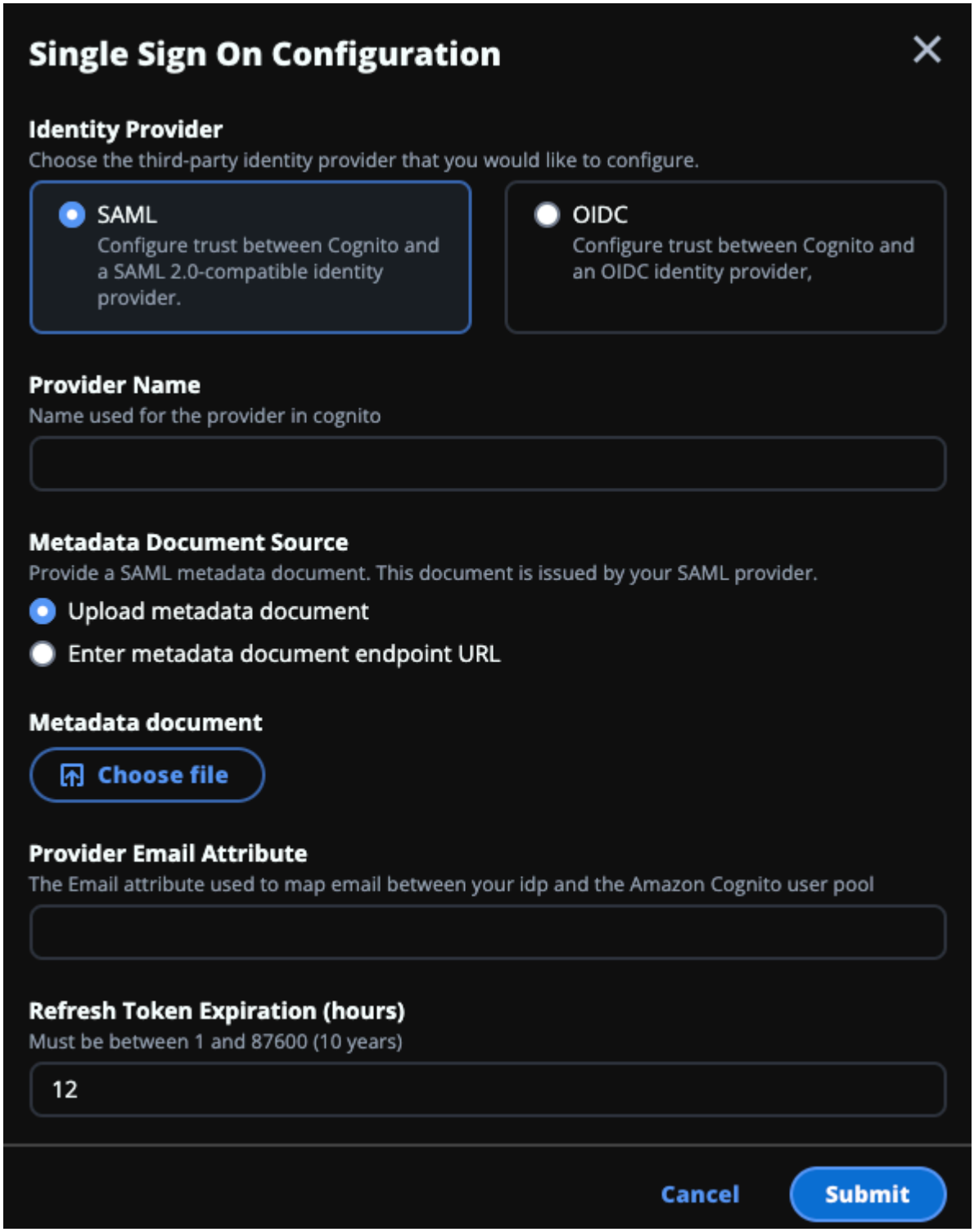
Konfigurieren Sie RES für die Verwendung Ihres Identitätsanbieters

Um das Single Sign-On-Setup für RES abzuschließen

1. Melden Sie sich bei RES als Administrator oder Clusteradmin an.
2. Navigieren Sie zu Environment Management ⇒ Allgemeine Einstellungen ⇒ Identity Provider.



3. Wählen Sie unter Single Sign-On das Bearbeitungssymbol neben der Statusanzeige, um die Seite Single Sign-On-Konfiguration zu öffnen.



a. Wählen Sie für Identity Provider die Option SAML aus.

b. Geben Sie unter Anbietername einen eindeutigen Namen für Ihren Identitätsanbieter ein.

> **Note**
>
> Die folgenden Namen sind nicht zulässig:
>
> - Cognito
> - IdentityCenter

c. Wählen Sie unter Metadaten-Dokumentquelle die entsprechende Option aus und laden Sie das Metadaten-XML-Dokument hoch oder geben Sie die URL vom Identitätsanbieter an.

d. Geben Sie für Provider-E-Mail-Attribut den Textwert ein`email`.

e. Wählen Sie Absenden aus.

4. Laden Sie die Seite mit den Umgebungseinstellungen neu. Single Sign-On ist aktiviert, wenn die Konfiguration korrekt war.

Konfiguration Ihres Identitätsanbieters in einer Umgebung außerhalb der Produktionsumgebung

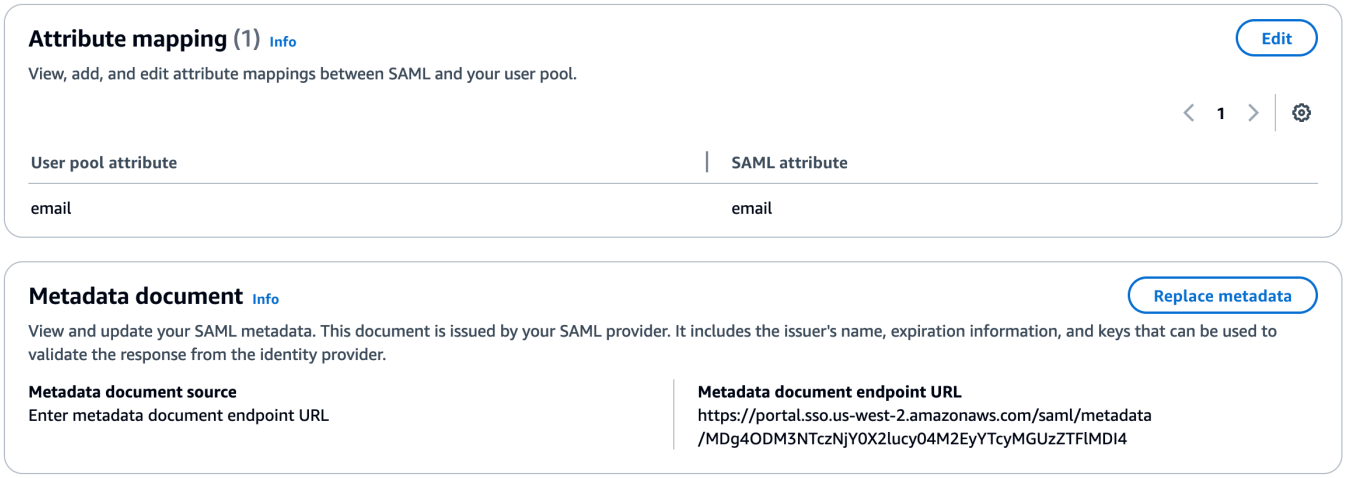
Wenn Sie die bereitgestellten externen Ressourcen verwendet haben, um eine RES-Umgebung außerhalb der Produktion zu erstellen, und IAM Identity Center als Ihren Identitätsanbieter konfiguriert haben, möchten Sie möglicherweise einen anderen Identitätsanbieter wie Okta konfigurieren. Das Formular zur RES-SSO-Aktivierung fragt nach drei Konfigurationsparametern:

1. Anbietername — Kann nicht geändert werden
2. Metadaten-Dokument oder URL — Kann geändert werden
3. E-Mail-Attribut des Anbieters — Kann geändert werden

Gehen Sie wie folgt vor, um das Metadatendokument und das E-Mail-Attribut des Anbieters zu ändern:

1. Melden Sie sich bei der Amazon-Cognito-Konsole an.
2. Wählen Sie in der Navigation die Option Benutzerpools aus.
3. Wählen Sie Ihren Benutzerpool aus, um die Übersicht über den Benutzerpool anzuzeigen.
4. Gehen Sie auf der Registerkarte Anmeldeerfahrung zur Anmeldung mit dem Federated Identity Provider und öffnen Sie Ihren konfigurierten Identity Provider.

5. Im Allgemeinen müssen Sie nur die Metadaten ändern und die Attributzuordnung unverändert lassen. Um die Attributzuordnung zu aktualisieren, wählen Sie Bearbeiten. Um das Metadatendokument zu aktualisieren, wählen Sie Metadaten ersetzen.



6. Wenn Sie die Attributzuordnung bearbeitet haben, müssen Sie die `<environment name>.cluster-settings` Tabelle in DynamoDB aktualisieren.

   a. Öffnen Sie die DynamoDB-Konsole und wählen Sie in der Navigation Tabellen aus.

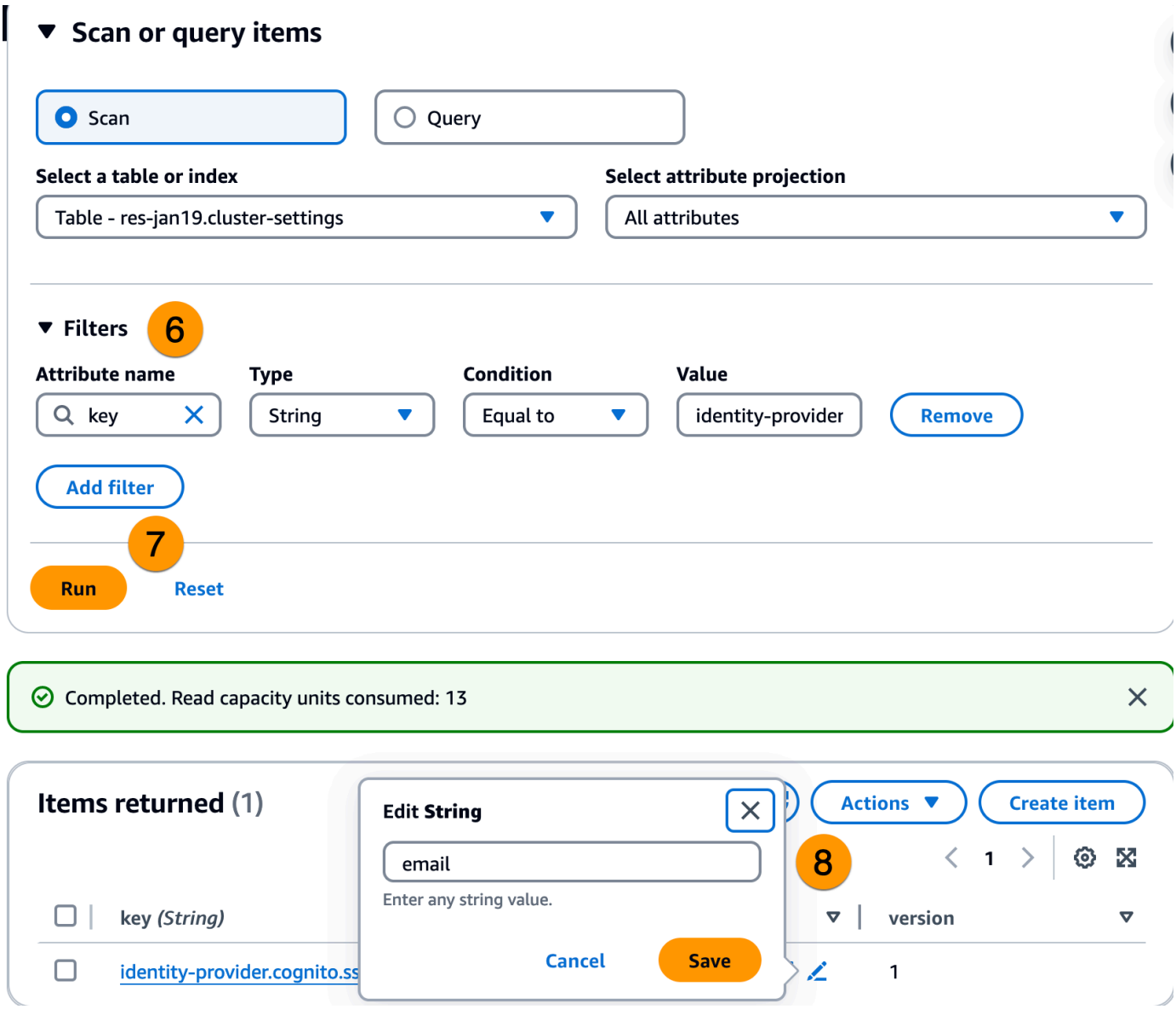
   b. Suchen Sie die **`<environment name>.cluster-settings`** Tabelle, wählen Sie sie aus und wählen Sie im Menü Aktionen die Option Elemente durchsuchen aus.

   c. Gehen Sie unter Elemente scannen oder abfragen zu Filter und geben Sie die folgenden Parameter ein:

      - Name des Attributs — `key`
      - Wert — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Wählen Sie Ausführen aus.

7. Suchen Sie unter Zurückgegebene Artikel nach der `identity-provider.cognito.sso_idp_provider_email_attribute` Zeichenfolge und wählen Sie Bearbeiten, um die Zeichenfolge so zu ändern, dass sie Ihren Änderungen in Amazon Cognito entspricht.



Debuggen von SAML-IdP-Problemen

SAML-Tracer — Sie können diese Erweiterung für den Chrome-Browser verwenden, um SAML-Anfragen zu verfolgen und die SAML-Assertion-Werte zu überprüfen. Weitere Informationen finden Sie unter SAML-Tracer im Chrome Web Store.

SAML-Entwicklertools — OneLogin stellt Tools bereit, mit denen Sie den SAML-codierten Wert dekodieren und die erforderlichen Felder in der SAML-Assertion überprüfen können. Weitere Informationen finden Sie auf der Website unter Base 64 Decode + Inflate. OneLogin

Amazon CloudWatch Logs — Sie können Ihre CloudWatch RES-Protokolle in Logs auf Fehler oder Warnungen überprüfen. Ihre Protokolle befinden sich in einer Protokollgruppe mit dem Namensformat`res-environment-name`/`cluster-manager`.

Amazon Cognito-Dokumentation — Weitere Informationen zur SAML-Integration mit Amazon Cognito finden Sie unter Hinzufügen von SAML-Identitätsanbietern zu einem Benutzerpool im Amazon Cognito Developer Guide.

Passwörter für Benutzer einrichten

1. Wählen Sie in der AWS Directory Service Konsole das Verzeichnis für den erstellten Stack aus.
2. Wählen Sie im Menü Aktionen die Option Benutzerpasswort zurücksetzen aus.
3. Wählen Sie den Benutzer aus und geben Sie ein neues Passwort ein.
4. Wählen Sie Passwort zurücksetzen.

Subdomains erstellen

Wenn Sie eine benutzerdefinierte Domain verwenden, müssen Sie Subdomänen einrichten, um die Web- und VDI-Teile Ihres Portals zu unterstützen.

> **Note**
>
> Wenn Sie die Bereitstellung in der Region AWS GovCloud (USA West) durchführen, richten Sie die Webanwendung und die VDI-Subdomänen im kommerziellen Partitionskonto ein, das die öffentlich gehostete Zone der Domäne hostet.

1. Öffnen Sie die Route 53 53-Konsole.
2. Suchen Sie die Domain, die Sie erstellt haben, und wählen Sie Create Record aus.
3. Geben Sie „web“ als Datensatznamen ein.
4. Wählen Sie CNAME als Datensatztyp.
5. Geben Sie unter Value den Link ein, den Sie in der ersten E-Mail erhalten haben.
6. Wählen Sie Create records (Datensätze erstellen).
7. Rufen Sie die NLB-Adresse ab, um einen Datensatz für das VDC zu erstellen.

   a. Öffnen Sie die AWS CloudFormation -Konsole.

   b. Wählen Sie `<environment-name>-vdc`.
   c. Wählen Sie Ressourcen und öffnen Sie`<environmentname>-vdc-external-nlb`.
   d. Kopieren Sie den DNS-Namen aus dem NLB.
8. Öffnen Sie die Route 53 53-Konsole.
9. Suchen Sie Ihre Domain und wählen Sie Create Record aus.
10. Geben Sie unter Datensatzname den Wert ein`vdc`.
11. Wählen Sie unter Datensatztyp die Option CNAME aus.
12. Geben Sie für den NLB den DNS ein.
13. Wählen Sie Datensatz erstellen.

Erstellen Sie ein ACM-Zertifikat

Standardmäßig hostet RES das Webportal unter einem Application Load Balancer, der die Domain amazonaws.com verwendet. Um Ihre eigene Domain zu verwenden, müssen Sie ein öffentliches SSL/TLS Zertifikat konfigurieren, das von Ihnen bereitgestellt oder von AWS Certificate Manager (ACM) angefordert wurde. Wenn Sie ACM verwenden, erhalten Sie einen AWS Ressourcennamen, den Sie als Parameter angeben müssen, um den SSL/TLS Kanal zwischen dem Client und dem Webservice-Host zu verschlüsseln.

> **Tip**
>
> Wenn Sie das Demopaket für externe Ressourcen bereitstellen, müssen Sie `PortalDomainName` bei der Bereitstellung des Stacks für externe Ressourcen die von Ihnen gewählte Domain eingeben. Externe Ressourcen erstellen

So erstellen Sie ein Zertifikat für benutzerdefinierte Domains:

1. Öffnen Sie die Konsole, AWS Certificate Managerum ein öffentliches Zertifikat anzufordern. Wenn Sie in AWS GovCloud (US-West) bereitstellen, erstellen Sie das Zertifikat in Ihrem GovCloud Partitionskonto.
2. Wählen Sie „Öffentliches Zertifikat anfordern“ und anschließend „Weiter“.
3. Fordern Sie unter Domainnamen ein Zertifikat für `*.PortalDomainName` sowohl als auch an`PortalDomainName`.
4. Wählen Sie unter Validierungsmethode die Option DNS-Validierung aus.

5. Wählen Sie Request (Anfrage).
6. Öffnen Sie in der Zertifikatsliste die angeforderten Zertifikate. Für jedes Zertifikat wird der Status Ausstehende Validierung angezeigt.

> **Note**
>
> Wenn Ihre Zertifikate nicht angezeigt werden, aktualisieren Sie die Liste.

7. Führen Sie eine der folgenden Aktionen aus:
   - Kommerzieller Einsatz:

     Wählen Sie in den Zertifikatsdetails für jedes angeforderte Zertifikat die Option Datensätze in Route 53 erstellen aus. Der Status des Zertifikats sollte in „Ausgestellt“ geändert werden.
   - GovCloud Bereitstellung:

     Wenn Sie in AWS GovCloud (US-West) bereitstellen, kopieren Sie den CNAME-Schlüssel und den CNAME-Wert. Verwenden Sie die Werte aus dem kommerziellen Partitionskonto, um einen neuen Datensatz in der Public Hosted Zone zu erstellen. Der Status des Zertifikats sollte in „Ausgestellt“ geändert werden.
8. Kopieren Sie den neuen Zertifikat-ARN zur Eingabe als Parameter für`ACMCertificateARNforWebApp`.

CloudWatch Amazon-Protokolle

Research and Engineering Studio erstellt CloudWatch während der Installation die folgenden Protokollgruppen. In der folgenden Tabelle finden Sie die Standardspeicherungen:

CloudWatch Gruppen protokollieren	Aufbewahrung
/aws/lambda/ < >-Cluster-Endpunkte installation-stack-name	Läuft niemals ab
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	Läuft niemals ab
/aws/lambda/ < >-cluster-einstellungen installation-stack-name	Läuft niemals ab

CloudWatch Gruppen protokollieren	Aufbewahrung
/aws/lambda/ < >-oauth-Anmeldeinformationen installation-stack-name	Läuft niemals ab
/aws/lambda/ < >- installation-stack-name self-signed-certificate	Läuft niemals ab
/aws/lambda/ < >- installation-stack-name update-cluster-prefix-list	Läuft niemals ab
/aws/lambda/ < >- installation-stack-name vdc-scheduled-event-transformer	Läuft niemals ab
/aws/lambda/ < >- -client-scope installation-stack-name vdc-update-cluster-manager	Läuft niemals ab
/< >/clustermanager installation-stack-name	3 Monate
/< >/vdc/controller installation-stack-name	3 Monate
/< >/vdc/dcv-broker installation-stack-name	3 Monate
/< >/vdc/ installation-stack-name dcv-connection-gateway	3 Monate

Wenn Sie die Standardspeicherung für eine Protokollgruppe ändern möchten, gehen Sie zur CloudWatch Konsole und folgen Sie den Anweisungen unter Logs unter CloudWatch Logs ändern.

Benutzerdefinierte Berechtigungsgrenzen festlegen

Ab 2024.04 können Sie optional von RES erstellte Rollen ändern, indem Sie benutzerdefinierte Berechtigungsgrenzen anhängen. Eine benutzerdefinierte Berechtigungsgrenze kann als Teil der AWS CloudFormation RES-Installation definiert werden, indem der ARN der Berechtigungsgrenze als Teil des IAMPermission Boundary-Parameters angegeben wird. Für RES-Rollen wird keine Berechtigungsgrenze festgelegt, wenn dieser Parameter leer gelassen wird. Im Folgenden finden Sie eine Liste der Aktionen, die für den Betrieb von RES-Rollen erforderlich sind. Stellen Sie sicher, dass jede Berechtigungsgrenze, die Sie verwenden möchten, ausdrücklich die folgenden Aktionen zulässt:

```
[
    {
        "Effect": "Allow",
        "Resource": "*",
        "Sid": "ResRequiredActions",
        "Action": [
            "access-analyzer:*",
            "account:GetAccountInformation",
            "account:ListRegions",
            "acm:*",
            "airflow:*",
            "amplify:*",
            "amplifybackend:*",
            "amplifyuibuilder:*",
            "aoss:*",
            "apigateway:*",
            "appflow:*",
            "application-autoscaling:*",
            "appmesh:*",
            "apprunner:*",
            "aps:*",
            "athena:*",
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
```

```
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
            "ecr:*",
            "ecs:*",
            "eks:*",
            "elastic-inference:*",
            "elasticache:*",
            "elasticbeanstalk:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "elasticmapreduce:*",
            "elastictranscoder:*",
            "es:*",
            "events:*",
            "firehose:*",
            "fis:*",
            "fms:*",
            "forecast:*",
            "fsx:*",
            "geo:*",
            "glacier:*",
            "glue:*",
            "grafana:*",
```

```
            "guardduty:*",
            "health:*",
            "iam:*",
            "identitystore:*",
            "imagebuilder:*",
            "inspector2:*",
            "inspector:*",
            "internetmonitor:*",
            "iot:*",
            "iotanalytics:*",
            "kafka:*",
            "kafkaconnect:*",
            "kinesis:*",
            "kinesisanalytics:*",
            "kms:*",
            "lambda:*",
            "lightsail:*",
            "logs:*",
            "memorydb:*",
            "mgh:*",
            "mobiletargeting:*",
            "mq:*",
            "neptune-db:*",
            "organizations:DescribeOrganization",
            "osis:*",
            "personalize:*",
            "pi:*",
            "pipes:*",
            "polly:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
            "resource-groups:*",
            "route53:*",
            "route53domains:*",
            "route53resolver:*",
            "rum:*",
            "s3:*",
```

```
            "sagemaker:*",
            "scheduler:*",
            "schemas:*",
            "sdb:*",
            "secretsmanager:*",
            "securityhub:*",
            "serverlessrepo:*",
            "servicecatalog:*",
            "servicequotas:*",
            "ses:*",
            "signer:*",
            "sns:*",
            "sqs:*",
            "ssm:*",
            "ssmmessages:*",
            "states:*",
            "storagegateway:*",
            "sts:*",
            "support:*",
            "tag:GetResources",
            "tag:GetTagKeys",
            "tag:GetTagValues",
            "textract:*",
            "timestream:*",
            "transcribe:*",
            "transfer:*",
            "translate:*",
            "vpc-lattice:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*",
            "wisdom:*",
            "xray:*"
        ]
    }
]
```

RES-Ready konfigurieren AMIs

Mit RES-Ready AMIs können Sie RES-Abhängigkeiten für virtuelle Desktop-Instanzen () VDIs auf Ihrem benutzerdefinierten System vorinstallieren. AMIs Mit RES-Ready AMIs verbessern Sie die

Startzeiten für VDI-Instanzen mithilfe der vorgefertigten Images. Mit EC2 Image Builder können Sie Ihre AMIs neuen Software-Stacks erstellen und registrieren. Weitere Informationen zu Image Builder finden Sie im Image Builder Builder-Benutzerhandbuch.

Bevor Sie beginnen, müssen Sie die neueste Version von RES bereitstellen.

Themen

- Bereiten Sie die IAM-Rolle für den Zugriff auf die RES-Umgebung vor
- EC2 Image Builder Builder-Komponente erstellen
- Bereiten Sie Ihr EC2 Image Builder Builder-Rezept vor
- EC2 Image Builder Builder-Infrastruktur konfigurieren
- Image Builder Builder-Image-Pipeline konfigurieren
- Image Builder Builder-Image-Pipeline ausführen
- Registrieren Sie einen neuen Software-Stack in RES

Bereiten Sie die IAM-Rolle für den Zugriff auf die RES-Umgebung vor

Um von EC2 Image Builder aus auf den RES-Umgebungsdienst zuzugreifen, müssen Sie eine IAM-Rolle namens RES- EC2 InstanceProfileForImageBuilder erstellen oder ändern. Informationen zur Konfiguration einer IAM-Rolle für die Verwendung in Image Builder finden Sie unter AWS Identity and Access Management (IAM) im Image Builder Builder-Benutzerhandbuch.

Ihre Rolle erfordert:

- Zu den vertrauenswürdigen Beziehungen gehört der EC2 Amazon-Service
- Amazon SSMManaged InstanceCore und EC2 InstanceProfileForImageBuilder Richtlinien
- Benutzerdefinierte RES-Richtlinie mit eingeschränktem DynamoDB- und Amazon S3 S3-Zugriff auf die bereitgestellte RES-Umgebung

  (Bei dieser Richtlinie kann es sich entweder um ein vom Kunden verwaltetes Dokument oder um ein vom Kunden integriertes Richtliniendokument handeln.)

Vertrauenswürdige Beziehungseinheit:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
            "Action": "sts:AssumeRole"
        }
    ]
}
```

RES-Richtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-
Account-ID}/idea/vdc/res-ready-install-script-packages/*"
        }
    ]
}
```

EC2 Image Builder Builder-Komponente erstellen

Folgen Sie den Anweisungen zum Erstellen einer Komponente mithilfe der Image Builder Builder-Konsole im Image Builder Builder-Benutzerhandbuch.

Geben Sie Ihre Komponentendetails ein:

1. Wählen Sie als Typ die Option Build aus.
2. Wählen Sie als Image-Betriebssystem (OS) entweder Linux oder Windows aus.
3. Geben Sie als Komponentenname einen aussagekräftigen Namen ein, z. **`research-and-engineering-studio-vdi-<operating-system>`** B.
4. Geben Sie die Versionsnummer Ihrer Komponente ein und fügen Sie optional eine Beschreibung hinzu.
5. Geben Sie für das Definitionsdokument die folgende Definitionsdatei ein. Wenn Sie auf Fehler stoßen, unterscheidet die YAML-Datei Leerzeichen und ist die wahrscheinlichste Ursache.

   Linux

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-linux
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
```

```
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
```

```
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-windows
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
```

```
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
 res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
       - name: Reboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
```

```
        inputs:
           delaySeconds: 0
```

6. Erstellen Sie alle optionalen Tags und wählen Sie Komponente erstellen.

Bereiten Sie Ihr EC2 Image Builder Builder-Rezept vor

Ein EC2 Image Builder Builder-Rezept definiert das Basis-Image, das als Ausgangspunkt für die Erstellung eines neuen Images verwendet werden soll, zusammen mit den Komponenten, die Sie hinzufügen, um Ihr Image anzupassen und zu überprüfen, ob alles wie erwartet funktioniert. Sie müssen entweder ein Rezept erstellen oder ändern, um das Ziel-AMI mit den erforderlichen RES-Softwareabhängigkeiten zu erstellen. Weitere Informationen zu Rezepten finden Sie unter Rezepte verwalten.

RES unterstützt die folgenden Image-Betriebssysteme:

- Amazon Linux 2 (x86 und ARM64)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Öffnen Sie die EC2 Image Builder Builder-Konsole unterhttps://console.aws.amazon.com/imagebuilder.
2. Wählen Sie unter Gespeicherte Ressourcen die Option Bildrezepte aus.
3. Wählen Sie Create image recipe (Image-Rezept erstellen) aus.
4. Geben Sie einen eindeutigen Namen und eine Versionsnummer ein.
5. Wählen Sie ein von RES unterstütztes Basis-Image aus.
6. Installieren Sie unter Instanzkonfiguration einen SSM-Agenten, falls keiner vorinstalliert ist. Geben Sie die Informationen unter Benutzerdaten und alle anderen benötigten Benutzerdaten ein.

> **Note**
>
> Informationen zur Installation eines SSM-Agenten finden Sie unter:
>
> - Manuelles Installieren des SSM-Agenten auf EC2 Instanzen für Linux

- Manuelles Installieren und Deinstallieren des SSM-Agenten auf EC2 Instanzen für Windows Server

7. Fügen Sie für Linux-basierte Rezepte die von Amazon verwaltete `aws-cli-version-2-linux` Build-Komponente zum Rezept hinzu. RES-Installationsskripten verwenden den AWS CLI , um VDI-Zugriff auf Konfigurationswerte für die DynamoDB-Clustereinstellungen bereitzustellen. Windows benötigt diese Komponente nicht.
8. Fügen Sie die EC2 Image Builder Builder-Komponente hinzu, die für Ihre Linux- oder Windows-Umgebung erstellt wurde, und geben Sie alle erforderlichen Parameterwerte ein. Die folgenden Parameter sind erforderliche Eingaben: AWSAccount ID, RESEnv Name, RESEnv Region und RESEnvReleaseVersion.

   > **Important**
   >
   > In Linux-Umgebungen müssen Sie diese Komponenten der Reihe nach hinzufügen, wobei die `aws-cli-version-2-linux` Build-Komponente zuerst hinzugefügt wird.

9. (Empfohlen) Fügen Sie die von Amazon verwaltete `simple-boot-test-<linux-or-windows>` Testkomponente hinzu, um zu überprüfen, ob das AMI gestartet werden kann. Dies ist eine Mindestrempfehlung. Sie können andere Testkomponenten auswählen, die Ihren Anforderungen entsprechen.
10. Füllen Sie bei Bedarf alle optionalen Abschnitte aus, fügen Sie weitere gewünschte Komponenten hinzu und wählen Sie „Rezept erstellen“.

Modify a recipe

Wenn Sie über ein vorhandenes EC2 Image Builder Builder-Rezept verfügen, können Sie es verwenden, indem Sie die folgenden Komponenten hinzufügen:

1. Fügen Sie für Linux-basierte Rezepte die von Amazon verwaltete `aws-cli-version-2-linux` Build-Komponente zum Rezept hinzu. RES-Installationsskripten verwenden den AWS CLI , um VDI-Zugriff auf Konfigurationswerte für die DynamoDB-Clustereinstellungen bereitzustellen. Windows benötigt diese Komponente nicht.
2. Fügen Sie die EC2 Image Builder Builder-Komponente hinzu, die für Ihre Linux- oder Windows-Umgebung erstellt wurde, und geben Sie alle erforderlichen Parameterwerte ein. Die folgenden Parameter sind erforderliche Eingaben: AWSAccount ID, RESEnv Name, RESEnv Region und RESEnvReleaseVersion.

> **Important**
>
> In Linux-Umgebungen müssen Sie diese Komponenten der Reihe nach hinzufügen, wobei die `aws-cli-version-2-linux` Build-Komponente zuerst hinzugefügt wird.

3. Füllen Sie bei Bedarf alle optionalen Abschnitte aus, fügen Sie weitere gewünschte Komponenten hinzu und wählen Sie Create recipe (Rezept erstellen).

EC2 Image Builder Builder-Infrastruktur konfigurieren

Sie können Infrastrukturkonfigurationen verwenden, um die EC2 Amazon-Infrastruktur anzugeben, die Image Builder zum Erstellen und Testen Ihres Image Builder Builder-Images verwendet. Für die Verwendung mit RES können Sie wählen, ob Sie eine neue Infrastrukturkonfiguration erstellen oder eine bestehende verwenden möchten.

- Informationen zum Erstellen einer neuen Infrastrukturkonfiguration finden Sie unter Erstellen einer Infrastrukturkonfiguration.
- Um eine bestehende Infrastrukturkonfiguration zu verwenden, aktualisieren Sie eine Infrastrukturkonfiguration.

So konfigurieren Sie Ihre Image Builder Builder-Infrastruktur:

1. Geben Sie für die IAM-Rolle die Rolle ein, in the section called “Bereiten Sie die IAM-Rolle für den Zugriff auf die RES-Umgebung vor” der Sie zuvor konfiguriert haben.
2. Wählen Sie als Instance-Typ einen Typ mit mindestens 4 GB Arbeitsspeicher aus, der die von Ihnen gewählte AMI-Basisarchitektur unterstützt. Siehe EC2 Amazon-Instance-Typen.
3. Für VPC-, Subnetz- und Sicherheitsgruppen müssen Sie den Internetzugang zulassen, um Softwarepakete herunterzuladen. Der Zugriff auf die `cluster-settings` DynamoDB-Tabelle und den Amazon S3 S3-Cluster-Bucket der RES-Umgebung muss ebenfalls erlaubt sein.

Image Builder Builder-Image-Pipeline konfigurieren

Die Image Builder Builder-Image-Pipeline stellt das Basis-Image, Komponenten zum Erstellen und Testen, die Infrastrukturkonfiguration und die Verteilungseinstellungen zusammen. Um eine Image-Pipeline für RES-Ready zu konfigurieren AMIs, können Sie wählen, ob Sie eine neue Pipeline

erstellen oder eine vorhandene verwenden möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von AMI-Image-Pipelines im Image Builder Builder-Benutzerhandbuch.

Create a new Image Builder pipeline

1. Öffnen Sie die Image Builder Builder-Konsole unterhttps://console.aws.amazon.com/imagebuilder.
2. Wählen Sie in der Navigation die Option Image-Pipelines aus.
3. Wählen Sie Image-Pipeline erstellen aus.
4. Geben Sie Ihre Pipeline-Details an, indem Sie einen eindeutigen Namen, eine optionale Beschreibung, einen Zeitplan und eine Häufigkeit eingeben.
5. Wählen Sie für Rezept auswählen die Option Bestehendes Rezept verwenden und wählen Sie das in erstellte Rezept austhe section called “Bereiten Sie Ihr EC2 Image Builder Builder-Rezept vor”. Vergewissern Sie sich, dass Ihre Rezeptdetails korrekt sind.
6. Wählen Sie für „Prozess zur Image-Erstellung definieren“ je nach Anwendungsfall entweder den Standard- oder den benutzerdefinierten Workflow aus. In den meisten Fällen sind die Standard-Workflows ausreichend. Weitere Informationen finden Sie unter Konfigurieren von Image-Workflows für Ihre EC2 Image Builder Builder-Pipeline.
7. Wählen Sie unter Infrastrukturkonfiguration definieren die Option Vorhandene Infrastrukturkonfiguration auswählen und wählen Sie die in erstellte Infrastrukturkonfiguration austhe section called “ EC2 Image Builder Builder-Infrastruktur konfigurieren”. Stellen Sie sicher, dass Ihre Infrastrukturdetails korrekt sind.
8. Wählen Sie unter Verteilungseinstellungen definieren die Option Verteilungseinstellungen mithilfe von Dienststandardwerten erstellen aus. Das Ausgabebild muss sich in derselben RES-Umgebung befinden AWS-Region wie Ihre RES-Umgebung. Unter Verwendung der Dienststandardwerte wird das Image in der Region erstellt, in der Image Builder verwendet wird.
9. Überprüfen Sie die Pipeline-Details und wählen Sie Pipeline erstellen aus.

Modify an existing Image Builder pipeline

1. Um eine bestehende Pipeline zu verwenden, ändern Sie die Details so, dass sie das in erstellte Rezept verwendenthe section called “Bereiten Sie Ihr EC2 Image Builder Builder-Rezept vor”.
2. Wählen Sie Änderungen speichern aus.

Image Builder Builder-Image-Pipeline ausführen

Um das konfigurierte Ausgabebild zu erstellen, müssen Sie die Image-Pipeline initiieren. Der Erstellungsvorgang kann je nach Anzahl der Komponenten im Image-Rezept möglicherweise bis zu einer Stunde dauern.

So führen Sie die Image-Pipeline aus:

1. Wählen Sie unter Image-Pipelines die Pipeline aus, die in the section called “Image Builder Builder-Image-Pipeline konfigurieren” erstellt wurde.
2. Wählen Sie unter Aktionen die Option Pipeline ausführen aus.

Registrieren Sie einen neuen Software-Stack in RES

1. Folgen Sie den Anweisungen unterthe section called “Software-Stacks () AMIs”, um einen Software-Stack zu registrieren.
2. Geben Sie als AMI-ID die AMI-ID des integrierten Ausgabe-Images einthe section called “Image Builder Builder-Image-Pipeline ausführen”.

Administratorhandbuch

Dieses Administratorhandbuch enthält zusätzliche Anweisungen für ein technisches Publikum zur weiteren Anpassung und Integration mit dem Research and Engineering Studio am AWS Produkt.

Themen

- Sitzungsverwaltung
- Verwaltung der Umgebung
- Verwaltung von Secrets
- Kostenüberwachung und -kontrolle

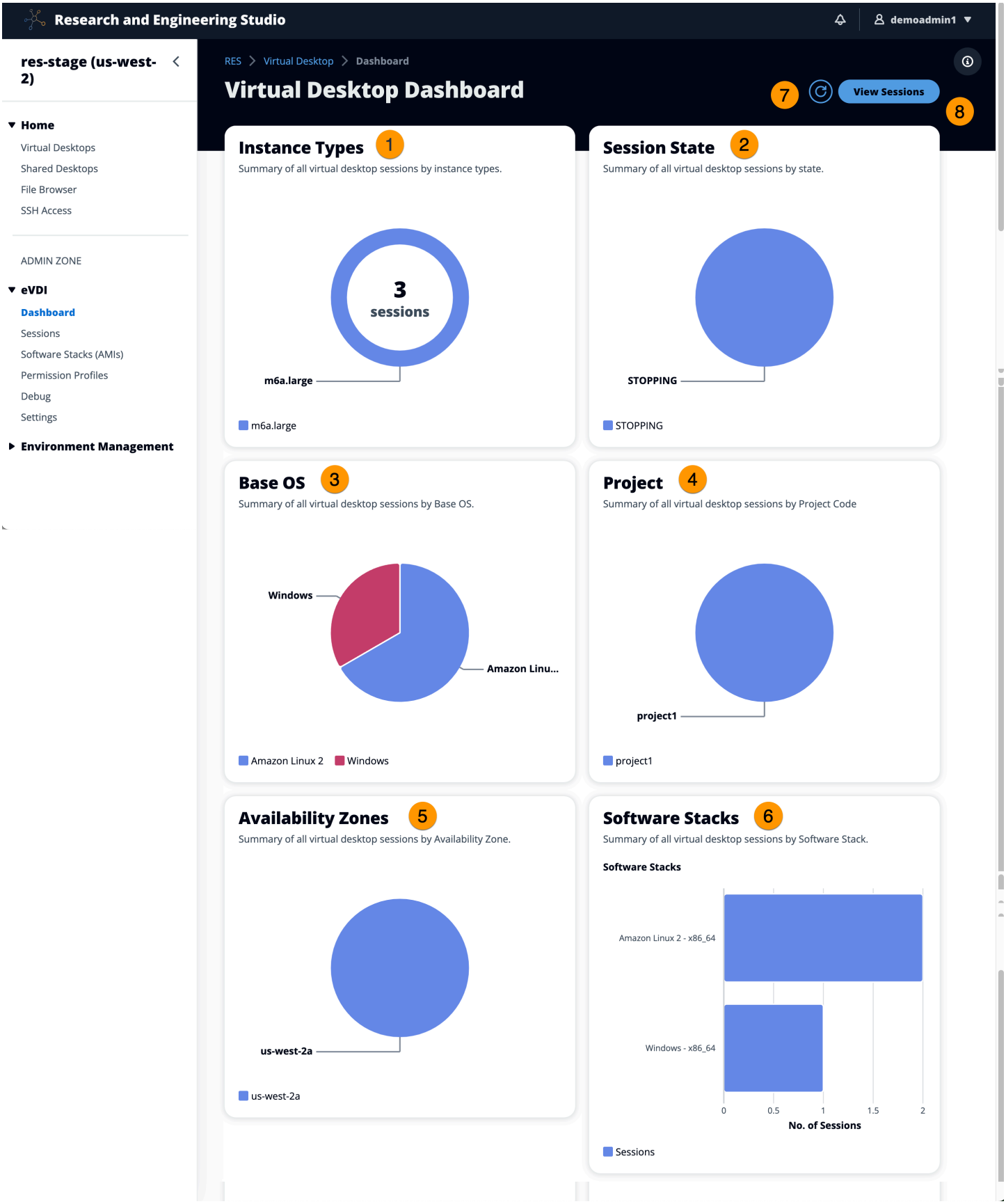
Sitzungsverwaltung

Die Sitzungsverwaltung bietet eine flexible und interaktive Umgebung für Entwicklungs- und Testsitzungen. Als Administratorbenutzer können Sie Benutzern erlauben, interaktive Sitzungen in ihren Projektumgebungen zu erstellen und zu verwalten.

Themen

- Dashboard
- Sitzungen
- Software-Stacks () AMIs
- Debugging
- Desktop-Einstellungen

Dashboard


Research and Engineering Studio
demoadmin1
res-stage (us-west-2)
Home
Virtual Desktops
Shared Desktops
File Browser
SSH Access
ADMIN ZONE
eVDI
Dashboard
Sessions
Software Stacks (AMIs)
Permission Profiles
Debug
Settings
Environment Management
RES > Virtual Desktop > Dashboard
Virtual Desktop Dashboard
7
View Sessions
8
Instance Types
1
Summary of all virtual desktop sessions by instance types.
3
sessions
m6a.large
m6a.large
Session State
2
Summary of all virtual desktop sessions by state.
STOPPING
STOPPING
Base OS
3
Summary of all virtual desktop sessions by Base OS.
Windows
Amazon Linu...
Amazon Linux 2
Windows
Project
4
Summary of all virtual desktop sessions by Project Code
project1
project1
Availability Zones
5
Summary of all virtual desktop sessions by Availability Zone.
us-west-2a
us-west-2a
Software Stacks
6
Summary of all virtual desktop sessions by Software Stack.
Software Stacks
Amazon Linux 2 - x86_64
Windows - x86_64
0
0.5
1
1.5
2
No. of Sessions
Sessions

Das Sitzungsverwaltungs-Dashboard bietet Administratoren einen schnellen Überblick über:

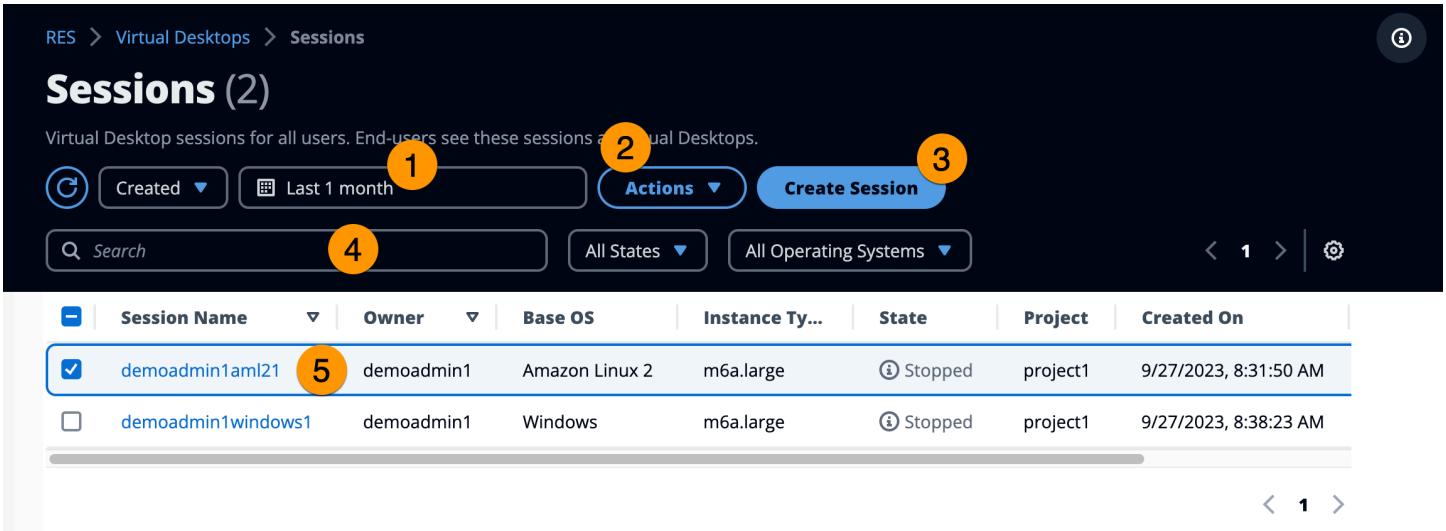
1. Instance-Typen
2. Sitzungsstatus
3. Basis-Betriebssystem
4. Projekte
5. Verfügbarkeitszonen
6. Software-Stapel

Darüber hinaus können Administratoren:

7. Aktualisieren Sie das Dashboard, um die Informationen zu aktualisieren.
8. Wählen Sie „Sitzungen anzeigen“, um zu „Sitzungen“ zu navigieren.

Sitzungen

Sessions zeigt alle virtuellen Desktops an, die in Research and Engineering Studio erstellt wurden. Auf der Seite „Sitzungen“ können Sie Sitzungsinformationen filtern und anzeigen oder eine neue Sitzung erstellen.



1. Verwenden Sie das Menü, um Ergebnisse nach Sitzungen zu filtern, die innerhalb eines bestimmten Zeitraums erstellt oder aktualisiert wurden.
2. Wählen Sie eine Sitzung aus und verwenden Sie das Aktionsmenü, um:
   a. Sitzung (en) fortsetzen

   b. Stop/Hibernate Sitzung (en)
   c. Stop/Hibernate Sitzung (en) erzwingen
   d. Sitzung (en) beenden
   e. Sitzung (en) beenden erzwingen
   f. Sitzung (en) Health
   g. Software-Stack erstellen
3. Wählen Sie Create Session, um eine neue Sitzung zu erstellen.
4. Suchen Sie anhand des Namens nach einer Sitzung und filtern Sie sie nach Status und Betriebssystem.
5. Wählen Sie den Sitzungsnamen, um weitere Details anzuzeigen.

Erstellen Sie eine Sitzung

1. Wählen Sie Sitzung erstellen. Das Modal „Neuen virtuellen Desktop starten“ wird geöffnet.
2. Geben Sie Details für die neue Sitzung ein.
3. (Optional.) Aktivieren Sie „Erweiterte Optionen anzeigen“, um zusätzliche Details wie Subnetz-ID und DCV-Sitzungstyp anzugeben.
4. Wählen Sie Absenden aus.

Launch New Virtual Desktop

Session Name
Enter a name for the virtual desktop

Session Name is required. Use any characters and form a name of length between 3 and 24 characters, inclusive.

User
Select the user to create the session for

Project
Select the project under which the session will get created

Operating System
Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack
Select the software stack for your virtual desktop

Enable Instance Hibernation
Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

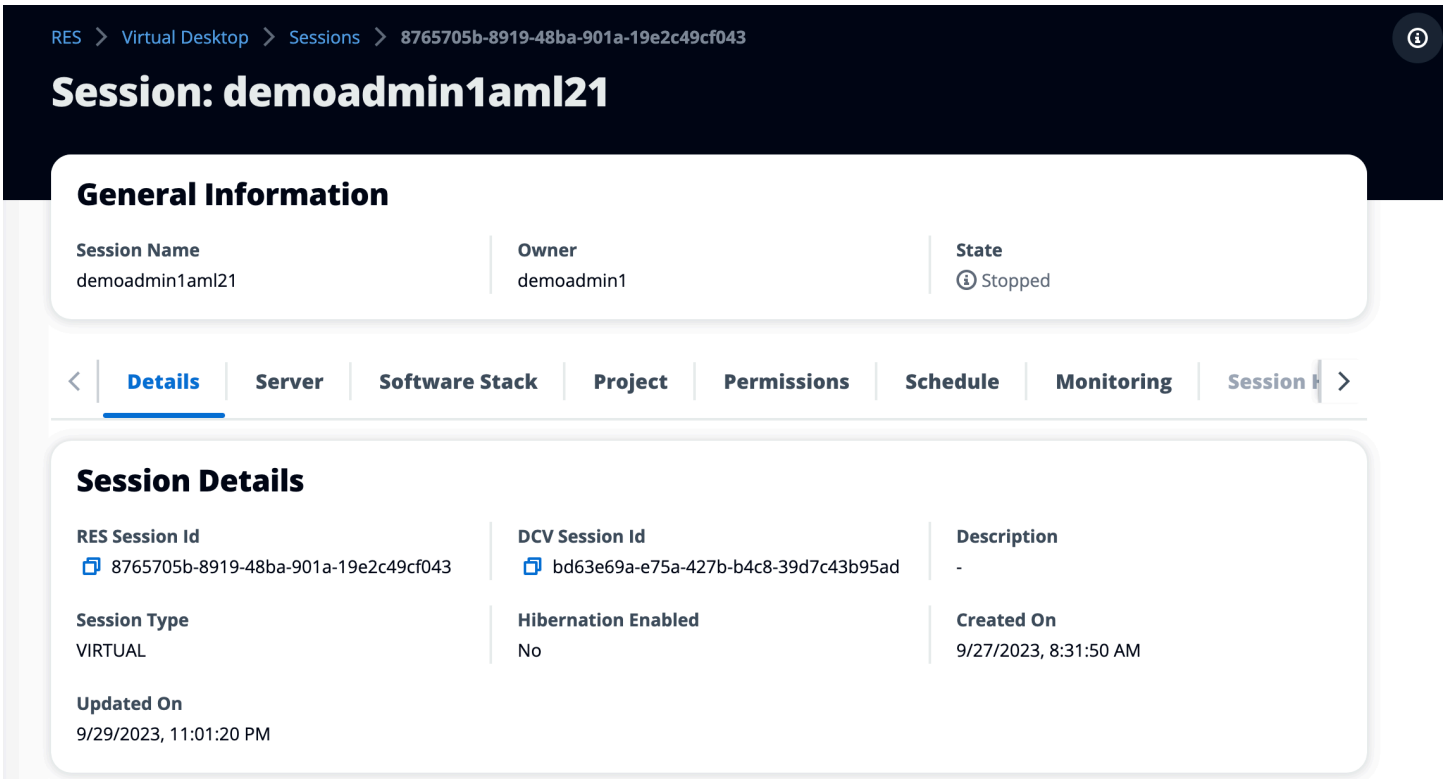
Virtual Desktop Size
Select a virtual desktop instance type

Storage Size (GB)
Enter the storage size for your virtual desktop in GBs

10

Einzelheiten der Sitzung

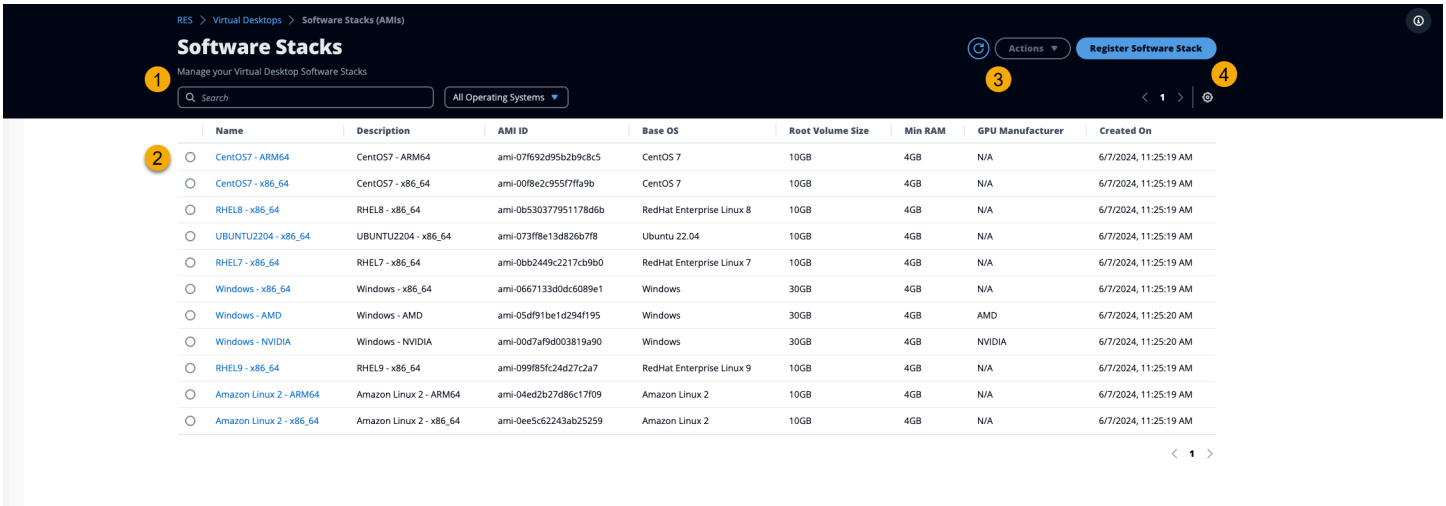
Wählen Sie in der Sitzungsliste den Sitzungsnamen aus, um die Sitzungsdetails anzuzeigen.



Software-Stacks () AMIs

> **Note**
>
> Um den bereitgestellten SO7 Cent-Softwarestack ausführen zu können AWS GovCloud (US), müssen Sie das AMI innerhalb AWS Marketplace Ihres verknüpften Standardkontos abonnieren.

Auf der Seite Software Stacks können Sie Amazon Machine Images (AMIs) konfigurieren und bestehende AMIs verwalten.



1. Um nach einem vorhandenen Software-Stack zu suchen, verwenden Sie das Betriebssystem-Dropdown-Menü, um nach Betriebssystem zu filtern.
2. Wählen Sie den Namen eines Software-Stacks, um Details zum Stack anzuzeigen.
3. Sobald Sie einen Software-Stack ausgewählt haben, verwenden Sie das Aktionsmenü, um den Stack zu bearbeiten und den Stack einem Projekt zuzuweisen.
4. Mit der Schaltfläche Software-Stack registrieren können Sie einen neuen Stack erstellen:
    1. Wählen Sie Software-Stack registrieren.
    2. Geben Sie Details für den neuen Software-Stack ein.
    3. Wählen Sie Absenden aus.

Register new Software Stack

Name

Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description

Enter a user friendly description for the software stack

AMI Id

Enter the AMI Id

AMI Id must start with ami-xxx

Operating System

Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer

Select the GPU Manufacturer for the software stack

N/A

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

10

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

10

Projects

Select applicable projects for the software stack

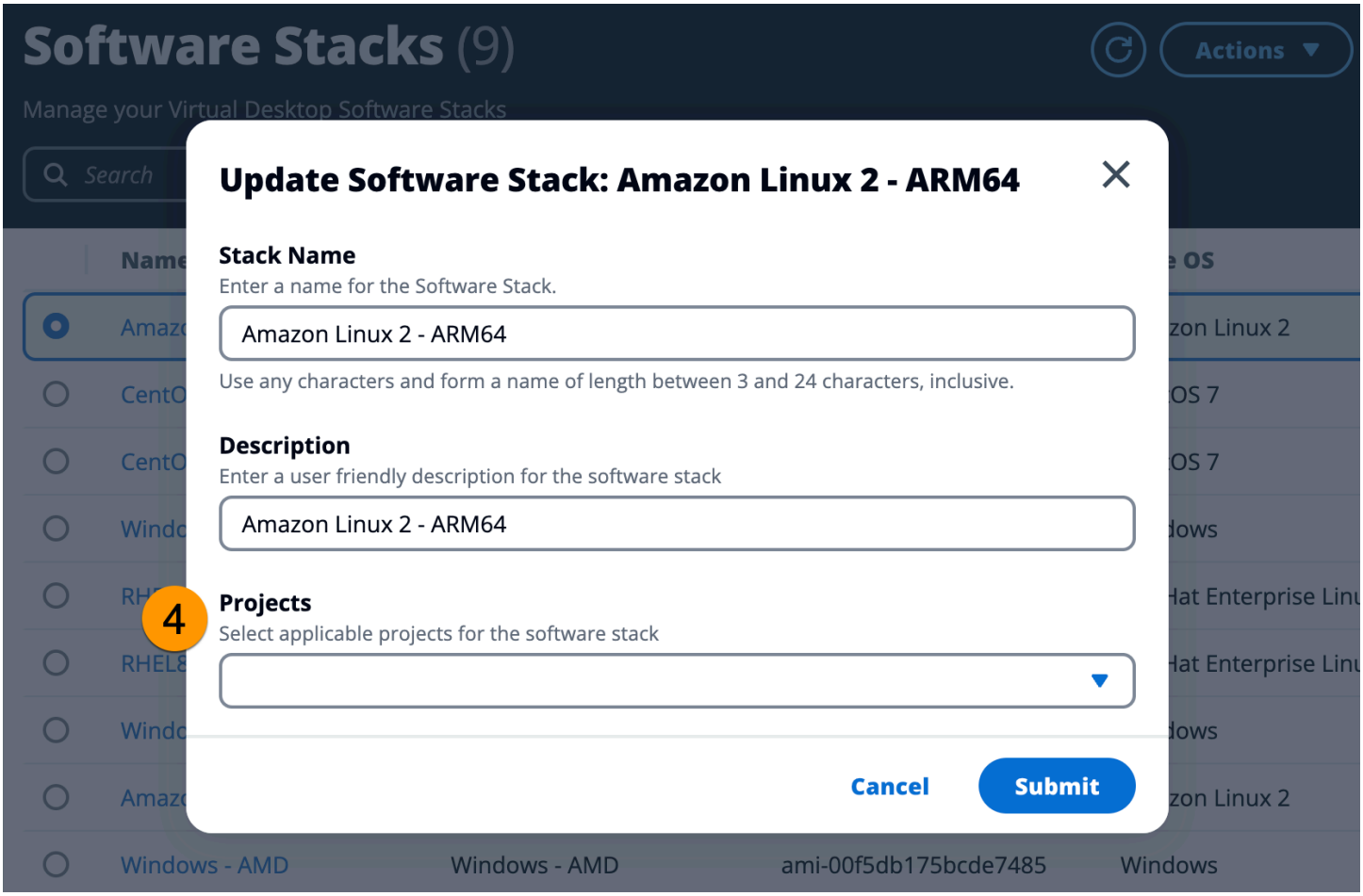
Weisen Sie einem Projekt einen Software-Stack zu

Wenn Sie einen neuen Software-Stack erstellen, können Sie den Stack Projekten zuweisen. Wenn Sie den Stack nach der ersten Erstellung zu einem Projekt hinzufügen müssen, gehen Sie wie folgt vor:

> **Note**
>
> Sie können Software-Stacks nur Projekten zuweisen, bei denen Sie Mitglied sind.

1. Wählen Sie auf der Seite Software-Stacks den Software-Stack aus, den Sie einem Projekt hinzufügen möchten.
2. Wählen Sie Aktionen.
3. Wählen Sie Bearbeiten aus.
4. Verwenden Sie das Drop-down-Menü Projekte, um das Projekt auszuwählen.
5. Wählen Sie Absenden aus.

Sie können den Software-Stack auch auf der Seite mit den Stack-Details bearbeiten.

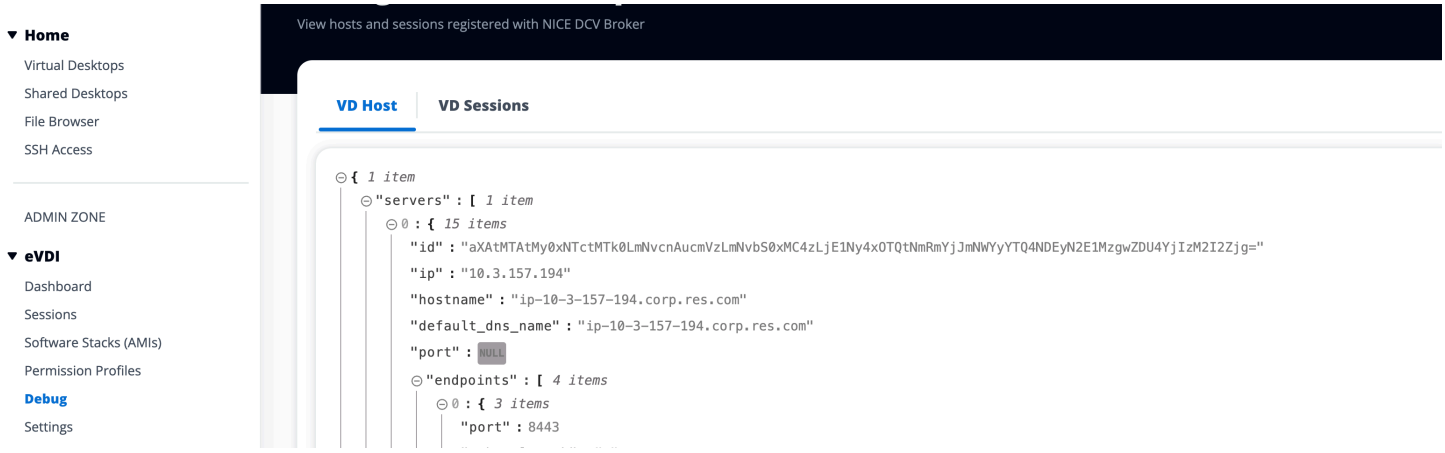


Details zum Software-Stack anzeigen

Wählen Sie aus der Liste der Software-Stacks den Namen des Software-Stacks aus, um Details anzuzeigen. Auf der Detailseite können Sie auch Bearbeiten wählen, um den Software-Stack zu bearbeiten.

Debugging

Im Debugging-Bereich wird der Nachrichtenverkehr im Zusammenhang mit den virtuellen Desktops angezeigt. Sie können dieses Fenster verwenden, um Aktivitäten zwischen Hosts zu beobachten. Auf der Registerkarte VD-Host werden instanzspezifische Aktivitäten angezeigt, und auf der Registerkarte VD-Sitzungen werden laufende Sitzungsaktivitäten angezeigt.



Desktop-Einstellungen

Sie können die Seite mit den Desktop-Einstellungen verwenden, um Ressourcen zu konfigurieren, die virtuellen Desktops zugeordnet sind. Die Registerkarte Server bietet Zugriff auf Einstellungen wie:

Timeout bei Leerlauf der DCV-Sitzung

Die Zeit, nach der die DCV-Sitzung automatisch getrennt wird. Dadurch wird der Status der Desktop-Sitzung nicht geändert. Die Sitzung wird lediglich entweder über den DCV-Client oder den Webbrowser geschlossen.

Warnung vor Timeout im Leerlauf

Die Zeit, nach der dem Client eine Warnung bei Leerlauf angezeigt wird.

Schwellenwert für die CPU-Auslastung

Die CPU-Auslastung, die als inaktiv betrachtet werden soll.

Zulässige Sitzungen pro Benutzer

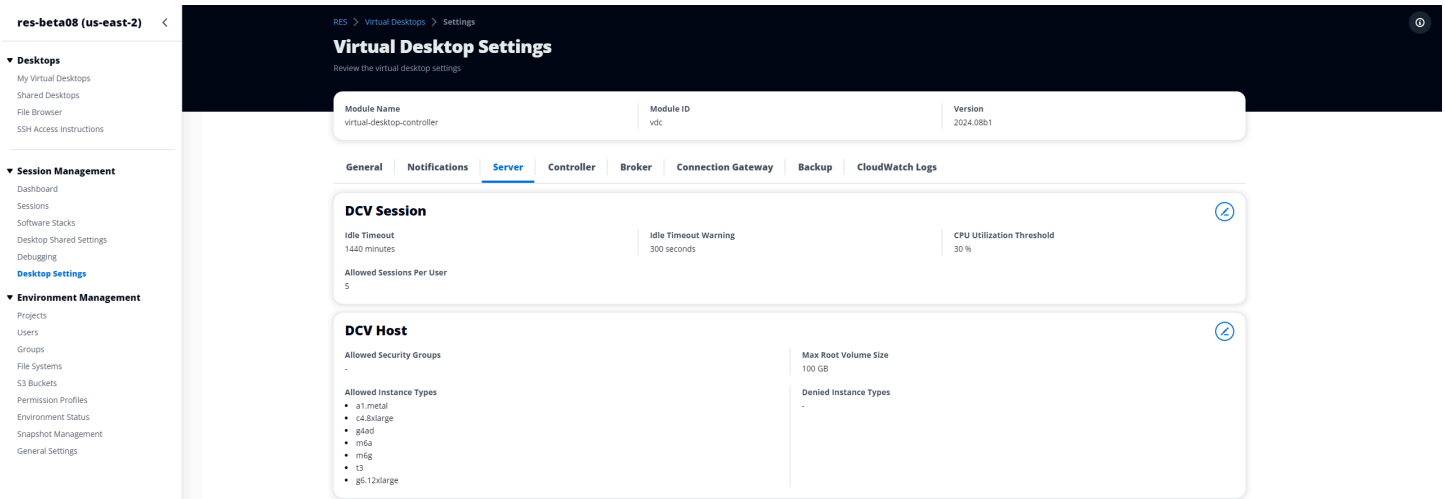
Die Anzahl der VDI-Sitzungen, die ein einzelner Benutzer zu einem bestimmten Zeitpunkt haben kann. Wenn ein Benutzer diesen Wert erreicht oder überschreitet, wird er daran gehindert, neue Sitzungen von der Seite Meine virtuellen Desktops aus zu starten. Die Möglichkeit, Sitzungen über die Sitzungsseite zu starten, wird durch diesen Wert nicht beeinträchtigt.

Max. Größe des Root-Volumes

Die Standardgröße des Root-Volumes in virtuellen Desktop-Sitzungen.

Zulässige Instanztypen

Die Liste der Instanzfamilien und -größen, die für diese RES-Umgebung gestartet werden können. Kombinationen aus Instance-Familie und Instance-Größe werden beide akzeptiert. Wenn Sie beispielsweise 'm7a' angeben, können alle Größen der m7a-Familie als VDI-Sitzungen gestartet werden. Wenn Sie 'm7a.24xlarge' angeben, kann nur m7a.24xlarge als VDI-Sitzung gestartet werden. Diese Liste wirkt sich auf alle Projekte in der Umgebung aus.



Verwaltung der Umgebung

Im Bereich Umweltmanagement von RES können Benutzer mit Administratorrechten isolierte Umgebungen für ihre Forschungs- und Ingenieurprojekte erstellen und verwalten. Diese Umgebungen können Rechenressourcen, Speicher und andere notwendige Komponenten umfassen, und das alles in einer sicheren Umgebung. Benutzer können diese Umgebungen so konfigurieren und anpassen, dass sie den spezifischen Anforderungen ihrer Projekte entsprechen. Dies erleichtert das Experimentieren, Testen und Iterieren ihrer Lösungen, ohne andere Projekte oder Umgebungen zu beeinträchtigen.

Themen

- Projekte
- Benutzer
- Gruppen
- Berechtigungsprofile
- Dateisysteme

- Umgebungsstatus
- Snapshot-Verwaltung
- Umgebungseinstellungen
- Amazon-S3-Buckets

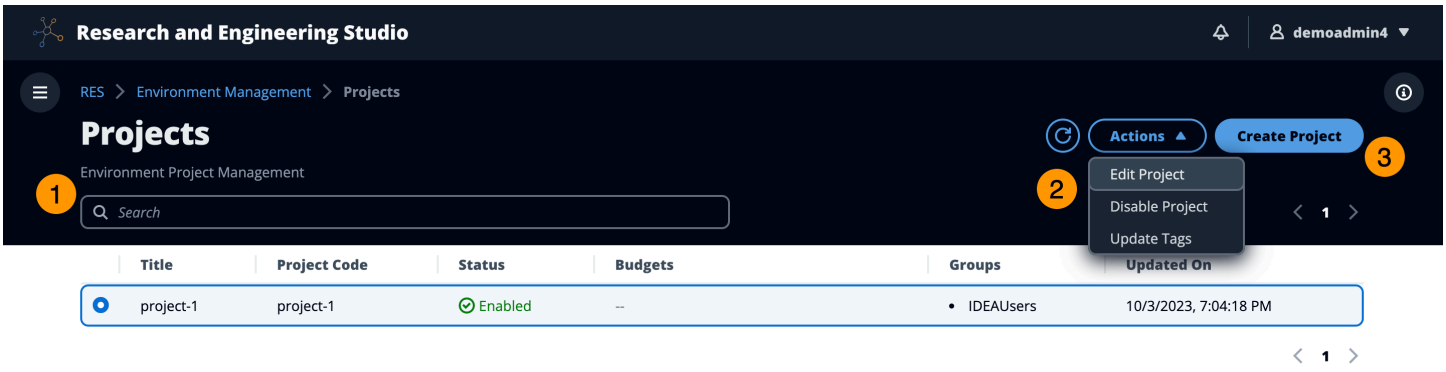
Projekte

Projekte bilden eine Grenze für virtuelle Desktops, Teams und Budgets. Wenn Sie ein Projekt erstellen, definieren Sie dessen Einstellungen, z. B. den Namen, die Beschreibung und die Umgebungskonfiguration. Projekte umfassen in der Regel eine oder mehrere Umgebungen, die an die spezifischen Anforderungen Ihres Projekts angepasst werden können, z. B. Art und Größe der Rechenressourcen, den Software-Stack und die Netzwerkkonfiguration.

Themen

- Projekte ansehen
- Erstellen eines Projekts
- Bearbeiten Sie ein Projekt
- Hinzufügen oder Entfernen von Tags aus einem Projekt
- Zeigen Sie die mit einem Projekt verknüpften Dateisysteme an
- Fügen Sie eine Startvorlage hinzu

Projekte ansehen



Das Projekte-Dashboard bietet eine Liste der Projekte, die Ihnen zur Verfügung stehen. Über das Projekte-Dashboard können Sie:

1. Sie können das Suchfeld verwenden, um Projekte zu finden.
2. Wenn ein Projekt ausgewählt ist, können Sie das Aktionsmenü verwenden, um:
   a. Bearbeiten Sie ein Projekt
   b. Ein Projekt deaktivieren oder aktivieren
   c. Projekt-Tags aktualisieren
3. Sie können Projekt erstellen wählen, um ein neues Projekt zu erstellen.

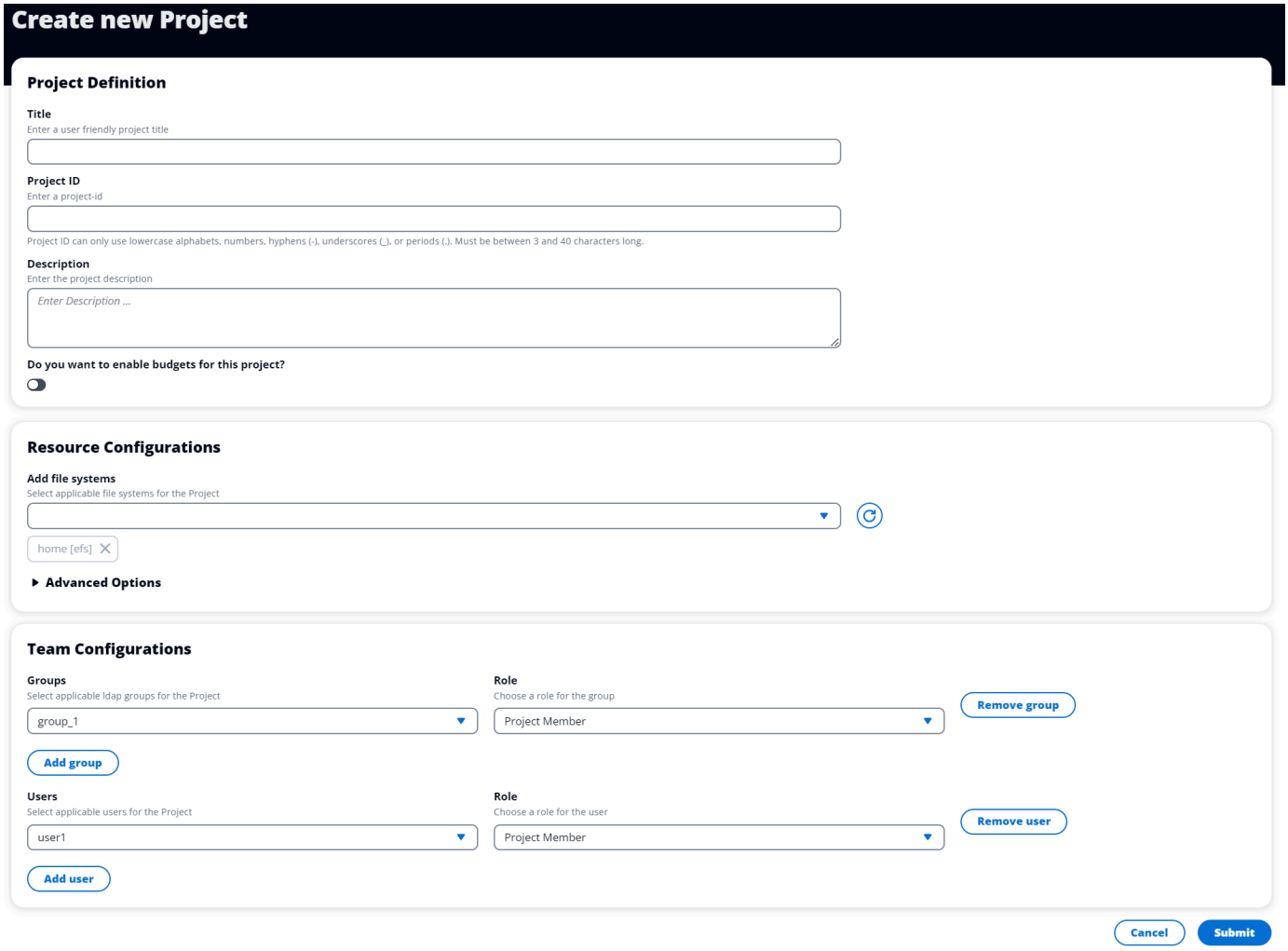
Erstellen eines Projekts

1. Wählen Sie Projekt erstellen aus.
2. Geben Sie die Projektdetails ein.

   Die Projekt-ID ist ein Ressourcen-Tag, mit dem die Kostenzuweisung verfolgt werden kann AWS Cost Explorer Service. Weitere Informationen finden Sie unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren.

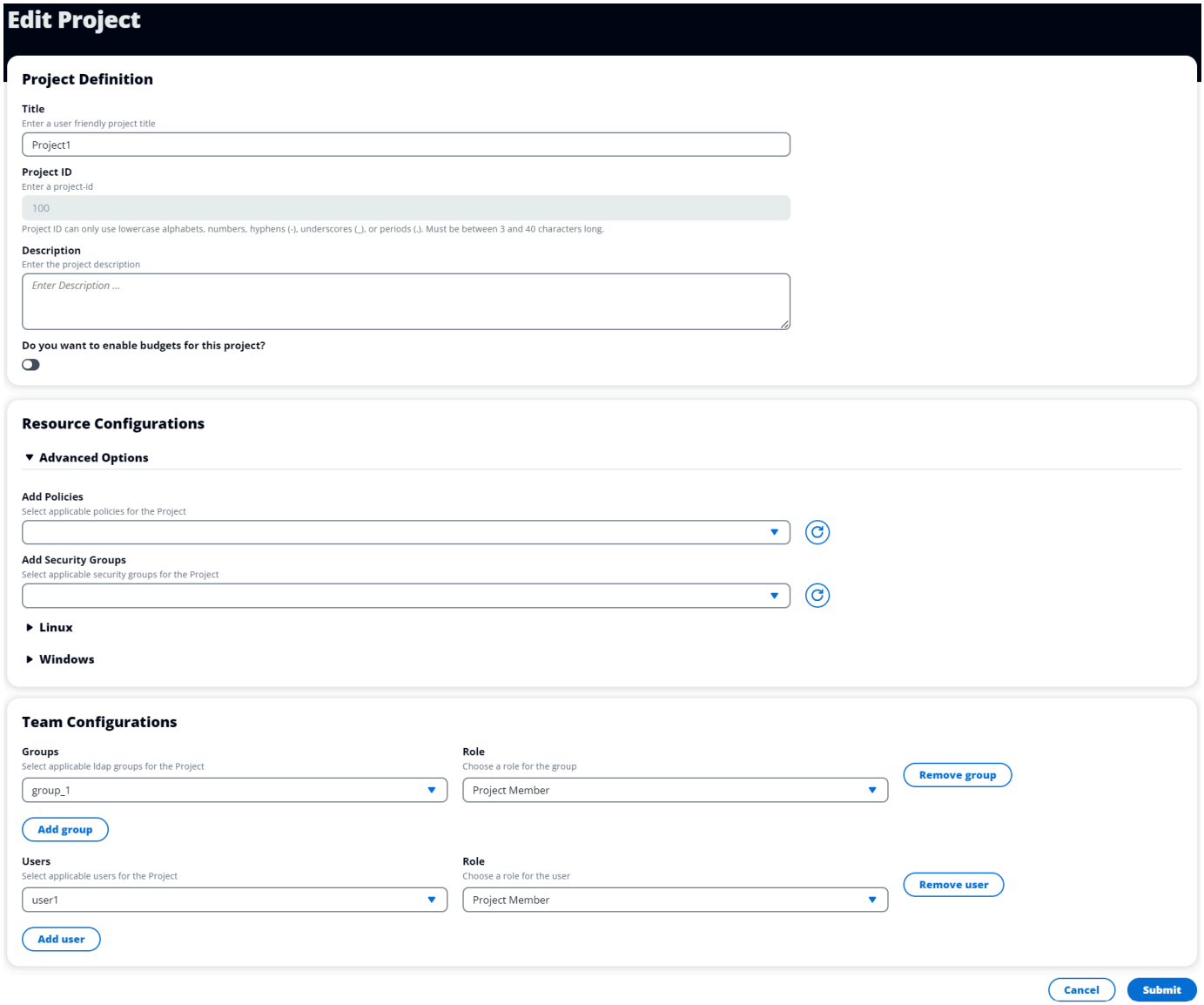
   > **Important**
   > Die Projekt-ID kann nach der Erstellung nicht geändert werden.

   Informationen zu den erweiterten Optionen finden Sie unterFügen Sie eine Startvorlage hinzu.
3. (Optional) Aktivieren Sie Budgets für das Projekt. Weitere Informationen zu Budgets finden Sie unterKostenüberwachung und -kontrolle.
4. Weisen Sie and/or Benutzergruppen die entsprechende Rolle zu („Projektmitglied“ oder „Projekteigentümer“). Hier Standardberechtigungsprofile finden Sie die Aktionen, die jede Rolle ausführen kann.
5. Wählen Sie Absenden aus.



Bearbeiten Sie ein Projekt

1. Wählen Sie ein Projekt in der Projektliste aus.
2. Wählen Sie im Menü Aktionen die Option Projekt bearbeiten.
3. Geben Sie Ihre Aktualisierungen ein. Wenn Sie Budgets aktivieren möchten, finden Sie Kostenüberwachung und -kontrolle weitere Informationen unter. Informationen zu den erweiterten Optionen finden Sie unterFügen Sie eine Startvorlage hinzu.
4. Wählen Sie Absenden aus.



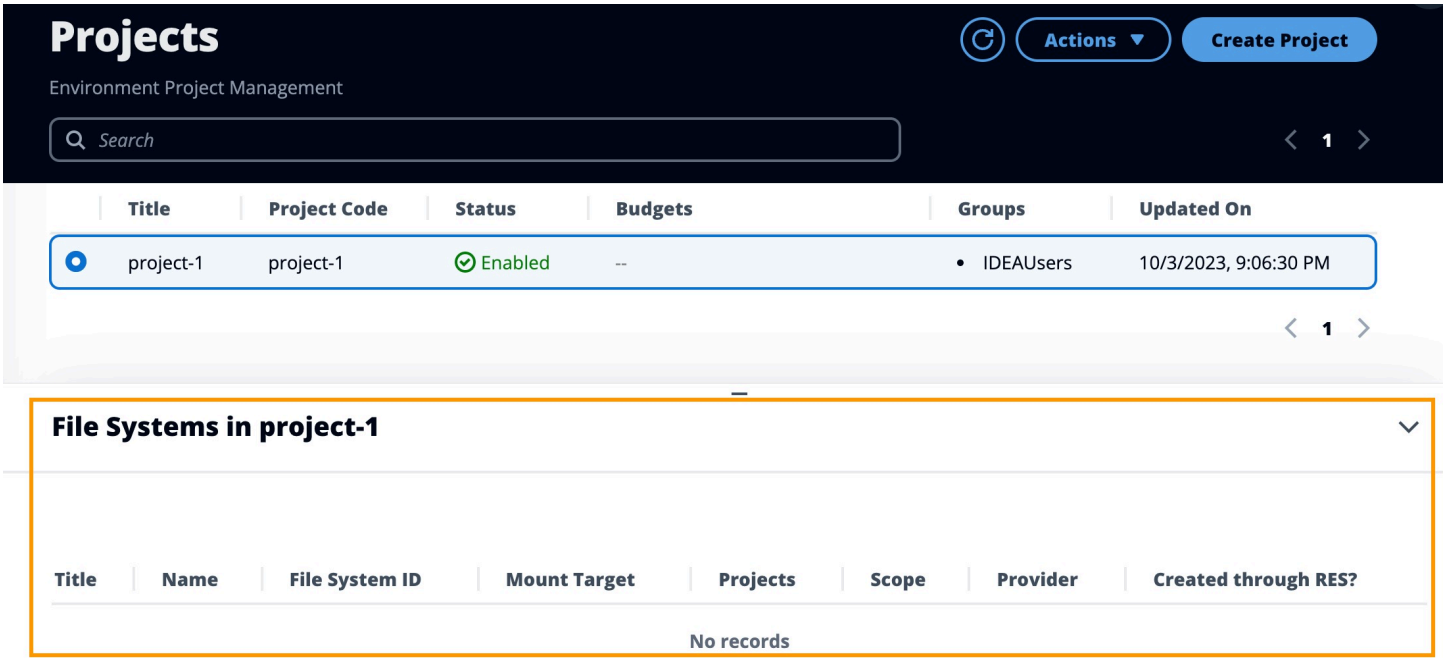
Hinzufügen oder Entfernen von Tags aus einem Projekt

Mit Projekt-Tags werden allen Instanzen, die im Rahmen dieses Projekts erstellt wurden, Tags zugewiesen.

1. Wählen Sie ein Projekt in der Projektliste aus.
2. Wählen Sie im Menü „Aktionen“ die Option „Tags aktualisieren“.
3. Wählen Sie „Tags hinzufügen“ und geben Sie einen Wert für „Schlüssel“ ein.
4. Um Tags zu entfernen, wählen Sie neben dem Tag, den Sie entfernen möchten, die Option Entfernen aus.

Zeigen Sie die mit einem Projekt verknüpften Dateisysteme an

Wenn ein Projekt ausgewählt ist, können Sie den Bereich Dateisysteme am unteren Bildschirmrand erweitern, um die mit dem Projekt verknüpften Dateisysteme anzuzeigen.



Fügen Sie eine Startvorlage hinzu

Wenn Sie ein Projekt erstellen oder bearbeiten, können Sie Startvorlagen mithilfe der erweiterten Optionen in der Projektkonfiguration hinzufügen. Startvorlagen bieten zusätzliche Konfigurationen wie Sicherheitsgruppen, IAM-Richtlinien und Startskripts für alle VDI-Instanzen innerhalb des Projekts.

Richtlinien hinzufügen

Sie können eine IAM-Richtlinie hinzufügen, um den VDI-Zugriff für alle im Rahmen Ihres Projekts bereitgestellten Instanzen zu steuern. Um eine Richtlinie zu integrieren, kennzeichnen Sie die Richtlinie mit dem folgenden Schlüssel-Wert-Paar:

```
res:Resource/vdi-host-policy
```

Weitere Informationen zu IAM-Rollen finden Sie unter Richtlinien und Berechtigungen in IAM.

Zusätzliche Sicherheitsgruppen

Sie können eine Sicherheitsgruppe hinzufügen, um die Ausgangs- und Eingangsdaten für alle VDI-Instanzen in Ihrem Projekt zu kontrollieren. Um eine Sicherheitsgruppe zu integrieren, kennzeichnen Sie die Sicherheitsgruppe mit dem folgenden Schlüssel-Wert-Paar:

```
res:Resource/vdi-security-group
```

Weitere Informationen zu Sicherheitsgruppen finden Sie unter Steuern des Datenverkehrs zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen im Amazon VPC-Benutzerhandbuch.

Fügen Sie Startskripte hinzu

Sie können Startskripts hinzufügen, die in allen VDI-Sitzungen innerhalb Ihres Projekts initiiert werden. RES unterstützt die Skriptinitiierung für Linux und Windows. Für die Skriptinitiierung können Sie eine der folgenden Optionen wählen:

Skript ausführen, wenn VDI gestartet wird

Diese Option initiiert das Skript am Anfang einer VDI-Instanz, bevor RES-Konfigurationen oder -Installationen ausgeführt werden.

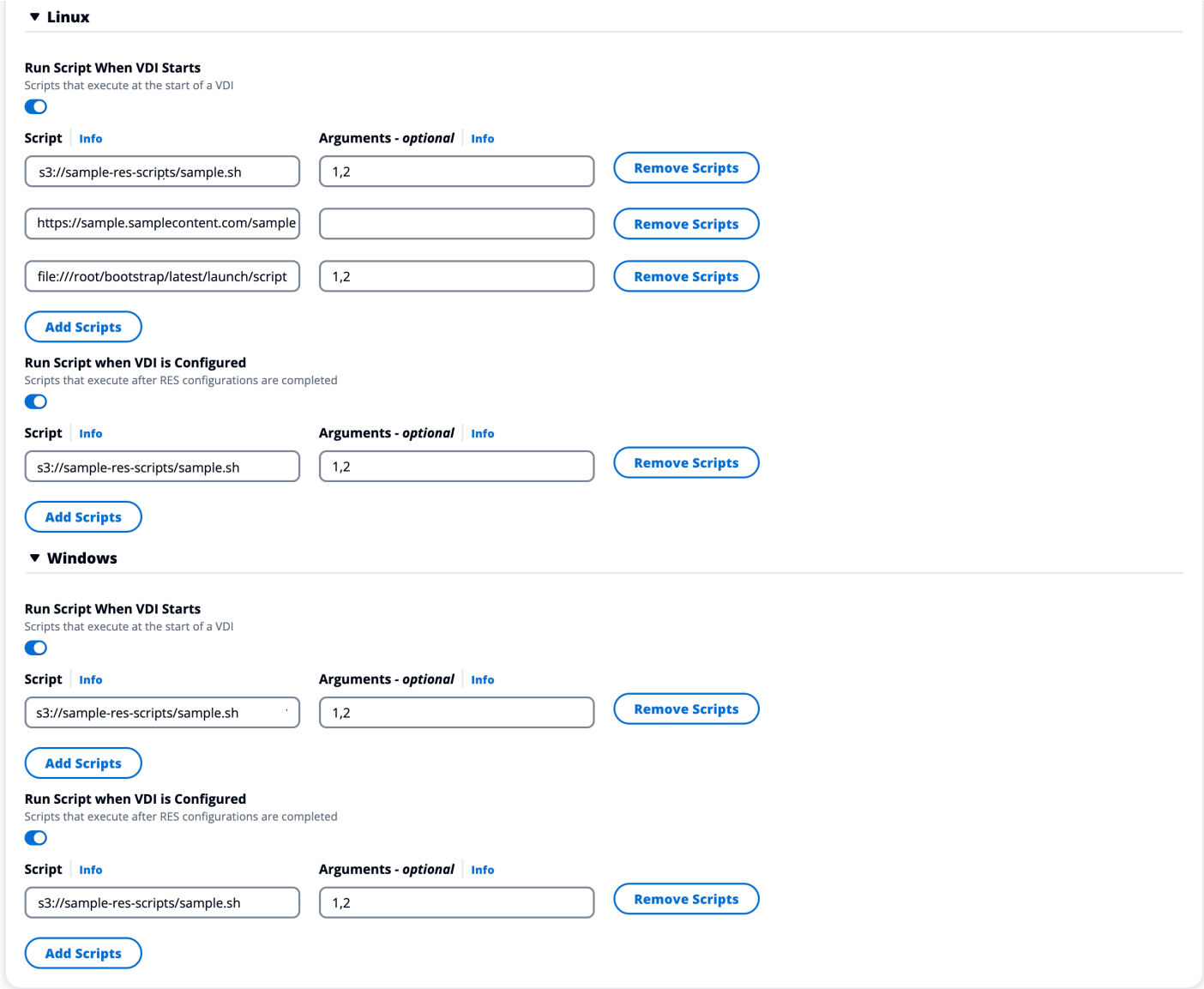
Führen Sie das Skript aus, wenn VDI konfiguriert ist

Diese Option initiiert das Skript nach Abschluss der RES-Konfigurationen.

Skripts unterstützen die folgenden Optionen:

Konfiguration des Skripts	Beispiel
S3-URI	s3://bucketname/script.sh
HTTPS-URL	https://sample.samplecontent.com/Beispiel
Lokale Datei	datei:///.sh user/scripts/example

Geben Sie für Argumente alle Argumente an, die durch ein Komma getrennt sind.

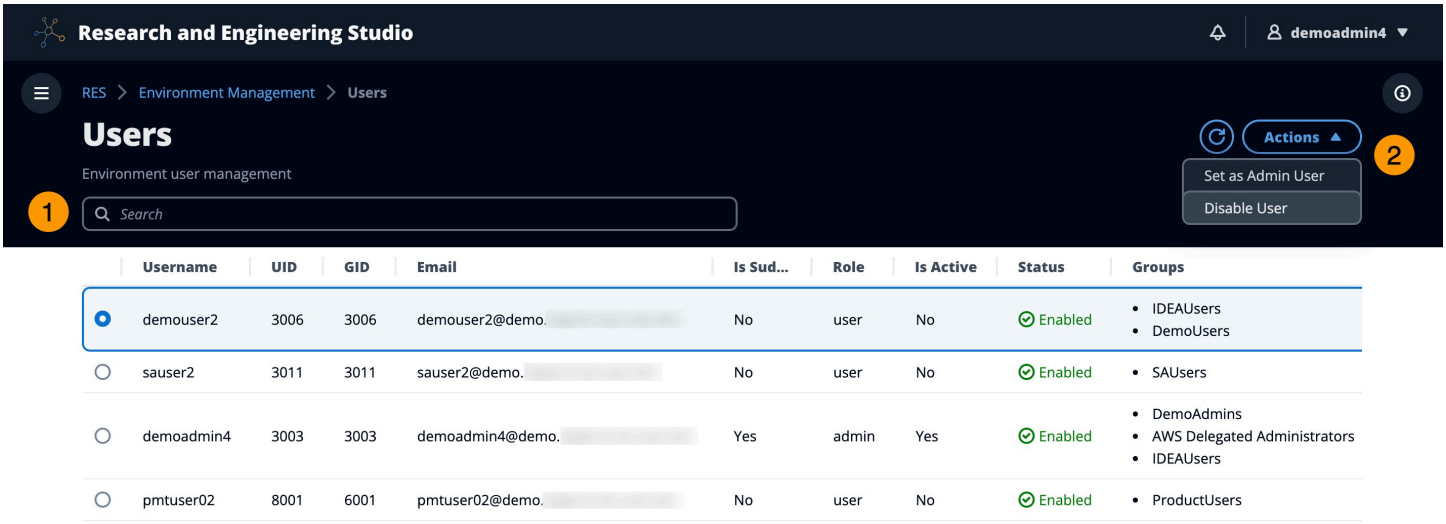


Beispiel für eine Projektkonfiguration

Benutzer

Alle Benutzer, die aus Ihrem Active Directory synchronisiert wurden, werden auf der Seite Benutzer angezeigt. Benutzer werden während der Konfiguration des Produkts vom Cluster-Admin-Benutzer synchronisiert. Weitere Informationen zur anfänglichen Benutzerkonfiguration finden Sie unter. Leitfaden zur Konfiguration

> **Note**
>
> Administratoren können nur Sitzungen für aktive Benutzer erstellen. Standardmäßig befinden sich alle Benutzer in einem inaktiven Status, bis sie sich bei der Produktumgebung anmelden. Wenn ein Benutzer inaktiv ist, bitten Sie ihn, sich anzumelden, bevor Sie eine Sitzung für ihn erstellen.

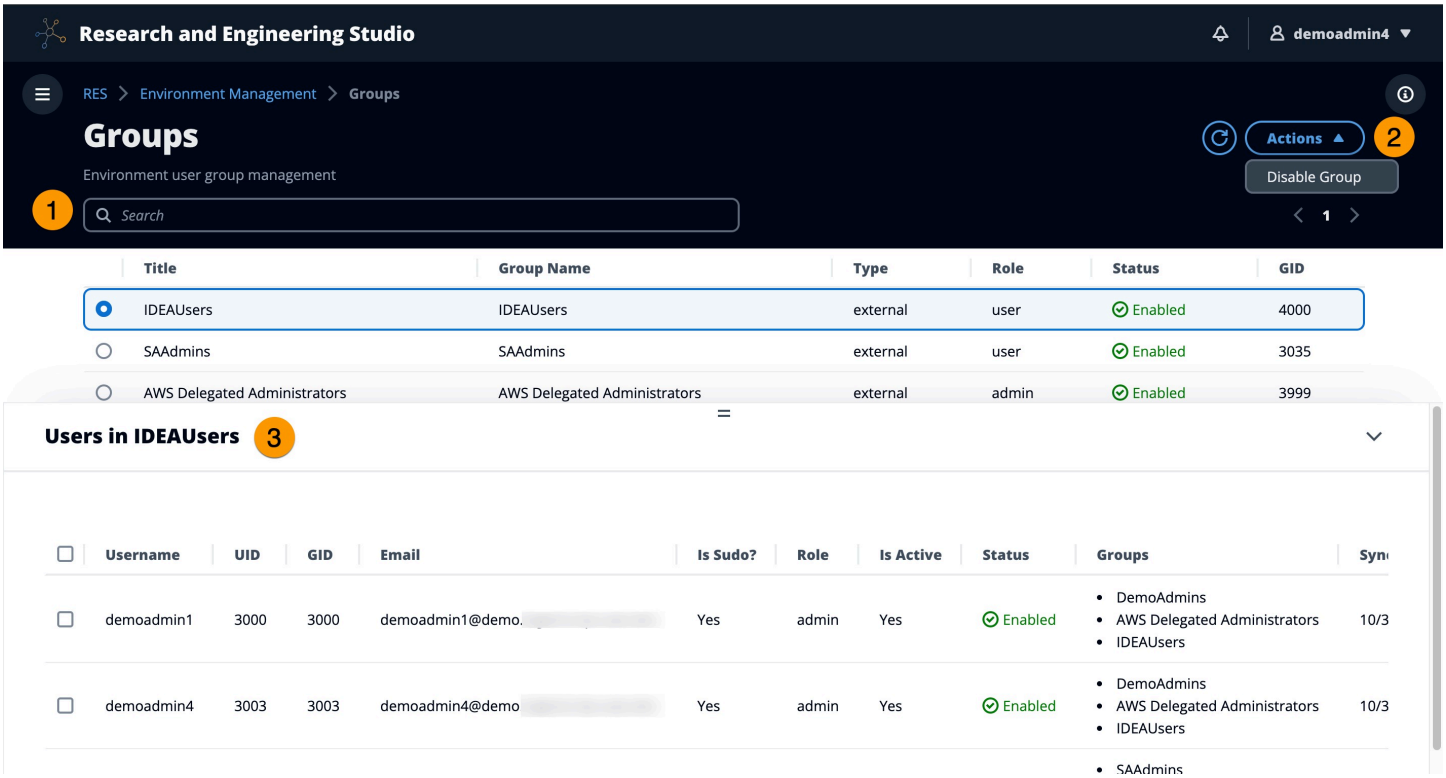


Auf der Benutzerseite können Sie:

1. Nach Benutzern suchen
2. Wenn ein Benutzername ausgewählt ist, verwenden Sie das Aktionsmenü, um:
   a. Als Admin-Benutzer festlegen
   b. Benutzer deaktivieren

Gruppen

Alle Gruppen, die aus dem Active Directory synchronisiert wurden, werden auf der Gruppenseite angezeigt. Weitere Informationen zur Konfiguration und Verwaltung von Gruppen finden Sie unterLeitfaden zur Konfiguration.



Auf der Seite Gruppen können Sie:

1. Suchen Sie nach Benutzergruppen.
2. Wenn eine Benutzergruppe ausgewählt ist, verwenden Sie das Aktionsmenü, um eine Gruppe zu deaktivieren oder zu aktivieren.
3. Wenn eine Benutzergruppe ausgewählt ist, können Sie den Bereich Benutzer am unteren Bildschirmrand erweitern, um die Benutzer in der Gruppe anzuzeigen.

Berechtigungsprofile

Übersicht

Research and Engineering Studio (RES) ermöglicht es einem Administratorbenutzer, benutzerdefinierte Berechtigungsprofile zu erstellen, die ausgewählten Benutzern zusätzliche Berechtigungen zur Verwaltung des Projekts gewähren, an dem sie beteiligt sind. Jedes Projekt verfügt über zwei Standard-Berechtigungsprofile — „Projektmitglied“ und „Projekteigentümer“ —, die nach der Bereitstellung angepasst werden können.

Derzeit können Administratoren mithilfe eines Berechtigungsprofils zwei Sammlungen von Berechtigungen gewähren:

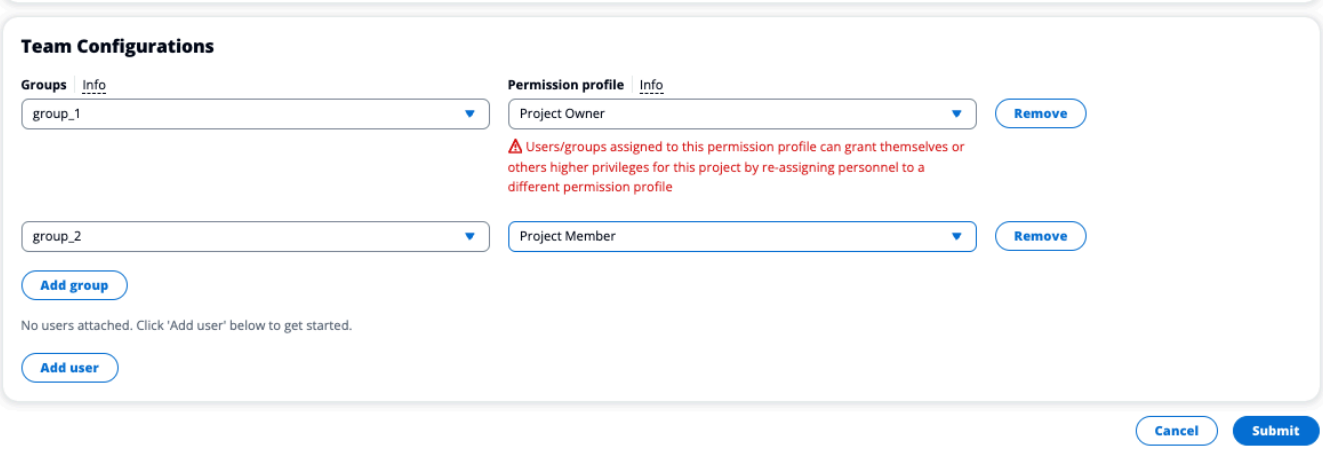
1. Projektmanagementberechtigungen, die aus „Projektmitgliedschaft aktualisieren“ bestehen, sodass ein bestimmter Benutzer andere Benutzer und Gruppen zu einem Projekt hinzufügen oder sie daraus entfernen kann, und „Projektstatus aktualisieren“, sodass ein bestimmter Benutzer ein Projekt aktivieren oder deaktivieren kann.
2. Die Berechtigungen für die Verwaltung von VDI-Sitzungen bestehen aus „Sitzung erstellen“, mit der ein bestimmter Benutzer eine VDI-Sitzung innerhalb seines Projekts erstellen kann, und „Sitzung eines anderen Benutzers erstellen/beenden“, mit dem ein bestimmter Benutzer die Sitzungen anderer Benutzer innerhalb eines Projekts erstellen oder beenden kann.

Auf diese Weise können Administratoren projektbasierte Berechtigungen an Nicht-Administratoren in ihrer Umgebung delegieren.

Berechtigungen für die Projektverwaltung

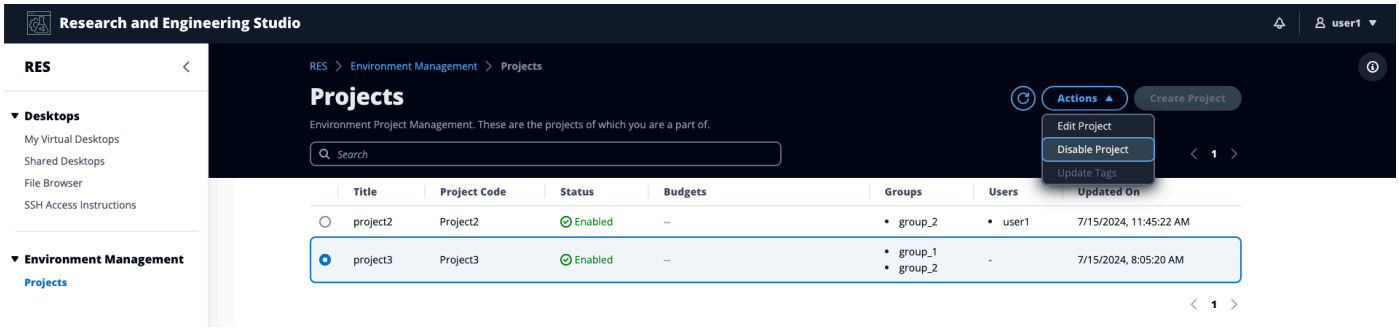
Projektmitgliedschaft aktualisieren

Mit dieser Berechtigung können Benutzer ohne Administratorrechte, denen sie erteilt wurde, Benutzer oder Gruppen zu einem Projekt hinzufügen und daraus entfernen. Sie ermöglicht ihnen auch, das Berechtigungsprofil festzulegen und die Zugriffsebene für alle anderen Benutzer und Gruppen für dieses Projekt festzulegen.



Projektstatus aktualisieren

Mit dieser Berechtigung können Benutzer ohne Administratorrechte, denen sie erteilt wurde, ein Projekt über die Schaltfläche Aktionen auf der Seite Projekte aktivieren oder deaktivieren.

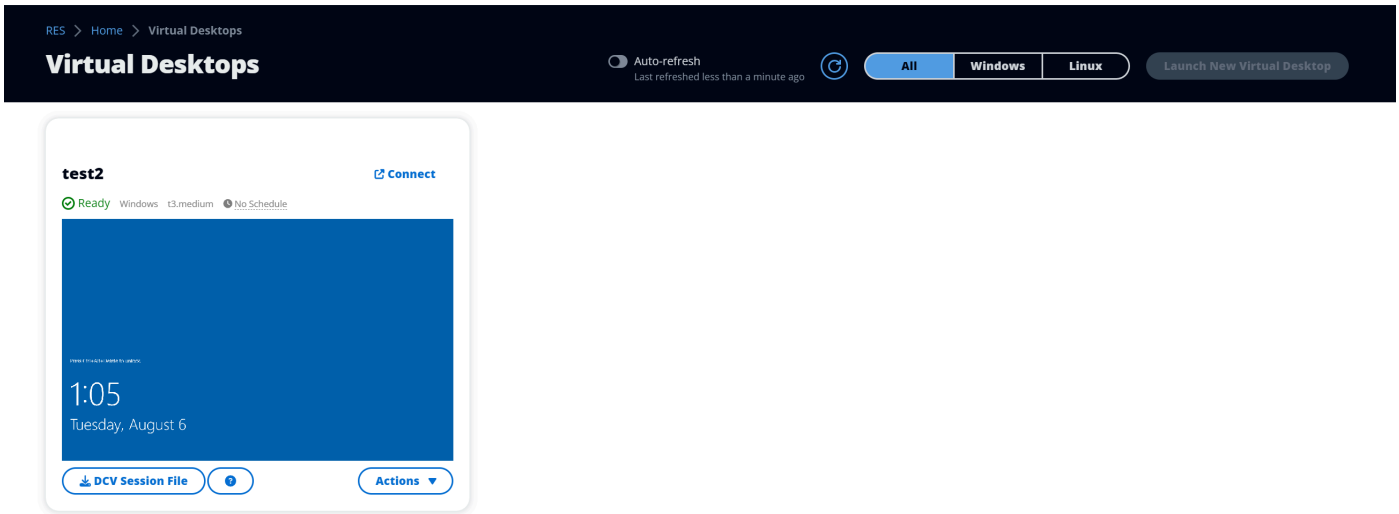


Berechtigungen für die Verwaltung von VDI-Sitzungen

Erstellen Sie eine Sitzung

Steuert, ob ein Benutzer auf der Seite Meine virtuellen Desktops seine eigene VDI-Sitzung starten darf. Deaktivieren Sie diese Option, um Benutzern ohne Administratorrechte die Möglichkeit zu verweigern, ihre eigenen VDI-Sitzungen zu starten. Benutzer können ihre eigenen VDI-Sitzungen jederzeit beenden und beenden.

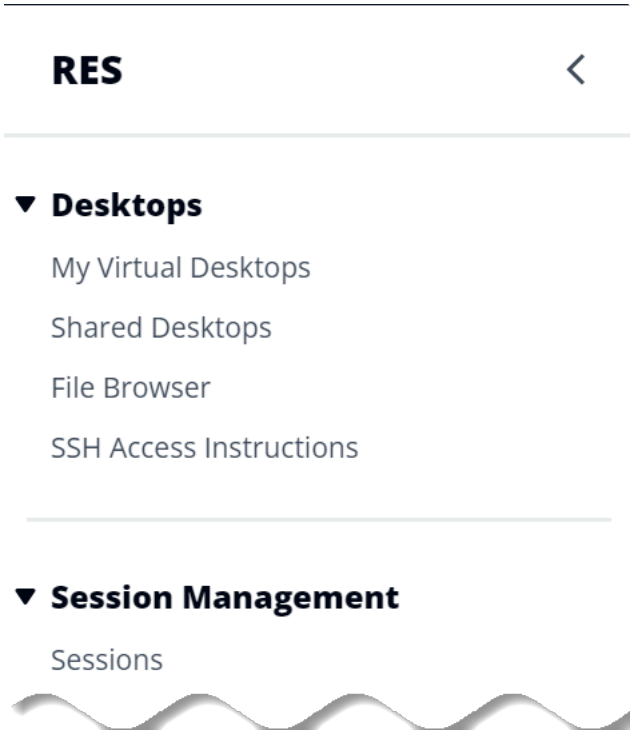
Wenn ein Benutzer ohne Administratorrechte keine Berechtigungen zum Erstellen einer Sitzung hat, wird die Schaltfläche „Neuen virtuellen Desktop starten“ für ihn deaktiviert, wie hier gezeigt:



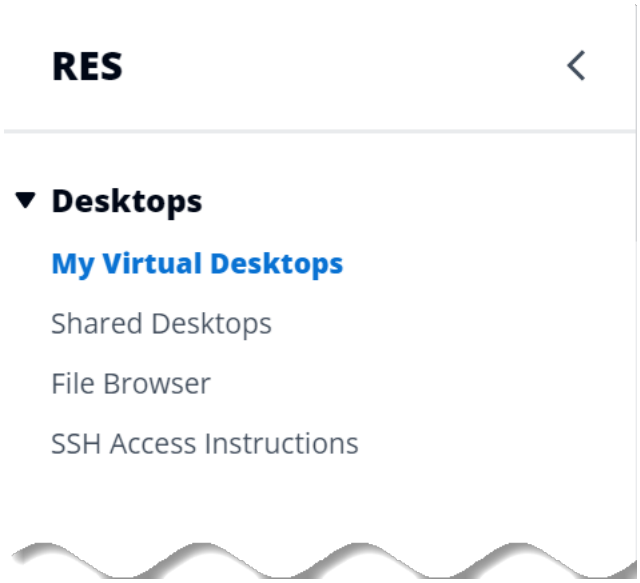
Erstellen oder beenden Sie die Sitzungen anderer

Ermöglicht Benutzern ohne Administratorrechte den Zugriff auf die Sitzungsseite über den linken Navigationsbereich. Diese Benutzer können VDI-Sitzungen für andere Benutzer in den Projekten starten, für die ihnen diese Berechtigung erteilt wurde.

Wenn ein Benutzer ohne Administratorrechte berechtigt ist, Sitzungen für andere Benutzer zu starten, wird in seinem linken Navigationsbereich unter Sitzungsverwaltung der Link Sitzungen angezeigt, wie hier dargestellt:



Wenn ein Benutzer ohne Administratorrechte nicht berechtigt ist, Sitzungen für andere zu erstellen, wird in seinem linken Navigationsbereich die Sitzungsverwaltung nicht angezeigt, wie hier gezeigt:

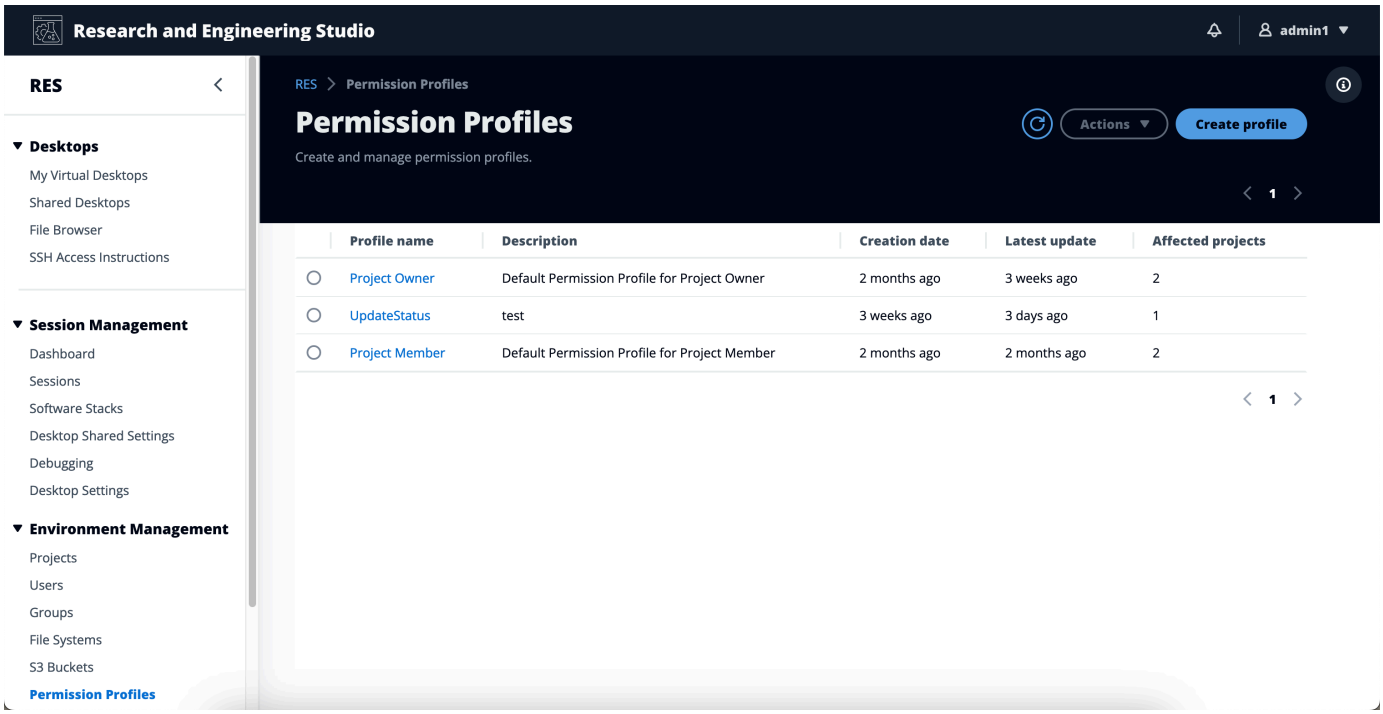


Verwaltung von Berechtigungsprofilen

Als RES-Administrator können Sie die folgenden Aktionen ausführen, um Berechtigungsprofile zu verwalten.

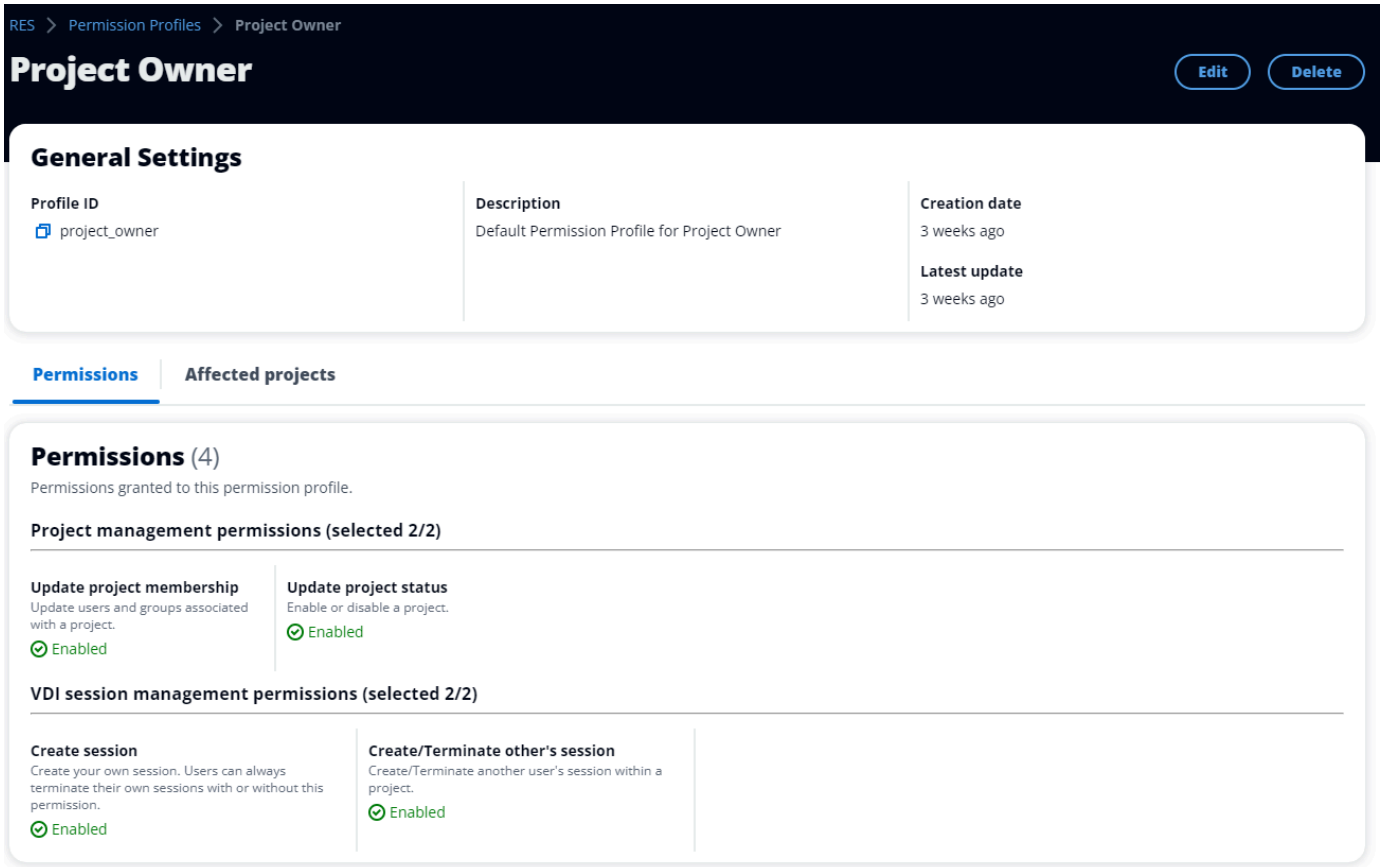
Berechtigungsprofile auflisten

- Wählen Sie auf der Konsolenseite von Research and Engineering Studio im linken Navigationsbereich die Option Berechtigungsprofile aus. Auf dieser Seite können Sie Berechtigungsprofile erstellen, aktualisieren, auflisten, anzeigen und löschen.

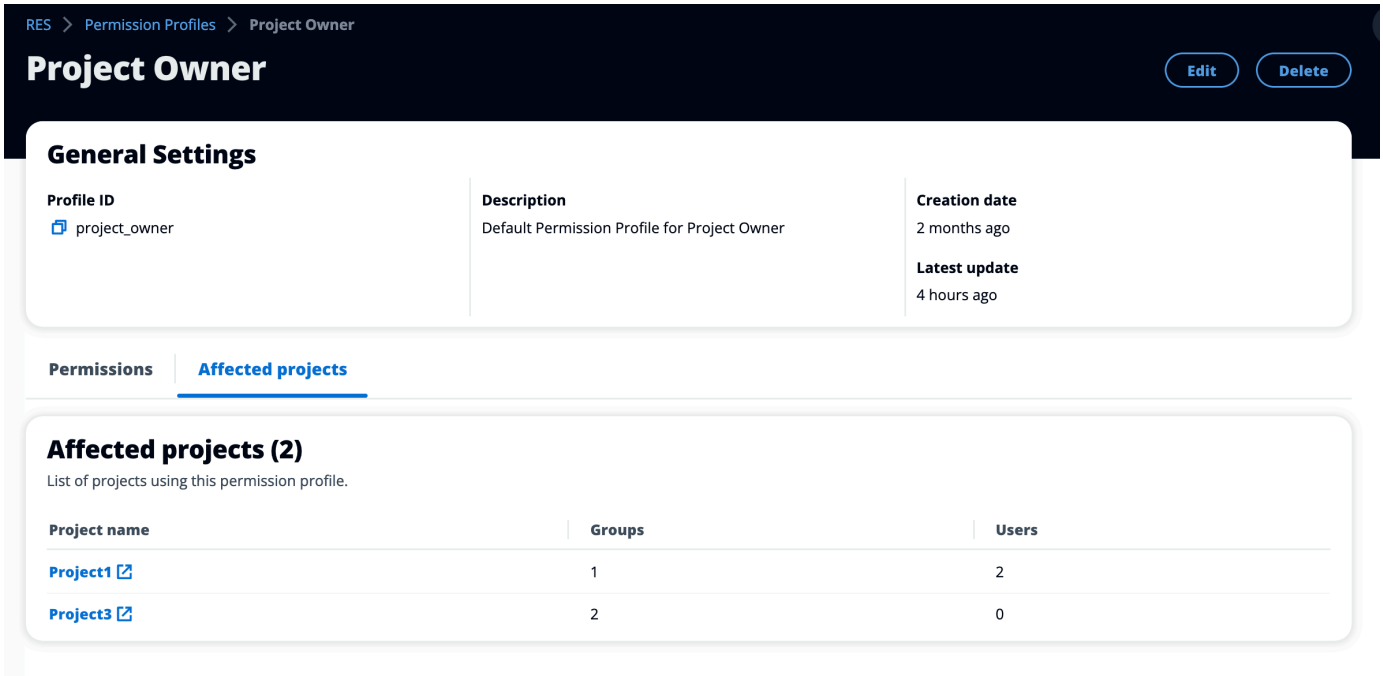


Berechtigungsprofile anzeigen

1. Wählen Sie auf der Hauptseite „Berechtigungsprofile“ den Namen des Berechtigungsprofils aus, das Sie anzeigen möchten. Auf dieser Seite können Sie das ausgewählte Berechtigungsprofil bearbeiten oder löschen.

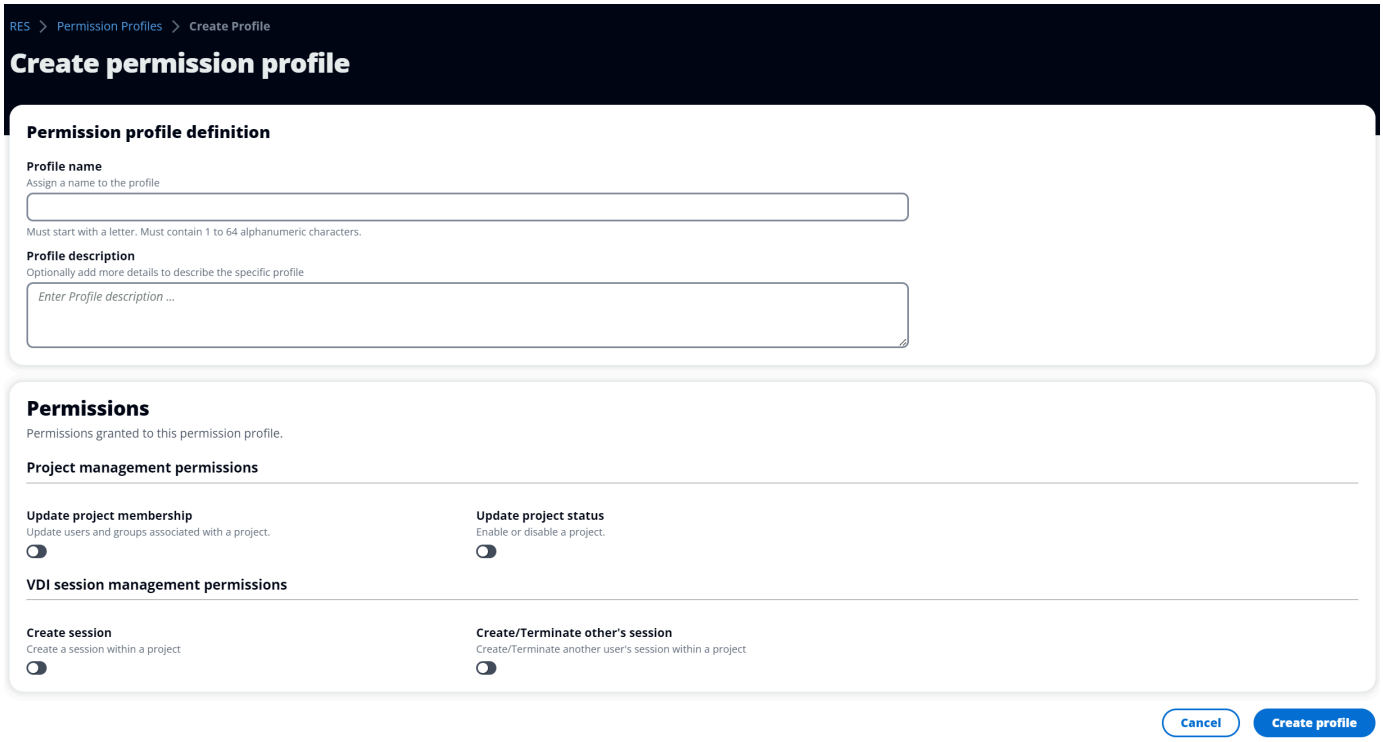


2. Wählen Sie den Tab Betroffene Projekte aus, um die Projekte anzuzeigen, die derzeit das Berechtigungsprofil verwenden.



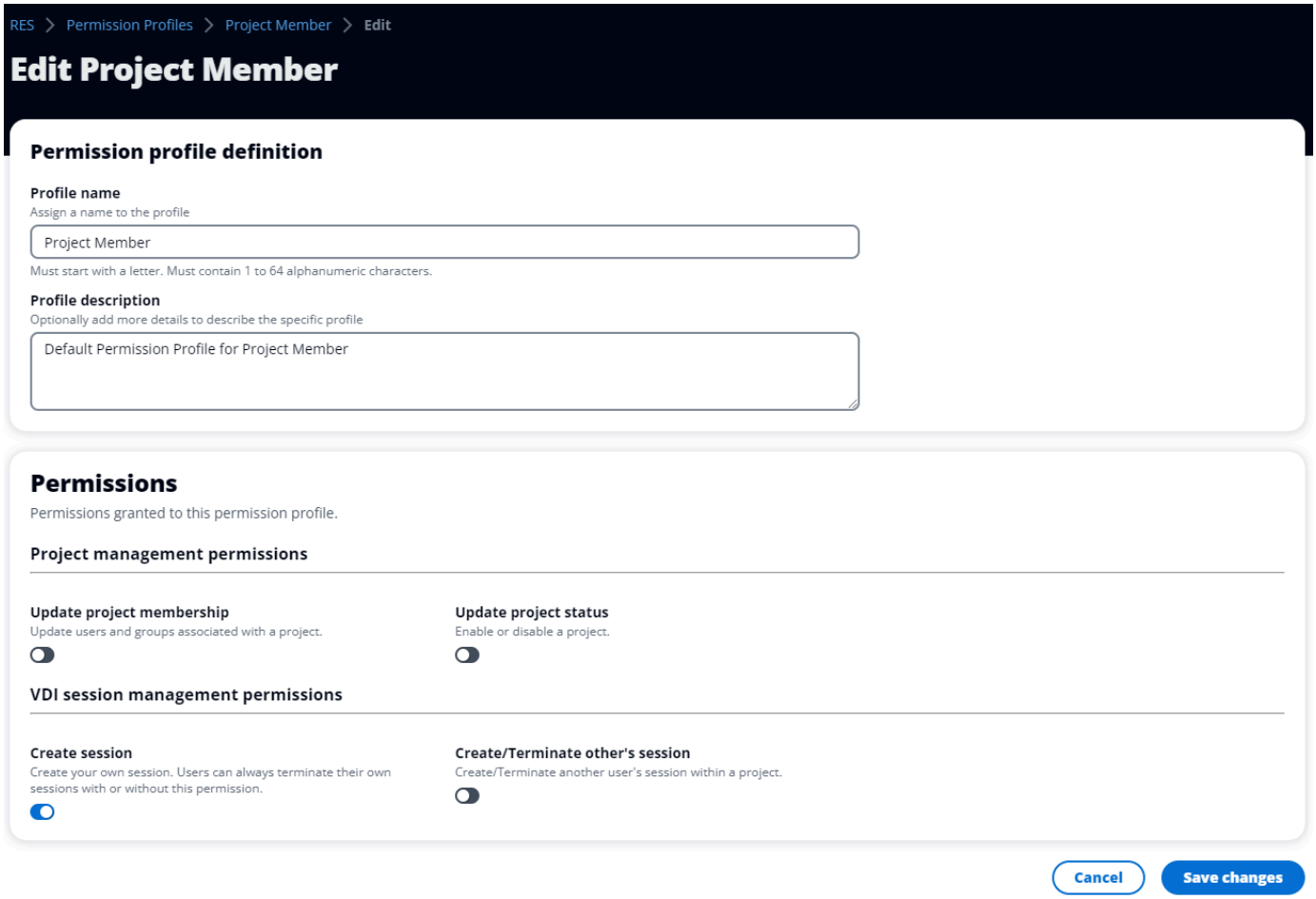
Berechtigungsprofile erstellen

1. Wählen Sie auf der Hauptseite „Berechtigungsprofile“ die Option Profil erstellen aus, um ein Berechtigungsprofil zu erstellen.
2. Geben Sie einen Namen und eine Beschreibung für das Berechtigungsprofil ein und wählen Sie dann die Berechtigungen aus, die Sie den Benutzern oder Gruppen gewähren möchten, die Sie diesem Profil zuweisen.



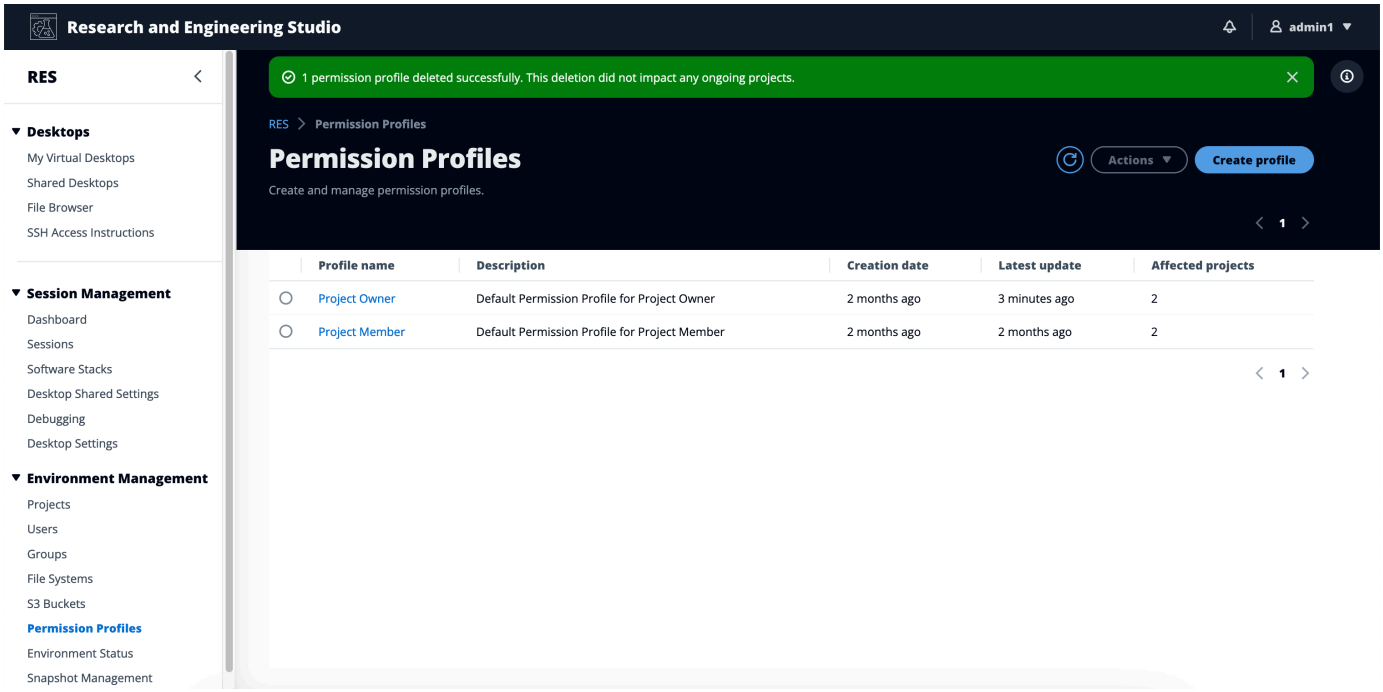
Berechtigungsprofile bearbeiten

- Wählen Sie auf der Hauptseite der Berechtigungsprofile ein Profil aus, indem Sie auf den Kreis neben dem Profil klicken, Aktionen auswählen und dann Profil bearbeiten auswählen, um das Berechtigungsprofil zu aktualisieren.



Berechtigungsprofile löschen

- Wählen Sie auf der Hauptseite mit den Berechtigungsprofilen ein Profil aus, indem Sie auf den Kreis neben dem Profil klicken, Aktionen und dann Profil löschen auswählen. Sie können kein Berechtigungsprofil löschen, das von einem vorhandenen Projekt verwendet wird.



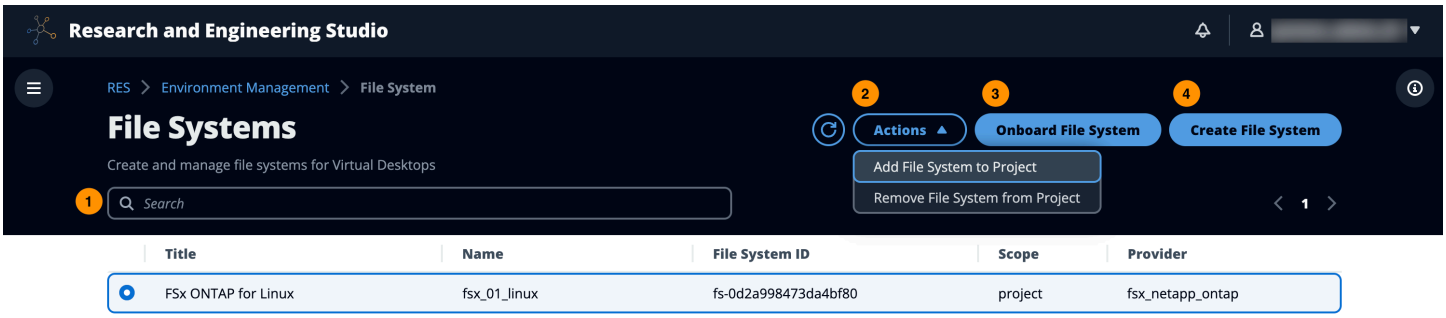
Standardberechtigungsprofile

Jedes RES-Projekt verfügt über zwei Standard-Berechtigungsprofile, die globale Administratoren konfigurieren können. (Darüber hinaus können globale Administratoren neue Berechtigungsprofile für ein Projekt erstellen und ändern.) Die folgende Tabelle zeigt die zulässigen Berechtigungen für die Standard-Berechtigungsprofile „Projektmitglied“ und „Projekteigentümer“. Berechtigungsprofile und die Berechtigungen, die sie ausgewählten Benutzern eines Projekts gewähren, gelten nur für das Projekt, zu dem sie gehören. Globale Administratoren sind Superuser, die über alle unten aufgeführten Berechtigungen für alle Projekte verfügen.

Berechtigungen	Beschreibung	Mitglied des Projekts	Eigentümer des Projekts	
Sitzung erstellen	Erstellen Sie Ihre eigene Sitzung. Benutzer können ihre eigenen Sitzungen jederzeit mit oder ohne diese Erlaubnis	X	X	

Berechtigungen	Beschreibung	Mitglied des Projekts	Eigentümer des Projekts	
	beenden und beenden.			
Sitzungen anderer erstellen /beenden	Erstellen oder beenden Sie die Sitzung eines anderen Benutzers innerhalb eines Projekts.		X	
Aktualisieren Sie die Projektmitgliedschaft	Aktualisieren Sie Benutzer und Gruppen, die einem Projekt zugeordnet sind.		X	
Projektstatus aktualisieren	Aktiviert oder deaktiviert ein Projekt.		X	

Dateisysteme



Auf der Seite Dateisysteme können Sie:

1. Suchen Sie nach Dateisystemen.
2. Wenn ein Dateisystem ausgewählt ist, verwenden Sie das Menü Aktionen, um:

   a. Fügen Sie das Dateisystem zu einem Projekt hinzu
   b. Entfernen Sie das Dateisystem aus einem Projekt
3. Integrieren Sie ein neues Dateisystem.
4. Erstellen eines Dateisystems.
5. Wenn ein Dateisystem ausgewählt ist, können Sie den Bereich am unteren Bildschirmrand erweitern, um Dateisystemdetails anzuzeigen.

Erstellen Sie ein Dateisystem

1. Klicken Sie auf Create File System (Dateisystem erstellen).
2. Geben Sie die Details für das neue Dateisystem ein.
3. Stellen Sie das Subnetz IDs von der VPC aus bereit. Sie finden das auf IDs der Registerkarte Environment Management > Einstellungen > Netzwerk.
4. Wählen Sie Absenden aus.

Create new File System

Title
Enter a user friendly file system title

Eg. EFS 01

Name
Enter a file system name

File System name can only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

File System Provider
Select applicable file system type

EFS

Projects
Select applicable project

Subnet ID 1
Enter subnet id to create mount target

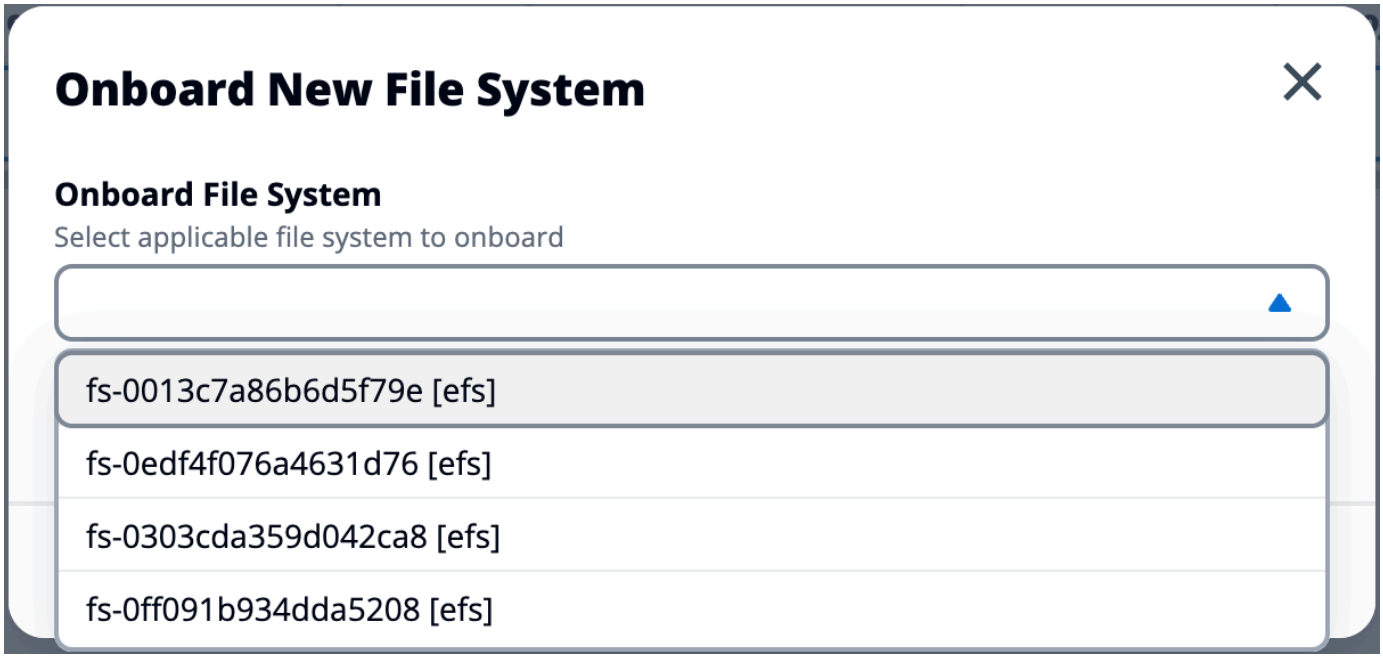
Subnet ID 2
Enter second subnet to create mount target

Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory
Enter directory to mount the file system

Integrieren Sie ein Dateisystem

1. Wählen Sie Onboard-Dateisystem.
2. Wählen Sie ein Dateisystem aus der Drop-down-Liste aus. Das Modal wird um zusätzliche Detaileinträge erweitert.



3. Geben Sie die Dateisystemdetails ein.
4. Wählen Sie Absenden aus.

Onboard New File System

Onboard File System

Select applicable file system to onboard

fs-0edf4f076a4631d76 [efs]

Title

Enter a user friendly file system title

File System Name

Enter a file system name

File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

Mount Directory

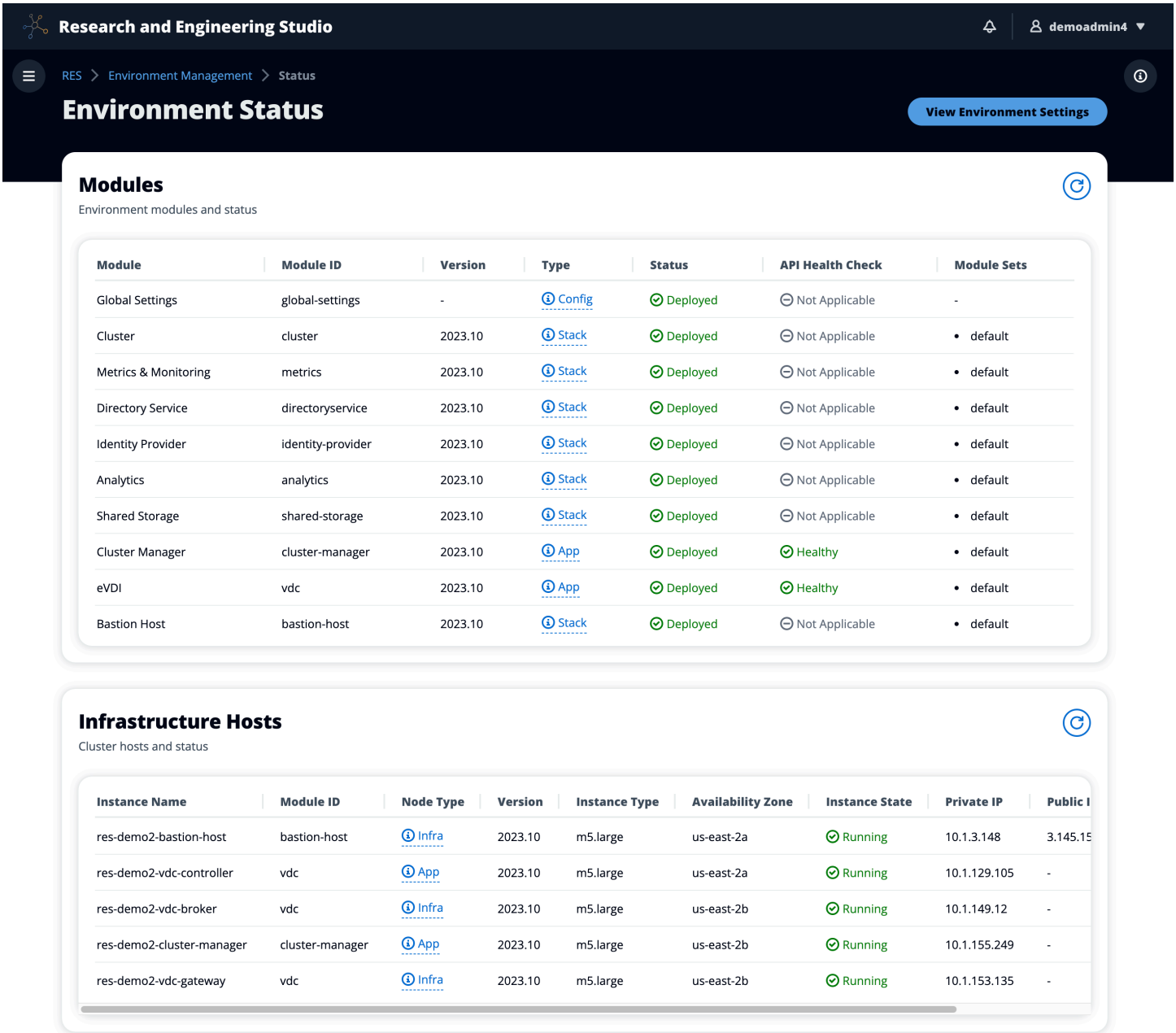
Enter directory to mount the file system

Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01

Cancel Submit

Umgebungsstatus

Auf der Seite Umgebungsstatus werden die im Produkt implementierte Software und die bereitgestellten Hosts angezeigt. Sie enthält Informationen wie Softwareversion, Modulnamen und andere Systeminformationen.

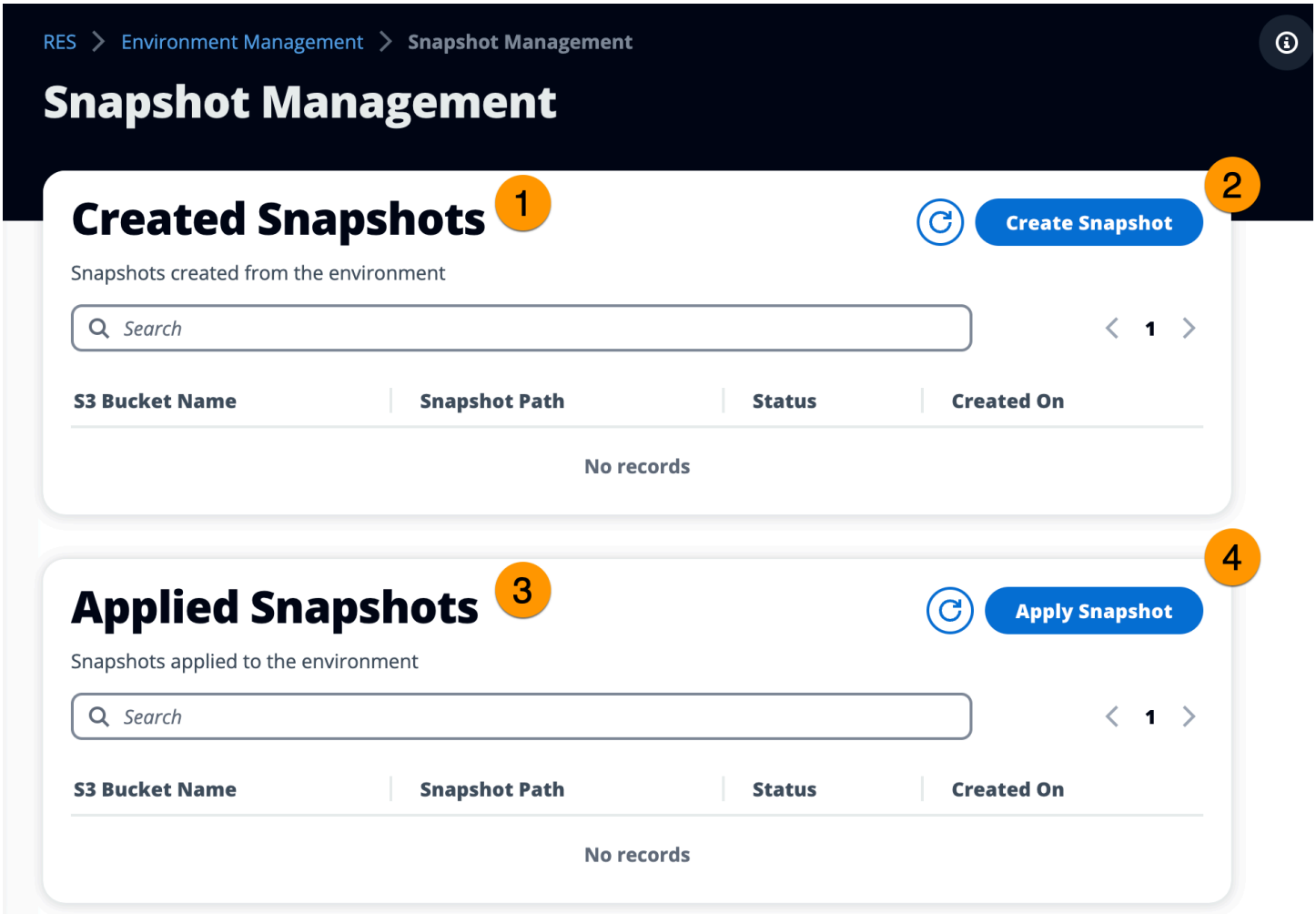


Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10	App	Deployed	Healthy	• default
eVDI	vdc	2023.10	App	Deployed	Healthy	• default
Bastion Host	bastion-host	2023.10	Stack	Deployed	Not Applicable	• default

Instance Name	Module ID	Node Type	Version	Instance Type	Availability Zone	Instance State	Private IP	Public I
res-demo2-bastion-host	bastion-host	Infra	2023.10	m5.large	us-east-2a	Running	10.1.3.148	3.145.15
res-demo2-vdc-controller	vdc	App	2023.10	m5.large	us-east-2a	Running	10.1.129.105	-
res-demo2-vdc-broker	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.149.12	-
res-demo2-cluster-manager	cluster-manager	App	2023.10	m5.large	us-east-2b	Running	10.1.155.249	-
res-demo2-vdc-gateway	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.153.135	-

Snapshot-Verwaltung

Das Snapshot-Management vereinfacht das Speichern und Migrieren von Daten zwischen Umgebungen und gewährleistet so Konsistenz und Genauigkeit. Mit Snapshots können Sie Ihren Umgebungsstatus speichern und Daten in eine neue Umgebung mit demselben Status migrieren.



Auf der Snapshot-Verwaltungsseite können Sie:

1. Alle erstellten Snapshots und ihren Status anzeigen.
2. Erstellen Sie einen Snapshot. Bevor Sie einen Snapshot erstellen können, müssen Sie einen Bucket mit den entsprechenden Berechtigungen erstellen.
3. Alle angewendeten Snapshots und ihren Status anzeigen.
4. Wenden Sie einen Snapshot an.

Snapshot erstellen

Bevor Sie einen Snapshot erstellen können, müssen Sie einen Amazon S3 S3-Bucket mit den erforderlichen Berechtigungen bereitstellen. Informationen zum Erstellen eines Buckets finden Sie unter Erstellen eines Buckets. Wir empfehlen, die Bucket-Versionierung und die Serverzugriffsprotokollierung zu aktivieren. Diese Einstellungen können nach der Bereitstellung auf der Registerkarte „Eigenschaften“ des Buckets aktiviert werden.

> **Note**
>
> Der Lebenszyklus dieses Amazon S3 S3-Buckets wird nicht innerhalb des Produkts verwaltet. Sie müssen den Bucket-Lebenszyklus von der Konsole aus verwalten.

So fügen Sie dem Bucket Berechtigungen hinzu:

1. Wählen Sie den Bucket, den Sie erstellt haben, aus der Buckets-Liste aus.
2. Wählen Sie die Registerkarte Berechtigungen.
3. Wählen Sie unter Bucket-Richtlinie Bearbeiten aus.
4. Fügen Sie der Bucket-Richtlinie die folgende Anweisung hinzu. Ersetzen Sie diese Werte durch Ihre eigenen Werte:
   - AWS_ACCOUNT_ID
   - NAME DER RES_UMGEBUNG
   - AWS_REGION
   - S3_BUCKETNAME

   > **Important**
   >
   > Es gibt begrenzte Versionszeichenfolgen, die von unterstützt werden. AWS Weitere Informationen finden Sie unter https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

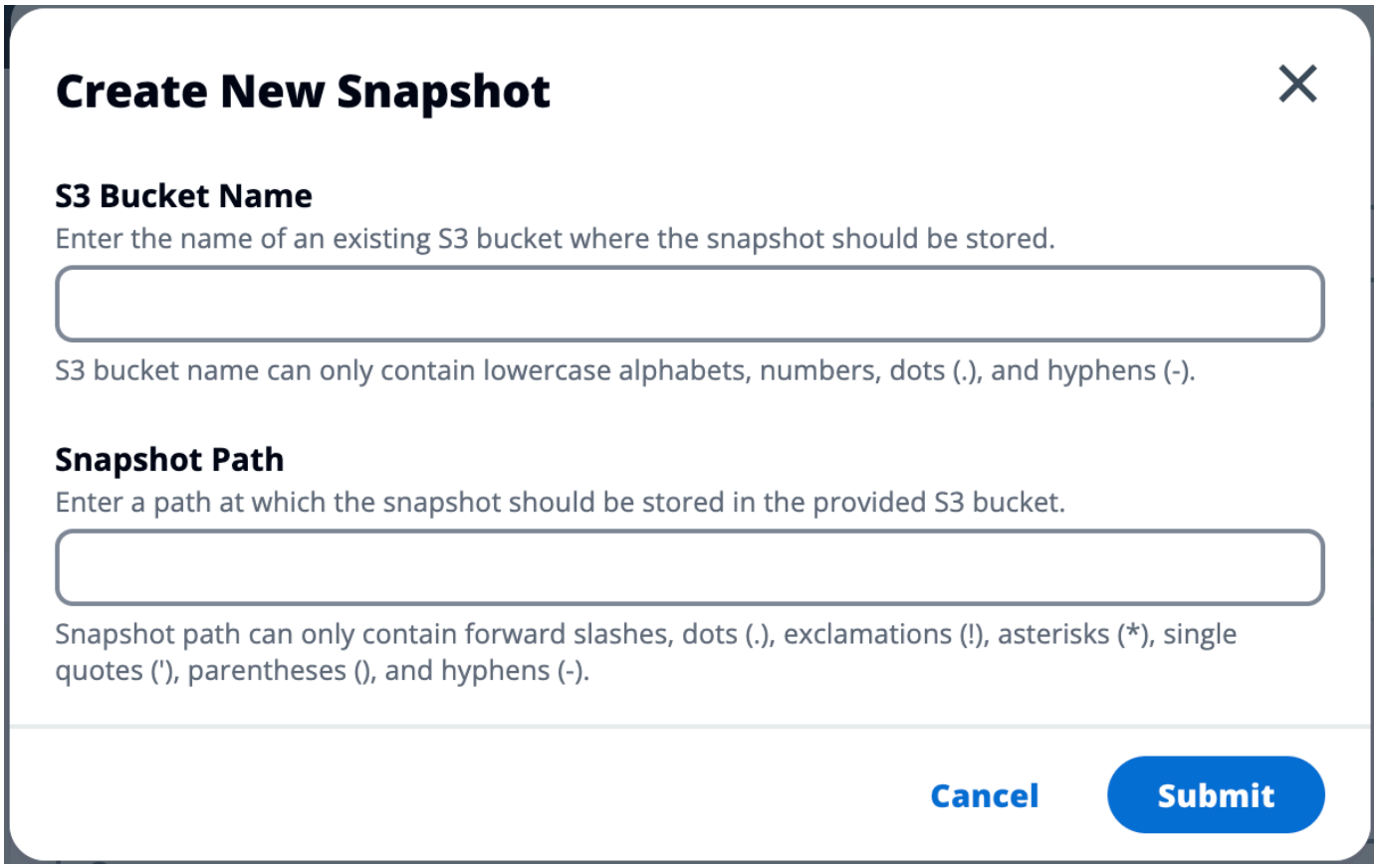
JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
```

```
}
```

Um den Snapshot zu erstellen:

1. Wählen Sie Create Snapshot (Snapshot erstellen) aus.
2. Geben Sie den Namen des Amazon S3 S3-Buckets ein, den Sie erstellt haben.
3. Geben Sie den Pfad ein, in dem der Snapshot im Bucket gespeichert werden soll. Beispiel, **`october2023/23`**.
4. Wählen Sie Absenden aus.



5. Wählen Sie nach fünf bis zehn Minuten auf der Seite Snapshots die Option Aktualisieren aus, um den Status zu überprüfen. Ein Snapshot ist erst gültig, wenn sich der Status von IN_PROGRESS auf COMPLETED ändert.

Wenden Sie einen Snapshot an

Sobald Sie einen Snapshot einer Umgebung erstellt haben, können Sie diesen Snapshot auf eine neue Umgebung anwenden, um Daten zu migrieren. Sie müssen dem Bucket eine neue Richtlinie hinzufügen, die es der Umgebung ermöglicht, den Snapshot zu lesen.

Durch das Anwenden eines Snapshots werden Daten wie Benutzerberechtigungen, Projekte, Software-Stacks, Berechtigungsprofile und Dateisysteme mit ihren Verknüpfungen in eine neue Umgebung kopiert. Benutzersitzungen werden nicht repliziert. Wenn der Snapshot angewendet wird, überprüft er die Basisinformationen der einzelnen Ressourceneinträge, um festzustellen, ob sie bereits vorhanden sind. Bei doppelten Datensätzen überspringt der Snapshot die Erstellung von Ressourcen in der neuen Umgebung. Bei Datensätzen, die ähnlich sind, z. B. einen gemeinsamen Namen oder Schlüssel, aber andere grundlegende Ressourceninformationen variieren, wird ein neuer Datensatz mit einem geänderten Namen und Schlüssel erstellt, wobei die folgende Konvention verwendet wird:`RecordName_SnapshotRESVersion_ApplySnapshotID`. Der `ApplySnapshotID` sieht aus wie ein Zeitstempel und kennzeichnet jeden Versuch, einen Snapshot anzuwenden.

Während der Snapshot-Anwendung überprüft der Snapshot die Verfügbarkeit von Ressourcen. Ressourcen, die für die neue Umgebung nicht verfügbar sind, werden nicht erstellt. Bei Ressourcen mit einer abhängigen Ressource prüft der Snapshot, ob die abhängige Ressource verfügbar ist. Wenn die abhängige Ressource nicht verfügbar ist, wird die Hauptressource ohne die abhängige Ressource erstellt.

Wenn die neue Umgebung nicht wie erwartet funktioniert oder ausfällt, können Sie in den CloudWatch Protokollen in der Protokollgruppe `/res-<env-name>/cluster-manager` nach Einzelheiten suchen. Jedes Protokoll wird mit dem Tag [Snapshot anwenden] versehen. Sobald Sie einen Snapshot angewendet haben, können Sie seinen Status the section called “Snapshot-Verwaltung” auf der Seite überprüfen.

So fügen Sie dem Bucket Berechtigungen hinzu:

1. Wählen Sie den Bucket, den Sie erstellt haben, aus der Buckets-Liste aus.
2. Wählen Sie die Registerkarte Berechtigungen.
3. Wählen Sie unter Bucket-Richtlinie Bearbeiten aus.
4. Fügen Sie der Bucket-Richtlinie die folgende Anweisung hinzu. Ersetzen Sie diese Werte durch Ihre eigenen Werte:

   - AWS_ACCOUNT_ID

- RES_ENVIRONMENT_NAME
- AWS_REGION
- S3_BUCKETNAME

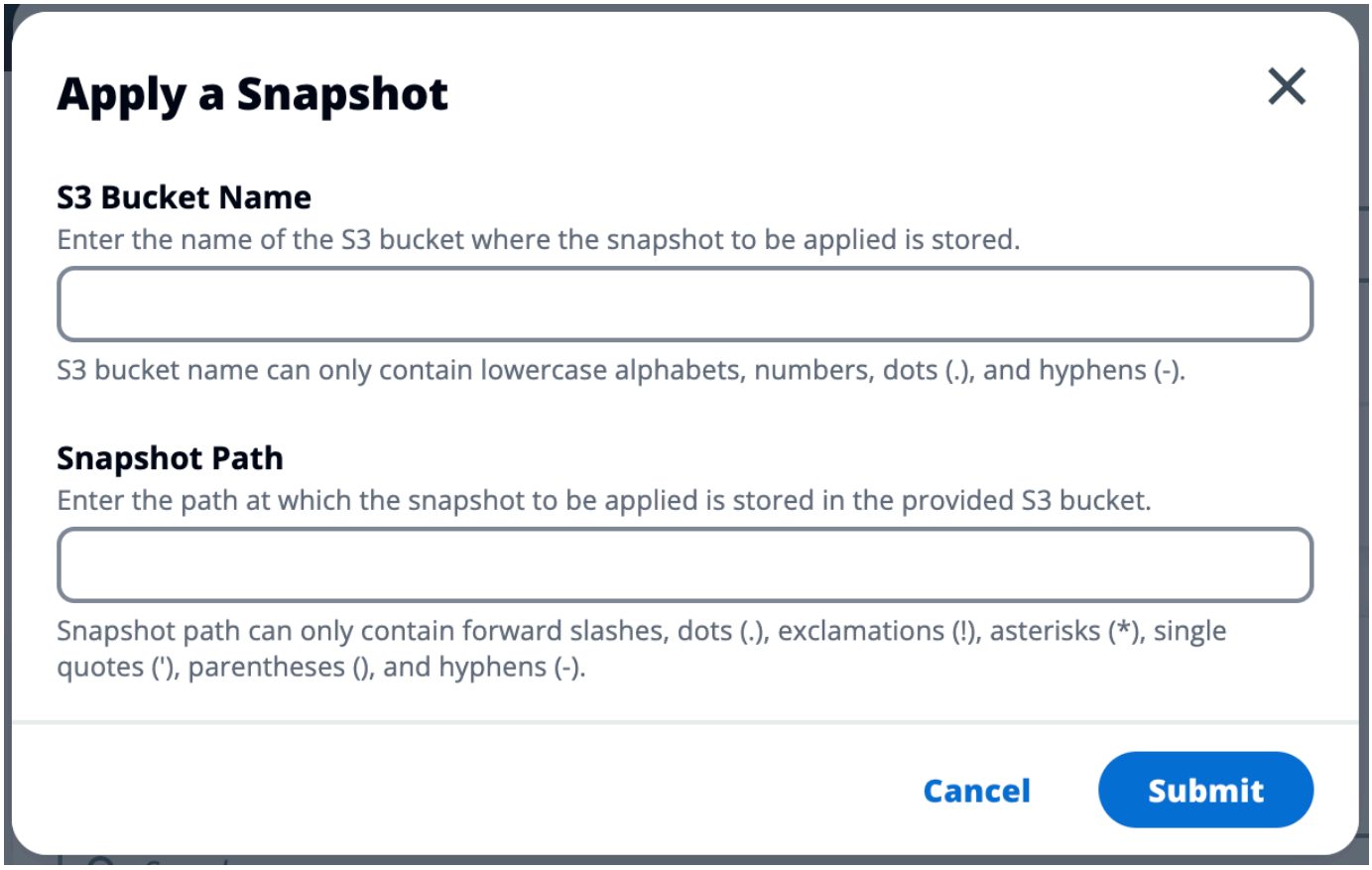
JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
```

```
    ]
}
```

So wenden Sie den Snapshot an:

1. Wählen Sie Snapshot anwenden.
2. Geben Sie den Namen des Amazon S3 S3-Buckets ein, der den Snapshot enthält.
3. Geben Sie den Dateipfad zum Snapshot innerhalb des Buckets ein.
4. Wählen Sie Absenden aus.



5. Wählen Sie nach fünf bis zehn Minuten auf der Snapshot-Verwaltungsseite die Option Aktualisieren aus, um den Status zu überprüfen.

Umgebungseinstellungen

In den Umgebungseinstellungen werden Details zur Produktkonfiguration angezeigt, z. B.:

- Allgemeines

Zeigt Informationen wie den Administrator-Benutzernamen und die E-Mail-Adresse des Benutzers an, der das Produkt bereitgestellt hat. Sie können den Titel des Webportals und den Copyright-Text bearbeiten.

- Identitätsanbieter

  Zeigt Informationen wie den Single Sign-On-Status an.

- Netzwerk

  Zeigt die VPC-ID und die Präfixliste IDs für den Zugriff an.

- Directory Service

  Zeigt Active Directory-Einstellungen und den ARN des Service Account Secrets Manager für Benutzername und Passwort an.

Amazon-S3-Buckets

Themen

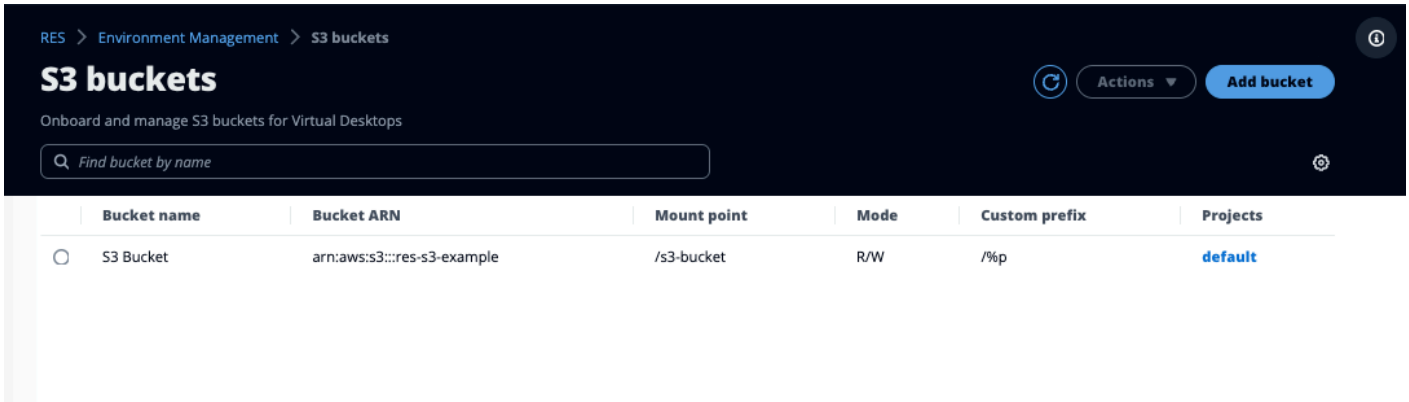
- Mounten Sie einen Amazon S3 S3-Bucket
- Einen Amazon S3 S3-Bucket hinzufügen
- Einen Amazon S3 S3-Bucket bearbeiten
- Einen Amazon S3 S3-Bucket entfernen
- Datenisolierung
- Kontoübergreifender Bucket-Zugriff
- Verhinderung der Datenexfiltration in einer privaten VPC
- Fehlerbehebung
- Wird aktiviert CloudTrail

Mounten Sie einen Amazon S3 S3-Bucket

Research and Engineering Studio (RES) unterstützt das Mounten von Amazon S3 S3-Buckets auf Linux Virtual Desktop Infrastructure (VDI) -Instances. RES-Administratoren können S3-Buckets in RES integrieren, sie an Projekte anhängen, ihre Konfiguration bearbeiten und Buckets auf der Registerkarte S3-Buckets unter Environment Management entfernen.

Das S3-Buckets-Dashboard bietet eine Liste der integrierten S3-Buckets, die Ihnen zur Verfügung stehen. Über das S3-Buckets-Dashboard können Sie:

1. Verwenden Sie Bucket hinzufügen, um einen S3-Bucket in RES zu integrieren.
2. Wählen Sie einen S3-Bucket aus und verwenden Sie das Aktionsmenü, um:
   - Bearbeiten Sie einen Bucket
   - Einen Bucket entfernen
3. Verwenden Sie das Suchfeld, um nach dem Bucket-Namen zu suchen und integrierte S3-Buckets zu finden.



Einen Amazon S3 S3-Bucket hinzufügen

So fügen Sie Ihrer RES-Umgebung einen S3-Bucket hinzu:

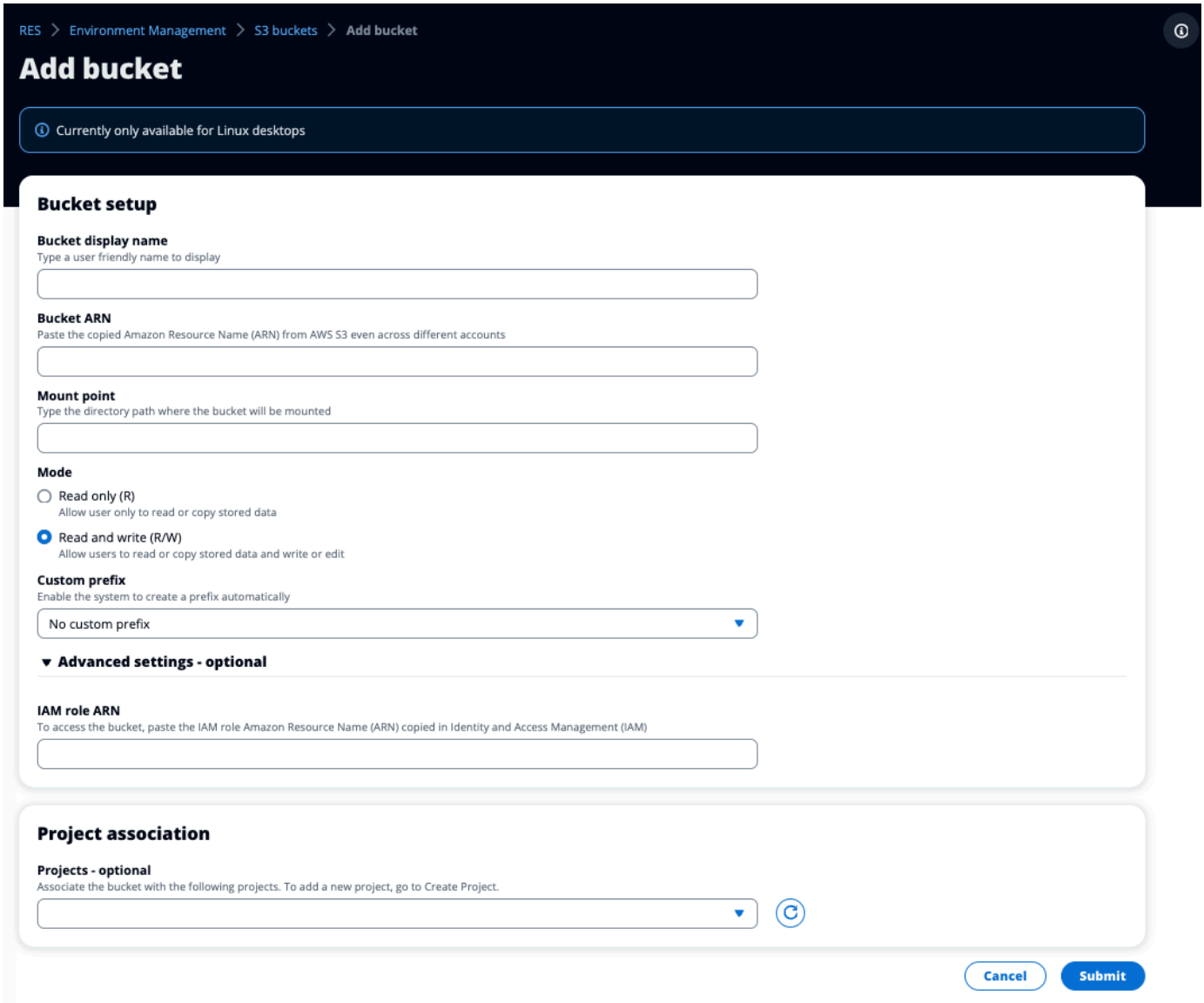
1. Wählen Sie Add bucket (Bucket hinzufügen) aus.
2. Geben Sie die Bucket-Details wie Bucket-Name, ARN und Bereitstellungspunkt ein.

> **Important**
>
> - Der bereitgestellte Bucket ARN, der Bereitstellungspunkt und der bereitgestellte Modus können nach der Erstellung nicht geändert werden.
> - Der Bucket-ARN kann ein Präfix enthalten, das den integrierten S3-Bucket von diesem Präfix isoliert.

3. Wählen Sie einen Modus aus, in dem Sie Ihren Bucket einbinden möchten.

> **Important**
>
> - Weitere Informationen Datenisolierung zur Datenisolierung mit bestimmten Modi finden Sie unter.

4. Unter Erweiterte Optionen können Sie einen IAM-Rollen-ARN angeben, um die Buckets für den kontoübergreifenden Zugriff bereitzustellen. Folgen Sie den Schritten unterKontoübergreifender Bucket-Zugriff, um die erforderliche IAM-Rolle für den kontoübergreifenden Zugriff zu erstellen.
5. (Optional) Ordnen Sie den Bucket Projekten zu, die später geändert werden können. Ein S3-Bucket kann jedoch nicht in die vorhandenen VDI-Sitzungen eines Projekts eingebunden werden. Nur Sitzungen, die gestartet werden, nachdem das Projekt dem Bucket zugeordnet wurde, werden den Bucket mounten.
6. Wählen Sie Absenden aus.



Einen Amazon S3 S3-Bucket bearbeiten

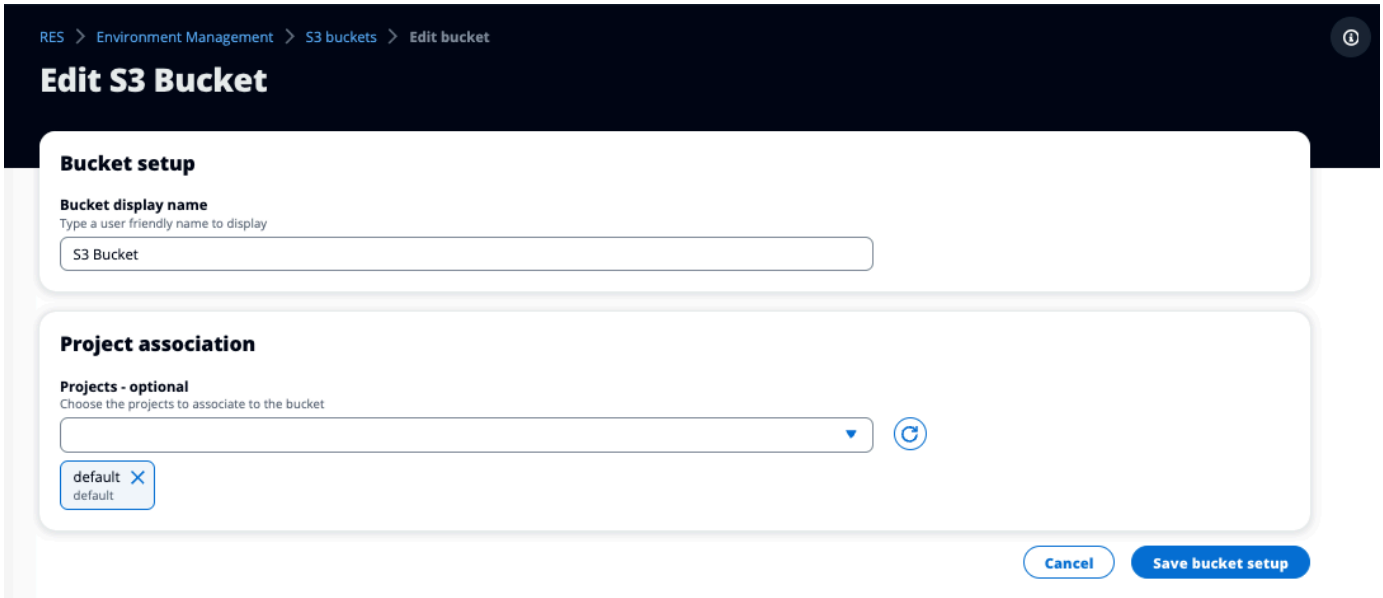
1. Wählen Sie einen S3-Bucket in der S3-Buckets-Liste aus.
2. Wählen Sie im Menü Aktionen die Option Bearbeiten.
3. Geben Sie Ihre Aktualisierungen ein.

> **Important**
>
> - Wenn Sie ein Projekt einem S3-Bucket zuordnen, wird der Bucket nicht in die vorhandenen VDI-Instanzen (Virtual Desktop Infrastructure) dieses Projekts

eingebunden. Der Bucket wird nur für VDI-Sitzungen bereitgestellt, die in einem Projekt gestartet werden, nachdem der Bucket diesem Projekt zugeordnet wurde.

- Das Trennen eines Projekts von einem S3-Bucket hat keine Auswirkungen auf die Daten im S3-Bucket, führt jedoch dazu, dass Desktop-Benutzer den Zugriff auf diese Daten verlieren.

4. Wählen Sie Bucket-Setup speichern.



Einen Amazon S3 S3-Bucket entfernen

1. Wählen Sie einen S3-Bucket in der S3-Buckets-Liste aus.
2. Wählen Sie im Menü Aktionen die Option Entfernen aus.

> **Important**
>
> - Sie müssen zuerst alle Projektzuordnungen aus dem Bucket entfernen.
> - Der Entfernungsvorgang hat keine Auswirkungen auf die Daten im S3-Bucket. Es entfernt nur die Zuordnung des S3-Buckets zu RES.
> - Wenn Sie einen Bucket entfernen, verlieren bestehende VDI-Sitzungen nach Ablauf der Anmeldeinformationen dieser Sitzung (~1 Stunde) den Zugriff auf den Inhalt dieses Buckets.

Datenisolierung

Wenn Sie RES einen S3-Bucket hinzufügen, haben Sie die Möglichkeit, die Daten innerhalb des Buckets für bestimmte Projekte und Benutzer zu isolieren. Auf der Seite Bucket hinzufügen können Sie den Modus Schreibgeschützt (R) oder Lesen und Schreiben (R/W) wählen.

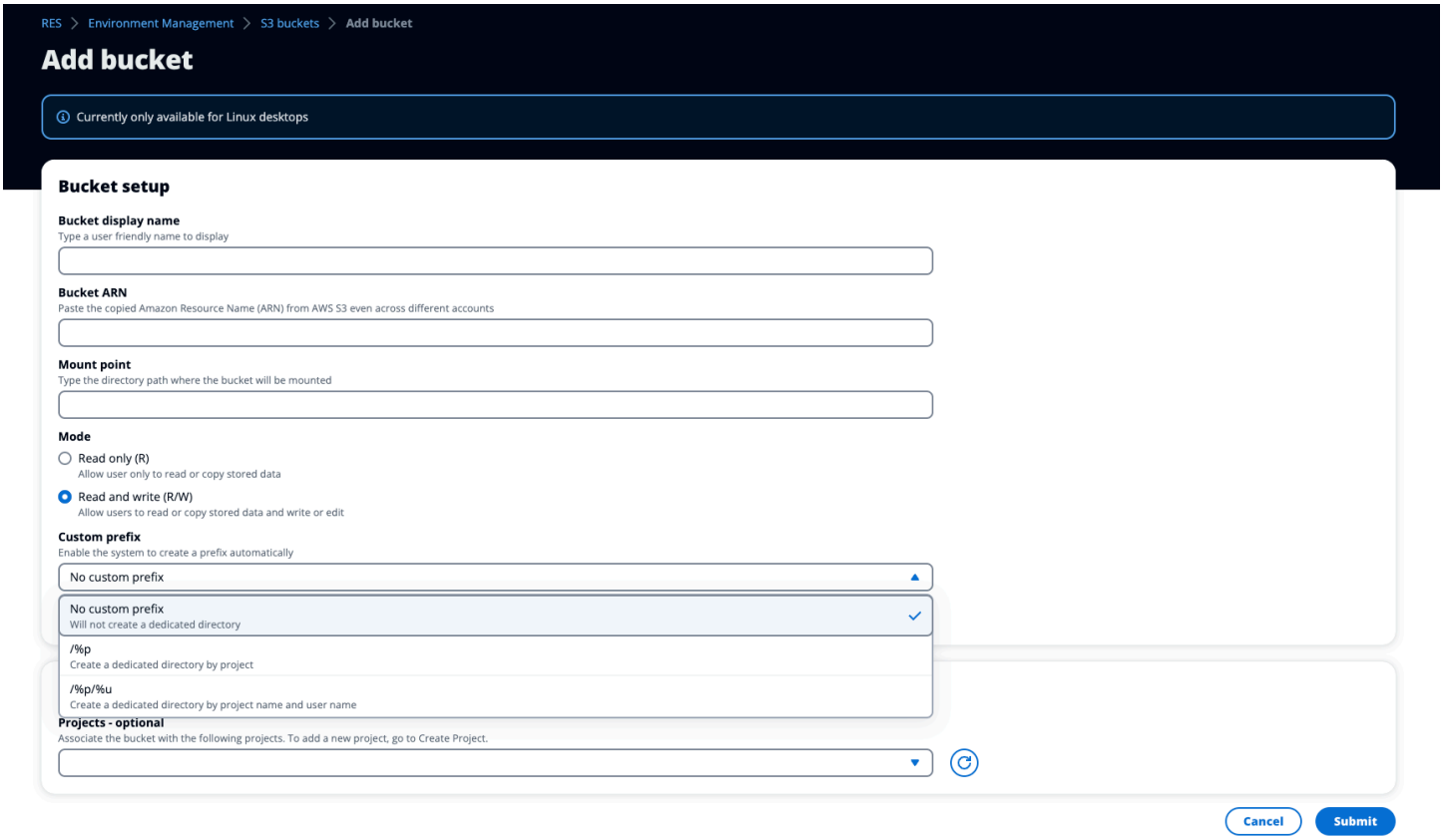
Nur lesen

Wenn ausgewählt, `Read Only (R)` wird die Datenisolierung basierend auf dem Präfix des Bucket-ARN (Amazon Resource Name) erzwungen. Wenn ein Administrator beispielsweise mithilfe des ARN einen Bucket zu RES hinzufügt `arn:aws:s3:::`*`bucket-name/example-data`*`/` und diesen Bucket mit Projekt A und Projekt B verknüpft, können Benutzer, die von Projekt A und Projekt B VDIs aus starten, nur die Daten lesen, die sich *`bucket-name`* unter dem Pfad befinden*`/example-data`*. Sie haben keinen Zugriff auf Daten außerhalb dieses Pfads. Wenn dem Bucket-ARN kein Präfix angehängt wird, wird der gesamte Bucket für jedes damit verknüpfte Projekt verfügbar gemacht.

Lesen und Schreiben

Wenn diese Option ausgewählt `Read and Write (R/W)` ist, wird die Datenisolierung weiterhin auf der Grundlage des Präfix des Bucket-ARN erzwungen, wie oben beschrieben. Dieser Modus bietet zusätzliche Optionen, mit denen Administratoren variablenbasierte Präfixe für den S3-Bucket angeben können. Wenn diese Option ausgewählt `Read and Write (R/W)` ist, wird ein Abschnitt Benutzerdefiniertes Präfix verfügbar, der ein Dropdownmenü mit den folgenden Optionen bietet:

- Kein benutzerdefiniertes Präfix
- /%p
- /%p/%u



Keine benutzerdefinierte Datenisolierung

Wenn die Option Benutzerdefiniertes Präfix ausgewählt `No custom prefix` ist, wird der Bucket ohne benutzerdefinierte Datenisolierung hinzugefügt. Dadurch können alle mit dem Bucket verknüpften Projekte Lese- und Schreibzugriff haben. Wenn ein Administrator beispielsweise mithilfe des ARN `arn:aws:s3:::`*`bucket-name`* mit `No custom prefix` selected einen Bucket zu RES hinzufügt und diesen Bucket mit Projekt A und Projekt B verknüpft, haben Benutzer, die von Projekt A und Projekt B VDIs aus starten, uneingeschränkten Lese- und Schreibzugriff auf den Bucket.

Datenisolierung auf Projektebene

Wenn diese Option für Benutzerdefiniertes Präfix ausgewählt `/%p` ist, werden die Daten im Bucket für jedes spezifische Projekt isoliert, das dem Bucket zugeordnet ist. Die `%p` Variable steht für den Projektcode. Wenn ein Administrator beispielsweise einen Bucket zu RES hinzufügt, indem er den ARN `arn:aws:s3:::`*`bucket-name`* mit `/%p` selected und einem Mount-Point von `/`*`bucket`* verwendet und diesen Bucket mit Projekt A und Projekt B verknüpft, kann Benutzer A in Projekt A eine Datei schreiben`/`*`bucket`*. Benutzer B in Projekt A kann auch die Datei sehen, in

die Benutzer A geschrieben hat*/bucket*. Wenn Benutzer B jedoch einen VDI in Projekt B startet und hineinschaut*/bucket*, wird er die Datei, die Benutzer A geschrieben hat, nicht sehen, da die Daten nach Projekten isoliert sind. Die Datei, die Benutzer A geschrieben hat, befindet sich im S3-Bucket unter dem Präfix, `/ProjectA` während Benutzer B nur darauf zugreifen kann, `/ProjectB` wenn er sie VDIs von Projekt B aus verwendet.

Datenisolierung auf Projekt- und Benutzerebene

Wenn die Option Benutzerdefiniertes Präfix ausgewählt `/%p/%u` ist, werden die Daten im Bucket für jedes spezifische Projekt und jeden Benutzer, der diesem Projekt zugeordnet ist, isoliert. Die `%p` Variable stellt den Projektcode und den Benutzernamen `%u` dar. Ein Administrator fügt beispielsweise einen Bucket zu RES hinzu, indem er den ARN `arn:aws:s3:::`*bucket-name* mit `/%p/%u` selected und dem Mount-Point von verwendet*/bucket*. Dieser Bucket ist mit Projekt A und Projekt B verknüpft. Benutzer A in Projekt A kann eine Datei schreiben*/bucket*. Im Gegensatz zum vorherigen Szenario, bei dem es nur um `%p` Isolation ging, kann Benutzer B in diesem Fall die Datei, in die Benutzer A geschrieben hat, nicht sehen*/bucket*, da die Daten sowohl vom Projekt als auch vom Benutzer isoliert sind. Die Datei, die Benutzer A geschrieben hat, befindet sich im S3-Bucket unter dem Präfix, `/ProjectA/UserA` während Benutzer B nur darauf zugreifen kann`/ProjectA/UserB`, wenn er sie VDIs in Projekt A verwendet.

Kontoübergreifender Bucket-Zugriff

RES ist in der Lage, Buckets von anderen AWS Konten aus zu mounten, sofern diese Buckets über die richtigen Berechtigungen verfügen. Im folgenden Szenario möchte eine RES-Umgebung in Konto A einen S3-Bucket in Konto B bereitstellen.

Schritt 1: Erstellen Sie eine IAM-Rolle in dem Konto, in dem RES bereitgestellt wird (dies wird als Konto A bezeichnet):

1. Melden Sie sich bei der AWS Management Console für das RES-Konto an, das Zugriff auf den S3-Bucket benötigt (Konto A).
2. Öffnen Sie die IAM-Konsole:
   a. Navigieren Sie zum IAM-Dashboard.
   b. Klicken Sie im Navigationsbereich auf Policies (Richtlinien).
3. Erstellen Sie eine Richtlinie:
   a. Wählen Sie Richtlinie erstellen.

b. Wählen Sie den Tab JSON.

c. Fügen Sie die folgende JSON-Richtlinie ein (*<BUCKET-NAME>*ersetzen Sie sie durch den Namen des S3-Buckets in Konto B):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

d. Klicken Sie auf Weiter.

4. Überprüfen und erstellen Sie die Richtlinie:

   a. Geben Sie einen Namen für die Richtlinie ein (z. B. AccessPolicy „S3“).

   b. Fügen Sie eine optionale Beschreibung hinzu, um den Zweck der Richtlinie zu erläutern.

   c. Überprüfen Sie die Richtlinie und wählen Sie Richtlinie erstellen aus.

5. Öffnen Sie die IAM-Konsole:

   a. Navigieren Sie zum IAM-Dashboard.

   b. Wählen Sie im Navigationsbereich die Option Roles (Rollen) aus.

6. Eine Rolle erstellen:

   a. Wählen Sie Create rule (Regel erstellen) aus.

b. Wählen Sie Benutzerdefinierte Vertrauensrichtlinie als Typ der vertrauenswürdigen Entität aus.

c. Fügen Sie die folgende JSON-Richtlinie ein (*<ACCOUNT_ID>*ersetzen Sie sie durch die tatsächliche Konto-ID von Konto A, *<ENVIRONMENT_NAME>* durch den Umgebungsnamen der RES-Bereitstellung und *<REGION>* durch die AWS Region, in der RES bereitgestellt wird):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::<ACCOUNT_ID>:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-<REGION>"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. Wählen Sie „Weiter“.

7. Berechtigungsrichtlinien anhängen:

   a. Suchen Sie nach der Richtlinie, die Sie zuvor erstellt haben, und wählen Sie sie aus.

   b. Wählen Sie „Weiter“.

8. Markieren, überprüfen und erstellen Sie die Rolle:

   a. Geben Sie einen Rollennamen ein (z. B. AccessRole „S3“).

   b. Wählen Sie unter Schritt 3 die Option Tag hinzufügen aus und geben Sie dann den folgenden Schlüssel und Wert ein:

      - Schlüssel: `res:Resource`
      - Wert: `s3-bucket-iam-role`

   c. Überprüfen Sie die Rolle und wählen Sie Rolle erstellen aus.

9. Verwenden Sie die IAM-Rolle in RES:
    a. Kopieren Sie den von Ihnen erstellten IAM-Rollen-ARN.
    b. Melden Sie sich bei der RES-Konsole an.
    c. Wählen Sie im linken Navigationsbereich S3 Bucket aus.
    d. Wählen Sie Bucket hinzufügen und füllen Sie das Formular mit dem kontoübergreifenden S3-Bucket-ARN aus.
    e. Wählen Sie das Drop-down-Menü Erweiterte Einstellungen — optional aus.
    f. Geben Sie den Rollen-ARN in das Feld IAM-Rollen-ARN ein.
    g. Wählen Sie Bucket hinzufügen aus.

Schritt 2: Ändern Sie die Bucket-Richtlinie in Konto B

1. Melden Sie sich bei der AWS Management Console für Konto B an.
2. Öffnen Sie die S3-Konsole:
    a. Navigieren Sie zum S3-Dashboard.
    b. Wählen Sie den Bucket aus, für den Sie Zugriff gewähren möchten.
3. Bearbeiten Sie die Bucket-Richtlinie:
    a. Wählen Sie den Tab „Berechtigungen“ und dann „Bucket-Richtlinie“.
    b. Fügen Sie die folgende Richtlinie hinzu, um der IAM-Rolle von Konto A aus Zugriff auf den Bucket zu gewähren (*<AccountA_ID>*ersetzen Sie ihn durch die tatsächliche Konto-ID von Konto A und *<BUCKET-NAME>* durch den Namen des S3-Buckets):

        JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
```

```
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

c. Wählen Sie Save (Speichern).

Verhinderung der Datenexfiltration in einer privaten VPC

Um zu verhindern, dass Benutzer Daten aus sicheren S3-Buckets in ihre eigenen S3-Buckets in ihrem Konto exfiltrieren, können Sie einen VPC-Endpunkt anhängen, um Ihre private VPC zu sichern. Die folgenden Schritte zeigen, wie Sie einen VPC-Endpunkt für den S3-Dienst erstellen, der den Zugriff auf S3-Buckets in Ihrem Konto sowie auf alle zusätzlichen Konten mit kontoübergreifenden Buckets unterstützt.

1. Öffnen Sie die Amazon VPC-Konsole:
   a. Melden Sie sich bei der AWS Management Console an.
   b. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Erstellen Sie einen VPC-Endpunkt für S3:
   a. Wählen Sie im linken Navigationsbereich Endpoints aus.
   b. Wählen Sie Endpunkt erstellen aus.
   c. Stellen Sie sicher, dass bei Servicekategorie die Option AWS Services ausgewählt ist.
   d. Geben Sie im Feld Dienstname „S3“ ein `com.amazonaws.<region>.s3` (`<region>`ersetzen Sie es durch Ihre AWS Region) oder suchen Sie danach.
   e. Wählen Sie den S3-Dienst aus der Liste aus.
3. Endpunkteinstellungen konfigurieren:
   a. Wählen Sie für VPC die VPC aus, in der Sie den Endpunkt erstellen möchten.

b. Wählen Sie für Subnetze beide privaten Subnetze aus, die während der Bereitstellung für die VDI-Subnetze verwendet wurden.

c. Stellen Sie sicher, dass die Option „DNS-Name aktivieren“ aktiviert ist. Dadurch kann der private DNS-Hostname in die Endpunkt-Netzwerkschnittstellen aufgelöst werden.

4. Konfigurieren Sie die Richtlinie zur Zugriffsbeschränkung:

   a. Wählen Sie unter Richtlinie die Option Benutzerdefiniert aus.

   b. Geben Sie im Richtlinieneditor eine Richtlinie ein, die den Zugriff auf Ressourcen in Ihrem Konto oder einem bestimmten Konto einschränkt. Hier ist ein Beispiel für eine Richtlinie (*mybucket*ersetzen Sie sie durch Ihren S3-Bucket-Namen *111122223333* und *444455556666* durch das entsprechende AWS Konto IDs , auf das Sie zugreifen möchten):

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::mybucket",
                "arn:aws:s3:::mybucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",   // Your Account ID
                        "444455556666"    // Another Account ID
                    ]
                }
            }
        }
    ]
}
```

5. Erstellen Sie den Endpunkt:

   a. Überprüfen Sie die Einstellungen.

   b. Wählen Sie Endpunkt erstellen aus.

6. Überprüfen Sie den Endpunkt:

   a. Sobald der Endpunkt erstellt wurde, navigieren Sie in der VPC-Konsole zum Abschnitt Endpoints.
   b. Wählen Sie den neu erstellten Endpunkt aus.
   c. Stellen Sie sicher, dass der Status verfügbar ist.

Indem Sie diese Schritte ausführen, erstellen Sie einen VPC-Endpunkt, der S3-Zugriff ermöglicht, der auf Ressourcen innerhalb Ihres Kontos oder einer bestimmten Konto-ID beschränkt ist.

Fehlerbehebung

Wie überprüft man, ob ein Bucket nicht auf einem VDI bereitgestellt werden kann

Wenn ein Bucket nicht auf einem VDI bereitgestellt werden kann, gibt es einige Stellen, an denen Sie nach Fehlern suchen können. Gehen Sie wie folgt vor.

1. Überprüfen Sie die VDI-Protokolle:

   a. Melden Sie sich bei der AWS Management Console an.
   b. Öffnen Sie die EC2 Konsole und navigieren Sie zu Instances.
   c. Wählen Sie die VDI-Instanz aus, die Sie gestartet haben.
   d. Stellen Sie über den Session Manager eine Connect zum VDI her.
   e. Führen Sie die folgenden Befehle aus:

      ```
      sudo su
      cd ~/bootstrap/logs
      ```

      Hier finden Sie die Bootstrap-Protokolle. Die Details eines Fehlers finden Sie in der `configure.log.{time}` Datei.

      Weitere Informationen finden Sie außerdem im `/etc/message` Protokoll.

2. Überprüfen Sie die CloudWatch Lambda-Protokolle von Custom Credential Broker:

   a. Melden Sie sich bei der AWS Management Console an.
   b. Öffnen Sie die CloudWatch Konsole und navigieren Sie zu Protokollgruppen.

   c. Suchen Sie nach der Protokollgruppe`/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.

   d. Untersuchen Sie die erste verfügbare Protokollgruppe und suchen Sie nach Fehlern in den Protokollen. Diese Protokolle enthalten Details zu potenziellen Problemen bei der Bereitstellung temporärer benutzerdefinierter Anmeldeinformationen für das Mounten von S3-Buckets.

3. Überprüfen Sie die benutzerdefinierten Credential Broker CloudWatch API-Gateway-Protokolle:

   a. Melden Sie sich bei der AWS Management Console an.

   b. Öffnen Sie die CloudWatch Konsole und navigieren Sie zu Protokollgruppen.

   c. Suchen Sie nach der Protokollgruppe`<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`.

   d. Untersuchen Sie die erste verfügbare Protokollgruppe und suchen Sie nach Fehlern in den Protokollen. Diese Protokolle enthalten Details zu allen Anfragen und Antworten an das API Gateway für benutzerdefinierte Anmeldeinformationen, die für das Mounten der S3-Buckets erforderlich sind.

Wie bearbeitet man die IAM-Rollenkonfiguration eines Buckets nach dem Onboarding

1. Melden Sie sich bei der AWS DynamoDB-Konsole an.
2. Wählen Sie die Tabelle aus:

   a. Wählen Sie im linken Navigationsbereich Tabellen aus.

   b. Suchen und wählen Sie`<stack-name>.cluster-settings`.

3. Scannen Sie die Tabelle:

   a. Wählen Sie Tabellenelemente durchsuchen aus.

   b. Stellen Sie sicher, dass Scannen ausgewählt ist.

4. Einen Filter hinzufügen:

   a. Wählen Sie Filter aus, um den Bereich für den Filtereintrag zu öffnen.

   b. Stellen Sie den Filter so ein, dass er Ihrem Schlüssel entspricht

      - Attribut: Geben Sie den Schlüssel ein.
      - Bedingung: Wählen Sie Beginnt mit.

- Wert: Geben `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` Sie replace `<filesystem_id>` mit dem Wert des Dateisystems ein, das geändert werden muss.

5. Führen Sie den Scan aus:

   Wählen Sie Ausführen, um den Scan mit dem Filter auszuführen.

6. Überprüfen Sie den Wert:

   Wenn der Eintrag vorhanden ist, stellen Sie sicher, dass der Wert mit dem richtigen IAM-Rollen-ARN korrekt festgelegt ist.

   Wenn der Eintrag nicht existiert:

   a. Wählen Sie Element erstellen aus.
   b. Geben Sie die Artikeldetails ein:
      - Geben Sie für das identifizierende Attribut ein`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
      - Fügen Sie den richtigen IAM-Rollen-ARN hinzu.
   c. Wählen Sie Speichern aus, um das Element hinzuzufügen.

7. Starten Sie die VDI-Instanzen neu:

   Starten Sie die Instance neu, um sicherzustellen VDIs , dass diejenigen, die von der falschen IAM-Rolle betroffen ARN, erneut bereitgestellt werden.

Wird aktiviert CloudTrail

Um die Aktivierung CloudTrail in Ihrem Konto über die CloudTrail Konsole vorzunehmen, folgen Sie den Anweisungen unter Erstellen eines Trails mit der CloudTrail Konsole im AWS CloudTrail Benutzerhandbuch. CloudTrail protokolliert den Zugriff auf S3-Buckets, indem die IAM-Rolle aufgezeichnet wird, die darauf zugegriffen hat. Dies kann mit einer Instanz-ID verknüpft werden, die mit einem Projekt oder Benutzer verknüpft ist.

Verwaltung von Secrets

Research and Engineering Studio verwaltet die folgenden Geheimnisse mithilfe von AWS Secrets Manager. RES erstellt Geheimnisse automatisch bei der Erstellung der Umgebung. Geheimnisse,

die der Administrator bei der Erstellung der Umgebung eingegeben hat, werden als Parameter eingegeben.

Secret-Name	Beschreibung	RES generiert	Admin hat eingegeben
<envname>- sso-client-secret	Geheimer Single OAuth2 Sign-On-Client für die Umgebung	✓	
<envname>- vdc-client-secret	vdc ClientSecret	✓	
<envname>- vdc-client-id	vdc ClientId	✓	
<envname>vdc-gateway-certificate-private- -Taste	Privater Schlüssel für das selbstsignierte Zertifikat für die Domäne	✓	
<envname>- vdc-gateway-certificate-certificate	Selbstsigniertes Zertifikat für die Domain	✓	
<envname>- cluster-manager-client-secret	Clustermanager ClientSecret	✓	
<envname>- cluster-manager-client-id	Clustermanager ClientId	✓	
<envname>- external-private-key	Privater Schlüssel für das selbstsignierte Zertifikat für die Domäne	✓	

Secret-Name	Beschreibung	RES generiert	Admin hat eingegeben
<envname>-externes Zertifikat	Selbstsigniertes Zertifikat für die Domain	✓	
<envname>- internal-private-key	Privater Schlüssel für das selbstsig nierte Zertifikat für die Domäne	✓	
<envname>-internes Zertifikat	Selbstsigniertes Zertifikat für die Domain	✓	
<envname>-Verzeich nisdienst- ServiceAc countUsername			✓
<envname>-Verzeich nisdienst- ServiceAc countPassword			✓

Die folgenden geheimen ARN-Werte sind in der <envname>Tabelle -cluster-settings in DynamoDB enthalten:

Schlüssel	Quelle
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	Stack
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	Stack
cluster.load_balancers.internal_alb.certificates.private_key_se cret_arn	Stack

Schlüssel	Quelle
directoryservice.root_username_secret_arn	
vdc.client_secret	Stack
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	Stack
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	Stack
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	Stack
clustermanager.client_secret	

Kostenüberwachung und -kontrolle

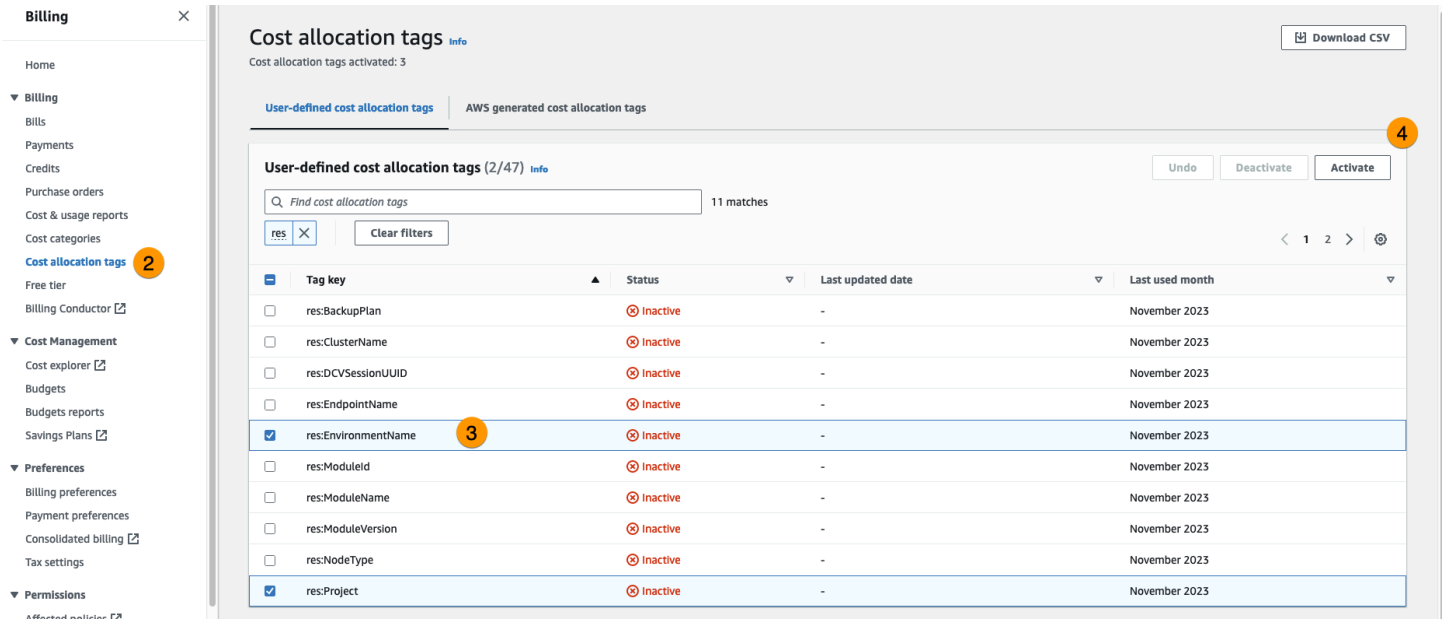
> **Note**
>
> Das Zuordnen von Research and Engineering Studio-Projekten zu AWS Budgets wird in AWS GovCloud (US) nicht unterstützt.

Wir empfehlen, über den AWS Cost Explorer ein Budget zu erstellen, um die Kosten besser verwalten zu können. Die Preise sind freibleibend. Vollständige Informationen finden Sie auf der Preisseite der einzelnenthe section called “AWS Dienstleistungen in diesem Produkt”.

Um die Kostenverfolgung zu erleichtern, können Sie RES-Projekte den innerhalb von ihnen erstellten Budgets zuordnen AWS Budgets. Sie müssen zunächst die Umgebungs-Tags innerhalb der Tags für die Zuordnung von Abrechnungskosten aktivieren.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Fakturierung und Kostenmanagement Konsole unter https://console.aws.amazon.com/costmanagement/.

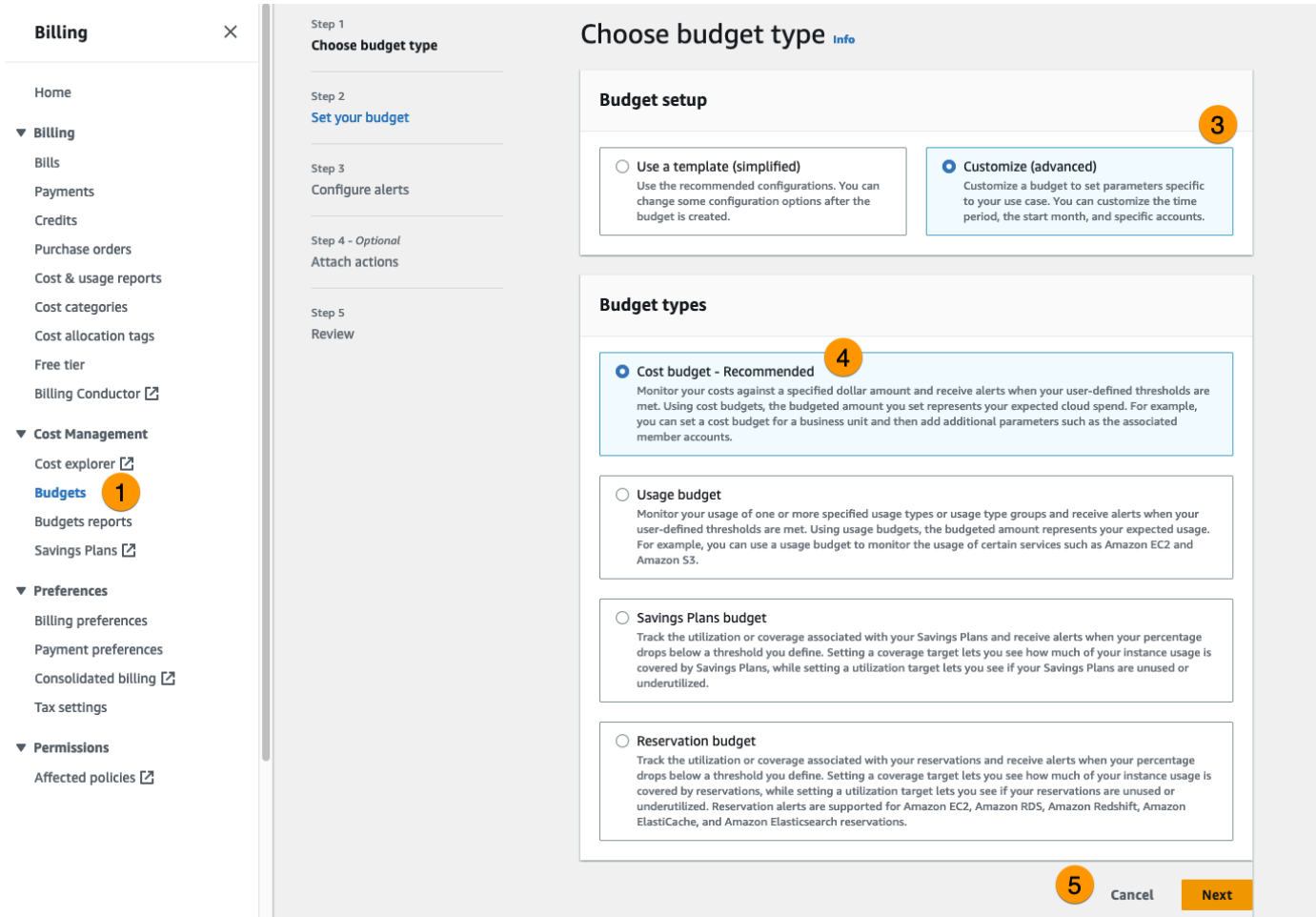
2. Wählen Sie Tags für die Kostenzuweisung aus.
3. Suchen Sie nach den `res:EnvironmentName` Tags `res:Project` und wählen Sie sie aus.
4. Wählen Sie Activate.



> **Note**
>
> Es kann bis zu einem Tag dauern, bis die RES-Tags nach der Bereitstellung angezeigt werden.

So erstellen Sie ein Budget für RES-Ressourcen:

1. Wählen Sie in der Abrechnungskonsole Budgets aus.
2. Wählen Sie „Budget erstellen“.
3. Wählen Sie unter Budgeteinstellungen die Option Anpassen (erweitert) aus.
4. Wählen Sie unter Budgettypen die Option Kostenbudget — Empfohlen aus.
5. Wählen Sie Weiter aus.

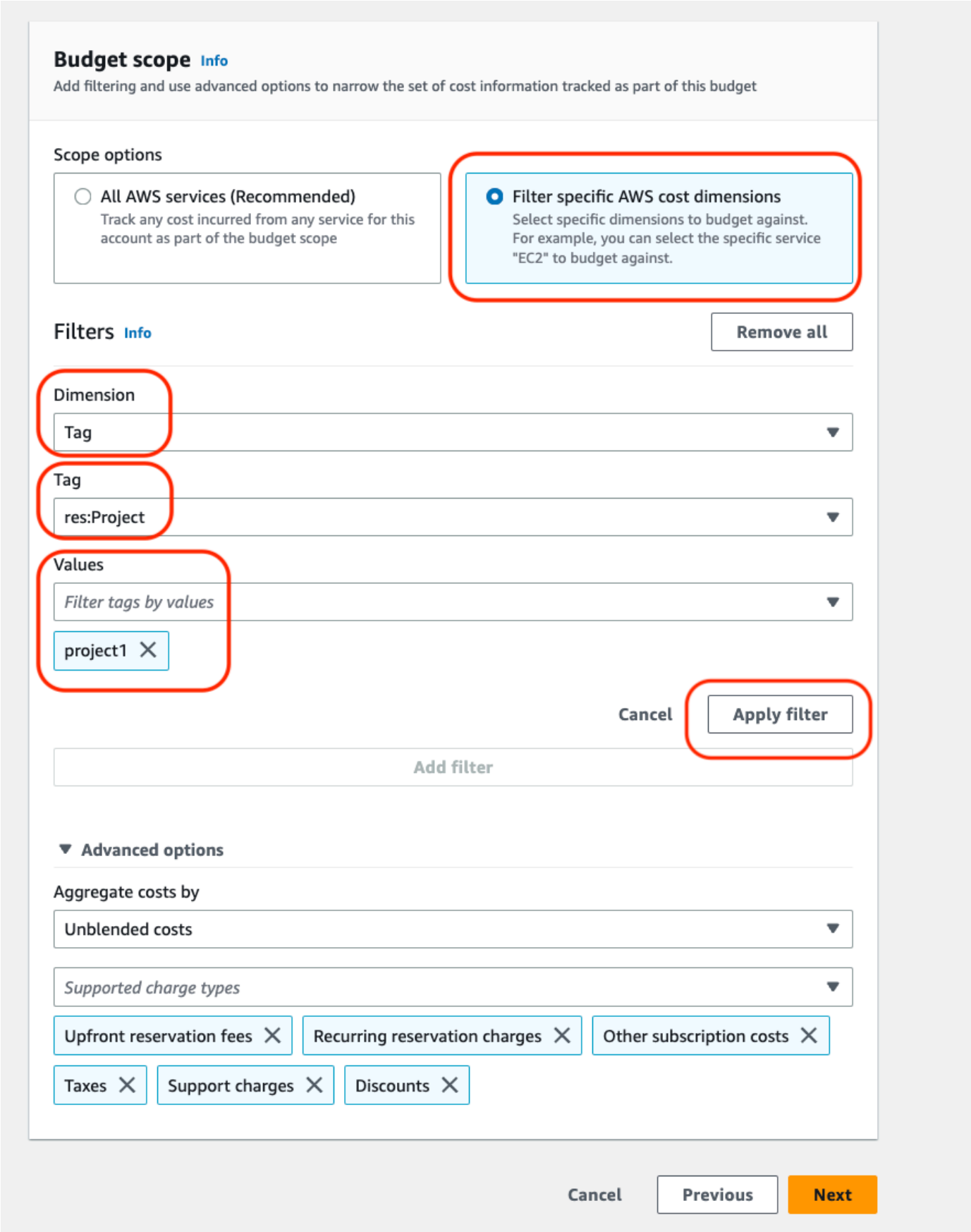


6. Geben Sie unter Details eine aussagekräftige Budgetbezeichnung für Ihr Budget ein, um es von anderen Budgets in Ihrem Konto zu unterscheiden. Zum Beispiel [EnvironmentName] - [ProjectName] - [BudgetName].
7. Geben Sie unter Budgetbetrag festlegen den für Ihr Projekt budgetierten Betrag ein.
8. Wählen Sie unter Budgetumfang die Option Spezifische AWS Kostendimensionen filtern aus.
9. Wählen Sie Add filter.
10. Wählen Sie unter Dimension die Option Tag aus.
11. Wählen Sie unter Tag die Option Res:Project aus.

> **Note**
>
> Es kann bis zu zwei Tage dauern, bis Tags und Werte verfügbar sind. Sie können ein Budget erstellen, sobald der Projektname verfügbar ist.

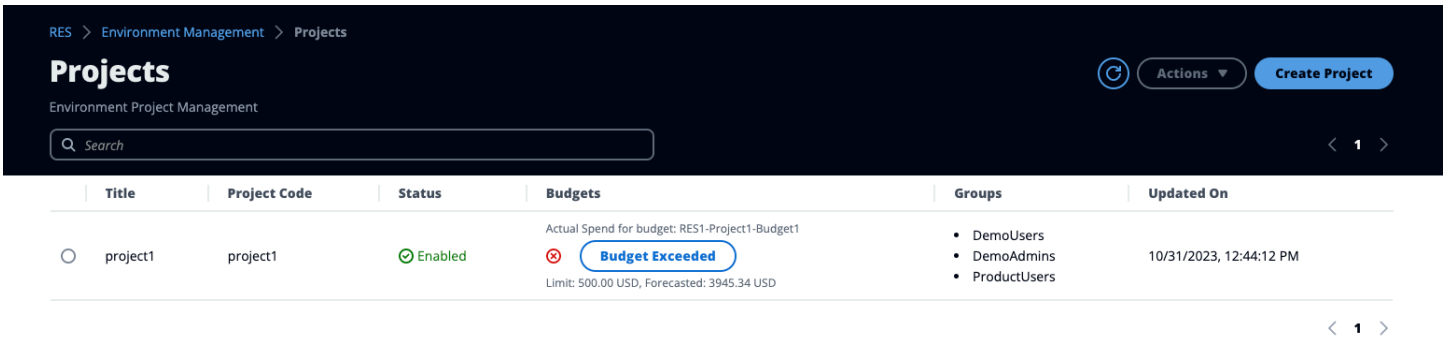
12. Wählen Sie unter Werte den Projektnamen aus.

13. Wählen Sie Filter anwenden aus, um den Projektfilter dem Budget zuzuordnen.
14. Wählen Sie Weiter aus.


Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Filters Info
Remove all
Dimension
Tag
Tag
res:Project
Values
Filter tags by values
project1
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. (Optional.) Fügen Sie einen Warnschwellenwert hinzu.
16. Wählen Sie Weiter aus.
17. (Optional.) Wenn eine Warnung konfiguriert wurde, verwenden Sie Attach actions, um die gewünschten Aktionen mit der Warnung zu konfigurieren.
18. Wählen Sie Weiter aus.
19. Überprüfen Sie die Budgetkonfiguration und vergewissern Sie sich, dass unter Zusätzliche Budgetparameter das richtige Tag festgelegt wurde.
20. Wählen Sie Budget erstellen aus.

Nachdem das Budget erstellt wurde, können Sie das Budget für Projekte aktivieren. Informationen zum Aktivieren von Budgets für ein Projekt finden Sie unterthe section called “Bearbeiten Sie ein Projekt”. Virtuelle Desktops werden am Start gehindert, wenn das Budget überschritten wird. Wenn das Budget überschritten wird, während ein Desktop gestartet wird, funktioniert der Desktop weiter.



Wenn Sie Ihr Budget ändern müssen, kehren Sie zur Konsole zurück, um den Budgetbetrag zu bearbeiten. Es kann bis zu fünfzehn Minuten dauern, bis die Änderung in RES wirksam wird. Alternativ können Sie ein Projekt bearbeiten, um ein Budget zu deaktivieren.

Benutze das Produkt

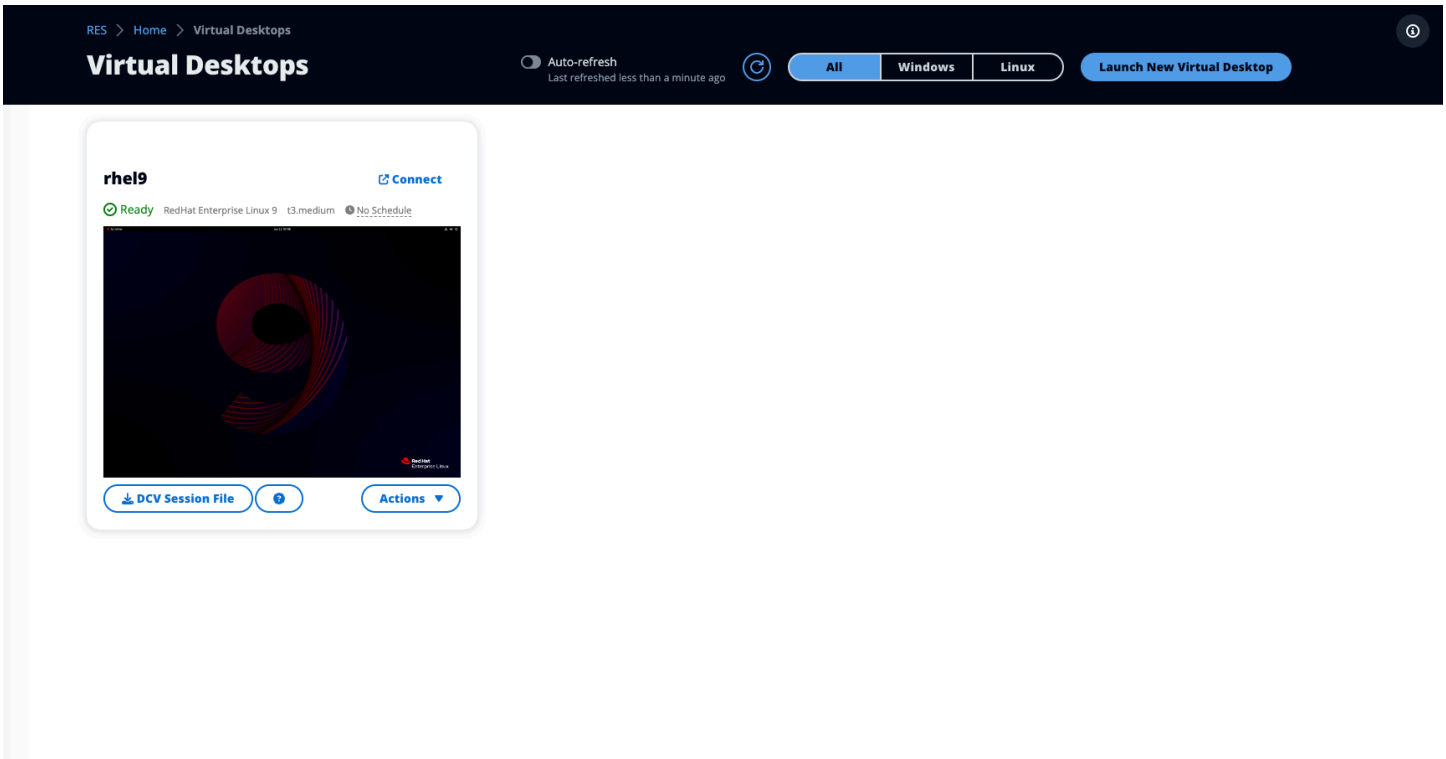
Dieser Abschnitt bietet Benutzern Anleitungen zur Verwendung virtueller Desktops für die Zusammenarbeit mit anderen Benutzern.

Themen

- Virtuelle Desktops
- Gemeinsam genutzte Desktops
- Dateibrowser
- SSH-Zugriff

Virtuelle Desktops

Mit dem VDI-Modul (Virtual Desktop Interface) können Benutzer virtuelle Windows- oder Linux-Desktops erstellen und verwalten. AWS Benutzer können EC2 Amazon-Instances mit ihren bevorzugten Tools und Anwendungen starten, die vorinstalliert und konfiguriert sind.



Unterstützte Betriebssysteme

RES unterstützt derzeit das Starten virtueller Desktops mit den folgenden Betriebssystemen:

- Amazon Linux 2 (x86 und ARM64)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Starten Sie einen neuen Desktop

1. Wählen Sie im Menü Meine virtuellen Desktops aus.
2. Wählen Sie „Neuen virtuellen Desktop starten“.
3. Geben Sie die Details für Ihren neuen Desktop ein.
4. Wählen Sie Absenden aus.

Eine neue Karte mit Ihren Desktop-Informationen wird sofort angezeigt, und Ihr Desktop ist innerhalb von 10-15 Minuten einsatzbereit. Die Startzeit hängt vom ausgewählten Bild ab. RES erkennt GPU-Instanzen und installiert die entsprechenden Treiber.

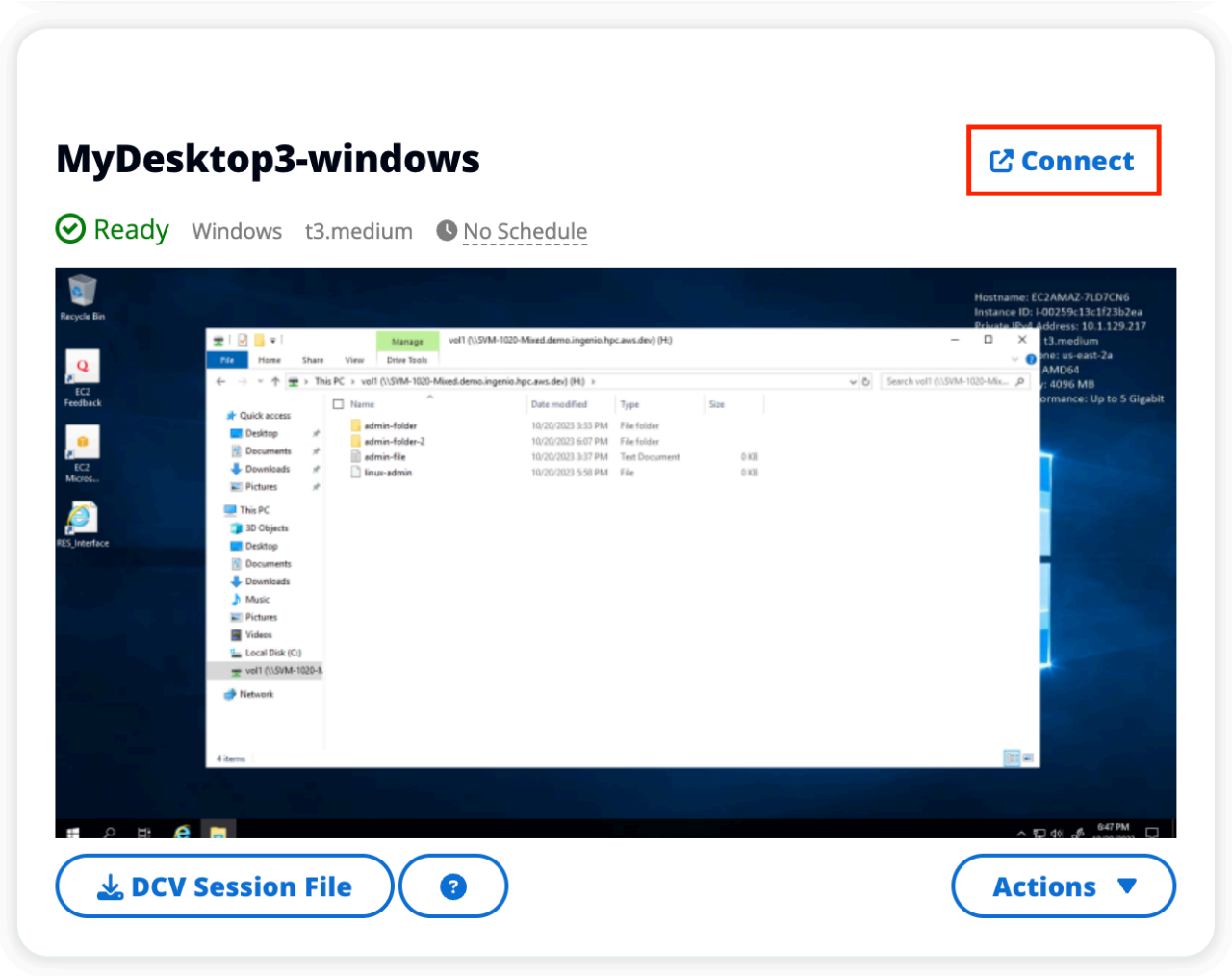
Greifen Sie auf Ihren Desktop zu

Um auf einen virtuellen Desktop zuzugreifen, wählen Sie die Karte für den Desktop aus und stellen Sie entweder über den Web- oder den DCV-Client eine Verbindung her.

Web connection

Der Zugriff auf Ihren Desktop über den Webbrowser ist die einfachste Verbindungsmethode.

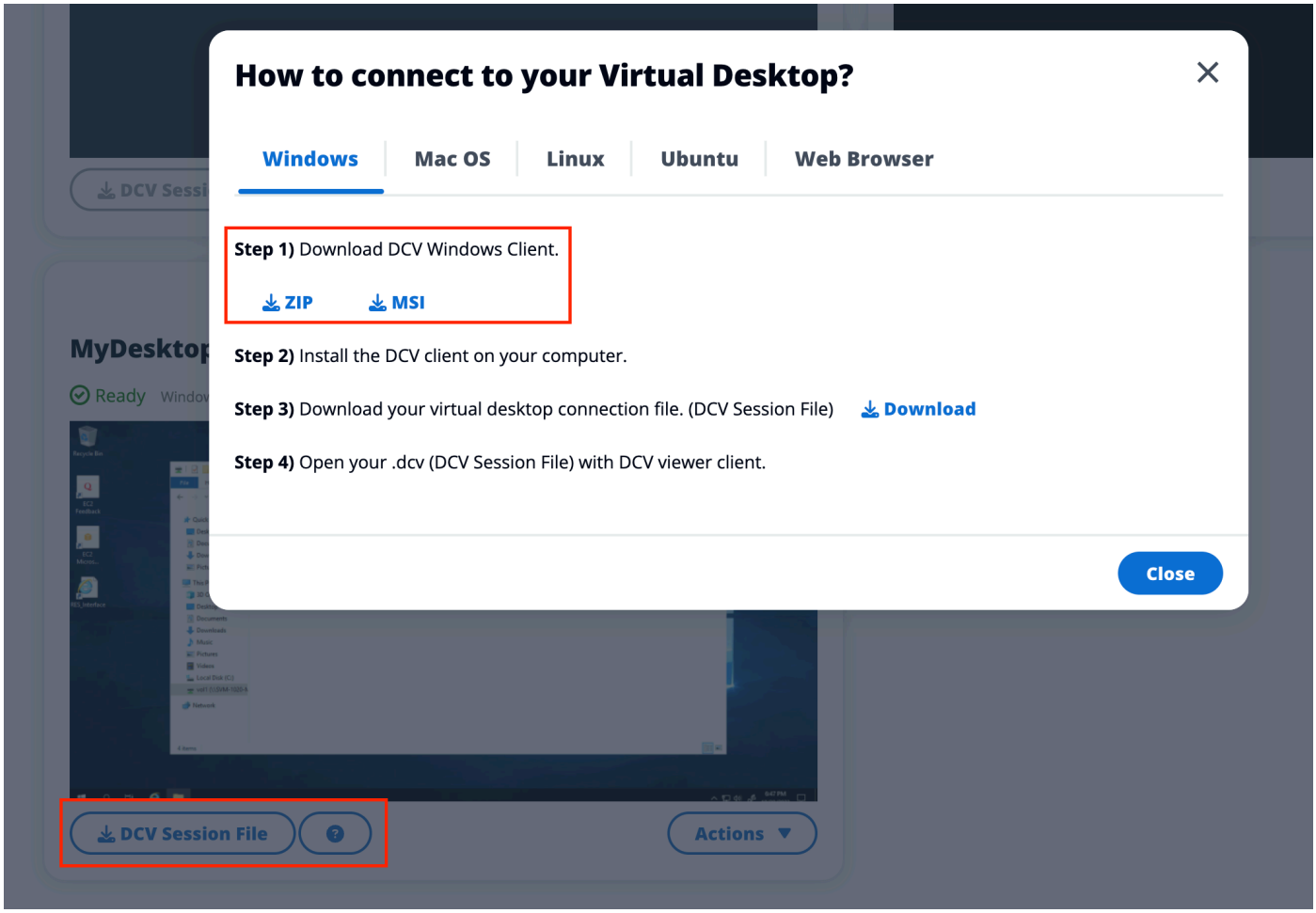
- Wählen Sie Connect oder wählen Sie das Vorschaubild, um direkt über Ihren Browser auf Ihren Desktop zuzugreifen.



DCV connection

Der Zugriff auf Ihren Desktop über einen DCV-Client bietet die beste Leistung. So greifen Sie über DCV zu:

1. Wählen Sie DCV-Sitzungsdatei, um die herunterzuladen. `dcv`Datei. Sie benötigen einen DCV-Client, der auf Ihrem System installiert ist.
2. Für Installationsanweisungen wählen Sie die Option? Symbol.



Kontrollieren Sie Ihren Desktop-Status

Um den Status Ihres Desktops zu kontrollieren:

1. Wählen Sie Aktionen.
2. Wählen Sie Virtual Desktop State. Sie haben vier Status zur Auswahl:

   - Stoppen

     Bei einer gestoppten Sitzung gehen keine Daten verloren, und Sie können eine gestoppte Sitzung jederzeit neu starten.

   - Starten Sie neu

     Startet die aktuelle Sitzung neu.

   - Beenden

Beendet eine Sitzung dauerhaft. Das Beenden einer Sitzung kann zu Datenverlust führen, wenn Sie kurzlebigen Speicher verwenden. Sie sollten Ihre Daten vor dem Beenden im RES-Dateisystem sichern.

- In den Ruhezustand versetzen

  Ihr Desktop-Status wird im Arbeitsspeicher gespeichert. Wenn Sie den Desktop neu starten, werden Ihre Anwendungen wieder aufgenommen, aber alle Remoteverbindungen können verloren gehen. Nicht alle Instances unterstützen den Ruhezustand, und die Option ist nur verfügbar, wenn sie bei der Instanzerstellung aktiviert wurde. Informationen darüber, ob Ihre Instance diesen Status unterstützt, finden Sie unter Voraussetzungen für den Ruhezustand.

Ändern Sie einen virtuellen Desktop

Sie können die Hardware Ihres virtuellen Desktops aktualisieren oder den Sitzungsnamen ändern.

1. Bevor Sie Änderungen an der Instanzgröße vornehmen, müssen Sie die Sitzung beenden:

   a. Wählen Sie Aktionen.

   b. Wählen Sie Virtual Desktop State.

   c. Wählen Sie Beenden aus.

   > **Note**
   >
   > Sie können die Desktop-Größe für Sitzungen im Ruhezustand nicht aktualisieren.

2. Nachdem Sie bestätigt haben, dass der Desktop gestoppt wurde, wählen Sie Aktionen und dann Sitzung aktualisieren.
3. Ändern Sie den Sitzungsnamen oder wählen Sie die gewünschte Desktop-Größe aus.
4. Wählen Sie Absenden aus.
5. Sobald Ihre Instances aktualisiert sind, starten Sie Ihren Desktop neu:

   a. Wählen Sie Aktionen.

   b. Wählen Sie Virtual Desktop State.

   c. Wählen Sie Starten.

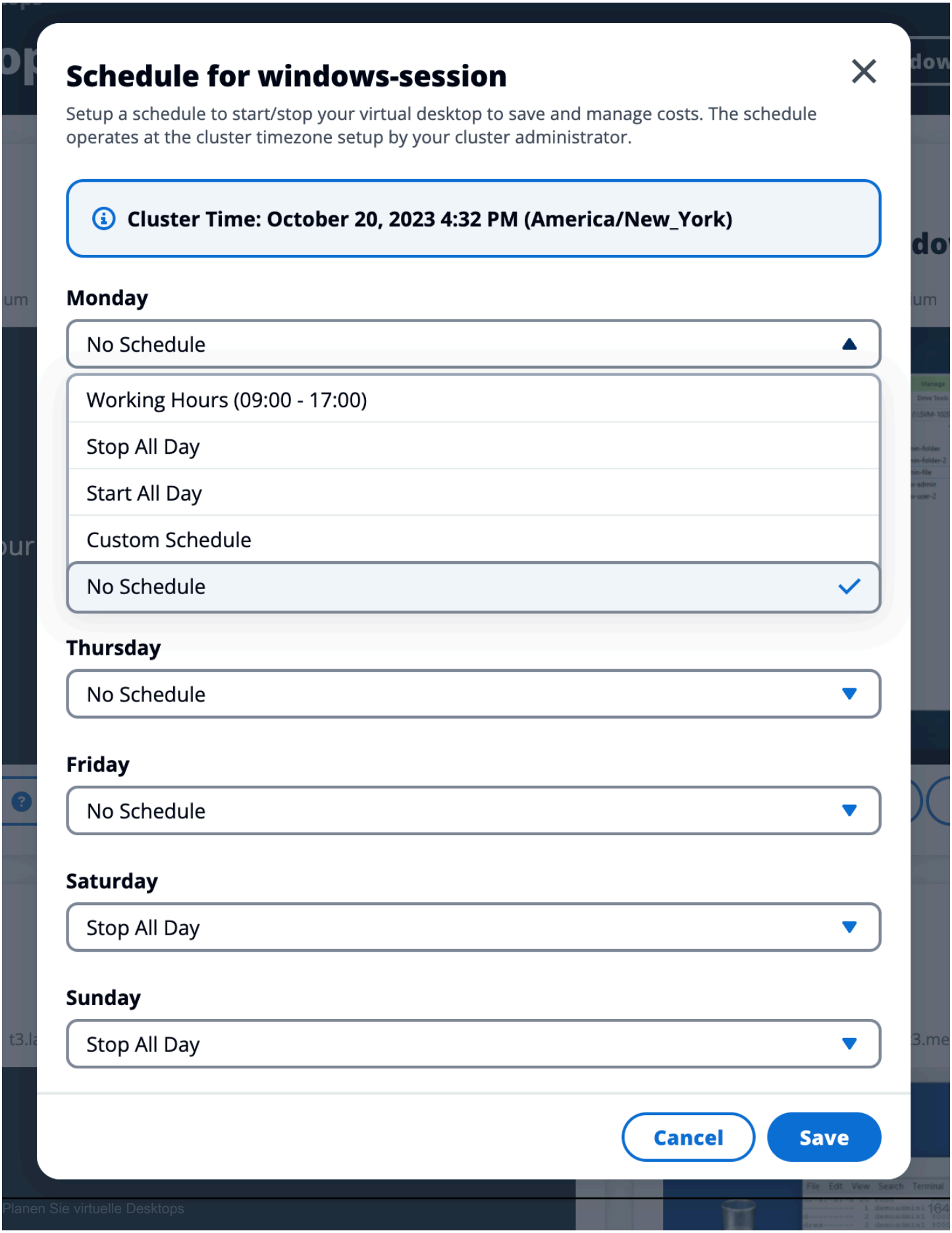
Sitzungsinformationen abrufen

1. Wählen Sie Aktionen.
2. Wählen Sie „Informationen anzeigen“.

Virtuelle Desktops planen

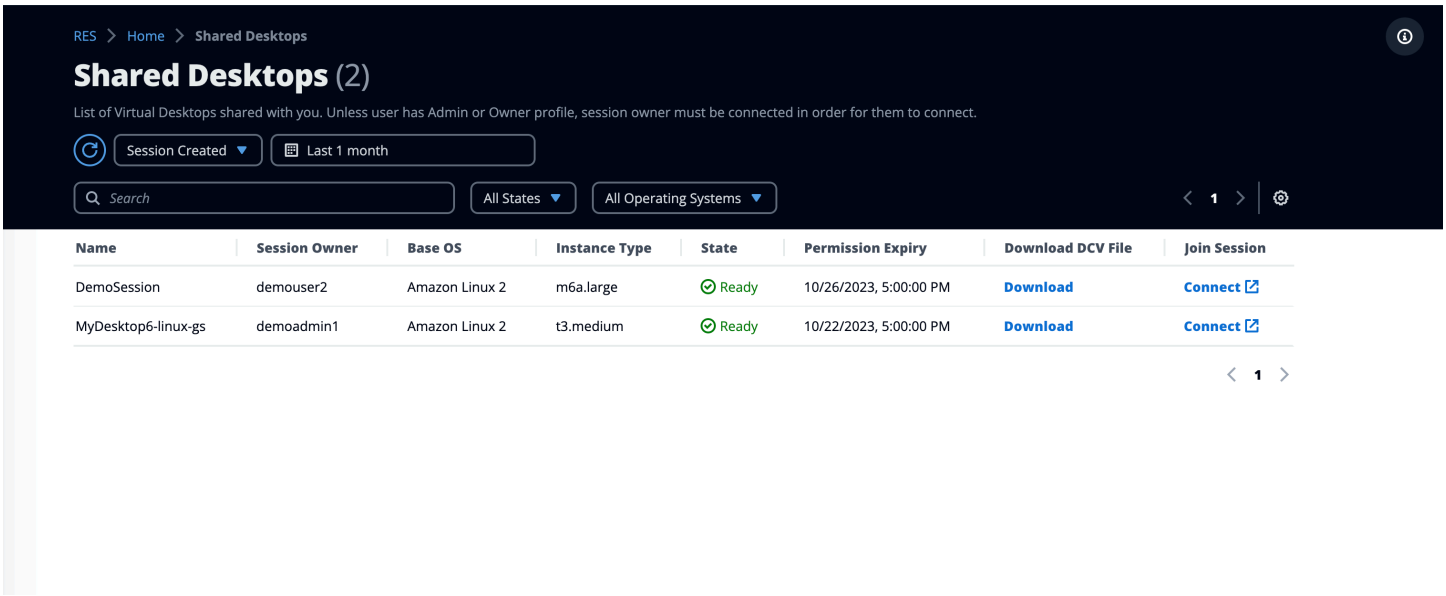
Standardmäßig haben virtuelle Desktops keinen Zeitplan und bleiben aktiv, bis Sie die Sitzung beenden oder beenden. Desktops werden auch angehalten, wenn sie inaktiv sind, um versehentliche Stopps zu verhindern. Ein Ruhezustand liegt vor, wenn keine aktive Verbindung besteht und die CPU-Auslastung mindestens 15 Minuten lang unter 15% liegt. Sie können einen Zeitplan so konfigurieren, dass Ihr Desktop automatisch gestartet und gestoppt wird.

1. Wählen Sie Aktionen.
2. Wählen Sie Schedule aus.
3. Lege deinen Zeitplan für jeden Tag fest.
4. Wählen Sie Speichern.


Schedule for windows-session
Setup a schedule to start/stop your virtual desktop to save and manage costs. The schedule operates at the cluster timezone setup by your cluster administrator.
Cluster Time: October 20, 2023 4:32 PM (America/New_York)
Monday
No Schedule
Working Hours (09:00 - 17:00)
Stop All Day
Start All Day
Custom Schedule
No Schedule
Thursday
No Schedule
Friday
No Schedule
Saturday
Stop All Day
Sunday
Stop All Day
Cancel
Save

Gemeinsam genutzte Desktops

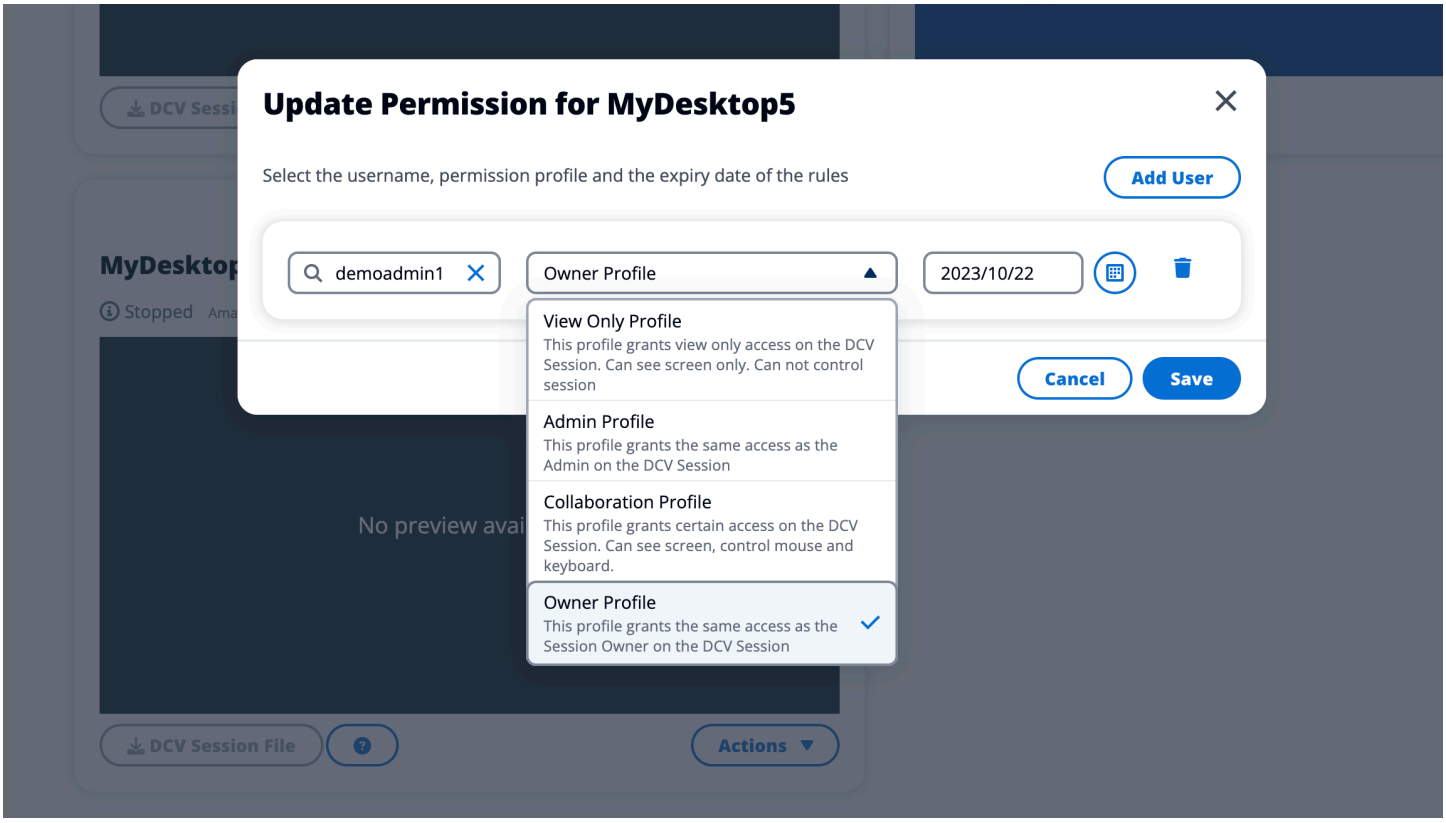
Auf Shared Desktops können Sie die Desktops sehen, die für Sie freigegeben wurden. Um eine Verbindung zu einem Desktop herzustellen, muss auch der Sitzungsbesitzer verbunden sein, es sei denn, Sie sind Administrator oder Besitzer.



Beim Teilen einer Sitzung können Sie die Berechtigungen für Ihre Mitarbeiter konfigurieren. Sie können beispielsweise einem Teamkollegen, mit dem Sie zusammenarbeiten, nur Lesezugriff gewähren.

Teilen Sie einen Desktop

1. Wählen Sie in Ihrer Desktop-Sitzung Aktionen aus.
2. Wählen Sie Sitzungsberechtigungen aus.
3. Wählen Sie den Benutzer und die Berechtigungsstufe aus. Sie können auch eine Ablaufzeit festlegen.
4. Wählen Sie Speichern.



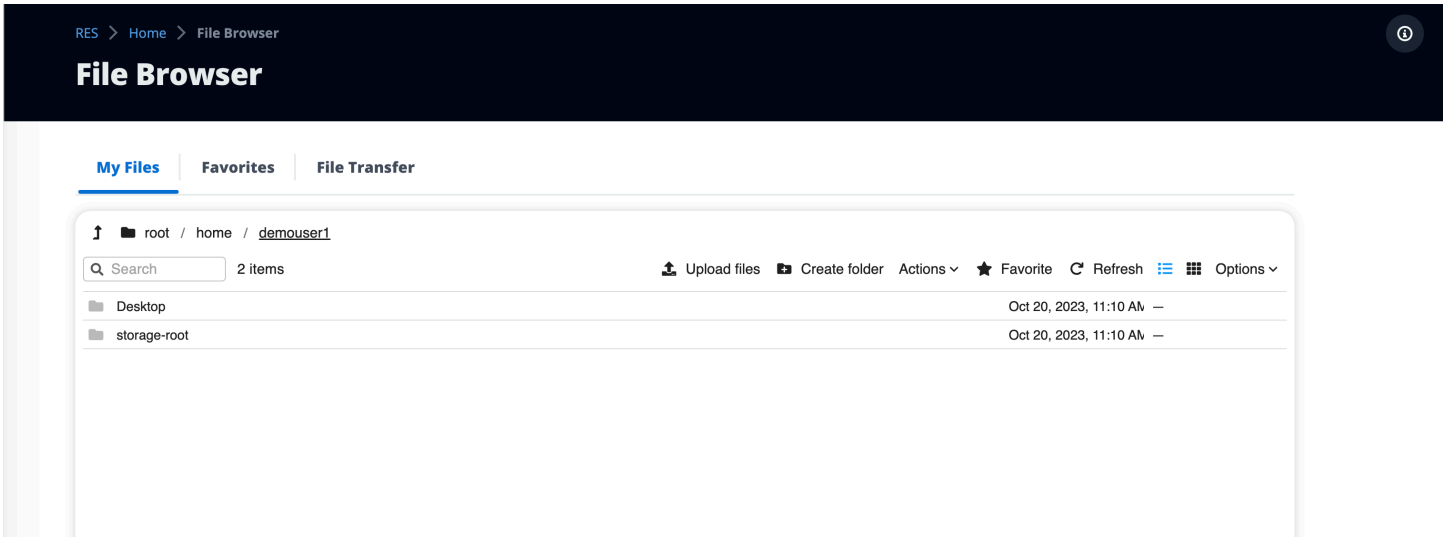
Weitere Informationen zu Berechtigungen finden Sie unterthe section called “Berechtigungsprofile”.

Greifen Sie auf einen gemeinsam genutzten Desktop zu

Unter Shared Desktops können Sie sich die für Sie freigegebenen Desktops ansehen und eine Verbindung zu einer Instanz herstellen. Sie können entweder über einen Webbrowser oder über DCV beitreten. Folgen Sie den Anweisungen unter, um eine Verbindung herzustellen. the section called “Greifen Sie auf Ihren Desktop zu”

Dateibrowser

Der Dateibrowser ermöglicht Ihnen den Zugriff auf Dateisysteme über das Webportal. Sie können alle verfügbaren Dateien, für die Sie Zugriffsrechte haben, im zugrunde liegenden Dateisystem verwalten. Backend-Speicher (Amazon EFS) ist für alle Linux-Knoten verfügbar. Für Linux- und Windows-Knoten ist FSx für ONTAP verfügbar. Das Aktualisieren von Dateien auf Ihrem virtuellen Desktop entspricht dem Aktualisieren einer Datei über das Terminal oder den webbasierten Dateibrowser.



Datei (en) hochladen

1. Wählen Sie Datei hochladen.
2. Legen Sie entweder Dateien ab oder suchen Sie nach Dateien, die Sie hochladen möchten.
3. Wählen Sie Dateien hochladen (n).

Datei (en) löschen

1. Wählen Sie die Datei (en) aus, die Sie löschen möchten.
2. Wählen Sie Aktionen.
3. Wählen Sie Dateien löschen.

Alternativ können Sie auch mit der rechten Maustaste auf eine Datei oder einen Ordner klicken und Dateien löschen wählen.

Favoriten verwalten

Um wichtige Dateien und Ordner anzuheften, können Sie sie zu den Favoriten hinzufügen.

1. Wählen Sie eine Datei oder einen Ordner aus.
2. Wählen Sie Favorit.

Alternativ können Sie mit der rechten Maustaste auf eine Datei oder einen Ordner klicken und Favorit wählen.

> **Note**
>
> Favoriten werden im lokalen Browser gespeichert. Wenn Sie Ihren Browser wechseln oder den Cache leeren, müssen Sie Ihre Favoriten erneut anheften.

Dateien bearbeiten

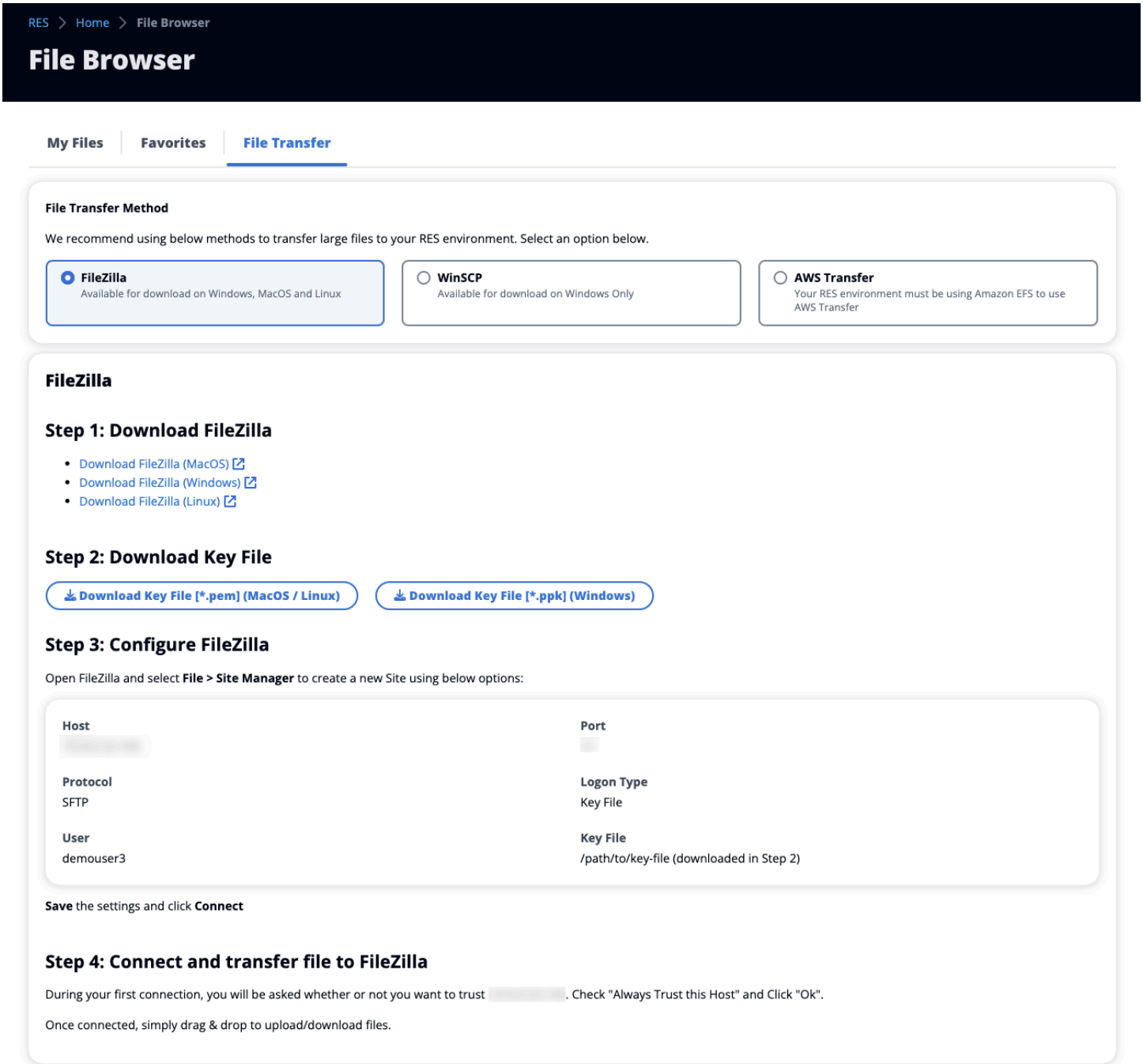
Sie können den Inhalt textbasierter Dateien im Webportal bearbeiten.

1. Wählen Sie die Datei aus, die Sie aktualisieren möchten. Ein Modal wird mit dem Inhalt der Datei geöffnet.
2. Nehmen Sie Ihre Aktualisierungen vor und wählen Sie Speichern.

Übertragen von Dateien

Verwenden Sie File Transfer, um externe Dateiübertragungsanwendungen zum Übertragen von Dateien zu verwenden. Sie können aus den folgenden Anwendungen auswählen und den Anweisungen auf dem Bildschirm folgen, um Dateien zu übertragen.

- FileZilla (Windows, macOS, Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)



SSH-Zugriff

Um SSH für den Zugriff auf den Bastion-Host zu verwenden:

1. Wählen Sie im RES-Menü die Option SSH-Zugriff.

2. Folgen Sie den Anweisungen auf dem Bildschirm, um entweder SSH oder PuTTY für den Zugriff zu verwenden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Überwachung des Systems und zur Behebung bestimmter Probleme, die auftreten können.

Themen

- Allgemeines Debuggen und Überwachen
- Problem RunBooks
- Bekannte Probleme

Ausführlicher Inhalt:

- Allgemeines Debuggen und Überwachen
  - Nützliche Quellen für Protokoll- und Ereignisinformationen
    - Protokolldateien auf EC2 Amazon-Instances in der Umgebung
    - CloudFormation Stapel
    - Systemausfälle aufgrund eines Problems, das sich in der Gruppenaktivität von Amazon EC2 Auto Scaling widerspiegelt
  - Typisches Erscheinungsbild der EC2 Amazon-Konsole
    - Infrastruktur-Hosts
    - Infrastruktur-Hosts und virtuelle Desktops
    - Hosts im Status „Beendet“
    - Nützliche Befehle im Zusammenhang mit Active Directory (AD) als Referenz
  - Windows-DCV-Debuggen
  - Finden Sie Informationen zur NICE DCV DCV-Version
- Problem RunBooks
  - Probleme bei der Installation
    - AWS CloudFormation Der Stapel kann nicht erstellt werden und die Meldung "WaitCondition hat eine fehlgeschlagene Nachricht erhalten. Fehler: Staaten. TaskFailed“
    - E-Mail-Benachrichtigung wurde nicht empfangen, nachdem AWS CloudFormation Stacks erfolgreich erstellt wurden
    - Instanzen laufen oder der VDC-Controller ist ausgefallen

- Der CloudFormation Umgebungsstapel kann aufgrund eines Fehlers beim abhängigen Objekt nicht gelöscht werden
- Bei der Erstellung der Umgebung ist ein Fehler für den CIDR-Blockparameter aufgetreten
- CloudFormation Fehler bei der Stapelerstellung während der Umgebungserstellung
- Die Erstellung eines Stacks für externe Ressourcen (Demo) schlägt mit AdDomainAdminNode CREATE_FAILED fehl

- Probleme mit der Identitätsverwaltung
  - Ich bin nicht berechtigt, iam auszuführen: PassRole
  - Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf mein Research and Engineering Studio über AWS Ressourcen ermöglichen
  - Wenn ich mich bei der Umgebung anmelde, kehre ich sofort zur Anmeldeseite zurück
  - Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden
  - Der Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES
  - Der Benutzer ist beim Erstellen einer Sitzung nicht verfügbar
  - Fehler beim Überschreiten der Größenbeschränkung im CloudWatch Cluster-Manager-Protokoll
- Speicher
  - Ich habe das Dateisystem über RES erstellt, aber es wird nicht auf den VDI-Hosts bereitgestellt
  - Ich habe ein Dateisystem über RES integriert, aber es wird nicht auf den VDI-Hosts bereitgestellt
  - Ich kann von VDI-Hosts aus nicht read/write einschalten
    - Beispiele für Anwendungsfälle im Umgang mit Berechtigungen
  - Ich habe Amazon FSx for NetApp ONTAP von RES aus erstellt, aber es ist meiner Domain nicht beigetreten
- Snapshots
  - Ein Snapshot hat den Status Fehlgeschlagen
  - Ein Snapshot kann nicht angewendet werden, da die Protokolle darauf hinweisen, dass die Tabellen nicht importiert werden konnten.
- Infrastruktur
  - Load Balancer-Zielgruppen ohne fehlerfreie Instanzen

- Virtuelle Desktops werden gestartet

- Ein virtueller Desktop, der zuvor funktionierte, kann keine erfolgreiche Verbindung mehr herstellen
    - Ich kann nur 5 virtuelle Desktops starten
    - Windows-Desktop-Verbindungsversuche schlagen fehl mit der Meldung „Die Verbindung wurde geschlossen“. Transportfehler“
    - VDIs steckt im Bereitstellungsstatus fest
    - VDIs nach dem Start in den Fehlerstatus wechseln
- Virtuelle Desktop-Komponente
    - Die EC2 Amazon-Instance wird in der Konsole wiederholt als beendet angezeigt
    - Die vdc-Controller-Instanz läuft, weil sie dem AD nicht beitreten konnte. /Das eVDI-Modul zeigt die fehlgeschlagene API-Zustandsprüfung
    - Das Projekt erscheint nicht im Pulldown, wenn Sie den Software-Stack bearbeiten, um es hinzuzufügen
    - Clustermanager Amazon CloudWatch Log zeigt „< user-home-init > Konto noch nicht verfügbar. wartet darauf, dass der Benutzer synchronisiert wird“ (wobei das Konto ein Benutzername ist)
    - Auf dem Windows-Desktop wird beim Anmeldeversuch die Meldung „Ihr Konto wurde deaktiviert“ angezeigt. Bitte wenden Sie sich an Ihren Administrator.“
    - Probleme mit den DHCP-Optionen bei der external/customer AD-Konfiguration
    - Firefox-Fehler MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING
- Löschen von Umgebungen
    - res-xxx-cluster Der Stapel befindet sich im Status „DELETE_FAILED“ und kann aufgrund des Fehlers „Rolle ist ungültig oder kann nicht angenommen werden“ nicht manuell gelöscht werden
    - Protokolle sammeln
    - VDI-Protokolle werden heruntergeladen
    - Protokolle von EC2 Linux-Instanzen werden heruntergeladen
    - Protokolle von EC2 Windows-Instanzen herunterladen
    - Sammeln von ECS-Protokollen für den WaitCondition Fehler
- Demo-Umgebung
    - Anmeldefehler in der Demo-Umgebung bei der Bearbeitung der Authentifizierungsanfrage an den Identitätsanbieter

- Bekannte Probleme 2024.x
  - Bekannte Probleme 2024.x
    - (2024.06) Das Anwenden des Snapshots schlägt fehl, wenn der AD-Gruppenname Leerzeichen enthält
    - (2024.04-2024.04.02) Die angegebene IAM-Berechtigungsgrenze ist nicht an die Rolle der VDI-Instanzen gebunden
    - (2024.04.02 und früher) Windows NVIDIA-Instanzen in ap-southeast-2 (Sydney) können nicht gestartet werden
    - (2024.04 und 2024.04.01) Fehler beim Löschen von RES in GovCloud
    - (2024.04 - 2024.04.02) Der virtuelle Linux-Desktop bleibt beim Neustart möglicherweise im Status „RESUMING“ hängen
    - (2024.04.02 und früher) Fehler beim Synchronisieren von AD-Benutzern, deren SAMAccount Namensattribut Großbuchstaben oder Sonderzeichen enthält
    - (2024.04.02 und früher) Der private Schlüssel für den Zugriff auf den Bastion-Host ist ungültig
    - (2024.06 und früher) Gruppenmitglieder wurden während der AD-Synchronisierung nicht mit RES synchronisiert
    - (2024.06 und früher) CVE-2024-6387, Regre, Sicherheitslücke in und Ubuntu SSHion RHEL9 VDIs

Allgemeines Debuggen und Überwachen

Dieser Abschnitt enthält Informationen darüber, wo Informationen innerhalb von RES zu finden sind.

- Nützliche Quellen für Protokoll- und Ereignisinformationen
  - Protokolldateien auf EC2 Amazon-Instances in der Umgebung
  - CloudFormation Stapel
  - Systemausfälle aufgrund eines Problems, das sich in der Gruppenaktivität von Amazon EC2 Auto Scaling widerspiegelt
- Typisches Erscheinungsbild der EC2 Amazon-Konsole
  - Infrastruktur-Hosts
  - Infrastruktur-Hosts und virtuelle Desktops
  - Hosts im Status „Beendet“
  - Nützliche Befehle im Zusammenhang mit Active Directory (AD) als Referenz

- Windows-DCV-Debuggen
- Finden Sie Informationen zur NICE DCV DCV-Version

Nützliche Quellen für Protokoll- und Ereignisinformationen

Es stehen verschiedene Informationsquellen zur Verfügung, auf die bei der Problembehandlung und Überwachung zurückgegriffen werden kann.

Protokolldateien auf EC2 Amazon-Instances in der Umgebung

Protokolldateien sind auf den EC2 Amazon-Instances vorhanden, die von RES verwendet werden. Der SSM Session Manager kann verwendet werden, um eine Sitzung mit der Instance zu öffnen, um diese Dateien zu untersuchen.

Auf Infrastrukturinstanzen wie dem Cluster-Manager und dem VDC-Controller befinden sich Anwendungs- und andere Protokolle an den folgenden Orten.

- /.log opt/idea/app/logs/application
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- /var/log/messages
- /-data.log var/log/user
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

Auf einem virtuellen Linux-Desktop enthalten die folgenden Dateien nützliche Protokolldateien

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages

Unter Windows finden Sie die Protokolle für virtuelle Desktop-Instanzen unter

- PS C:\\ ProgramData n ice\ dcv\ log
- PS C:\\ ProgramData n Eis\\ Protokoll DCVSession ManagerAgent

Unter Windows finden Sie die Protokollierung einiger Anwendungen unter:

- PS C:\Program Files\ NICE\ DCV\ Server\ bin

Unter Windows befinden sich die NICE-DCV-Zertifikatsdateien unter:

- C:\Windows\System32\config\systemprofile\AppData\ Local\ NICE\ dcv\

Amazon CloudWatch Log-Gruppen

Die Amazon EC2 - und AWS Lambda Rechenressourcen protokollieren Informationen in Amazon CloudWatch Log Groups. Die darin enthaltenen Protokolleinträge können nützliche Informationen zur Behebung potenzieller Probleme oder für allgemeine Informationen liefern.

Diese Gruppen sind wie folgt benannt:

- `/aws/lambda/<envname>-/ - lambda related`
- `/<envname>/`
  - `cluster-manager/ - main infrastructure host`
  - `vdc/ - virtual desktop related`
    - `dcv-broker/ - desktop related`
    - `dcv-connection-gateway/ - desktop related`
    - `controller/ - main desktop controller host`
    - `dcv-session/ - desktop session related`

Bei der Untersuchung von Protokollgruppen kann es hilfreich sein, anhand von Zeichenketten in Groß- und Kleinbuchstaben zu filtern, z. B. im Folgenden. Dadurch werden nur die Meldungen ausgegeben, die die angegebenen Zeichenketten enthalten.

```
?"ERROR" ?"error"
```

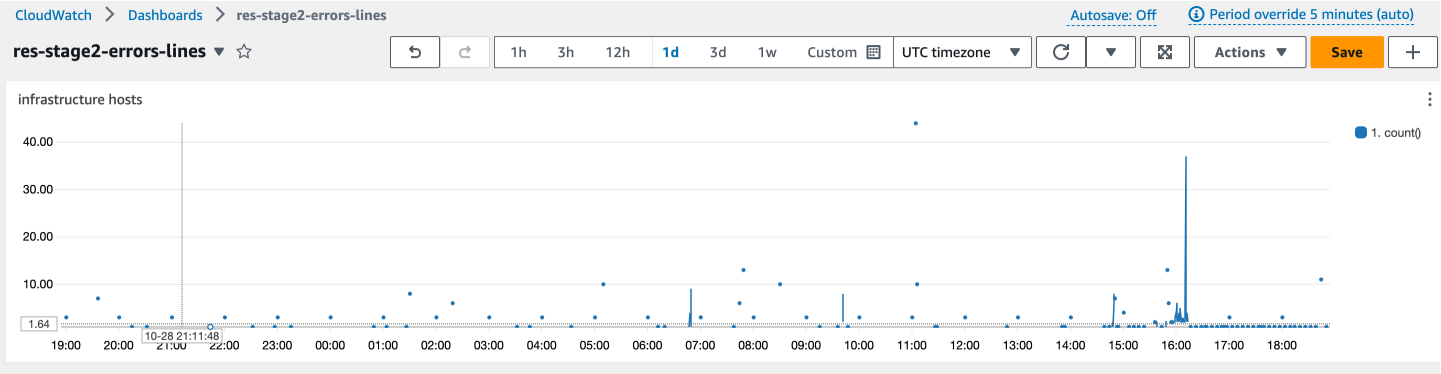
Eine weitere Methode zur Problemüberwachung besteht darin, CloudWatch Amazon-Dashboards zu erstellen, die Widgets enthalten, die die gewünschten Daten anzeigen.

Ein Beispiel ist die Erstellung eines Widgets, das das Auftreten der Zeichenketten error und ERROR zählt und sie als Linien grafisch darstellt. Diese Methode macht es einfacher, das Auftreten potenzieller Probleme oder Trends zu erkennen, die auf eine Änderung des Musters hindeuten.

Das Folgende ist ein Beispiel dafür für die Infrastruktur-Hosts. Um dies zu verwenden, verketten Sie die Abfragezeilen und ersetzen Sie die `<region>` Attribute `<envname>` und durch die entsprechenden Werte.

```
{
    "widgets": [
        {
            "type": "log",
            "x": 0,
            "y": 0,
            "width": 24,
            "height": 6,
            "properties": {
                "query": "SOURCE '/<envname>/vdc/controller' |
                    SOURCE '/<envname>/cluster-manager' |
                    SOURCE '/<envname>/vdc/dcv-broker' |
                   SOURCE '/<envname>/vdc/dcv-connection-gateway' |
                    fields @timestamp, @message, @logStream, @log\n|
                    filter @message like /(?i)(error|ERROR)/\n|
                    sort @timestamp desc|
                    stats count() by bin(30s)",
                "region": "<region>",
                "title": "infrastructure hosts",
                "view": "timeSeries",
                "stacked": false
            }
        }
    ]
}
```

Ein Beispiel für das Dashboard könnte wie folgt aussehen:



CloudFormation Stapel

Die bei der Umgebungserstellung erstellten CloudFormation Stapel enthalten Ressourcen, Ereignis- und Ausgabeinformationen, die mit der Konfiguration der Umgebung verknüpft sind.

Für jeden Stapel finden Sie auf der Registerkarte Ereignisse, Ressourcen und Ausgaben Informationen zu den Stacks.

RES-Stapel:

- <envname>-Bootstrap
- <envname>-Cluster
- <envname>-Metriken
- <envname>- Verzeichnisdienst
- <envname>-Identitätsanbieter
- <envname>-gemeinsam genutzter Speicher
- <envname>-Clustermanager
- <envname>-dc
- <envname>-Bastion-Gastgeber

Demo Environment Stack (Wenn Sie eine Demo-Umgebung bereitstellen und diese externen Ressourcen nicht zur Verfügung haben, können Sie AWS High Performance Compute-Rezepte verwenden, um Ressourcen für eine Demo-Umgebung zu generieren.)

- <envname>
- <envname>-Netzwerke
- <envname>- DirectoryService
- <envname>-Lagerung
- <envname>- WindowsManagementHost

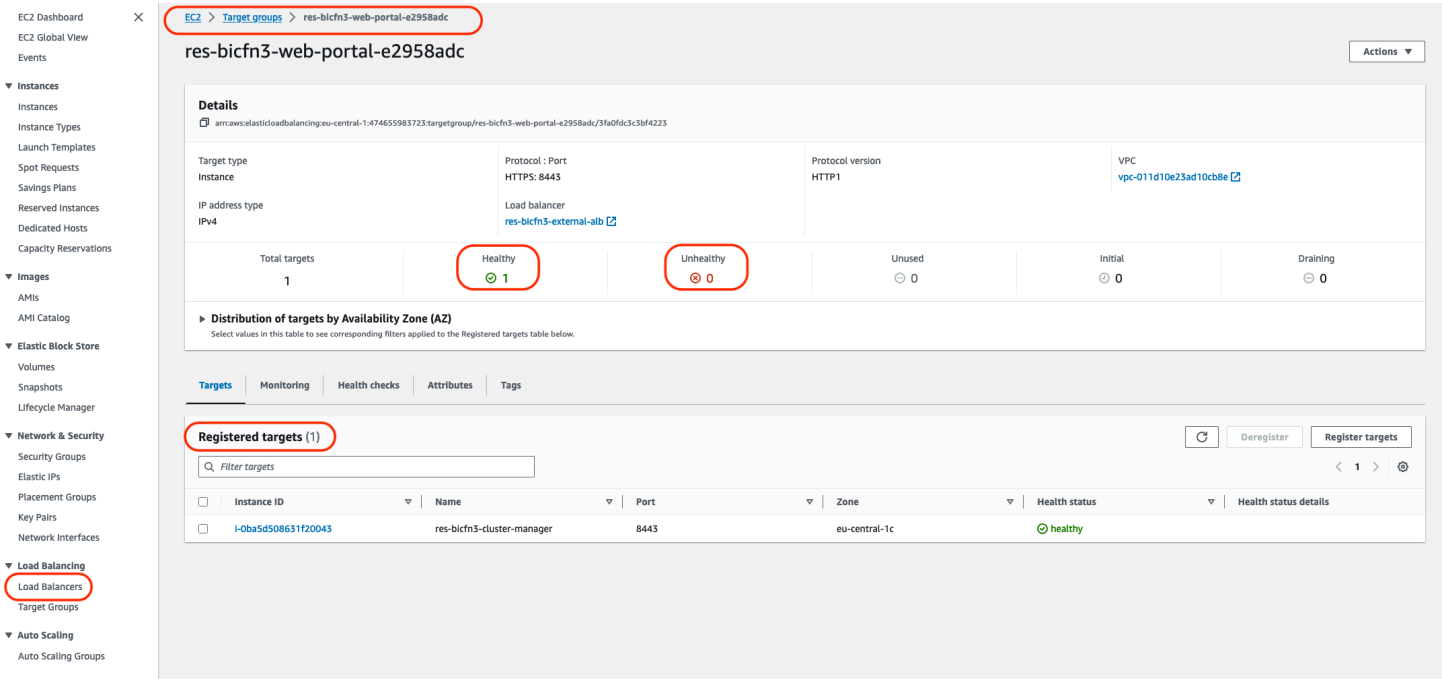
Systemausfälle aufgrund eines Problems, das sich in der Gruppenaktivität von Amazon EC2 Auto Scaling widerspiegelt

Wenn die RES UIs auf Serverfehler hinweisen, kann die Ursache eine Anwendungssoftware oder ein anderes Problem sein.

Jede der Autoscaling-Gruppen (ASGs) der EC2 Amazon-Instance für die Infrastruktur enthält eine Registerkarte „Aktivität“, die nützlich sein kann, um Skalierungsaktivitäten für die Instances zu erkennen. Wenn UI-Seiten auf Fehler hinweisen oder nicht zugänglich sind, überprüfen Sie in der EC2 Amazon-Konsole nach mehreren beendeten Instances und überprüfen Sie auf der Registerkarte Auto Scaling Group Activity die entsprechende ASG, um festzustellen, ob EC2 Amazon-Instances zyklisch laufen.

Falls ja, verwenden Sie die zugehörige CloudWatch Amazon-Protokollgruppe für die Instance, um festzustellen, ob Fehler protokolliert werden, die auf die Ursache des Problems hinweisen könnten. Möglicherweise ist es auch möglich, die SSM-Sitzungskonsole zu verwenden, um eine Sitzung für eine laufende Instance dieses Typs zu öffnen und die Protokolldateien auf der Instance zu untersuchen, um eine Ursache zu ermitteln, bevor die Instance von der ASG als fehlerhaft markiert und beendet wird.

Wenn dieses Problem auftritt, zeigt die ASG-Konsole möglicherweise Aktivitäten an, die der folgenden ähneln.

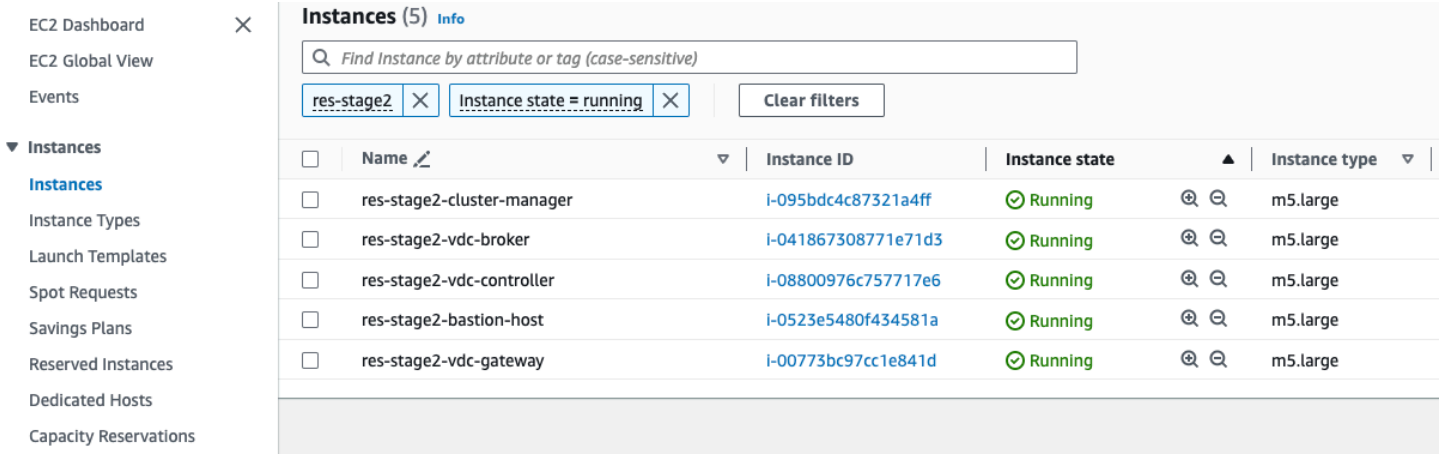


Typisches Erscheinungsbild der EC2 Amazon-Konsole

Dieser Abschnitt enthält Screenshots des Systems, das in verschiedenen Zuständen betrieben wird.

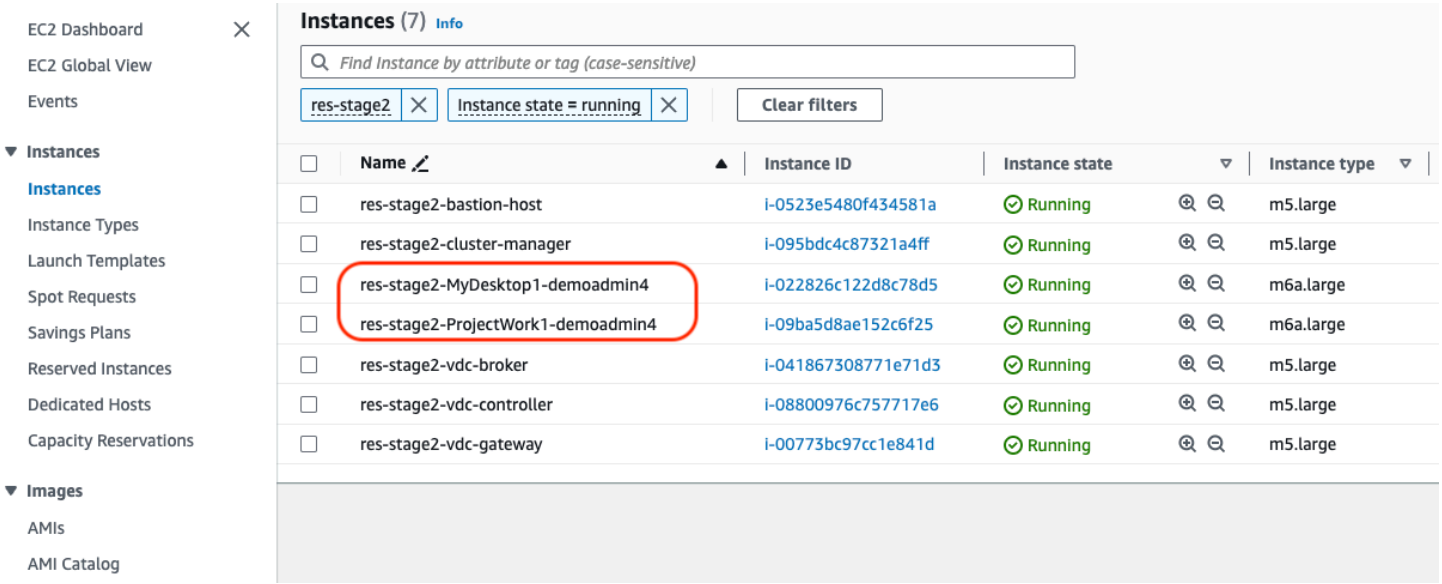
Infrastruktur-Hosts

Wenn keine Desktops laufen, sieht die EC2 Amazon-Konsole in der Regel wie folgt aus. Bei den angezeigten Instances handelt es sich um die RES-Infrastruktur, die Amazon EC2 hostet. Das Präfix in einem Instanznamen ist der Name der RES-Umgebung.



Infrastruktur-Hosts und virtuelle Desktops

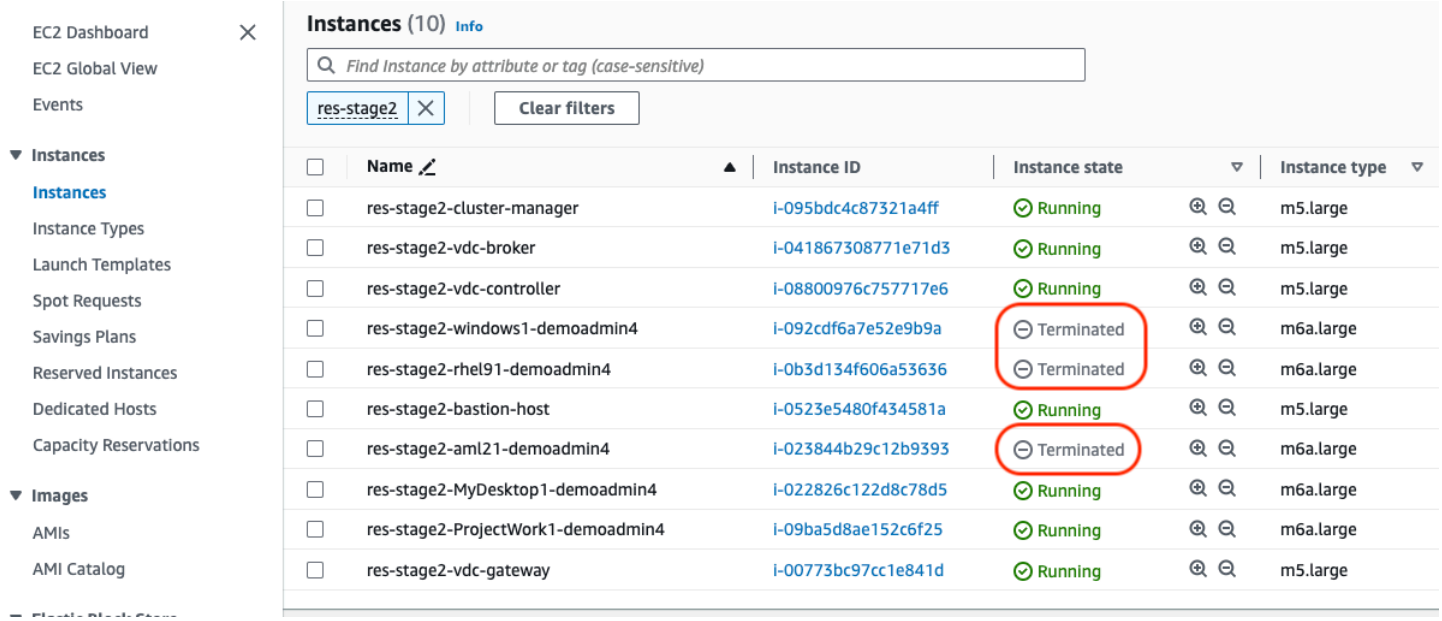
Wenn virtuelle Desktops in der EC2 Amazon-Konsole ausgeführt werden, sehen sie ähnlich wie folgt aus. In diesem Fall sind die virtuellen Desktops rot gekennzeichnet. Das Suffix zum Instanznamen ist der Benutzer, der den Desktop erstellt hat. Der Name in der Mitte ist der Sitzungsname, der beim Start festgelegt wurde. Dabei handelt es sich entweder um den Standardnamen MyDesktop "" oder um den vom Benutzer festgelegten Namen.



Hosts im Status „Beendet“

Wenn die EC2 Amazon-Konsole beendete Instances anzeigt, handelt es sich in der Regel um Desktop-Hosts, die beendet wurden. Wenn die Konsole Infrastruktur-Hosts in einem beendeten Zustand enthält, insbesondere wenn es mehrere vom gleichen Typ gibt, kann dies auf ein laufendes Systemproblem hinweisen.

Die folgende Abbildung zeigt Desktop-Instances, die beendet wurden.



Nützliche Befehle im Zusammenhang mit Active Directory (AD) als Referenz

Im Folgenden finden Sie Beispiele für Befehle im Zusammenhang mit LDAP, die auf Infrastrukturhosts eingegeben werden können, um Informationen zur AD-Konfiguration anzuzeigen. Die Domäne und andere verwendete Parameter sollten denen entsprechen, die bei der Erstellung der Umgebung eingegeben wurden.

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>
```

Windows-DCV-Debuggen

Auf einem Windows-Desktop können Sie die zugehörige Sitzung wie folgt auflisten:

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe'list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
 name:windows1)
```

Finden Sie Informationen zur NICE DCV DCV-Version

NICE DCV wird für virtuelle Desktop-Sitzungen verwendet. AWS NICE DCV. Die folgenden Beispiele zeigen, wie die Version der installierten DCV-Software ermittelt wird.

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

NICE DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe' version

NICE DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Problem RunBooks

Der folgende Abschnitt enthält Probleme, die auftreten können, sowie Hinweise zur Behebung des Problems.

- Probleme bei der Installation
  - AWS CloudFormation Der Stapel kann nicht erstellt werden und die Meldung "WaitCondition hat eine fehlgeschlagene Nachricht erhalten. Fehler: Staaten. TaskFailed“
  - E-Mail-Benachrichtigung wurde nicht empfangen, nachdem AWS CloudFormation Stacks erfolgreich erstellt wurden
  - Instanzen laufen oder der VDC-Controller ist ausgefallen
  - Der CloudFormation Umgebungsstapel kann aufgrund eines Fehlers beim abhängigen Objekt nicht gelöscht werden
  - Bei der Erstellung der Umgebung ist ein Fehler für den CIDR-Blockparameter aufgetreten
  - CloudFormation Fehler bei der Stapelerstellung während der Umgebungserstellung
  - Die Erstellung eines Stacks für externe Ressourcen (Demo) schlägt mit AdDomainAdminNode CREATE_FAILED fehl
- Probleme mit der Identitätsverwaltung
  - Ich bin nicht berechtigt, iam auszuführen: PassRole
  - Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf mein Research and Engineering Studio über AWS Ressourcen ermöglichen
  - Wenn ich mich bei der Umgebung anmelde, kehre ich sofort zur Anmeldeseite zurück
  - Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden
  - Der Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES
  - Der Benutzer ist beim Erstellen einer Sitzung nicht verfügbar
  - Fehler beim Überschreiten der Größenbeschränkung im CloudWatch Cluster-Manager-Protokoll
- Speicher
  - Ich habe das Dateisystem über RES erstellt, aber es wird nicht auf den VDI-Hosts bereitgestellt
  - Ich habe ein Dateisystem über RES integriert, aber es wird nicht auf den VDI-Hosts bereitgestellt
  - Ich kann von VDI-Hosts aus nicht read/write einschalten
    - Beispiele für Anwendungsfälle im Umgang mit Berechtigungen
  - Ich habe Amazon FSx for NetApp ONTAP von RES aus erstellt, aber es ist meiner Domain nicht beigetreten
- Snapshots
  - Ein Snapshot hat den Status Fehlgeschlagen
  - Ein Snapshot kann nicht angewendet werden, da die Protokolle darauf hinweisen, dass die Tabellen nicht importiert werden konnten.

- Infrastruktur
  - Load Balancer-Zielgruppen ohne fehlerfreie Instanzen
- Virtuelle Desktops werden gestartet
  - Ein virtueller Desktop, der zuvor funktionierte, kann keine erfolgreiche Verbindung mehr herstellen
  - Ich kann nur 5 virtuelle Desktops starten
  - Windows-Desktop-Verbindungsversuche schlagen fehl mit der Meldung „Die Verbindung wurde geschlossen“. Transportfehler“
  - VDIs steckt im Bereitstellungsstatus fest
  - VDIs nach dem Start in den Fehlerstatus wechseln
- Virtuelle Desktop-Komponente
  - Die EC2 Amazon-Instance wird in der Konsole wiederholt als beendet angezeigt
  - Die vdc-Controller-Instanz läuft, weil sie dem AD nicht beitreten konnte. /Das eVDI-Modul zeigt die fehlgeschlagene API-Zustandsprüfung
  - Das Projekt erscheint nicht im Pulldown, wenn Sie den Software-Stack bearbeiten, um es hinzuzufügen
  - Clustermanager Amazon CloudWatch Log zeigt „< user-home-init > Konto noch nicht verfügbar. wartet darauf, dass der Benutzer synchronisiert wird“ (wobei das Konto ein Benutzername ist)
  - Auf dem Windows-Desktop wird beim Anmeldeversuch die Meldung „Ihr Konto wurde deaktiviert“ angezeigt. Bitte wenden Sie sich an Ihren Administrator.“
  - Probleme mit den DHCP-Optionen bei der external/customer AD-Konfiguration
  - Firefox-Fehler MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING
- Löschen von Umgebungen
  - res-xxx-cluster Der Stapel befindet sich im Status „DELETE_FAILED“ und kann aufgrund des Fehlers „Rolle ist ungültig oder kann nicht angenommen werden“ nicht manuell gelöscht werden
  - Protokolle sammeln
  - VDI-Protokolle werden heruntergeladen
  - Protokolle von EC2 Linux-Instanzen werden heruntergeladen
  - Protokolle von EC2 Windows-Instanzen herunterladen
  - Sammeln von ECS-Protokollen für den WaitCondition Fehler
- Demo-Umgebung

- Anmeldefehler in der Demo-Umgebung bei der Bearbeitung der Authentifizierungsanfrage an den Identitätsanbieter

Probleme bei der Installation

Themen

- AWS CloudFormation Der Stapel kann nicht erstellt werden und die Meldung "WaitCondition hat eine fehlgeschlagene Nachricht erhalten. Fehler: Staaten. TaskFailed“
- E-Mail-Benachrichtigung wurde nicht empfangen, nachdem AWS CloudFormation Stacks erfolgreich erstellt wurden
- Instanzen laufen oder der VDC-Controller ist ausgefallen
- Der CloudFormation Umgebungsstapel kann aufgrund eines Fehlers beim abhängigen Objekt nicht gelöscht werden
- Bei der Erstellung der Umgebung ist ein Fehler für den CIDR-Blockparameter aufgetreten
- CloudFormation Fehler bei der Stapelerstellung während der Umgebungserstellung
- Die Erstellung eines Stacks für externe Ressourcen (Demo) schlägt mit AdDomainAdminNode CREATE_FAILED fehl

.....

AWS CloudFormation Der Stapel kann nicht erstellt werden und die Meldung "WaitCondition hat eine fehlgeschlagene Nachricht erhalten. Fehler: Staaten. TaskFailed“

Um das Problem zu identifizieren, untersuchen Sie die Amazon CloudWatch Amazon-Protokollgruppe`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. Wenn es mehrere Protokollgruppen mit demselben Namen gibt, überprüfen Sie die erste verfügbare. Eine Fehlermeldung in den Protokollen enthält weitere Informationen zu dem Problem.

> **Note**
>
> Stellen Sie sicher, dass die Parameterwerte keine Leerzeichen enthalten.

.....

E-Mail-Benachrichtigung wurde nicht empfangen, nachdem AWS CloudFormation Stacks erfolgreich erstellt wurden

Wenn nach der erfolgreichen Erstellung der AWS CloudFormation Stacks keine E-Mail-Einladung empfangen wurde, überprüfen Sie Folgendes:

1. Vergewissern Sie sich, dass der E-Mail-Adressparameter korrekt eingegeben wurde.

   Wenn die E-Mail-Adresse falsch ist oder kein Zugriff möglich ist, löschen Sie die Research and Engineering Studio-Umgebung und stellen Sie sie erneut bereit.
2. Suchen Sie in der EC2 Amazon-Konsole nach Hinweisen auf zyklische Instances.

   Wenn EC2 Amazon-Instances mit dem `<envname>` Präfix als beendet angezeigt werden und dann durch eine neue Instance ersetzt werden, liegt möglicherweise ein Problem mit der Netzwerk- oder Active Directory-Konfiguration vor.
3. Wenn Sie die AWS High Performance Compute-Rezepte zur Erstellung Ihrer externen Ressourcen bereitgestellt haben, stellen Sie sicher, dass die VPC, die privaten und öffentlichen Subnetze und andere ausgewählte Parameter vom Stack erstellt wurden.

   Wenn einer der Parameter falsch ist, müssen Sie möglicherweise die RES-Umgebung löschen und erneut bereitstellen. Weitere Informationen finden Sie unter Deinstalliere das Produkt.
4. Wenn Sie das Produkt mit Ihren eigenen externen Ressourcen bereitgestellt haben, stellen Sie sicher, dass das Netzwerk und das Active Directory der erwarteten Konfiguration entsprechen.

   Die Bestätigung, dass Infrastrukturinstanzen erfolgreich dem Active Directory beigetreten sind, ist von entscheidender Bedeutung. Probieren Sie die Schritte unter austhe section called “Instanzen laufen oder der VDC-Controller ist ausgefallen”, um das Problem zu lösen.

.....

Instanzen laufen oder der VDC-Controller ist ausgefallen

Die wahrscheinlichste Ursache für dieses Problem ist die Unfähigkeit der Ressource (n), eine Verbindung zum Active Directory herzustellen oder diesem beizutreten.

Um das Problem zu überprüfen:

1. Starten Sie von der Befehlszeile aus eine Sitzung mit SSM auf der laufenden Instanz des vdc-Controllers.
2. Führen Sie `sudo su -`.
3. Führen Sie `systemctl status sssd`.

Wenn der Status inaktiv oder ausgefallen ist oder Sie Fehler in den Protokollen sehen, konnte die Instanz Active Directory nicht beitreten.

```
[root@ip-                ]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
 Main PID: 31248 (sssd)
   CGroup: /system.slice/sssd.service
           ├─31248 /usr/sbin/sssd -i --logger=files
           ├─31249 /usr/libexec/sssd/sssd_be --domain corp.res.com --uid 0 --gid 0 --logger=files
           ├─31251 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           └─31252 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files

Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
```

Might see “inactive”/“failed” here

Might see errors highlighted in RED here

SSM-Fehlerprotokoll

Um das Problem zu lösen:

- Führen Sie von derselben Befehlszeileninstanz aus, `cat /root/bootstrap/logs/userdata.log` um die Protokolle zu untersuchen.

Das Problem könnte eine von drei möglichen Ursachen haben.

Ursache 1: Falsche LDAP-Verbindungsdetails eingegeben

Überprüfen Sie die Protokolle. Wenn Sie sehen, dass sich Folgendes mehrfach wiederholt, konnte die Instanz dem Active Directory nicht beitreten.

```
+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
```

```
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))
```

1. Stellen Sie sicher, dass die Parameterwerte für Folgendes bei der Erstellung des RES-Stacks korrekt eingegeben wurden.
   - directoryservice.ldap_connection_uri
   - Verzeichnisservice.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - Verzeichnisdienst.Name
2. Aktualisieren Sie alle falschen Werte in der DynamoDB-Tabelle. Die Tabelle befindet sich in der DynamoDB-Konsole unter Tabellen. Der Tabellenname sollte sein. **`<stack name>`**`.cluster-settings`
3. Nachdem Sie die Tabelle aktualisiert haben, löschen Sie den Cluster-Manager und den VDC-Controller, auf denen derzeit die Umgebungsinstanzen ausgeführt werden. Auto Scaling startet neue Instances mit den neuesten Werten aus der DynamoDB-Tabelle.

Ursache 2: Falscher Benutzername eingegeben ServiceAccount

Wenn die Logs zurückgegeben werden`Insufficient permissions to modify computer account`, könnte der bei der Stack-Erstellung eingegebene ServiceAccount Name falsch sein.

1. Öffnen Sie in der AWS Konsole den Secrets Manager.
2. Suchen Sie nach `directoryserviceServiceAccountUsername`. Das Geheimnis sollte sein**`<stack name>`**`-directoryservice-ServiceAccountUsername`.

3. Öffnen Sie das Geheimnis, um die Detailseite anzuzeigen. Wählen Sie unter Geheimer Wert die Option Geheimen Wert abrufen und anschließend Klartext aus.
4. Wenn der Wert aktualisiert wurde, löschen Sie die derzeit laufenden Cluster-Manager- und VDC-Controller-Instanzen der Umgebung. Auto Scaling startet neue Instances mit dem neuesten Wert von Secrets Manager.

Ursache 3: Falsches ServiceAccount Passwort eingegeben

Wenn die Protokolle angezeigt werden`Invalid credentials`, ist das bei der Stack-Erstellung eingegebene ServiceAccount Passwort möglicherweise falsch.

1. Öffnen Sie in der AWS Konsole den Secrets Manager.
2. Suchen Sie nach `directoryserviceServiceAccountPassword`. Das Geheimnis sollte sein**`<stack name>`**`-directoryservice-ServiceAccountPassword`.
3. Öffnen Sie das Geheimnis, um die Detailseite anzuzeigen. Wählen Sie unter Geheimer Wert die Option Geheimen Wert abrufen und anschließend Klartext aus.
4. Wenn Sie das Passwort vergessen haben oder sich nicht sicher sind, ob das eingegebene Passwort korrekt ist, können Sie das Passwort in Active Directory und Secrets Manager zurücksetzen.
   a. So setzen Sie das Passwort zurück in AWS Managed Microsoft AD:
      i. Öffnen Sie die AWS Konsole und gehen Sie zu AWS Directory Service.
      ii. Wählen Sie die Verzeichnis-ID für Ihr RES-Verzeichnis aus und wählen Sie Aktionen aus.
      iii. Wählen Sie Benutzerkennwort zurücksetzen.
      iv. Geben Sie den ServiceAccount Nutzernamen ein.
      v. Geben Sie ein neues Passwort ein und wählen Sie Passwort zurücksetzen.
   b. So setzen Sie das Passwort in Secrets Manager zurück:
      i. Öffnen Sie die AWS Konsole und gehen Sie zu Secrets Manager.
      ii. Suchen Sie nach `directoryserviceServiceAccountPassword`. Das Geheimnis sollte sein**`<stack name>`**`-directoryservice-ServiceAccountPassword`.
      iii. Öffnen Sie das Geheimnis, um die Detailseite anzuzeigen. Wählen Sie unter Geheimer Wert die Option Geheimen Wert abrufen und anschließend Klartext aus.

   iv. Wählen Sie Bearbeiten aus.
   v. Legen Sie ein neues Passwort für den ServiceAccount Benutzer fest und wählen Sie Speichern aus.
5. Wenn Sie den Wert aktualisiert haben, löschen Sie die derzeit laufenden Cluster-Manager- und VDC-Controller-Instanzen der Umgebung. Auto Scaling startet neue Instanzen mit dem neuesten Wert.

.....

Der CloudFormation Umgebungsstapel kann aufgrund eines Fehlers beim abhängigen Objekt nicht gelöscht werden

Wenn das Löschen des **`<env-name>`**`-vdc` CloudFormation Stacks aufgrund eines Fehlers bei einem abhängigen Objekt wie dem fehlschlägt`vdcdcvhostsecuritygroup`, könnte dies an einer EC2 Amazon-Instance liegen, die mithilfe der Konsole in einem von RES erstellten Subnetz oder einer Sicherheitsgruppe gestartet wurde. AWS

Um das Problem zu lösen, suchen und beenden Sie alle EC2 Amazon-Instances, die auf diese Weise gestartet wurden. Anschließend können Sie mit dem Löschen der Umgebung fortfahren.

.....

Bei der Erstellung der Umgebung ist ein Fehler für den CIDR-Blockparameter aufgetreten

Beim Erstellen einer Umgebung wird ein Fehler für den CIDR-Blockparameter mit dem Antwortstatus [FAILED] angezeigt.

Beispiel für einen Fehler:

```
Failed to update cluster prefix list:
        An error occurred (InvalidParameterValue) when calling the
 ModifyManagedPrefixList operation:
        The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
 in the following form: 10.0.0.0/16.
```

Um das Problem zu beheben, ist das erwartete Format x.x.x.0/24 oder x.x.x.0/32.

.....

CloudFormation Fehler bei der Stapelerstellung während der Umgebungserstellung

Das Erstellen einer Umgebung umfasst eine Reihe von Vorgängen zur Erstellung von Ressourcen. In einigen Regionen kann ein Kapazitätsproblem auftreten, das dazu führt, dass die CloudFormation Stack-Erstellung fehlschlägt.

Wenn dies der Fall ist, löschen Sie die Umgebung und versuchen Sie erneut, sie zu erstellen. Alternativ können Sie die Erstellung in einer anderen Region wiederholen.

.....

Die Erstellung eines Stacks für externe Ressourcen (Demo) schlägt mit AdDomainAdminNode CREATE_FAILED fehl

Wenn die Erstellung des Demo-Umgebungsstapels mit dem folgenden Fehler fehlschlägt, kann dies daran liegen, dass EC2 Amazon-Patches während der Bereitstellung nach dem Start der Instance unerwartet auftreten.

```
AdDomainAdminNode CREATE_FAILED  Failed to receive 1 resource signal(s) within the
 specified duration
```

Um die Ursache des Fehlers zu ermitteln:

1. Überprüfen Sie im SSM State Manager, ob das Patchen konfiguriert ist und ob es für alle Instanzen konfiguriert ist.
2. Prüfen Sie in der RunCommand/Automation SSM-Ausführungshistorie, ob die Ausführung eines SSM-Dokuments im Zusammenhang mit dem Start einer Instanz zusammenfällt.
3. Überprüfen Sie in den Protokolldateien für die EC2 Amazon-Instances der Umgebung die lokale Instance-Protokollierung, um festzustellen, ob die Instance während der Bereitstellung neu gestartet wurde.

Wenn das Problem durch das Patchen verursacht wurde, verzögern Sie das Patchen für die RES-Instances mindestens 15 Minuten nach dem Start.

.....

Probleme mit der Identitätsverwaltung

Die meisten Probleme mit Single Sign-On (SSO) und Identitätsmanagement treten aufgrund von Fehlkonfigurationen auf. Informationen zur Einrichtung Ihrer SSO-Konfiguration finden Sie unter:

- the section called “SSO mit IAM Identity Center einrichten”
- the section called “Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)”

Informationen zur Behebung anderer Probleme im Zusammenhang mit der Identitätsverwaltung finden Sie in den folgenden Themen zur Problembehebung:

Themen

- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf mein Research and Engineering Studio über AWS Ressourcen ermöglichen
- Wenn ich mich bei der Umgebung anmelde, kehre ich sofort zur Anmeldeseite zurück
- Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden
- Der Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES
- Der Benutzer ist beim Erstellen einer Sitzung nicht verfügbar
- Fehler beim Überschreiten der Größenbeschränkung im CloudWatch Cluster-Manager-Protokoll

.....

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die iam: PassRole -Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an RES übergeben können.

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Dienst übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer namens marymajor versucht, die Konsole zu verwenden, um eine Aktion in RES auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen Marys Richtlinien aktualisiert werden, damit sie die iam: -Aktion ausführen kann. PassRole Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

.....

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf mein Research and Engineering Studio über AWS Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, wie Sie den Zugriff auf Ihre Ressourcen mit Ihren AWS Konten gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS Konto, das Sie besitzen.
- Informationen dazu, wie Sie AWS Konten von Drittanbietern Zugriff auf Ihre Ressourcen gewähren, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf AWS Konten, die Dritten gehören.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Unterschiede zwischen IAM-Rollen und ressourcenbasierten Richtlinien.

.....

Wenn ich mich bei der Umgebung anmelde, kehre ich sofort zur Anmeldeseite zurück

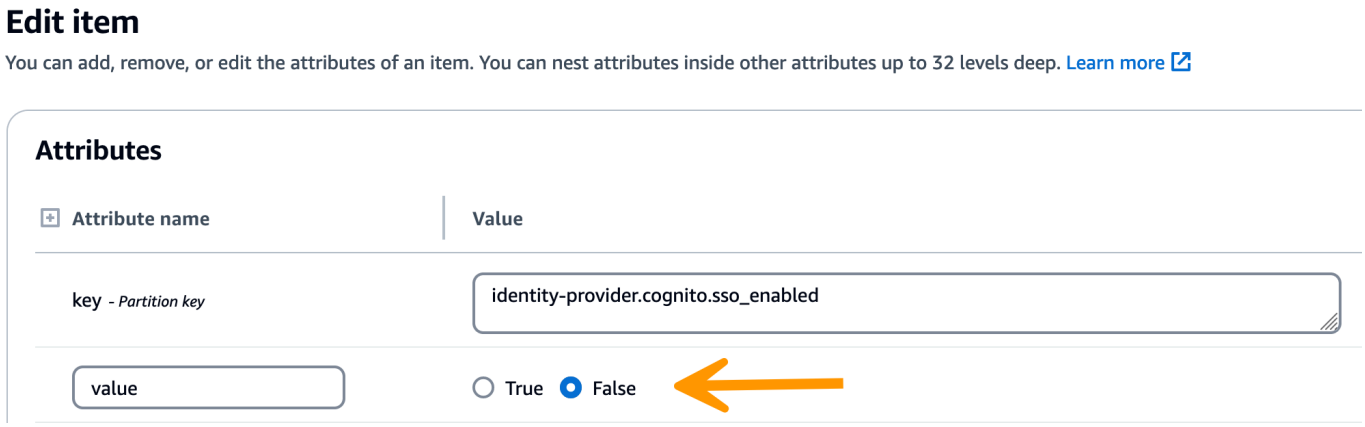
Dieses Problem tritt auf, wenn Ihre SSO-Integration falsch konfiguriert ist. Um das Problem zu ermitteln, überprüfen Sie die Controller-Instanzprotokolle und überprüfen Sie die Konfigurationseinstellungen auf Fehler.

Um die Protokolle zu überprüfen:

1. Öffnen Sie die CloudWatch -Konsole.
2. Suchen Sie unter Protokollgruppen nach der Gruppe mit dem Namen/`<environment-name>`/`cluster-manager`.
3. Öffnen Sie die Protokollgruppe, um nach Fehlern in den Protokolldatenströmen zu suchen.

Um die Konfigurationseinstellungen zu überprüfen:

1. Öffnen Sie die DynamoDB-Konsole
2. Suchen Sie unter Tabellen nach der Tabelle mit dem Namen. `<environment-name>`.`cluster-settings`
3. Öffnen Sie die Tabelle und wählen Sie Tabellenelemente durchsuchen aus.
4. Erweitern Sie den Bereich Filter und geben Sie die folgenden Variablen ein:
   - Attributname — Schlüssel
   - Zustand — enthält
   - Wert — sso
5. Wählen Sie Ausführen aus.
6. Stellen Sie in der zurückgegebenen Zeichenfolge sicher, dass die SSO-Konfigurationswerte korrekt sind. Wenn sie falsch sind, ändern Sie den Wert des Schlüssels sso_enabled in False.



7. Kehren Sie zur RES-Benutzeroberfläche zurück, um SSO neu zu konfigurieren.

.....

Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden

Wenn ein Benutzer beim Versuch, sich an der RES-Schnittstelle anzumelden, den Fehler „Benutzer nicht gefunden“ erhält und der Benutzer in Active Directory präsent ist:

- Wenn der Benutzer nicht in RES vorhanden ist und Sie ihn kürzlich zu AD hinzugefügt haben
  - Es ist möglich, dass der Benutzer noch nicht mit RES synchronisiert ist. RES synchronisiert stündlich, sodass Sie nach der nächsten Synchronisierung möglicherweise warten müssen, um zu überprüfen, ob der Benutzer hinzugefügt wurde. Um sofort zu synchronisieren, folgen Sie den Schritten unterDer Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES.
- Wenn der Benutzer in RES präsent ist:
  1. Stellen Sie sicher, dass die Attributzuordnung korrekt konfiguriert ist. Weitere Informationen finden Sie unter Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO).
  2. Stellen Sie sicher, dass der SAML-Betreff und die SAML-E-Mail beide der E-Mail-Adresse des Benutzers zugeordnet sind.

.....

Der Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES

Wenn Sie einen Benutzer zum Active Directory hinzugefügt haben, dieser jedoch in RES fehlt, muss die AD-Synchronisierung ausgelöst werden. Die AD-Synchronisierung wird stündlich von einer Lambda-Funktion durchgeführt, die AD-Einträge in die RES-Umgebung importiert. Gelegentlich kommt es zu Verzögerungen, bis der nächste Synchronisierungsvorgang ausgeführt wird, nachdem Sie neue Benutzer oder Gruppen hinzugefügt haben. Sie können die Synchronisierung manuell über den Amazon Simple Queue Service initiieren.

Initiieren Sie den Synchronisierungsvorgang manuell:

1. Öffnen Sie die Amazon-SQS-Konsole.
2. Wählen Sie unter Warteschlangen die Option aus`<environment-name>-cluster-manager-tasks.fifo`.
3. Wählen Sie Nachrichten senden und empfangen aus.
4. Geben Sie als Nachrichtentext Folgendes ein:

```
{ "name": "adsync.sync-from-ad", "payload": {} }
```

5. Geben Sie für Nachrichtengruppen-ID Folgendes ein: **`adsync.sync-from-ad`**
6. Geben Sie als Nachrichtendeduplizierungs-ID eine zufällige alphanumerische Zeichenfolge ein. Dieser Eintrag muss sich von allen Anrufen unterscheiden, die innerhalb der letzten fünf Minuten getätigt wurden. Andernfalls wird die Anfrage ignoriert.

.....

Der Benutzer ist beim Erstellen einer Sitzung nicht verfügbar

Wenn Sie als Administrator eine Sitzung erstellen, aber feststellen, dass ein Benutzer, der sich im Active Directory befindet, beim Erstellen einer Sitzung nicht verfügbar ist, muss sich der Benutzer möglicherweise zum ersten Mal anmelden. Sitzungen können nur für aktive Benutzer erstellt werden. Aktive Benutzer müssen sich mindestens einmal bei der Umgebung anmelden.

.....

Fehler beim Überschreiten der Größenbeschränkung im CloudWatch Cluster-Manager-Protokoll

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11,
 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

Wenn Sie diesen Fehler im CloudWatch Cluster-Manager-Protokoll erhalten, hat die LDAP-Suche möglicherweise zu viele Benutzerdatensätze zurückgegeben. Um dieses Problem zu beheben, erhöhen Sie das Limit für LDAP-Suchergebnisse Ihres IDP.

.....

Speicher

Themen

- Ich habe das Dateisystem über RES erstellt, aber es wird nicht auf den VDI-Hosts bereitgestellt
- Ich habe ein Dateisystem über RES integriert, aber es wird nicht auf den VDI-Hosts bereitgestellt
- Ich kann von VDI-Hosts aus nicht read/write einschalten
- Ich habe Amazon FSx for NetApp ONTAP von RES aus erstellt, aber es ist meiner Domain nicht beigetreten

.....

Ich habe das Dateisystem über RES erstellt, aber es wird nicht auf den VDI-Hosts bereitgestellt

Die Dateisysteme müssen sich im Status „Verfügbar“ befinden, bevor sie von VDI-Hosts bereitgestellt werden können. Gehen Sie wie folgt vor, um zu überprüfen, ob sich das Dateisystem im erforderlichen Zustand befindet.

Amazon EFS

1. Gehen Sie zur Amazon EFS-Konsole.
2. Vergewissern Sie sich, dass der Dateisystemstatus Verfügbar ist.
3. Wenn der Dateisystemstatus nicht verfügbar ist, warten Sie, bevor Sie VDI-Hosts starten.

1. Gehen Sie zur FSx Amazon-Konsole.
2. Vergewissern Sie sich, dass der Status verfügbar ist.
3. Wenn der Status nicht verfügbar ist, warten Sie, bevor Sie VDI-Hosts starten.

.....

Ich habe ein Dateisystem über RES integriert, aber es wird nicht auf den VDI-Hosts bereitgestellt

Für die in RES integrierten Dateisysteme sollten die erforderlichen Sicherheitsgruppenregeln so konfiguriert sein, dass VDI-Hosts die Dateisysteme mounten können. Da diese Dateisysteme extern in RES erstellt werden, verwaltet RES die zugehörigen Sicherheitsgruppenregeln nicht.

Die Sicherheitsgruppe, die den integrierten Dateisystemen zugeordnet ist, sollte den folgenden eingehenden Datenverkehr zulassen:

- NFS-Verkehr (Port: 2049) von den Linux-VDC-Hosts
- SMB-Verkehr (Port: 445) von den Windows VDC-Hosts

.....

Ich kann von VDI-Hosts aus nicht read/write einschalten

ONTAP unterstützt den Sicherheitsstil UNIX, NTFS und MIXED für die Volumes. Die Sicherheitsstile bestimmen, welche Art von Berechtigungen ONTAP zur Steuerung des Datenzugriffs verwendet und welcher Clienttyp diese Berechtigungen ändern kann.

Wenn ein Volume beispielsweise den UNIX-Sicherheitsstil verwendet, können SMB-Clients aufgrund des Multiprotokollcharakters von ONTAP trotzdem auf Daten zugreifen (vorausgesetzt, sie authentifizieren und autorisieren). ONTAP verwendet jedoch UNIX-Berechtigungen, die nur UNIX-Clients mit systemeigenen Tools ändern können.

Beispiele für Anwendungsfälle im Umgang mit Berechtigungen

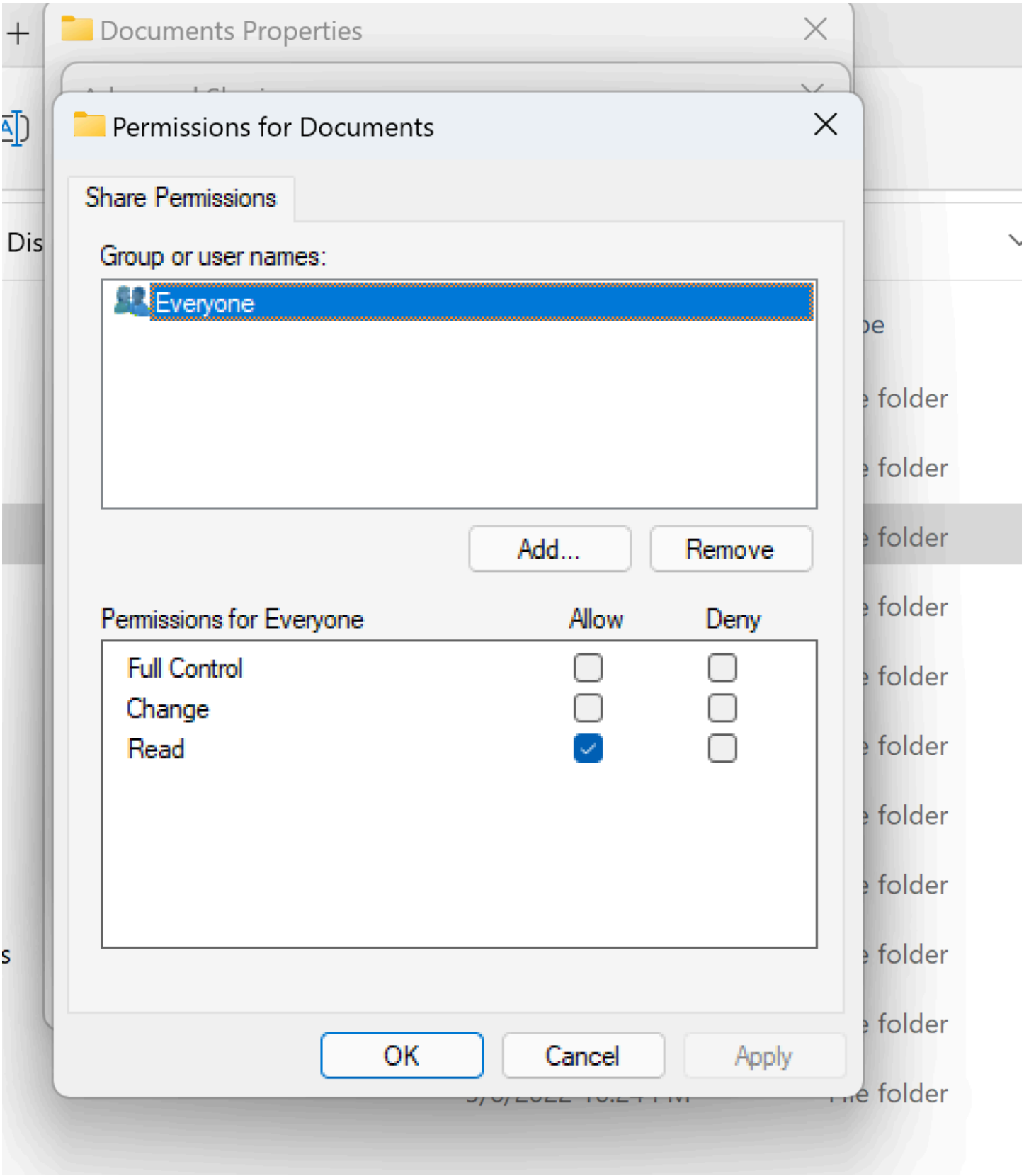
Verwenden eines Volumes im UNIX-Stil mit Linux-Workloads

Berechtigungen können vom Sudoer für andere Benutzer konfiguriert werden. Im Folgenden würden beispielsweise alle Mitglieder über `<group-ID>` volle read/write Berechtigungen für das `/<project-name>` Verzeichnis verfügen:

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

Verwenden eines Datenträgers im NTFS-Stil bei Linux- und Windows-Workloads

Freigabeberechtigungen können mithilfe der Freigabeeigenschaften eines bestimmten Ordners konfiguriert werden. Wenn Sie beispielsweise einen Benutzer `user_01` und einen Ordner angebenmy`folder`, können Sie Berechtigungen für `Full ControlChange`, oder `Read` für `Allow` oder festlegen`Deny`:


Documents Properties
Permissions for Documents
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

Wenn das Volume sowohl von Linux- als auch von Windows-Clients verwendet werden soll, müssen wir auf der SVM eine Namenszuordnung einrichten, die jeden Linux-Benutzernamen demselben Benutzernamen mit dem NetBIOS-Domänennamenformat Domäne\ Benutzername zuordnet. Dies ist für die Übersetzung zwischen Linux- und Windows-Benutzern erforderlich. Weitere Informationen finden Sie unter Aktivieren von Multiprotokoll-Workloads mit Amazon FSx für NetApp ONTAP.

.....

Ich habe Amazon FSx for NetApp ONTAP von RES aus erstellt, aber es ist meiner Domain nicht beigetreten

Wenn Sie Amazon FSx für NetApp ONTAP derzeit von der RES-Konsole aus erstellen, wird das Dateisystem bereitgestellt, aber es tritt der Domain nicht bei. Informationen zum Hinzufügen der erstellten ONTAP-Dateisystem-SVM zu Ihrer Domain finden Sie unter Beitreten SVMs zu einem Microsoft Active Directory und folgen Sie den Schritten auf der FSx Amazon-Konsole. Stellen Sie sicher, dass die erforderlichen Berechtigungen an das Amazon FSx Service-Konto in AD delegiert wurden. Sobald die SVM der Domain erfolgreich beitritt, gehen Sie zu SVM-Zusammenfassung > Endpoints > SMB-DNS-Name und kopieren Sie den DNS-Namen, da Sie ihn später benötigen werden.

Nachdem es der Domäne hinzugefügt wurde, bearbeiten Sie den SMB-DNS-Konfigurationsschlüssel in der DynamoDB-Tabelle mit den Clustereinstellungen:

1. Gehen Sie zur Amazon DynamoDB DynamoDB-Konsole.
2. Wählen Sie Tabellen und dann. `<stack-name>-cluster-settings`
3. Erweitern Sie unter Tabellenelemente durchsuchen die Option Filter und geben Sie den folgenden Filter ein:
   - Attributname — Schlüssel
   - Bedingung — Entspricht
   - Wert - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. Wählen Sie den zurückgesandten Artikel aus und klicken Sie dann auf Aktionen, Artikel bearbeiten.
5. Aktualisieren Sie den Wert mit dem SMB-DNS-Namen, den Sie zuvor kopiert haben.
6. Wählen Sie Speichern und schließen aus.

Stellen Sie außerdem sicher, dass die dem Dateisystem zugeordnete Sicherheitsgruppe den in File System Access Control with Amazon VPC empfohlenen Datenverkehr zulässt. Neue VDI-Hosts, die das Dateisystem verwenden, können nun die zur Domäne gehörende SVM und das Dateisystem mounten.

Alternativ können Sie ein vorhandenes Dateisystem einbinden, das bereits mit Ihrer Domain verknüpft ist. Wählen Sie dazu unter Environment Management die Option Dateisysteme, Onboard-Dateisystem aus.

.....

Snapshots

Themen

- Ein Snapshot hat den Status Fehlgeschlagen
- Ein Snapshot kann nicht angewendet werden, da die Protokolle darauf hinweisen, dass die Tabellen nicht importiert werden konnten.

.....

Ein Snapshot hat den Status Fehlgeschlagen

Wenn ein Snapshot auf der Seite RES-Snapshots den Status Fehlgeschlagen hat, kann die Ursache ermittelt werden, indem Sie in der CloudWatch Amazon-Protokollgruppe für den Cluster-Manager nach dem Zeitpunkt suchen, zu dem der Fehler aufgetreten ist.

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
  asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
  creating the snapshot: An error occurred (TableNotFoundException)
  when calling the UpdateContinuousBackups operation:
  Table not found: res-demo.accounts.sequence-config
```

.....

Ein Snapshot kann nicht angewendet werden, da die Protokolle darauf hinweisen, dass die Tabellen nicht importiert werden konnten.

Wenn ein Snapshot aus einer früheren Umgebung nicht in einer neuen Umgebung angewendet werden kann, suchen Sie in den CloudWatch Protokollen nach dem Cluster-Manager, um das

Problem zu identifizieren. Wenn das Problem darauf hinweist, dass die erforderlichen Tabellen nicht importiert wurden, überprüfen Sie, ob sich der Snapshot in einem gültigen Zustand befindet.

1. Laden Sie die Datei metadata.json herunter und überprüfen Sie, ob die Datei ExportStatus für die verschiedenen Tabellen den Status ABGESCHLOSSEN hat. Stellen Sie sicher, dass das Feld für die verschiedenen Tabellen festgelegt ist`ExportManifest`. Wenn Sie den oben genannten Feldsatz nicht finden, befindet sich der Snapshot in einem ungültigen Zustand und kann nicht mit der Funktion „Snapshot anwenden“ verwendet werden.
2. Nachdem Sie die Erstellung eines Snapshots initiiert haben, stellen Sie sicher, dass der Snapshot-Status in RES auf ABGESCHLOSSEN wechselt. Die Erstellung eines Snapshots dauert bis zu 5 bis 10 Minuten. Laden Sie die Seite Snapshot-Verwaltung neu oder besuchen Sie sie erneut, um sicherzustellen, dass der Snapshot erfolgreich erstellt wurde. Dadurch wird sichergestellt, dass sich der erstellte Snapshot in einem gültigen Zustand befindet.

.....

Infrastruktur

Themen

- Load Balancer-Zielgruppen ohne fehlerfreie Instanzen

.....

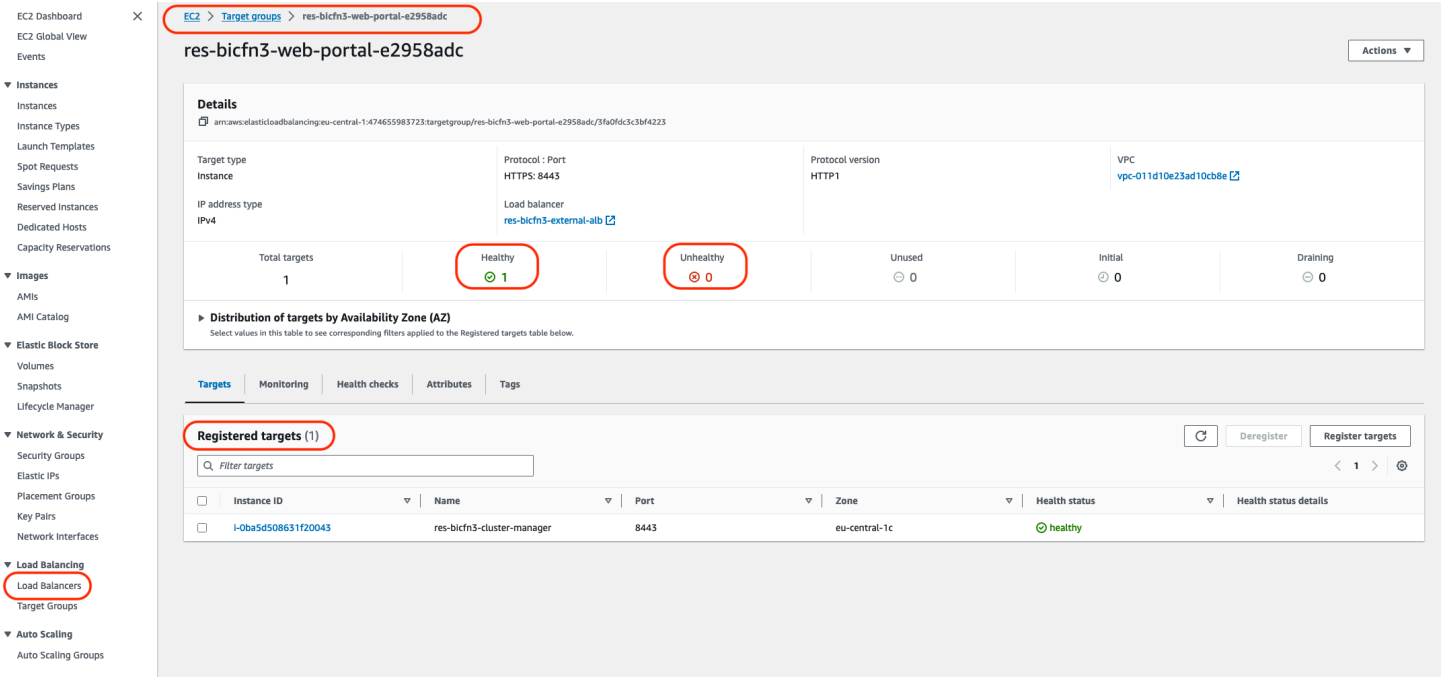
Load Balancer-Zielgruppen ohne fehlerfreie Instanzen

Wenn Probleme wie Serverfehlermeldungen in der Benutzeroberfläche angezeigt werden oder Desktop-Sitzungen keine Verbindung herstellen können, kann dies auf ein Problem in der Infrastruktur der EC2 Amazon-Instances hinweisen.

Um die Ursache des Problems zu ermitteln, suchen Sie zunächst in der EC2 Amazon-Konsole nach EC2 Amazon-Instances, die anscheinend wiederholt beendet und durch neue Instances ersetzt werden. In diesem Fall kann die Ursache anhand der CloudWatch Amazon-Protokolle ermittelt werden.

Eine andere Methode besteht darin, die Load Balancer im System zu überprüfen. Ein Hinweis darauf, dass möglicherweise Systemprobleme vorliegen, ist, wenn ein Load Balancer auf der EC2 Amazon-Konsole keine registrierten fehlerfreien Instances anzeigt.

Ein Beispiel für ein normales Erscheinungsbild finden Sie hier:



Wenn der Health-Eintrag 0 ist, bedeutet dies, dass keine EC2 Amazon-Instance für die Bearbeitung von Anfragen verfügbar ist.

Wenn der Eintrag Unhealthy nicht 0 ist, deutet dies darauf hin, dass eine EC2 Amazon-Instance möglicherweise zyklisch läuft. Dies kann daran liegen, dass die installierte Anwendungssoftware die Integritätsprüfungen nicht bestanden hat.

Wenn sowohl die Einträge „Gesund“ als auch „Unhealthy“ den Wert 0 haben, deutet dies auf eine mögliche Fehlkonfiguration des Netzwerks hin. Beispielsweise verfügen die öffentlichen und privaten Subnetze möglicherweise nicht über entsprechende Subnetze. AZs Wenn dieser Zustand eintritt, wird auf der Konsole möglicherweise zusätzlicher Text angezeigt, der darauf hinweist, dass der Netzwerkstatus vorhanden ist.

.....

Virtuelle Desktops werden gestartet

Themen

- Ein virtueller Desktop, der zuvor funktionierte, kann keine erfolgreiche Verbindung mehr herstellen
- Ich kann nur 5 virtuelle Desktops starten
- Windows-Desktop-Verbindungsversuche schlagen fehl mit der Meldung „Die Verbindung wurde geschlossen“. Transportfehler“

- VDIs steckt im Bereitstellungsstatus fest
- VDIs nach dem Start in den Fehlerstatus wechseln

.....

Ein virtueller Desktop, der zuvor funktionierte, kann keine erfolgreiche Verbindung mehr herstellen

Wenn eine Desktop-Verbindung geschlossen wird oder Sie keine Verbindung mehr herstellen können, liegt das Problem möglicherweise daran, dass die zugrunde liegende EC2 Amazon-Instance ausfällt oder die EC2 Amazon-Instance außerhalb der RES-Umgebung beendet oder gestoppt wurde. Der Status der Admin-Benutzeroberfläche zeigt möglicherweise weiterhin den Status Bereit an, aber Versuche, eine Verbindung herzustellen, schlagen fehl.

Die EC2 Amazon-Konsole sollte verwendet werden, um festzustellen, ob die Instance beendet oder gestoppt wurde. Wenn sie gestoppt wurde, versuchen Sie erneut, sie zu starten. Wenn der Status beendet ist, muss ein weiterer Desktop erstellt werden. Alle Daten, die im Home-Verzeichnis des Benutzers gespeichert wurden, sollten weiterhin verfügbar sein, wenn die neue Instanz gestartet wird.

Wenn die Instanz, die zuvor ausgefallen ist, immer noch auf der Admin-Benutzeroberfläche angezeigt wird, muss sie möglicherweise über die Admin-Benutzeroberfläche beendet werden.

.....

Ich kann nur 5 virtuelle Desktops starten

Das Standardlimit für die Anzahl der virtuellen Desktops, die ein Benutzer starten kann, ist 5. Dies kann von einem Administrator über die Admin-Benutzeroberfläche wie folgt geändert werden:

- Gehen Sie zu den Desktop-Einstellungen.
- Wählen Sie die Registerkarte Server aus.
- Klicken Sie im Bereich DCV-Sitzung rechts auf das Bearbeitungssymbol.
- Ändern Sie den Wert unter Zulässige Sitzungen pro Benutzer auf den gewünschten neuen Wert.
- Wählen Sie Absenden aus.
- Aktualisieren Sie die Seite, um zu bestätigen, dass die neue Einstellung vorhanden ist.

.....

Windows-Desktop-Verbindungsversuche schlagen fehl mit der Meldung „Die Verbindung wurde geschlossen“. Transportfehler“

Wenn eine Windows-Desktop-Verbindung mit dem UI-Fehler „Die Verbindung wurde geschlossen“ fehlschlägt. „Transportfehler“: Die Ursache kann auf ein Problem in der DCV-Serversoftware zurückzuführen sein, das mit der Zertifikatserstellung auf der Windows-Instanz zusammenhängt.

Die CloudWatch Amazon-Protokollgruppe protokolliert `<envname>/vdc/dcv-connection-gateway` möglicherweise den Fehler beim Verbindungsversuch mit Meldungen, die den folgenden ähneln:

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]

Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

In diesem Fall besteht eine Lösung möglicherweise darin, den SSM Session Manager zu verwenden, um eine Verbindung zur Windows-Instance herzustellen und die folgenden 2 Dateien zu entfernen, die sich auf Zertifikate beziehen:

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
```

```
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

Die Dateien sollten automatisch neu erstellt werden und ein nachfolgender Verbindungsversuch könnte erfolgreich sein.

Wenn diese Methode das Problem behebt und wenn bei Neustarts von Windows-Desktops derselbe Fehler auftritt, verwenden Sie die Funktion „Software-Stack erstellen“, um einen neuen Windows-Softwarestack der festen Instanz mit den neu generierten Zertifikatsdateien zu erstellen. Dadurch kann ein Windows-Softwarestack entstehen, der für erfolgreiche Starts und Verbindungen verwendet werden kann.

.....

VDIs steckt im Bereitstellungsstatus fest

Wenn ein Desktop-Start in der Admin-Benutzeroberfläche im Bereitstellungsstatus verbleibt, kann dies mehrere Gründe haben.

Um die Ursache zu ermitteln, überprüfen Sie die Protokolldateien auf der Desktop-Instanz und suchen Sie nach Fehlern, die das Problem verursachen könnten. Dieses Dokument enthält eine Liste von Protokolldateien und CloudWatch Amazon-Protokollgruppen, die relevante Informationen im Abschnitt Nützliche Protokoll- und Ereignisinformationsquellen enthalten.

Im Folgenden sind mögliche Ursachen für dieses Problem aufgeführt.

- Die verwendete AMI-ID wurde als Software-Stack registriert, wird aber von RES nicht unterstützt.

  Das Bootstrap-Bereitstellungsskript konnte nicht abgeschlossen werden, da das AMI nicht über die erwartete Konfiguration oder die erforderlichen Tools verfügt. Die Protokolldateien auf der Instance, z. B. `/root/bootstrap/logs/` auf einer Linux-Instance, können diesbezüglich nützliche Informationen enthalten. AMIs IDs aus dem AWS Marketplace funktionieren möglicherweise nicht für RES-Desktop-Instanzen. Sie müssen getestet werden, um zu bestätigen, ob sie unterstützt werden.
- Benutzerdatenskripts werden nicht ausgeführt, wenn die virtuelle Windows-Desktop-Instanz von einem benutzerdefinierten AMI aus gestartet wird.

  Standardmäßig werden Benutzerdatenskripts einmal ausgeführt, wenn eine EC2 Amazon-Instance gestartet wird. Wenn Sie ein AMI aus einer vorhandenen virtuellen Desktop-Instance erstellen, dann einen Software-Stack beim AMI registrieren und versuchen, einen anderen virtuellen Desktop

mit diesem Software-Stack zu starten, werden Benutzerdatenskripts auf der neuen virtuellen Desktop-Instance nicht ausgeführt.

Um das Problem zu beheben, öffnen Sie ein PowerShell Befehlsfenster als Administrator auf der ursprünglichen virtuellen Desktop-Instance, mit der Sie das AMI erstellt haben, und führen Sie den folgenden Befehl aus:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Erstellen Sie dann ein neues AMI aus der Instance. Sie können das neue AMI verwenden, um Software-Stacks zu registrieren und anschließend neue virtuelle Desktops zu starten. Beachten Sie, dass Sie denselben Befehl auch für die Instance ausführen können, die im Bereitstellungsstatus verbleibt, und die Instance neu starten können, um die virtuelle Desktop-Sitzung zu reparieren. Beim Starten eines anderen virtuellen Desktops über das falsch konfigurierte AMI treten Sie jedoch erneut auf dasselbe Problem.

.....

VDIs nach dem Start in den Fehlerstatus wechseln

Mögliches Problem 1: Das Home-Dateisystem hat ein Verzeichnis für den Benutzer mit unterschiedlichen POSIX-Berechtigungen.

Dies könnte das Problem sein, mit dem Sie konfrontiert sind, wenn die folgenden Szenarien zutreffen:

1. Die bereitgestellte RES-Version ist 2024.01 oder höher.
2. Während der Bereitstellung des RES-Stacks `EnableLdapIDMapping` wurde das Attribut für auf gesetzt. `True`
3. Das bei der Bereitstellung des RES-Stacks angegebene Home-Dateisystem wurde in einer Version vor RES 2024.01 oder in einer früheren Umgebung mit der Einstellung auf verwendet. `EnableLdapIDMapping` `False`

Lösungsschritte: Löschen Sie die Benutzerverzeichnisse im Dateisystem.

1. SSM zum Cluster-Manager-Host.
2. `cd /home`.
3. `ls`- sollte Verzeichnisse mit Verzeichnisnamen auflisten, die mit Benutzernamen übereinstimmen, wie`admin1`,`admin2`.. und so weiter.

4. Löscht die Verzeichnisse,`sudo rm -r 'dir_name'`. Löschen Sie nicht die Verzeichnisse ssm-user und ec2-user.
5. Wenn die Benutzer bereits mit der neuen Umgebung synchronisiert sind, löschen Sie die Benutzer aus der DDB-Tabelle des Benutzers (außer clusteradmin).
6. AD-Synchronisierung initiieren — `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` im Cluster-Manager Amazon ausführen. EC2
7. Starten Sie die VDI-Instanz im `Error` Status von der RES-Webseite aus neu. Stellen Sie sicher, dass der VDI in etwa 20 Minuten in den `Ready` Status übergeht.

.....

Virtuelle Desktop-Komponente

Themen

- Die EC2 Amazon-Instance wird in der Konsole wiederholt als beendet angezeigt
- Die vdc-Controller-Instanz läuft, weil sie dem AD nicht beitreten konnte. /Das eVDI-Modul zeigt die fehlgeschlagene API-Zustandsprüfung
- Das Projekt erscheint nicht im Pulldown, wenn Sie den Software-Stack bearbeiten, um es hinzuzufügen
- Clustermanager Amazon CloudWatch Log zeigt „< user-home-init > Konto noch nicht verfügbar. wartet darauf, dass der Benutzer synchronisiert wird“ (wobei das Konto ein Benutzername ist)
- Auf dem Windows-Desktop wird beim Anmeldeversuch die Meldung „Ihr Konto wurde deaktiviert“ angezeigt. Bitte wenden Sie sich an Ihren Administrator.“
- Probleme mit den DHCP-Optionen bei der external/customer AD-Konfiguration
- Firefox-Fehler MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

.....

Die EC2 Amazon-Instance wird in der Konsole wiederholt als beendet angezeigt

Wenn eine Infrastruktur-Instance in der EC2 Amazon-Konsole wiederholt als beendet angezeigt wird, kann die Ursache in ihrer Konfiguration liegen und vom Typ der Infrastruktur-Instance abhängen. Im Folgenden finden Sie Methoden, um die Ursache zu ermitteln.

Wenn die vdc-controller-Instance in der EC2 Amazon-Konsole wiederholt den Status „Beendet“ anzeigt, kann dies an einem falschen Secret-Tag liegen. Geheimnisse, die von RES verwaltet werden, haben Tags, die als Teil der IAM-Zugriffskontrollrichtlinien verwendet werden, die den EC2 Amazon-Infrastruktur-Instances zugeordnet sind. Wenn der vdc-Controller zyklisch läuft und der folgende Fehler in der CloudWatch Protokollgruppe erscheint, kann dies daran liegen, dass ein Geheimnis nicht korrekt markiert wurde. Beachten Sie, dass das Geheimnis mit dem folgenden Tag versehen werden muss:

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

Die CloudWatch Amazon-Protokollmeldung für diesen Fehler wird etwa wie folgt aussehen:

```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Überprüfen Sie die Tags auf der EC2 Amazon-Instance und vergewissern Sie sich, dass sie mit der obigen Liste übereinstimmen.

.....

Die vdc-Controller-Instanz läuft, weil sie dem AD nicht beitreten konnte. /Das eVDI-Modul zeigt die fehlgeschlagene API-Zustandsprüfung

Wenn das eVDI-Modul die Zustandsprüfung nicht besteht, wird im Abschnitt Umgebungsstatus Folgendes angezeigt.

Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

In diesem Fall besteht der allgemeine Pfad zum Debuggen darin, in die CloudWatchCluster-Manager-Protokolle zu schauen. (Suchen Sie nach der Protokollgruppe mit dem Namen.) `<env-name>/cluster-manager`

Mögliche Probleme:

- Wenn die Protokolle den Text enthalten`Insufficient permissions`, stellen Sie sicher, dass der ServiceAccount Benutzername, der bei der Erstellung des Res-Stacks angegeben wurde, richtig geschrieben ist.

  Beispiel für eine Protokollzeile:

  ```
  Insufficient permissions to modify computer account:
   CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
   000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - Sie können über die SecretsManager Konsole auf den bei der RES-Bereitstellung angegebenen ServiceAccount Benutzernamen zugreifen. Suchen Sie im Secrets Manager nach dem entsprechenden Secret und wählen Sie Retrieve Plain Text aus. Wenn der Benutzername falsch

ist, wählen Sie Bearbeiten aus, um den Geheimwert zu aktualisieren. Beenden Sie die aktuellen Cluster-Manager- und VDC-Controller-Instanzen. Die neuen Instanzen werden sich in einem stabilen Zustand befinden.

- Der Benutzername muss "ServiceAccount" lauten, wenn Sie die Ressourcen verwenden, die durch den bereitgestellten externen Ressourcenstapel erstellt wurden. Wenn der `DisableADJoin` Parameter bei der Bereitstellung von RES auf False gesetzt wurde, stellen Sie sicher, dass der Benutzer ServiceAccount "" über die erforderlichen Berechtigungen zum Erstellen von Computerobjekten im AD verfügt.

- Wenn der verwendete Benutzername korrekt war, die Protokolle jedoch den Text enthalten`Invalid credentials`, ist das von Ihnen eingegebene Passwort möglicherweise falsch oder abgelaufen.

  Beispiel für eine Protokollzeile:

```
{'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
 'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
 data 532, v4563'}
```

  - Sie können das Passwort, das Sie bei der Erstellung der Umgebung eingegeben haben, lesen, indem Sie in der Secrets Manager-Konsole auf das Geheimnis zugreifen, das das Passwort speichert. Wählen Sie das Geheimnis aus (z. B.`<env_name>directoryserviceServiceAccountPassword`) und wählen Sie Klartext abrufen aus.

  - Wenn das Passwort im Secret falsch ist, wählen Sie Bearbeiten aus, um den Wert im Secret zu aktualisieren. Beenden Sie die aktuellen Cluster-Manager- und VDC-Controller-Instanzen. Die neuen Instanzen verwenden das aktualisierte Passwort und befinden sich in einem stabilen Zustand.

  - Wenn das Passwort korrekt ist, kann es sein, dass das Passwort im verbundenen Active Directory abgelaufen ist. Sie müssen zuerst das Passwort im Active Directory zurücksetzen und dann das Geheimnis aktualisieren. Sie können das Benutzerkennwort im Active Directory von der Directory Service Console aus zurücksetzen:

    1. Wählen Sie die entsprechende Verzeichnis-ID
    2. Wählen Sie Aktionen, Benutzerkennwort zurücksetzen und füllen Sie dann das Formular mit dem Benutzernamen (z. B. "ServiceAccount„) und dem neuen Passwort aus.

3. Wenn sich das neu eingestellte Passwort vom vorherigen Passwort unterscheidet, aktualisieren Sie das Passwort im entsprechenden Secret Manager-Geheimnis (z. `<env_name>directoryserviceServiceAccountPassword` B.
4. Beenden Sie die aktuellen Cluster-Manager- und VDC-Controller-Instanzen. Die neuen Instanzen werden sich in einem stabilen Zustand befinden.

.....

Das Projekt erscheint nicht im Pulldown, wenn Sie den Software-Stack bearbeiten, um es hinzuzufügen

Dieses Problem kann mit dem folgenden Problem im Zusammenhang mit der Synchronisierung des Benutzerkontos mit AD zusammenhängen. Wenn dieses Problem auftritt, überprüfen Sie die CloudWatch Amazon-Protokollgruppe des Cluster-Managers auf den Fehler "`<user-home-init> account not available yet. waiting for user to be synced`", um festzustellen, ob die Ursache dieselbe ist oder zusammenhängt.

.....

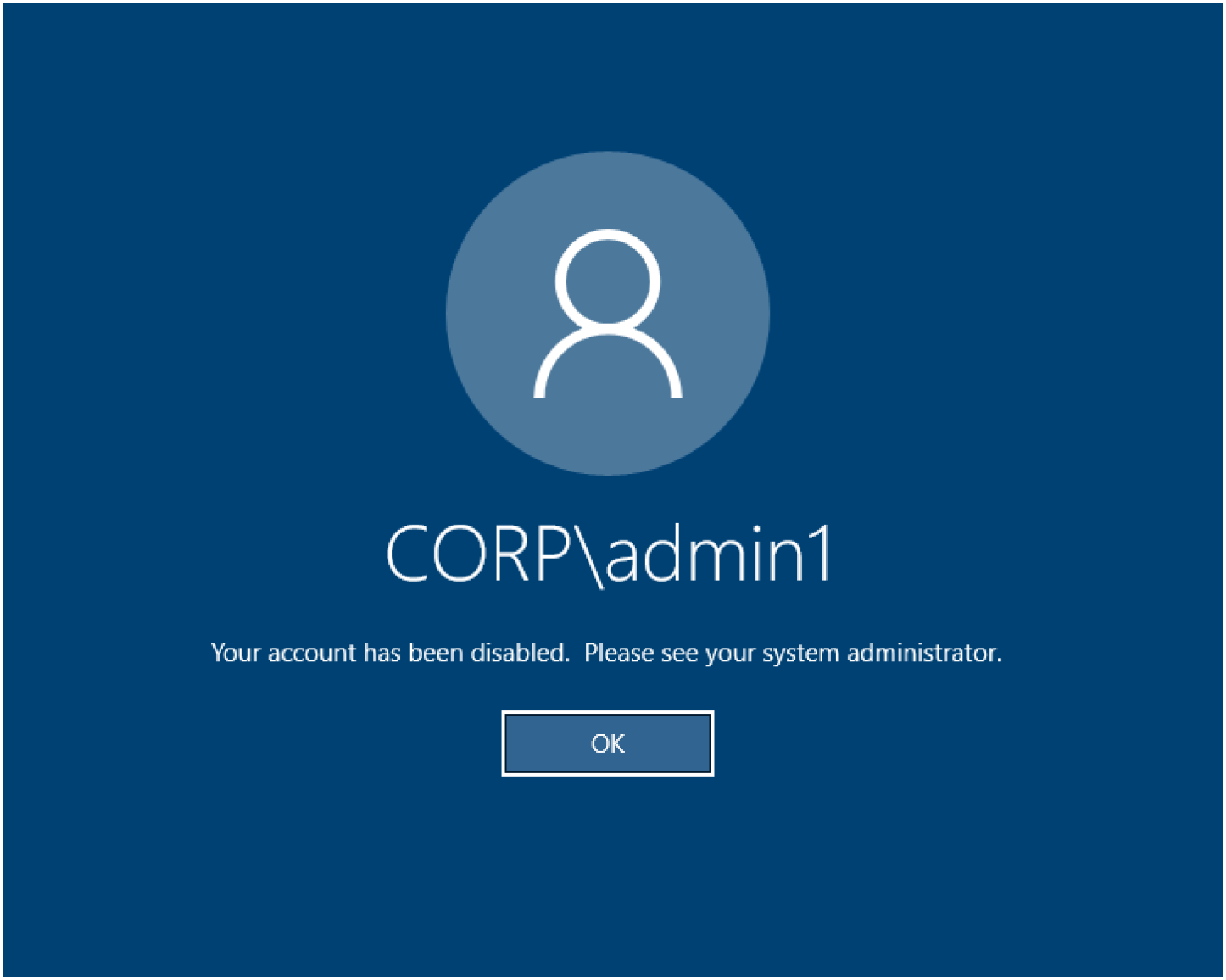
Clustermanager Amazon CloudWatch Log zeigt „< user-home-init > Konto noch nicht verfügbar. wartet darauf, dass der Benutzer synchronisiert wird“ (wobei das Konto ein Benutzername ist)

Der SQS-Abonnent ist beschäftigt und steckt in einer Endlosschleife fest, weil er nicht auf das Benutzerkonto zugreifen kann. Dieser Code wird ausgelöst, wenn versucht wird, während der Benutzersynchronisierung ein Home-Dateisystem für einen Benutzer zu erstellen.

Der Grund, warum es nicht in der Lage ist, auf das Benutzerkonto zuzugreifen, ist möglicherweise, dass RES für das verwendete AD nicht korrekt konfiguriert wurde. Ein Beispiel könnte sein, dass der bei der Erstellung der BI/RES Umgebung verwendete `ServiceAccountUsername` Parameter nicht der richtige Wert war, z. B. die Verwendung von "ServiceAccount" anstelle von „Admin“.

.....

Auf dem Windows-Desktop wird beim Anmeldeversuch die Meldung „Ihr Konto wurde deaktiviert“ angezeigt. Bitte wenden Sie sich an Ihren Administrator.“



Wenn sich der Benutzer auf einem gesperrten Bildschirm nicht wieder anmelden kann, kann dies darauf hindeuten, dass der Benutzer in dem für RES konfigurierten AD deaktiviert wurde, nachdem er sich erfolgreich über SSO angemeldet hat.

Die SSO-Anmeldung sollte fehlschlagen, wenn das Benutzerkonto in AD deaktiviert wurde.

.....

Probleme mit den DHCP-Optionen bei der external/customer AD-Konfiguration

Wenn Sie bei der Verwendung von RES `"The connection has been closed. Transport error"` mit Ihrem eigenen Active Directory auf einen Fehler bei virtuellen Windows-Desktops stoßen, suchen Sie im dcv-connection-gateway CloudWatch Amazon-Protokoll nach etwas Ähnlichem wie dem Folgenden:

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }

Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Wenn Sie einen AD-Domänencontroller für Ihre DHCP-Optionen für Ihre eigene VPC verwenden, müssen Sie:

1. Fügen Sie den beiden Domänencontrollern AmazonProvided DNS hinzu. IPs
2. Setzen Sie den Domainnamen auf ec2.internal.

Ein Beispiel wird hier gezeigt. Ohne diese Konfiguration gibt der Windows-Desktop einen Transportfehler RES/DCV aus, weil nach dem Hostnamen ip-10-0-x-xx.ec2.internal gesucht wird.

.....

Firefox-Fehler MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Wenn Sie den Firefox-Webbrowser verwenden, wird möglicherweise die Fehlermeldung vom Typ MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING angezeigt, wenn Sie versuchen, eine Verbindung zu einem virtuellen Desktop herzustellen.

Die Ursache ist, dass der RES-Webserver mit TLS + Stapling On eingerichtet ist, aber nicht mit Stapling Validation reagiert (siehe https://support.mozilla). org/en-US/questions/1372483.

Sie können dies beheben, indem Sie den Anweisungen unter / mozilla_pkix_error_required_tls_feature_missing folgen. https://really-simple-ssl.com

.....

Löschen von Umgebungen

Themen

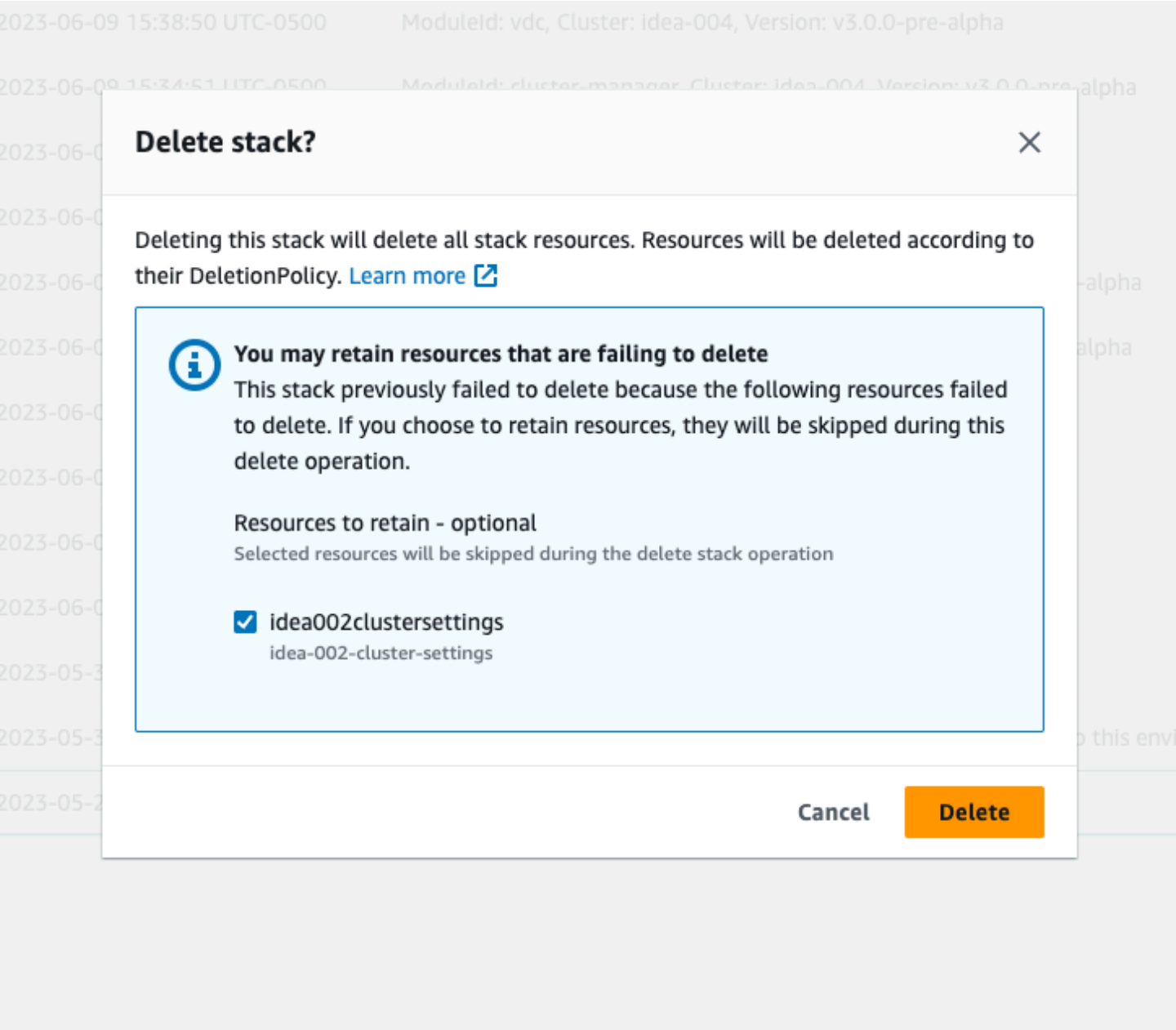
- res-xxx-cluster Der Stapel befindet sich im Status „DELETE_FAILED“ und kann aufgrund des Fehlers „Rolle ist ungültig oder kann nicht angenommen werden“ nicht manuell gelöscht werden
- Protokolle sammeln
- VDI-Protokolle werden heruntergeladen
- Protokolle von EC2 Linux-Instanzen werden heruntergeladen
- Protokolle von EC2 Windows-Instanzen herunterladen
- Sammeln von ECS-Protokollen für den WaitCondition Fehler

.....

res-xxx-cluster Der Stapel befindet sich im Status „DELETE_FAILED“ und kann aufgrund des Fehlers „Rolle ist ungültig oder kann nicht angenommen werden“ nicht manuell gelöscht werden

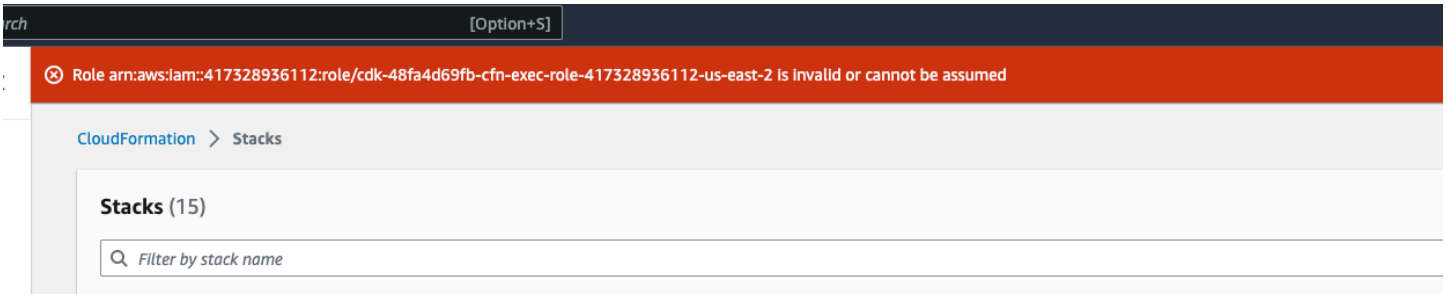
Wenn Sie feststellen, dass sich der Stapel res-xxx-cluster "" im Status „DELETE_FAILED“ befindet und nicht manuell gelöscht werden kann, können Sie ihn mit den folgenden Schritten löschen.

Wenn Sie sehen, dass sich der Stapel im Status „DELETE_FAILED“ befindet, versuchen Sie zunächst, ihn manuell zu löschen. Möglicherweise wird ein Dialogfeld angezeigt, in dem Delete Stack bestätigt wird. Wählen Sie Löschen aus.



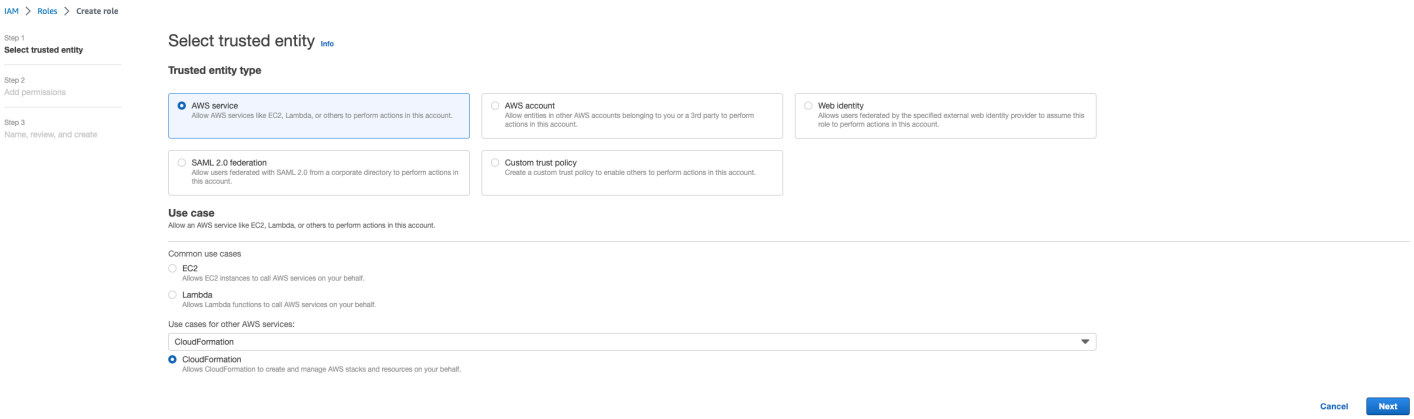
Selbst wenn Sie alle erforderlichen Stack-Ressourcen löschen, wird manchmal immer noch die Meldung angezeigt, dass Sie Ressourcen auswählen müssen, die beibehalten werden sollen. Wählen Sie in diesem Fall alle Ressourcen als „beizubehaltende Ressourcen“ aus und wählen Sie Löschen aus.

Möglicherweise wird ein Fehler angezeigt, der wie folgt aussieht `Role: arn:aws:iam::... is Invalid or cannot be assumed`



Das bedeutet, dass die Rolle, die zum Löschen des Stacks erforderlich ist, zuerst gelöscht wurde, bevor der Stapel gelöscht wurde. Um dies zu umgehen, kopieren Sie den Namen der Rolle. Gehen Sie zur IAM-Konsole und erstellen Sie eine Rolle mit diesem Namen. Verwenden Sie dabei die folgenden Parameter:

- Wählen Sie für den Typ Vertrauenswürdige Entität die Option AWS Service aus.
- Wählen Sie für Anwendungsfall unter `Use cases for other AWS services` „Wählen“ aus`CloudFormation`.



Klicken Sie auf Weiter. Stellen Sie sicher, dass Sie den Rollen " und `AWSCloudFormationFullAccess` '`AdministratorAccess`' die Berechtigungen geben. Ihre Bewertungsseite sollte so aussehen:

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
cdk-48fa4d69fb-cfn-exec-role-417328936112-us-east-2
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows CloudFormation to create and manage AWS stacks and resources on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities — Edit

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "",
6             "Effect": "Allow",
7             "Principal": {
8                 "Service": "cloudformation.amazonaws.com"
9             },
10            "Action": "sts:AssumeRole"
11        }
12    ]
13 }
```

Step 2: Add permissions — Edit

Permissions policy summary

Policy name	Type	Attached as
AWSCloudFormationFullAccess	AWS managed	Permissions policy
AdministratorAccess	AWS managed - job function	Permissions policy

Tags

Gehen Sie dann zurück zur CloudFormation Konsole und löschen Sie den Stack. Sie sollten es jetzt löschen können, seit Sie die Rolle erstellt haben. Gehen Sie abschließend zur IAM-Konsole und löschen Sie die von Ihnen erstellte Rolle.

.....

Protokolle sammeln

Von der EC2 Konsole aus bei einer EC2 Instanz anmelden

- Folgen Sie diesen Anweisungen, um sich bei Ihrer EC2 Linux-Instance anzumelden.
- Folgen Sie diesen Anweisungen, um sich bei Ihrer EC2 Windows-Instanz anzumelden. Öffnen Sie dann PowerShell Windows, um beliebige Befehle auszuführen.

Sammeln von Infrastruktur-Host-Protokollen

1. Cluster-Manager: Rufen Sie die Protokolle für den Clustermanager von den folgenden Stellen ab und hängen Sie sie an das Ticket an.
   a. Alle Protokolle aus der CloudWatch Protokollgruppe. `<env-name>/cluster-manager`

b. Alle Protokolle im `/root/bootstrap/logs` Verzeichnis auf der `<env-name>-cluster-manager` EC2 Instanz. Folgen Sie den Anweisungen unter „Von der EC2 Konsole aus bei einer EC2 Instanz anmelden“ am Anfang dieses Abschnitts, um sich bei Ihrer Instance anzumelden.

2. VDC-Controller: Rufen Sie die Logs für den vdc-Controller von den folgenden Stellen ab und hängen Sie sie an das Ticket an.

   a. Alle Protokolle aus der Protokollgruppe. CloudWatch `<env-name>/vdc-controller`

   b. Alle Protokolle im `/root/bootstrap/logs` Verzeichnis auf der `<env-name>-vdc-controller` EC2 Instanz. Folgen Sie den Anweisungen unter „Von der EC2 Konsole aus bei einer EC2 Instanz anmelden“ am Anfang dieses Abschnitts, um sich bei Ihrer Instance anzumelden.

Eine Möglichkeit, die Logs einfach abzurufen, besteht darin, den Anweisungen im Protokolle von EC2 Linux-Instanzen werden heruntergeladen Abschnitt zu folgen. Der Modulname wäre der Instanzname.

Sammeln von VDI-Protokollen

Identifizieren Sie die entsprechende EC2 Amazon-Instance

Wenn ein Benutzer einen VDI mit einem Sitzungsnamen starten würde`VDI1`, wäre `<env-name>-VDI1-<user name>` der entsprechende Name der Instance auf der EC2 Amazon-Konsole.

Sammeln Sie Linux-VDI-Protokolle

Melden Sie sich von der EC2 Amazon-Konsole aus bei der entsprechenden EC2 Amazon-Instance an, indem Sie den Anweisungen folgen, die zu Beginn dieses Abschnitts unter „Von der EC2 Konsole aus bei einer EC2 Instance anmelden“ verlinkt sind. Rufen Sie alle Protokolle unter den `/var/log/dcv/` Verzeichnissen `/root/bootstrap/logs` und auf der EC2 VDI-Amazon-Instance ab.

Eine Möglichkeit, die Protokolle abzurufen, besteht darin, sie auf S3 hochzuladen und dann von dort herunterzuladen. Dazu können Sie die folgenden Schritte ausführen, um alle Protokolle aus einem Verzeichnis abzurufen und sie dann hochzuladen:

1. Gehen Sie wie folgt vor, um die DCV-Protokolle in das `/root/bootstrap/logs` Verzeichnis zu kopieren:

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
```

```
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Folgen Sie nun den im nächsten Abschnitt aufgeführten SchrittenVDI-Protokolle werden heruntergeladen, um die Protokolle herunterzuladen.

Sammeln Sie Windows VDI-Protokolle

Melden Sie sich von der EC2 Amazon-Konsole aus bei der entsprechenden EC2 Amazon-Instance an, indem Sie den Anweisungen folgen, die zu Beginn dieses Abschnitts unter „Von der EC2 Konsole aus bei einer EC2 Instance anmelden“ verlinkt sind. Rufen Sie alle Protokolle unter dem `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` Verzeichnis auf der EC2 VDI-Instance ab.

Eine Möglichkeit, die Protokolle abzurufen, besteht darin, sie auf S3 hochzuladen und dann von dort herunterzuladen. Folgen Sie dazu den im nächsten Abschnitt aufgeführten SchrittenVDI-Protokolle werden heruntergeladen.

.....

VDI-Protokolle werden heruntergeladen

1. Aktualisieren Sie die IAM-Rolle der EC2 VDI-Instanz, um den S3-Zugriff zu ermöglichen.
2. Gehen Sie zur EC2 Konsole und wählen Sie Ihre VDI-Instanz aus.
3. Wählen Sie die IAM-Rolle aus, die sie verwendet.
4. Wählen Sie im Dropdownmenü Berechtigungen hinzufügen im Abschnitt Berechtigungsrichtlinien die Option Richtlinien anhängen aus und wählen Sie dann die FullAccess AmazonS3-Richtlinie aus.
5. Wählen Sie Berechtigungen hinzufügen aus, um diese Richtlinie anzuhängen.
6. Folgen Sie anschließend je nach VDI-Typ den unten aufgeführten Schritten, um die Protokolle herunterzuladen. Der Modulname wäre der Instanzname.
   a. Protokolle von EC2 Linux-Instanzen werden heruntergeladenfür Linux.
   b. Protokolle von EC2 Windows-Instanzen herunterladenfür Windows.
7. Bearbeiten Sie abschließend die Rolle, um die `AmazonS3FullAccess` Richtlinie zu entfernen.

> **Note**
>
> Alle VDIs verwenden dieselbe IAM-Rolle, nämlich `<env-name>-vdc-host-role-<region>`

.....

Protokolle von EC2 Linux-Instanzen werden heruntergeladen

Melden Sie sich bei der EC2 Instanz an, von der Sie Logs herunterladen möchten, und führen Sie die folgenden Befehle aus, um alle Logs in einen S3-Bucket hochzuladen:

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

Gehen Sie danach zur S3-Konsole, wählen Sie den Bucket mit dem Namen aus `<environment_name>-cluster-<region>-<aws_account_number>` und laden Sie die zuvor hochgeladene `<module_name>_logs.tar.gz` Datei herunter.

.....

Protokolle von EC2 Windows-Instanzen herunterladen

Melden Sie sich bei der EC2 Instanz an, von der Sie Protokolle herunterladen möchten, und führen Sie die folgenden Befehle aus, um alle Protokolle in einen S3-Bucket hochzuladen:

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
```

```
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

Gehen Sie danach zur S3-Konsole, wählen Sie den Bucket mit dem Namen aus `<environment_name>-cluster-<region>-<aws_account_number>` und laden Sie die zuvor hochgeladene `<module_name>_logs.zip` Datei herunter.

.....

Sammeln von ECS-Protokollen für den WaitCondition Fehler

1. Gehen Sie zum bereitgestellten Stack und wählen Sie die Registerkarte Ressourcen.
2. Erweitern Sie Deploy ResearchAndEngineeringStudio→ → Installer → Tasks CreateTaskDef→ CreateContainer→ und wählen Sie die Protokollgruppe aus LogGroup, um die CloudWatch Logs zu öffnen.
3. Besorgen Sie sich das neueste Protokoll aus dieser Protokollgruppe.

.....

Demo-Umgebung

Themen

- Anmeldefehler in der Demo-Umgebung bei der Bearbeitung der Authentifizierungsanfrage an den Identitätsanbieter

.....

Anmeldefehler in der Demo-Umgebung bei der Bearbeitung der Authentifizierungsanfrage an den Identitätsanbieter

Problem

Wenn Sie versuchen, sich anzumelden und die Meldung „Unerwarteter Fehler bei der Bearbeitung der Authentifizierungsanfrage an den Identitätsanbieter“ angezeigt wird, sind Ihre Passwörter

möglicherweise abgelaufen. Dies kann entweder das Passwort für den Benutzer sein, mit dem Sie sich anmelden möchten, oder Ihr Directory Service Directory-Dienstkonto.

Schadensbegrenzung

1. Setzen Sie die Benutzer- und Dienstkontokennwörter in der Directory Service Console zurück.
2. Aktualisieren Sie die Passwörter für das Dienstkonto in Secrets Manager so, dass sie mit dem neuen Passwort übereinstimmen, das Sie oben eingegeben haben:
   - für den Keycloak-Stack: PasswordSecret-... - -... RESExternal - DirectoryService-... mit Beschreibung: Passwort für Microsoft Active Directory
   - für RES: res- ServiceAccountPassword -... mit Beschreibung: Directory Service Directory-Dienstkontokennwort
3. Gehen Sie zur EC2 Konsole und beenden Sie die Cluster-Manager-Instanz. Auto Scaling Scaling-Regeln lösen automatisch die Bereitstellung einer neuen Instanz aus.

.....

Bekannte Probleme

- Bekannte Probleme 2024.x
  - (2024.06) Das Anwenden des Snapshots schlägt fehl, wenn der AD-Gruppenname Leerzeichen enthält
  - (2024.04-2024.04.02) Die angegebene IAM-Berechtigungsgrenze ist nicht an die Rolle der VDI-Instanzen gebunden
  - (2024.04.02 und früher) Windows NVIDIA-Instanzen in ap-southeast-2 (Sydney) können nicht gestartet werden
  - (2024.04 und 2024.04.01) Fehler beim Löschen von RES in GovCloud
  - (2024.04 - 2024.04.02) Der virtuelle Linux-Desktop bleibt beim Neustart möglicherweise im Status „RESUMING“ hängen
  - (2024.04.02 und früher) Fehler beim Synchronisieren von AD-Benutzern, deren SAMAccount Namensattribut Großbuchstaben oder Sonderzeichen enthält
  - (2024.04.02 und früher) Der private Schlüssel für den Zugriff auf den Bastion-Host ist ungültig
  - (2024.06 und früher) Gruppenmitglieder wurden während der AD-Synchronisierung nicht mit RES synchronisiert

- (2024.06 und früher) CVE-2024-6387, Regre, Sicherheitslücke in und Ubuntu SSHion RHEL9 VDIs

Bekannte Probleme 2024.x

.....

(2024.06) Das Anwenden des Snapshots schlägt fehl, wenn der AD-Gruppenname Leerzeichen enthält

Problem

RES 2024.06 kann keine Snapshots aus früheren Versionen anwenden, wenn die Namen der AD-Gruppen Leerzeichen enthalten.

Die CloudWatch Cluster-Manager-Protokolle (unter der `<environment-name>/cluster-manager` Protokollgruppe) werden während der AD-Synchronisierung den folgenden Fehler enthalten:

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

Der Fehler ist darauf zurückzuführen, dass RES nur Gruppennamen akzeptiert, die die folgenden Anforderungen erfüllen:

- Er kann nur ASCII-Kleinbuchstaben und -großbuchstaben, Ziffern, Bindestriche (-), Punkte (.) und Unterstriche (_) enthalten
- Ein Bindestrich (-) ist als erstes Zeichen nicht zulässig
- Er darf keine Leerzeichen enthalten.

Betroffene Versionen

2024.06

Schadensbegrenzung

1. Um das Patch-Skript und die Patch-Datei (patch.py und groupname_regex.patch) herunterzuladen, führen Sie den folgenden Befehl aus und `<output-directory>` ersetzen

Sie ihn durch das Verzeichnis, in dem Sie die Dateien ablegen möchten, und `<environment-name>` durch den Namen Ihrer RES-Umgebung:

a. Der Patch gilt nur für RES 2024.06

b. Das Patch-Skript erfordert AWS CLI v2, Python 3.9.16 oder höher und Boto3.

c. Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben:

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. Navigieren Sie zu dem Verzeichnis, in das das Patch-Skript und die Patch-Datei heruntergeladen wurden. Führen Sie den folgenden Patch-Befehl aus:

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Um die Cluster Manager-Instance für Ihre Umgebung neu zu starten, führen Sie die folgenden Befehle aus: Sie können die Instance auch über die Amazon EC2 Management Console beenden.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> Der Patch ermöglicht es AD-Gruppennamen, ASCII-Kleinbuchstaben und -großbuchstaben, Ziffern, Bindestriche (-), Punkte (.), Unterstriche (_) und Leerzeichen mit einer Gesamtlänge zwischen 1 und 30 (einschließlich) zu enthalten.

.....

(2024.04-2024.04.02) Die angegebene IAM-Berechtigungsgrenze ist nicht an die Rolle der VDI-Instanzen gebunden

Das Problem

Virtuelle Desktop-Sitzungen erben die Konfiguration der Berechtigungsgrenzen ihres Projekts nicht ordnungsgemäß. Dies ist darauf zurückzuführen, dass die durch den Parameter IAMPermission Grenze definierte Berechtigungsgrenze einem Projekt bei der Erstellung dieses Projekts nicht ordnungsgemäß zugewiesen wurde.

Betroffene Versionen

2024.04 - 2024.04.02

Schadensbegrenzung

Gehen Sie wie folgt vor, VDIs um die einem Projekt zugewiesene Rechtegrenze ordnungsgemäß zu vererben:

1. Um das Patch-Skript und die Patch-Datei (patch.py und vdi_host_role_permission_boundary.patch) herunterzuladen, führen Sie den folgenden Befehl aus und ersetzen Sie ihn durch das lokale Verzeichnis, in dem Sie die Dateien ablegen möchten: `<output-directory>`

   a. Der Patch gilt nur für RES 2024.04.02. Wenn Sie Version 2024.04 oder 2024.04.01 verwenden, können Sie die im öffentlichen Dokument für kleinere Versionsupdates aufgeführten Schritte befolgen, um Ihre Umgebung auf 2024.04.02 zu aktualisieren.

   b. Das Patch-Skript erfordert AWS CLI (v2), Python 3.9.16 oder höher und Boto3.

   c. Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Navigieren Sie zu dem Verzeichnis, in das das Patch-Skript und die Patch-Datei heruntergeladen wurden. Führen Sie den folgenden Patch-Befehl aus und `<environment-name>` ersetzen Sie ihn durch den Namen Ihrer RES-Umgebung:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Starten Sie die Cluster-Manager-Instanz in Ihrer Umgebung neu, indem Sie diesen Befehl ausführen und ihn durch den Namen Ihrer RES-Umgebung `<environment-name>` ersetzen. Sie können die Instance auch über die Amazon EC2 Management Console beenden.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 und früher) Windows NVIDIA-Instanzen in ap-southeast-2 (Sydney) können nicht gestartet werden

Das Problem

Amazon Machine Images (AMIs) werden verwendet, um virtuelle Desktops (VDIs) in RES mit bestimmten Konfigurationen einzurichten. Jedem AMI ist eine ID zugeordnet, die sich je nach Region unterscheidet. Die in RES zum Starten von Windows Nvidia-Instances in ap-southeast-2 (Sydney) konfigurierte AMI-ID ist derzeit falsch.

Die AMI-ID `ami-0e190f8939a996caf` für diese Art von Instanzkonfiguration ist in ap-southeast-2 (Sydney) falsch aufgeführt. Stattdessen `ami-027cf6e71e2e442f4` sollte die AMI-ID verwendet werden.

Benutzer erhalten die folgende Fehlermeldung, wenn sie versuchen, eine Instance mit dem `ami-0e190f8939a996caf` Standard-AMI zu starten.

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id ‘[ami-0e190f8939a996caf]’ does not exist
```

Schritte zur Reproduktion des Fehlers, einschließlich einer Beispielkonfigurationsdatei:

- Stellen Sie RES in der ap-southeast-2 bereit.
- Starten Sie eine Instance mit dem Windows-NVidia-Standard-Softwarestack (AMI-IDami-0e190f8939a996caf).

Betroffene Versionen

Alle RES-Versionen 2024.04.02 oder früher sind betroffen

Schadensbegrenzung

Die folgende Abhilfemaßnahme wurde auf der RES-Version 2024.01.01 getestet:

- Registrieren Sie einen neuen Software-Stack mit den folgenden Einstellungen
  - AMI ID: `ami-027cf6e71e2e442f4`
  - Betriebssystem: Windows
  - GPU-Hersteller: NVIDIA
  - Min. Speichergröße (GB): 30
  - min. RAM (GB): 4
- Verwenden Sie diesen Software-Stack, um Windows-NVIDIA-Instanzen zu starten

.....

(2024.04 und 2024.04.01) Fehler beim Löschen von RES in GovCloud

Das Problem

Während des RES-Löschworkflows inaktiviert `UnprotectCognitoUserPool` Lambda den Löschschutz für Cognito-Benutzerpools, die später gelöscht werden. Die Lambda-Ausführung wird von der `InstallerStateMachine` gestartet.

Aufgrund der Unterschiede in der AWS Standard-CLI-Version zwischen Commercial und GovCloud Regionen schlägt der `update_user_pool` Aufruf im Lambda in GovCloud Regionen fehl.

Kunden erhalten die folgende Fehlermeldung, wenn sie versuchen, RES in GovCloud Regionen zu löschen:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Schritte zur Reproduktion des Fehlers:

- Stellen Sie RES in einer GovCloud Region bereit
- Löschen Sie den RES-Stack

Betroffene Versionen

RES-Versionen 2024.04 und 2024.04.01

Schadensbegrenzung

Die folgende Abhilfemaßnahme wurde auf der RES-Version 2024.04 getestet:

- Öffne das `UnprotectCognitoUserPool` Lambda
  - Benennungskonvention: `<env-name>-InstallerTasksUnprotectCognitoUserPool-...`
- Laufzeiteinstellungen -> Bearbeiten -> Laufzeit wählen `Python 3.11` -> Speichern.
- Öffnen CloudFormation.

- RES-Stack löschen -> Retain Installer Resource DEAKTIVIERT lassen -> Löschen.

.....

(2024.04 - 2024.04.02) Der virtuelle Linux-Desktop bleibt beim Neustart möglicherweise im Status „RESUMING“ hängen

Das Problem

Virtuelle Linux-Desktops können im Status „FORTSETZEN“ hängen bleiben, wenn sie nach einem manuellen oder geplanten Stopp neu gestartet werden.

Nach dem Neustart der Instanz führt der AWS Systems Manager keine Remotebefehle aus, um eine neue DCV-Sitzung zu erstellen, und die folgende Protokollmeldung fehlt in den CloudWatch vdc-Controller-Protokollen (unter der Protokollgruppe): `<environment-name>/vdc/controller` CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Betroffene Versionen

2024.04 - 2024.04.02

Schadensbegrenzung

Gehen Sie wie folgt vor, um die virtuellen Desktops wiederherzustellen, die sich im Status „RESUMING“ befinden:

1. Stellen Sie von der Konsole aus eine SSH-Verbindung zur Probleminstanz her. EC2
2. Führen Sie die folgenden Befehle auf der Instanz aus:

   ```
   sudo su -
   /bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
   configure_post_reboot.sh
   sudo reboot
   ```

3. Warten Sie, bis die Instanz neu gestartet wird.

Um zu verhindern, dass bei neuen virtuellen Desktops dasselbe Problem auftritt:

1. Um das Patch-Skript und die Patch-Datei (patch.py und vdi_stuck_in_resuming_status.patch) herunterzuladen, führen Sie den folgenden Befehl aus und ersetzen Sie ihn durch das Verzeichnis, in dem Sie die Dateien ablegen möchten: `<output-directory>`

> **Note**
>
> - Der Patch gilt nur für RES 2024.04.02.
> - Das Patch-Skript erfordert AWS CLI v2, Python 3.9.16 oder höher und Boto3.
> - Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Navigieren Sie zu dem Verzeichnis, in das das Patch-Skript und die Patch-Datei heruntergeladen wurden. Führen Sie den folgenden Patch-Befehl aus und `<environment-name>` ersetzen Sie ihn durch den Namen Ihrer RES-Umgebung und `<aws-region>` durch die Region, in der RES bereitgestellt wird:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Um die VDC Controller-Instanz für Ihre Umgebung neu zu starten, führen Sie die folgenden Befehle aus und `<environment-name>` ersetzen Sie sie durch den Namen Ihrer RES-Umgebung:

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
```

```
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 und früher) Fehler beim Synchronisieren von AD-Benutzern, deren SAMAccount Namensattribut Großbuchstaben oder Sonderzeichen enthält

Das Problem

RES kann AD-Benutzer nicht synchronisieren, nachdem SSO für mindestens zwei Stunden eingerichtet wurde (zwei AD-Synchronisierungszyklen). Die CloudWatch Cluster-Manager-Protokolle (in der `<environment-name>/cluster-manager` Protokollgruppe) enthalten den folgenden Fehler bei der AD-Synchronisierung:

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

Der Fehler ist darauf zurückzuführen, dass RES nur einen SAMAccount Benutzernamen akzeptiert, der die folgenden Anforderungen erfüllt:

- Er kann nur ASCII-Kleinbuchstaben, Ziffern, Punkte (.) und Unterstriche (_) enthalten.
- Ein Punkt oder Unterstrich ist als erstes oder letztes Zeichen nicht zulässig.
- Es darf nicht zwei aufeinanderfolgende Punkte oder Unterstriche enthalten (z. B..., __, ._, _.).

Betroffene Versionen

2024.04.02 und früher

Schadensbegrenzung

1. Um das Patch-Skript und die Patch-Datei (patch.py und samaccountname_regex.patch) herunterzuladen, führen Sie den folgenden Befehl aus und ersetzen Sie ihn durch das Verzeichnis, in `<output-directory>` dem Sie die Dateien ablegen möchten:

> **Note**
>
> - Der Patch gilt nur für RES 2024.04.02.
> - Das Patch-Skript erfordert AWS CLI v2, Python 3.9.16 oder höher und Boto3.
> - Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
 ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. Navigieren Sie zu dem Verzeichnis, in das das Patch-Skript und die Patch-Datei heruntergeladen wurden. Führen Sie den folgenden Patch-Befehl aus und `<environment-name>` ersetzen Sie ihn durch den Namen Ihrer RES-Umgebung:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Um die Cluster Manager-Instanz für Ihre Umgebung neu zu starten, führen Sie die folgenden Befehle aus und `<environment-name>` ersetzen Sie sie durch den Namen Ihrer RES-Umgebung. Sie können die Instance auch über die Amazon EC2 Management Console beenden.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 und früher) Der private Schlüssel für den Zugriff auf den Bastion-Host ist ungültig

Das Problem

Wenn ein Benutzer den privaten Schlüssel für den Zugriff auf den Bastion-Host vom RES-Webportal herunterlädt, ist der Schlüssel nicht richtig formatiert — mehrere Zeilen werden als eine einzige Zeile heruntergeladen, wodurch der Schlüssel ungültig wird. Der Benutzer erhält die folgende Fehlermeldung, wenn er versucht, mit dem heruntergeladenen Schlüssel auf den Bastion-Host zuzugreifen:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

Betroffene Versionen

2024.04.02 und früher

Schadensbegrenzung

Wir empfehlen, Chrome zum Herunterladen der Schlüssel zu verwenden, da dieser Browser davon nicht betroffen ist.

Alternativ kann die Schlüsseldatei neu formatiert werden, indem eine neue Zeile danach `-----BEGIN PRIVATE KEY-----` und eine weitere neue Zeile unmittelbar davor erstellt wird. `-----END PRIVATE KEY-----`

.....

(2024.06 und früher) Gruppenmitglieder wurden während der AD-Synchronisierung nicht mit RES synchronisiert

Beschreibung des Fehlers

Gruppenmitglieder werden nicht richtig mit RES synchronisiert, wenn sich die GroupOU von der UserOU unterscheidet.

RES erstellt einen Ldapsearch-Filter, wenn versucht wird, Benutzer aus einer AD-Gruppe zu synchronisieren. Der aktuelle Filter verwendet fälschlicherweise den UserOU-Parameter anstelle des GroupOU-Parameters. Das Ergebnis ist, dass die Suche keine Benutzer zurückgibt. Dieses Verhalten tritt nur in Fällen auf, in denen sich UserSOU und GroupOU unterscheiden.

Betroffene Versionen

Dieses Problem betrifft alle RES-Versionen 2024.06 oder früher

Schadensbegrenzung

Gehen Sie wie folgt vor, um das Problem zu lösen:

1. Um das Skript patch.py und die Datei group_member_sync_bug_fix.patch herunterzuladen, führen Sie die folgenden Befehle aus. `<output-directory>` Ersetzen Sie dabei das lokale Verzeichnis, in das Sie die Dateien herunterladen möchten, und `<res_version>` durch die RES-Version, die Sie patchen möchten:

> **Note**
>
> - Das Patch-Skript erfordert AWS CLI v2, Python 3.9.16 oder höher und Boto3.
> - Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben.
> - Der Patch unterstützt nur die RES-Versionen 2024.04.02 und 2024.06. Wenn Sie 2024.04 oder 2024.04.01 verwenden, können Sie die unter aufgeführten Schritte ausführen, um Ihre Umgebung zunächst auf 2024.04.02 Kleinere Versionsupdates zu aktualisieren, bevor Sie den Patch anwenden.
> - RES-Version: RES 2024.04.02
>
> Link zum Herunterladen des Patches: 2024.04.02_group_member_sync_bug_fix.patch
> - RES-Version: RES 2024.06
>
> Link zum Herunterladen des Patches: 2024.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. Navigieren Sie zu dem Verzeichnis, in das das Patch-Skript und die Patch-Datei heruntergeladen wurden. Führen Sie den folgenden Patch-Befehl aus und `<environment-name>` ersetzen Sie ihn durch den Namen Ihrer RES-Umgebung:

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. Führen Sie die folgenden Befehle aus, um die Cluster-Manager-Instanz für Ihre Umgebung neu zu starten:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 und früher) CVE-2024-6387, Regre, Sicherheitslücke in und Ubuntu SSHion RHEL9 VDIs

Beschreibung des Fehlers

CVE-2024-6387, genannt RegreSSHion, wurde im OpenSSH-Server identifiziert. Diese Sicherheitsanfälligkeit ermöglicht es nicht authentifizierten Angreifern, beliebigen Code auf dem Zielserver auszuführen, was ein ernstes Risiko für Systeme darstellt, die OpenSSH für sichere Kommunikation verwenden.

Für RES besteht die Standardkonfiguration darin, über den Bastion-Host SSH auf virtuelle Desktops zuzugreifen, und der Bastion-Host ist von dieser Sicherheitsanfälligkeit nicht betroffen. Das Standard-AMI (Amazon Machine Image), für das wir bereitstellen, RHEL9 und Ubuntu2024 VDIs (Virtual Desktop Infrastructure) in ALLEN RES-Versionen verwenden jedoch eine OpenSSH-Version, die anfällig für Sicherheitsbedrohungen ist.

Das bedeutet, dass Existing RHEL9 und Ubuntu2024 ausnutzbar sein VDIs könnten, der Angreifer jedoch Zugriff auf den Bastion-Host benötigen würde.

Weitere Informationen zu dem Problem finden Sie hier.

Betroffene Versionen

Dieses Problem betrifft alle RES-Versionen 2024.06 oder früher.

Schadensbegrenzung

RHEL9 Sowohl Ubuntu als auch Ubuntu haben Patches für OpenSSH veröffentlicht, die die Sicherheitslücke beheben. Diese können mit dem jeweiligen Paketmanager der Plattform abgerufen werden.

Wenn Sie bereits ein vorhandenes RHEL9 oder ein vorhandenes Ubuntu haben VDIs, empfehlen wir Ihnen, die nachfolgenden VDIs Anweisungen für PATCH EXISTING zu befolgen. Um Future zu patchen VDIs, empfehlen wir, die VDIs Anweisungen von PATCH FUTURE zu befolgen. Diese Anweisungen beschreiben, wie Sie ein Skript ausführen, um das Plattform-Update auf Ihrem Computer anzuwenden VDIs.

PATCH VORHANDEN VDIs

1. Führen Sie den folgenden Befehl aus, der alle vorhandenen Ubuntu-Dateien patcht und RHEL9 VDIs:

a. Das Patch-Skript benötigt AWS CLI v2.

b. Konfigurieren Sie die AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über AWS Systems Manager Manager-Berechtigungen zum Senden eines Systems Manager Manager-Ausführungsbefehls verfügen.

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. Sie können auf der Seite „Befehl ausführen“ überprüfen, ob das Skript erfolgreich ausgeführt wurde. Klicken Sie auf die Registerkarte Befehlsverlauf, wählen Sie die neueste Befehls-ID aus und überprüfen Sie, ob für alle Instanzen IDs eine SUCCESS-Meldung angezeigt wird.

PATCHEN SIE DIE ZUKUNFT VDIs

1. Um das Patch-Skript und die Patch-Datei (patch.py und update_openssh.patch) herunterzuladen, führen Sie die folgenden Befehle aus und `<output-directory>` ersetzen Sie sie durch das Verzeichnis, in das Sie die Dateien herunterladen möchten, und durch den Namen Ihrer `<environment-name>` RES-Umgebung:

> **Note**
>
> - Der Patch gilt nur für RES 2024.06.
> - Das Patch-Skript erfordert AWS CLI (v2), Python 3.9.16 oder höher und Boto3.
> - Konfigurieren Sie Ihre Kopie der AWS CLI für das Konto und die Region, in der RES bereitgestellt wird, und stellen Sie sicher, dass Sie über S3-Berechtigungen verfügen, um in den von RES erstellten Bucket zu schreiben.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Führen Sie den folgenden Patch-Befehl aus:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. Starten Sie die VDC Controller-Instanz für Ihre Umgebung mit den folgenden Befehlen neu:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Important**
>
> Das Patchen von Future VDIs wird nur in den RES-Versionen 2024.06 und höher unterstützt. Um future VDIs in RES-Umgebungen mit Versionen vor 2024.06 zu patchen, aktualisieren Sie zunächst die RES-Umgebung auf 2024.06, indem Sie die Anweisungen unter verwenden:. Aktualisierungen der Hauptversionen

.....

Hinweise

Jede EC2 Amazon-Instance wird mit zwei Remote Desktop Services (Terminal Services) -Lizenzen für Verwaltungszwecke geliefert. Diese Informationen stehen Ihnen zur Verfügung, um Ihnen bei der Bereitstellung dieser Lizenzen für Ihre Administratoren zu helfen. Sie können auch verwenden AWS Systems Manager Session Manager, was das Remoting in EC2 Amazon-Instances ohne RDP und ohne RDP-Lizenzen ermöglicht. Wenn zusätzliche Remote Desktop Services-Lizenzen benötigt werden, CALs sollten Remote Desktop-Benutzer bei Microsoft oder einem Microsoft-Lizenzhändler erworben werden. Remote Desktop-Benutzer CALs mit aktiver Software Assurance haben die Vorteile von License Mobility und können auf AWS standardmäßige (gemeinsam genutzte) Mandantenumgebungen umgestellt werden. Informationen zur Nutzung von Lizenzen ohne Software Assurance- oder License Mobility-Vorteile finden Sie in diesem Abschnitt der häufig gestellten Fragen.

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt AWS aktuelle Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. AWS Die Verantwortlichkeiten und Verbindlichkeiten gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

Research and Engineering Studio on AWS ist unter den Bedingungen der Apache License Version 2.0 lizenziert, die bei der Apache Software Foundation erhältlich ist.

Überarbeitungen

Weitere Informationen finden Sie in der Datei CHANGELOG.md im Repository. GitHub

Datum	Änderung

August 2024	• Version 2024.08 veröffentlichen —
	  • Unterstützung für das Mounten von Amazon S3 S3-Buckets auf Linux Virtual Desktop Infrastructure (VDI) -Instances hinzugefügt. Siehe Amazon-S3-Buckets.
	  • Unterstützung für benutzerdefinierte Projektberechtigungen hinzugefügt, ein erweitertes Berechtigungsmodell, das die Anpassung vorhandener Rollen und das Hinzufügen benutzerdefinierter Rollen ermöglicht. Siehe Berechtigungsprofile.
	• Benutzerhandbuch: Der Abschnitt wurde erweitert. Fehlerbehebung

Juni 2024	• Veröffentlichungsversion 2024.06 — Ubuntu-Unterstützung, Rechte des Projektinhabers. • Benutzerhandbuch: hinzugefügt Erstellen Sie eine Demo-Umgebung
April 2024	Release-Version 2024.04 — AMIs RES-fähige Vorlagen und Vorlagen für den Projektstart
März 2024	Weitere Themen zur Problembehandlung, Aufbewahrung von CloudWatch Protokollen, Deinstallation von Nebenversionen
Februar 2024	Veröffentlichungsversion 2024.01.01 — aktualisierte Bereitstellungsvorlage
Januar 2024	Version 2024.01 veröffentlichen

Datum	Änderung
Dezember 2023	GovCloud Wegbeschreibungen und Vorlagen hinzugefügt
November 2023	Erstversion

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.