aws

Benutzerhandbuch

Forschungs- und Ingenieurstudio

Forschungs- und Ingenieurstudio: Benutzerhandbuch

Table of Contents

Übersicht

Research and Engineering Studio (RES) ist ein AWS unterstütztes Open-Source-Produkt, mit dem IT-Administratoren ein Webportal bereitstellen können, auf dem Wissenschaftler und Ingenieure technische Rechenlasten ausführen können. AWS 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 und VDIs zugreifen, 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 bereitgestellt werden.

Architekturdiagramm

Wenn Sie dieses Produkt mit den Standardparametern bereitstellen, werden die folgenden Komponenten in Ihrem bereitgestelltAWS-Konto.

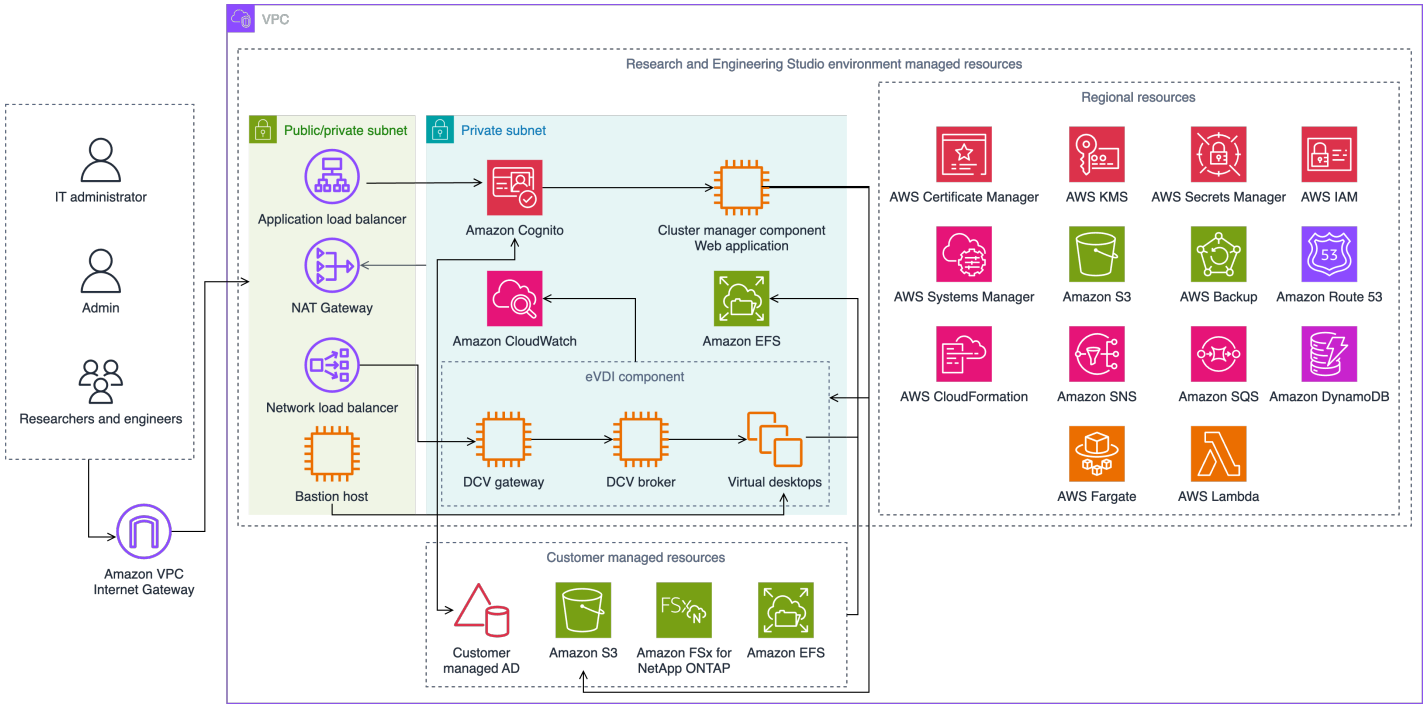


Abbildung 1: Research and Engineering Studio in AWS Architektur

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

Der allgemeine Prozessablauf für die mit der AWS CloudFormation Vorlage bereitgestellten Produktkomponenten lautet wie folgt:

1. RES installiert Komponenten für das Webportal sowie:

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

b. Metrikkomponente

   Amazon CloudWatch empfängt Metriken von den eVDI-Komponenten.

c. Bastion-Host-Komponente

   Administratoren können über SSH eine Verbindung zur Bastion-Hostkomponente 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, zu verwendenAWS Certificate Manager, 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 gemountet ist.
6. RES verwendet Amazon Cognito, um einen anfänglichen Bootstrap-Benutzer namens clusteradmin innerhalb von zu erstellen, und sendet temporäre Anmeldeinformationen an die E-Mail-Adresse, die bei der Installation angegeben wurde. Der Cluster-Administrator muss das Passwort bei der Erstanmeldung ändern.
7. Amazon Cognito lässt sich zur Berechtigungsverwaltung in das Active Directory und die Benutzeridentitäten Ihrer Organisation integrieren.
8. Sicherheitszonen ermöglichen es Administratoren, den Zugriff auf bestimmte Komponenten innerhalb des Produkts basierend auf Berechtigungen einzuschränken.

AWS -Services in diesem Produkt

AWS-Service	Beschreibung
Amazon Elastic Compute Cloud	Kern. Stellt die zugrunde liegenden Datenverarbeitungsservices 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-Gruppen hinter dem Load Balancer erstellt. ELB gleicht den Datenverkehr vom Webportal auf RES-Hosts aus.
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-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 zum Ausführen 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 Aktivitätsprotokolle für alle Amazon EC2-Hosts und Lambda-Funktionen bereit.
Amazon Simple Storage Service	Unterstützend. Speichert Anwendungs-Binärdateien für Host-Bootstrapping und -Konfiguration.
AWS Key Management Service	Unterstützend. Wird für die Verschlüsselung im Ruhezustand mit Amazon SQS-Warteschlangen, DynamoDB-Tabellen und Amazon SNSThemen verwendet.
AWS Secrets Manager	Unterstützend. Speichert Servicekonto-Anmeldeinformationen in Active Directory und selbstsignierte Zertifikate für VDIs.
AWS CloudFormation	Unterstützend. Stellt einen Bereitstellungsmechanismus für das Produkt bereit.
AWS Identity and Access Management	Unterstützend. Schränkt die Zugriffsebene für Hosts ein.
Amazon Route 53	Unterstützend. Erstellt eine privat gehostete Zone zum Auflösen des internen Load Balancers und des Bastion-Host-Domännamens.
Amazon Simple Queue Service	Unterstützend. Erstellt Aufgabenwarteschlangen zur Unterstützung asynchroner Ausführungen.

AWS-Service	Beschreibung
Amazon Simple Notification Service	Unterstützend. Unterstützt das Publication-Subscriber-Modell zwischen VDI-Komponenten wie Controller und 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 Amazon EC2-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/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für einen anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird ein erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

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 mit Amazon EC2 im Amazon EC2 EC2-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 die EC2-VPC Elastic IPs von fünf auf zehn

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden Service. AWS 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**
   >
   > Vergewissern Sie sich, 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 Installation des Produkts abschließt. Dieser Benutzer fungiert außerdem als Sicherheitsbenutzer, falls die Active Directory-Single-Sign-On-Integration fehlschlägt.
KeyPair		Das key pair, das für die Verbindung zu Infrastrukturhosts verwendet wird.
Client-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 bereit, die direkt auf die Weboberfläche und SSH auf den Bastion-Host zugreifen dürfen.

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.

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 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 -Services 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 Preisseite der einzelnen in diesem Produkt verwendeten AWS Dienste.

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 Amazon EC2 EC2-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-Instances, Dateisystem-CSR-Instances und Remote-VPN-Endpunkten zu kontrollieren und zu isolieren. Wir empfehlen Ihnen, die Sicherheitsgruppen zu überprüfen und den Zugriff bei 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.

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	
USA Ost (Ohio)	Canada (Central)

Name der Region	
USA Ost (Nord-Virginia)	Europe (Frankfurt)
USA West (Nordkalifornien)	Europa (Irland)
USA West (Oregon)	Europa (London)
Asien-Pazifik (Mumbai)	Europa (Milan)
Asien-Pazifik (Seoul)	Europa (Paris)
Asien-Pazifik (Singapur)	Israel (Tel Aviv)
Asien-Pazifik (Sydney)	AWS GovCloud (US-West)
Asien-Pazifik (Tokio)	

Kontingente

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

Kontingente für AWS Dienstleistungen 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 Amazon EC2 EC2-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.

ASG-Einstellungen können in der Amazon EC2 EC2-Konsole unter https://console.aws.amazon.com/ec2/ angepasst werden. Das Produkt erstellt standardmäßig vier ASGs, wobei jeder Name mit endet. `-asg` 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 zu ASGs finden Sie unter Skalieren der Größe Ihrer Auto Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

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

Themen

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/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für einen anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird ein erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

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 mit Amazon EC2 im Amazon EC2 EC2-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 die EC2-VPC Elastic IPs von fünf auf zehn

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden Service. AWS 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 für Ihren Domainnamen erstellte Hosting-Zone 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 sich 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

Wenn Sie Research and Engineering Studio auf bereitstellen AWS, werden von dem Produkt, das Sie benötigen, externe Ressourcen verwendet. RES geht davon aus, dass diese Ressourcen bei der Bereitstellung vorhanden sind.

- Netzwerke (VPC, öffentliche und private Subnetze)

  Hier werden Sie die EC2-Instances ausführen, die zum Hosten der 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 den Umgebungsseiten.

- 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

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

Amazon Machine Images (AMIs) vorbereiten

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 Amazon S3 S3-Lesezugriff und vertrauenswürdiger Identität als Amazon EC2.

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

    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 unter Service oder Anwendungsfall für Anwendungsfall die Option EC2 und dann Weiter aus.

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

    - Amazon S3 ReadOnlyAccess

- Amazon SSM ManagedInstanceCore
- EC 2 InstanceProfileForImageBuilder

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_dependencies
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: Amazon EC2 EC2-Komponente, die zuvor erstellt wurde. Geben Sie Ihre AWS-Konto ID und Ihren aktuellen Status AWS-Region 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 Amazon EC2 EC2-Konsole mit

Abschnitt	Parameter	Benutzereintrag

		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 Ausgabe-Image in der Region erstellt, in der der EC2 Image Builder Builder-Service verwendet wird.
   - Wenn Sie RES in mehreren Regionen bereitstellen möchten, können Sie Neue Distributionseinstellungen erstellen wählen 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*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*.cloudformation

AWS-Service	Service-Name
Amazon CloudWatch	com.amazonaws.*region*.monitoring
CloudWatch Amazon-Protokolle	com.amazonaws.*region*.logs
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*.elasticfilesystem
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon EventBridge	com.amazonaws.*region*.events
Amazon FSx	com.amazonaws.*region*.fsx
AWS Key Management Service	com.amazonaws.*region*.kms
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*.secretsmanager
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
Amazon SNS	com.amazonaws.*region*.sns

AWS-Service	Service-Name
Amazon SQS	com.amazonaws.*region*.sqs
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssmmessages

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. Gehen Sie zu Ihrer VPC-Konsole und identifizieren Sie die Routentabellen für die Subnetze, die Sie für Infrastrukturhosts 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 Infrastruktur/VDIS verwenden werden.

4. Ändern Sie die Sicherheitsgruppe der Proxyserver-EC2-Instance 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 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 “Amazon Machine Images (AMIs) vorbereiten”.
IsLoadBalancerInternetFacing	Auf „Falsch“ gesetzt.
LoadBalancerSubnets	Wählen Sie private Subnetze ohne Internetzugang.
InfrastructureHostSubnets	Wählen Sie private Subnetze ohne Internetzugang.
VdiSubnets	Wählen Sie private Subnetze ohne Internetzugang.

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 unter https://console.aws.amazon.com/cloudformation bei der 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`	Für das Active Directory verwendete Domäne. 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 Standardwert. 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 erforderlich. Wenn Sie einen angeben SubDomain, wird der Parameter dem DomainName angegebenen vorangestellt. 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. Hinweis: Das Passwort für diesen Benutzer muss die Anforderungen an die Passwortkomplexität für Active Directory erfüllen.
ServiceAccountPassword		Passwort, das zum Erstellen eines Dienstkontos verwendet wurde (`ReadOnlyUser`). Dieses Konto wird für die Synchronisation verwendet. Wichtig: Ab der Version 2024.06 von Research and Engineering Studio müssen Sie einen geheimen ARN angeben, der das Klartext-Passwort für die enthält. ServiceAccount Hinweis: Das Passwort für diesen Benutzer muss die Anforderungen an die Passwortkomplexität für Active Directory erfüllen.

Parameter	Standard	Beschreibung
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.
LDIFS3Path	`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 aufgefüllt, die eine Reihe von Benutzern im Active Directory erstellt. Die Datei finden Sie in der Datei res.ldif unter. 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.

Parameter	Standard	Beschreibung
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.
EnvironmentName	`res-[environment name]`	Wenn der angegeben `PortalDomainName` ist, wird dieser Parameter verwendet, um den generiert en Geheimnissen Tags hinzuzufügen, sodass sie in der Umgebung verwendet werden können. Dies muss mit dem `Environme ntName` Parameter übereinstimmen, der bei der Erstellung des RES-Stack s 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 Kontrollkästchen 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 der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
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- *[Nur Zahlen oder Buchstaben]*	(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-fähige AMIs konfigurieren.
SSH KeyPair		Das key pair, das für die Verbindung zu Infrastrukturhosts verwendet wird.
ClientIP	*x.x.x .0/24 oder x.x.x .0/32*	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 bereit, die direkt auf die Weboberfläche und SSH auf den Bastion-Host zugreifen dürfen.
ICH BIN PermissionBoundary		(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 verschied enen 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 Infrastru ktur-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.
ANZEIGE ShortName	*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.
LDAP-Verbindungs-URI		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	Res-Administratoren	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
Domain-TLS-ARN CertificateSecret		(Optional) Stellen Sie einen geheimen ARN für ein Domain-TLS-Zertifikat bereit, um die TLS-Kommunikation mit AD zu ermöglichen.
EnableLdapID-Mapping		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.
DisableAdJoin	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
CertificateSecretARN für VDI		(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.

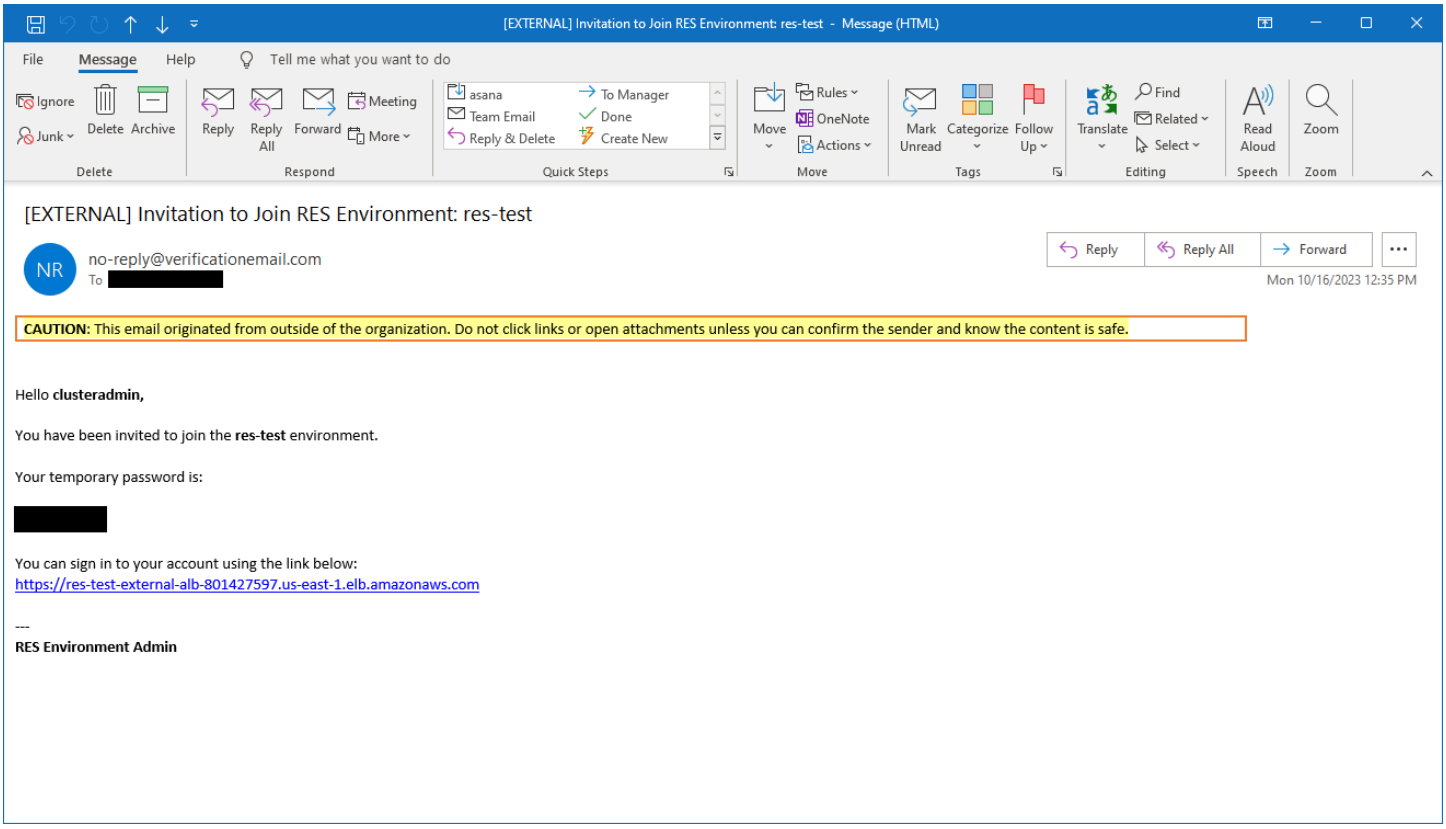
Parameter	Standard	Beschreibung
PrivateKeySecretARN für VDI		(Optional) Dieses ARN-Geheimnis speichert den privaten Schlüssel für das Zertifikat Ihres Webportals. Wenn Sie einen Portaldomänennamen für Ihre automatisierten externen Ressourcen festlegen, finden Sie diesen Wert auf der Registerkarte Ausgaben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

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

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 Amazon EFS-Konsole an AWS Management Console und öffnen Sie sie 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 Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie 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 Amazon S3 S3-Konsole an AWS Management Console und öffnen Sie sie 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

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. the section called “SSO mit IAM Identity Center einrichten” Wenn Sie über einen eigenen SAML 2.0-kompatiblen Identitätsanbieter verfügen, finden Sie weitere Informationen unter. the section called “Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)”

Themen

SSO mit IAM Identity Center einrichten

Wenn Sie noch kein Identity Center haben, das mit dem verwalteten Active Directory verbunden ist, beginnen Sie mitthe section called “Richten Sie ein Identitätszentrum ein”. Wenn Sie bereits ein Identity Center haben, das mit dem verwalteten Active Directory verbunden ist, beginnen Sie mitthe section called “Stellen Sie eine 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

Identity Center aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Öffnen Sie das Identity Center.
3. Wählen Sie Enable (Aktivieren) aus.
4. Wählen Sie Aktivieren mit AWS Organizations.
5. Klicken Sie auf Weiter.

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

Identity Center mit verwaltetem Active Directory verbinden

Führen Sie nach der Aktivierung von Identity Center die folgenden empfohlenen Einrichtungsschritte aus:

1. Wählen Sie in der Navigation 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. Wählen Sie Weiter aus.
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 Änderungen nicht mehr the section called “Identity Center mit verwaltetem Active Directory verbinden” abgeschlossen sind, sollte ein grünes Banner erscheinen.

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. Wählen Sie Weiter aus.
6. Überprüfen Sie Ihre Änderungen und wählen Sie Konfiguration speichern.
7. Der Synchronisierungsvorgang kann einige Minuten dauern. Wenn Sie eine Warnmeldung darüber erhalten, dass Benutzer nicht synchronisieren, wählen Sie Synchronisierung fortsetzen.

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.

Schritt 2: Connect zu einem Identitätscenter her

Einrichtung der Anwendung im Identity Center

1. Melden Sie sich unter https://console.aws.amazon.com/singlesignon/ beim IAM Identity Center an AWS Management Console und öffnen Sie es.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie Anwendung hinzufügen.
4. Wählen Sie unter Setup-Präferenzen die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
5. Wählen Sie unter Anwendungstyp die Option SAML 2.0 aus.
6. Wählen Sie Weiter aus.
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 das SSO mit dem RES-Portal konfigurieren.
9. Geben Sie unter Anwendungseigenschaften die Start-URL Ihrer Anwendung ein. Zum 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. Wählen Sie Absenden 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 $ {user:email} ein.
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 die E-Mail-Adresse ein.
7. Geben Sie unter Zuordnungen zu diesem Zeichenkettenwert oder Benutzerattribut in IAM Identity Center $ {user:email} ein.
8. Geben Sie unter Format den Wert unspecified ein.
9. Wählen Sie Änderungen speichern aus.

Benutzer zur Anwendung in 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 Assign users (Benutzer zuweisen) aus.

SSO in der RES-Umgebung einrichten

1. Öffnen Sie in der Research and Engineering Studio-Umgebung die Option Allgemeine Einstellungen unter Umgebungsmanagement.
2. Öffnen Sie die Registerkarte Identitätsanbieter.
3. Wählen Sie unter Single Sign-On die Schaltfläche 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 während kopiert haben the section called “Einrichtung der Anwendung im Identity Center”
    e. Geben Sie unter E-Mail-Attribut des Anbieters die E-Mail-Adresse 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

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). Diese Konfiguration erfordert die folgenden Parameter:
   - 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, müssen die folgenden Felder/Ansprüche auf die E-Mail-Adresse des Benutzers gesetzt sein:

- SAML-Betreff oder NameID

- SAML-E-Mail

4. Ihr IdP fügt der SAML-Assertion basierend auf der Konfiguration Felder/Ansprüche hinzu. 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`

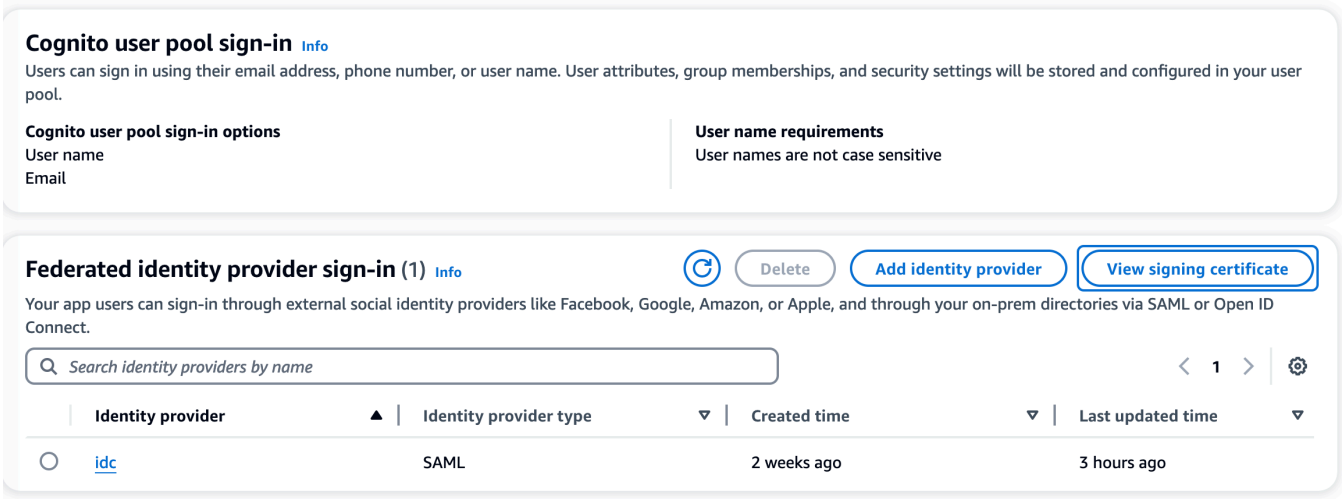
   Um die Domain-URL zu erhalten

   1. Melden Sie sich bei RES als Administrator 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.

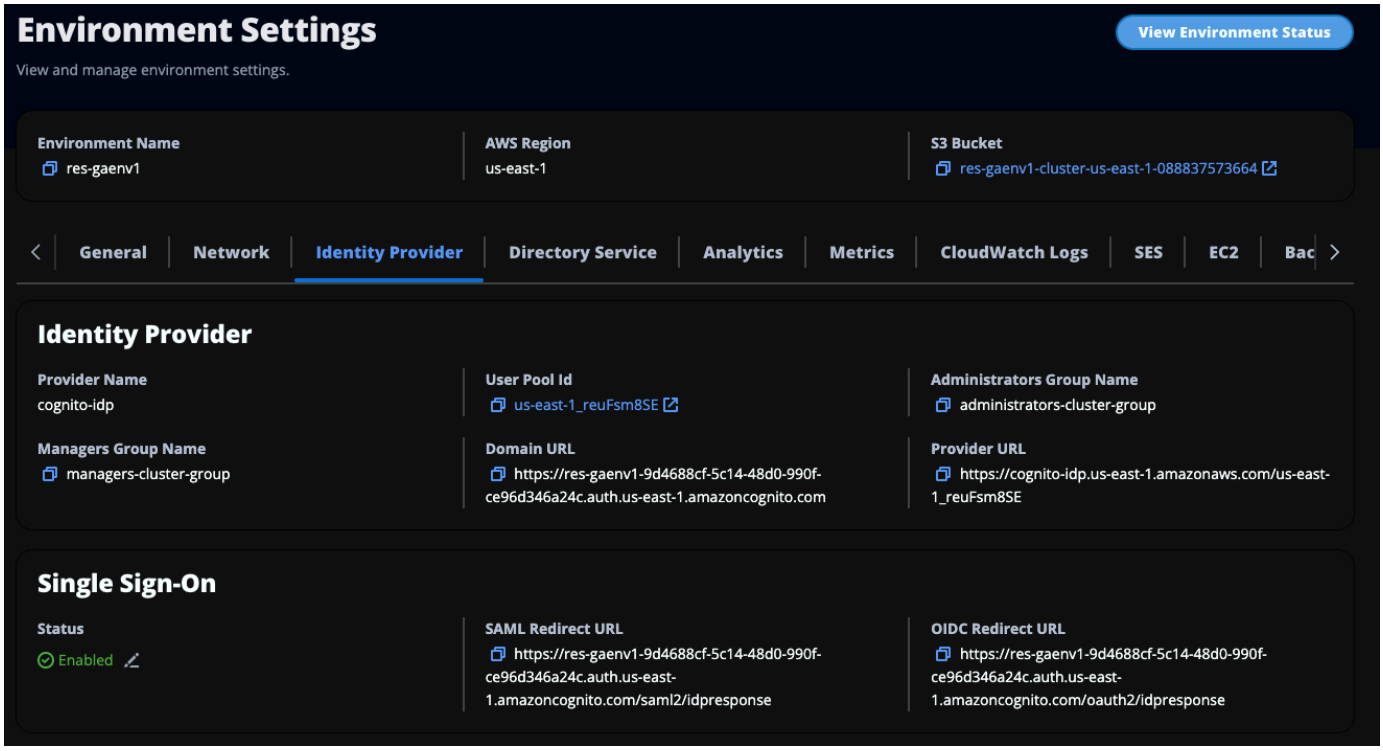
> **Note**
>
> Dies gilt nicht für Keycloak und IDC.

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.

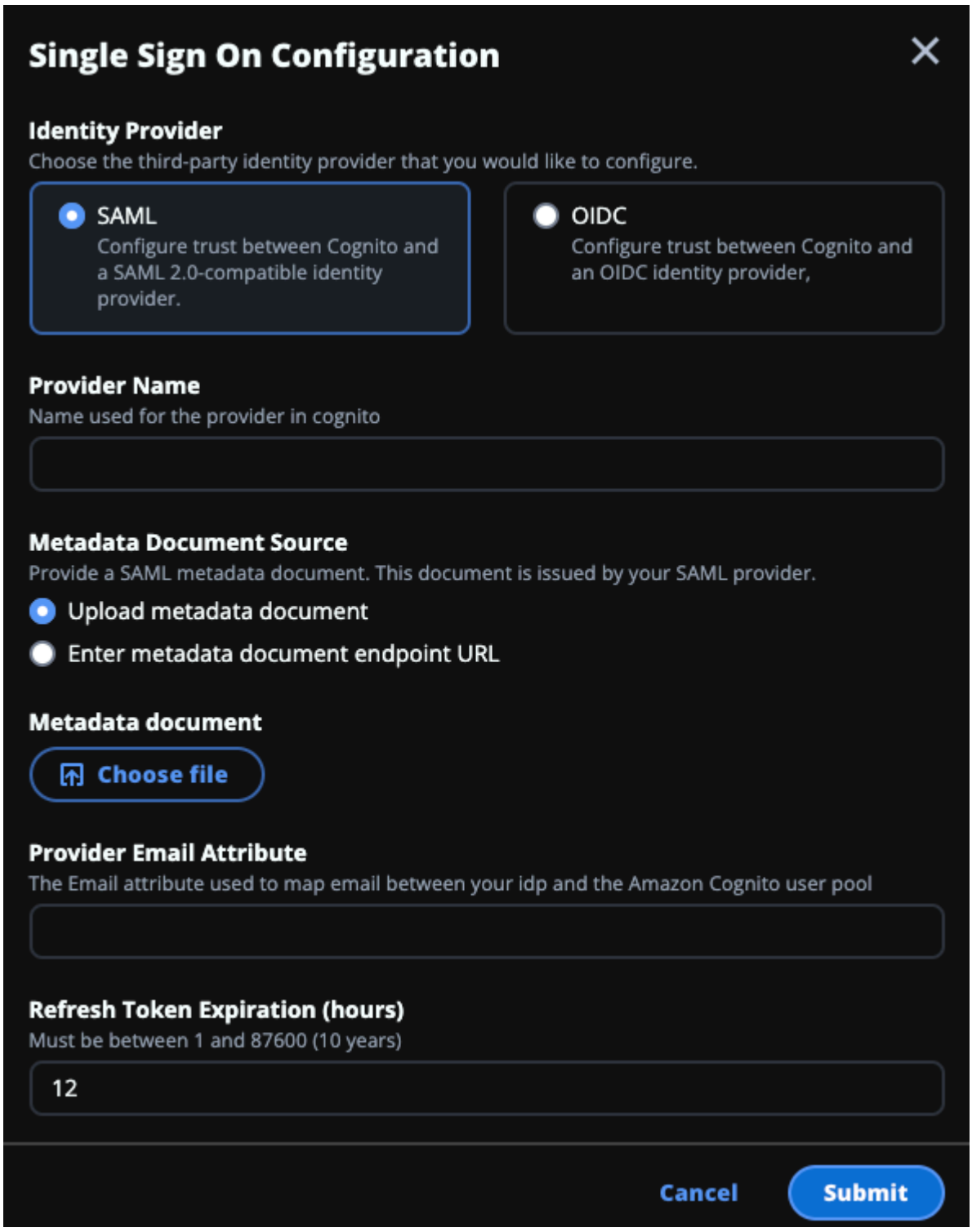
Konfigurieren Sie RES für die Verwendung Ihres Identitätsanbieters

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 als Identity Provider 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 das Anbieter-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

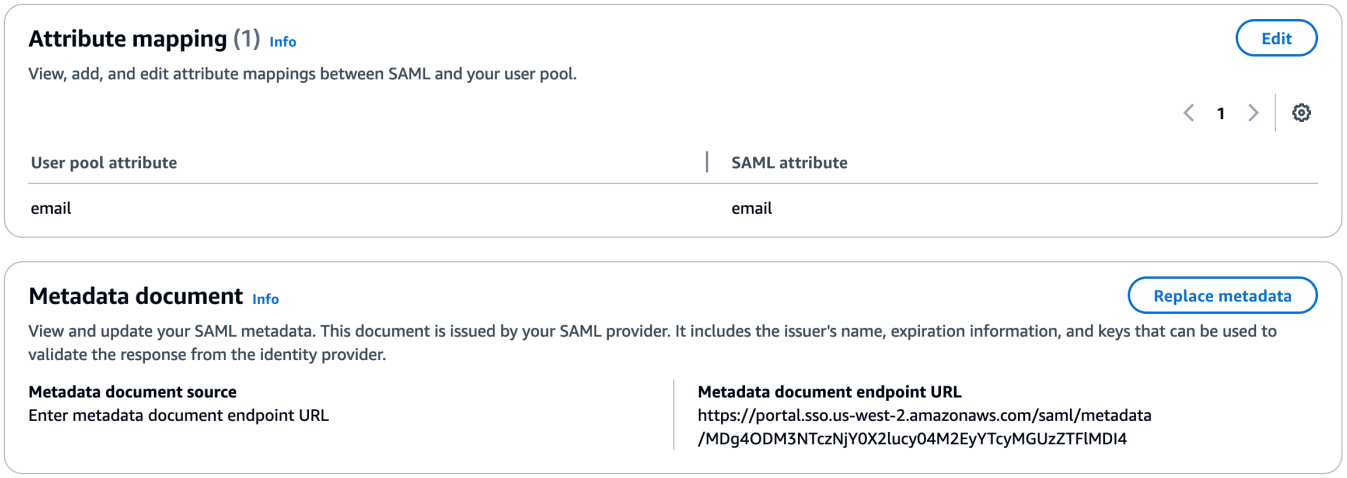
Wenn Sie die bereitgestellten externen Ressourcen verwendet haben, um eine RES-Umgebung außerhalb der Produktion zu erstellen, und IAM Identity Center als Ihren Identitätsanbieter konfiguriert haben, möchten Sie möglicherweise einen anderen Identitätsanbieter wie Okta konfigurieren. Das Formular zur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

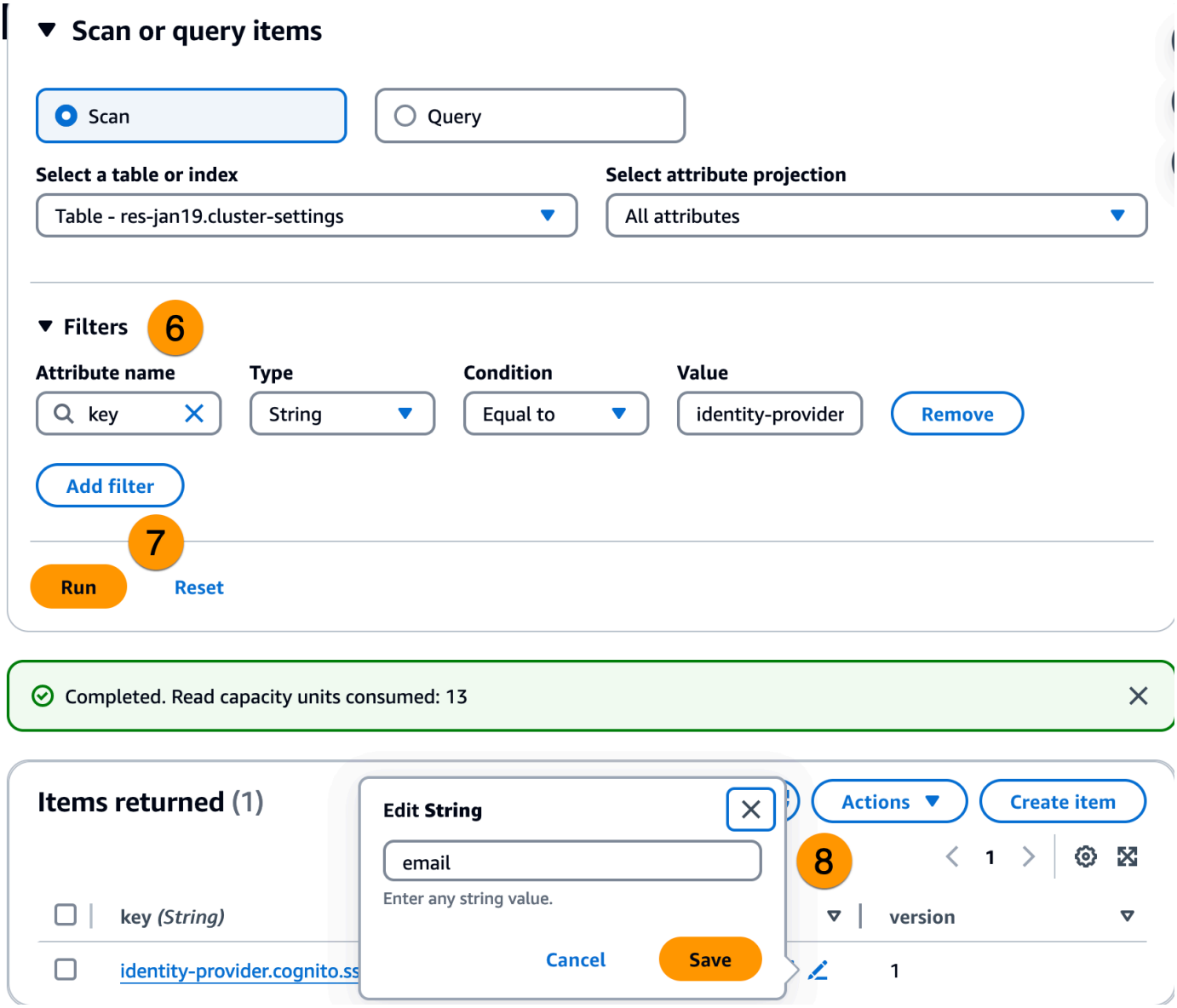
   b. Suchen Sie die **`<environment name>.cluster-settings`** Tabelle, wählen Sie sie aus und wählen Sie im Menü Aktionen die Option Elemente durchsuchen aus.

   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 an Ihre Änderungen in Amazon Cognito anzupassen.



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. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
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. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
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. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
9. Suchen Sie nach Ihrer 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 (ACM) angefordert wurde. AWS Certificate Manager 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. the section called “Erstellen Sie externe Ressourcen”

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:
   - Kommerzielle Bereitstellung: 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 installat ion-stack-name	Läuft niemals ab
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	Läuft niemals ab

CloudWatch Gruppen protokollieren	Aufbewahrung
/aws/lambda/ < >-cluster-einstellungen installation-stack-name	Läuft niemals ab
/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, können Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/ aufrufen und den Anweisungen zum Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs folgen.

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 PermissionBoundary IAM-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-fähige AMIs konfigurieren

Mit RES-fähigen AMIs können Sie RES-Abhängigkeiten für virtuelle Desktop-Instances (VDIs) auf Ihren benutzerdefinierten AMIs vorinstallieren. Die Verwendung von RES-fähigen AMIs verbessert die Startzeiten für VDI-Instanzen, die die vorgefertigten Images verwenden. Mit EC2 Image Builder können Sie Ihre AMIs als neue 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

Um von EC2 Image Builder aus auf den RES-Umgebungsdienst zuzugreifen, müssen Sie eine IAM-Rolle namens RES-EC2 erstellen oder ändern. InstanceProfileForImageBuilder 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 Amazon EC2-Service
- AmazonSSM ManagedInstanceCore - und EC2-Richtlinien InstanceProfileForImageBuilder
- 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-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

> **Note**
>
> CentOS 7 soll derzeit end-of-life am 30.06.2024 erscheinen. Research and Engineering Studio Version 2024.06 wird die letzte Version sein, die CentOS 7 unterstützt.

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)
- CentOS 7 (x86 und ARM64)
- RHEL 7 (x86), 8 (x86) und 9 (x86)
- 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 Image-Rezepte 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-Instances für Linux
> - Manuelles Installieren und Deinstallieren des SSM-Agenten auf EC2-Instances 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: AWSAccountID, RES EnvNameEnvRegion, RES 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: AWSAccountID, RES EnvNameEnvRegion, RES 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).

Konfiguration der EC2 Image Builder Builder-Infrastruktur

Sie können Infrastrukturkonfigurationen verwenden, um die Amazon EC2 EC2-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, der die von Ihnen gewählte AMI-Basisarchitektur unterstützt. Siehe Amazon EC2 EC2-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-fähige AMIs zu konfigurieren, 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 the section called “Konfiguration

der EC2 Image Builder Builder-Infrastruktur" erstellte Infrastrukturkonfiguration aus. 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.

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.

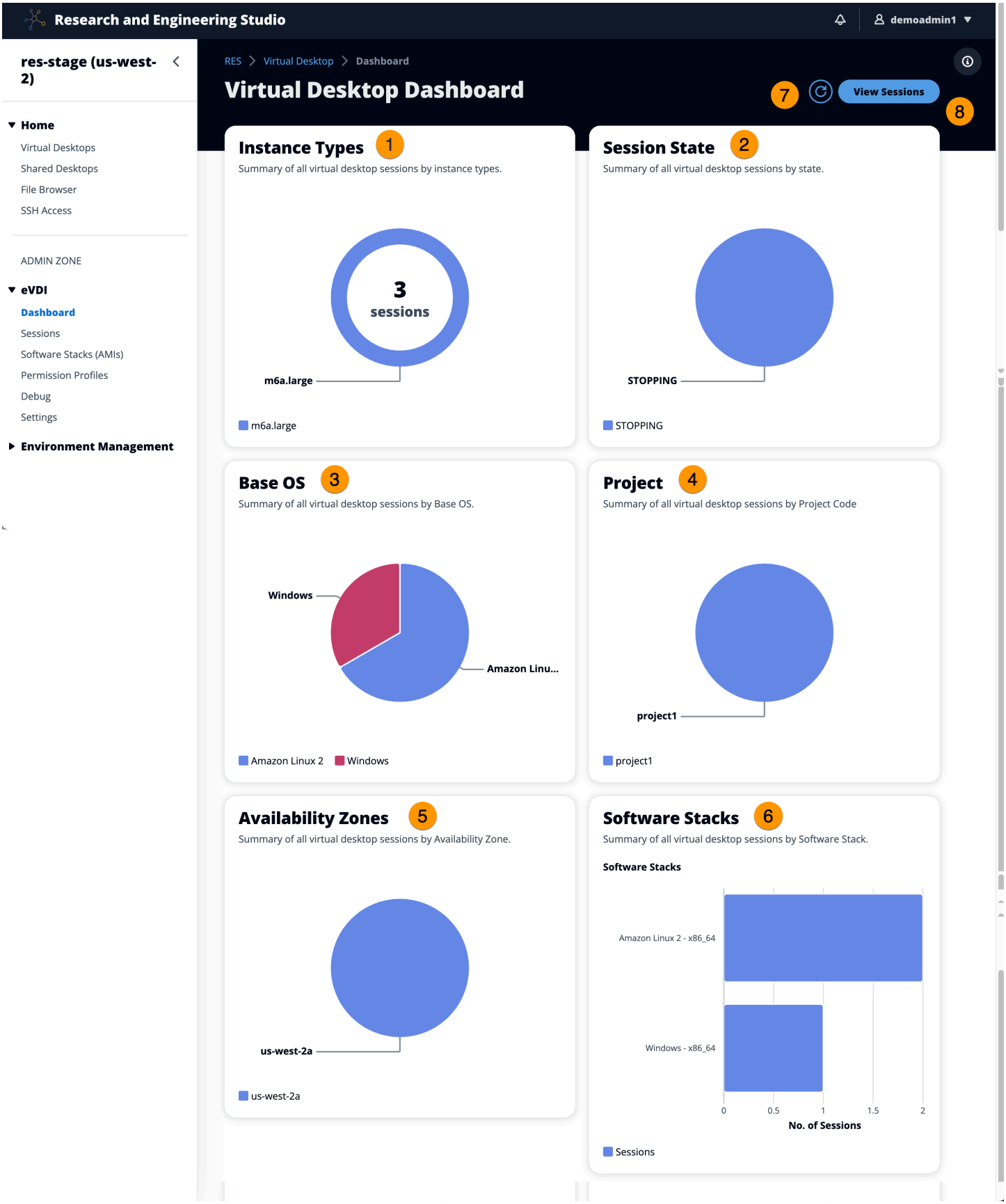
Themen

Sitzungsverwaltung

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


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:

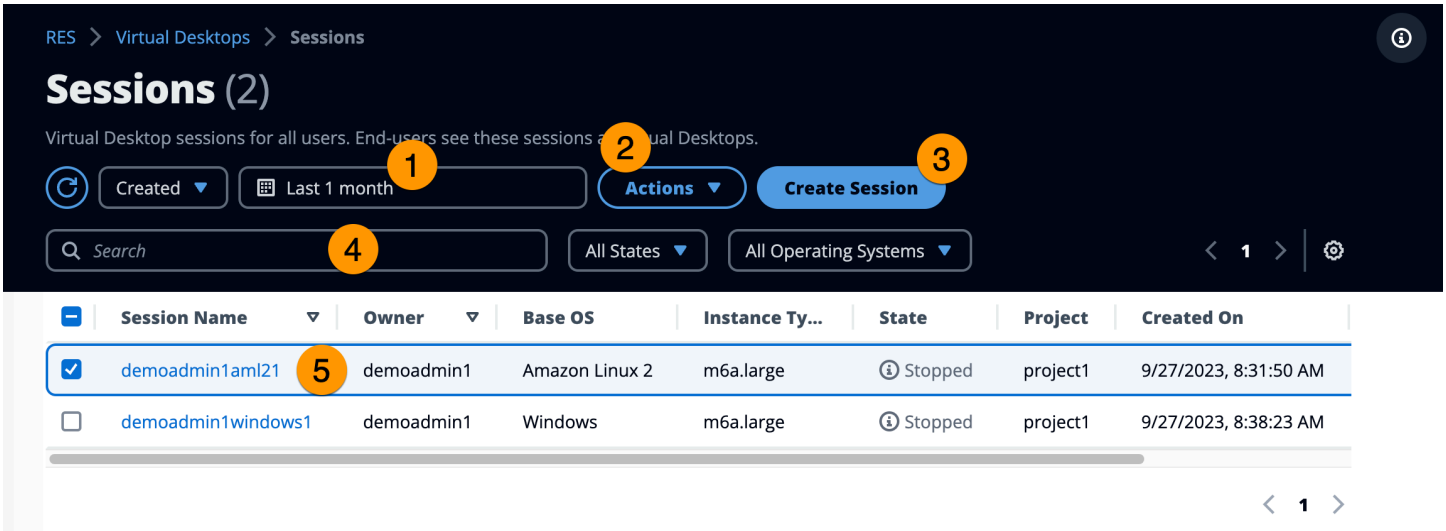
1. Instance-Typen
2. Sitzungsstatus
3. Basis-Betriebssystem
4. Projekte
5. Verfügbarkeitszonen
6. Software-Stapel

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. Sitzung (en) stoppen/in den Ruhezustand versetzen
c. Sitzung (en) beenden oder in den Ruhezustand versetzen
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.

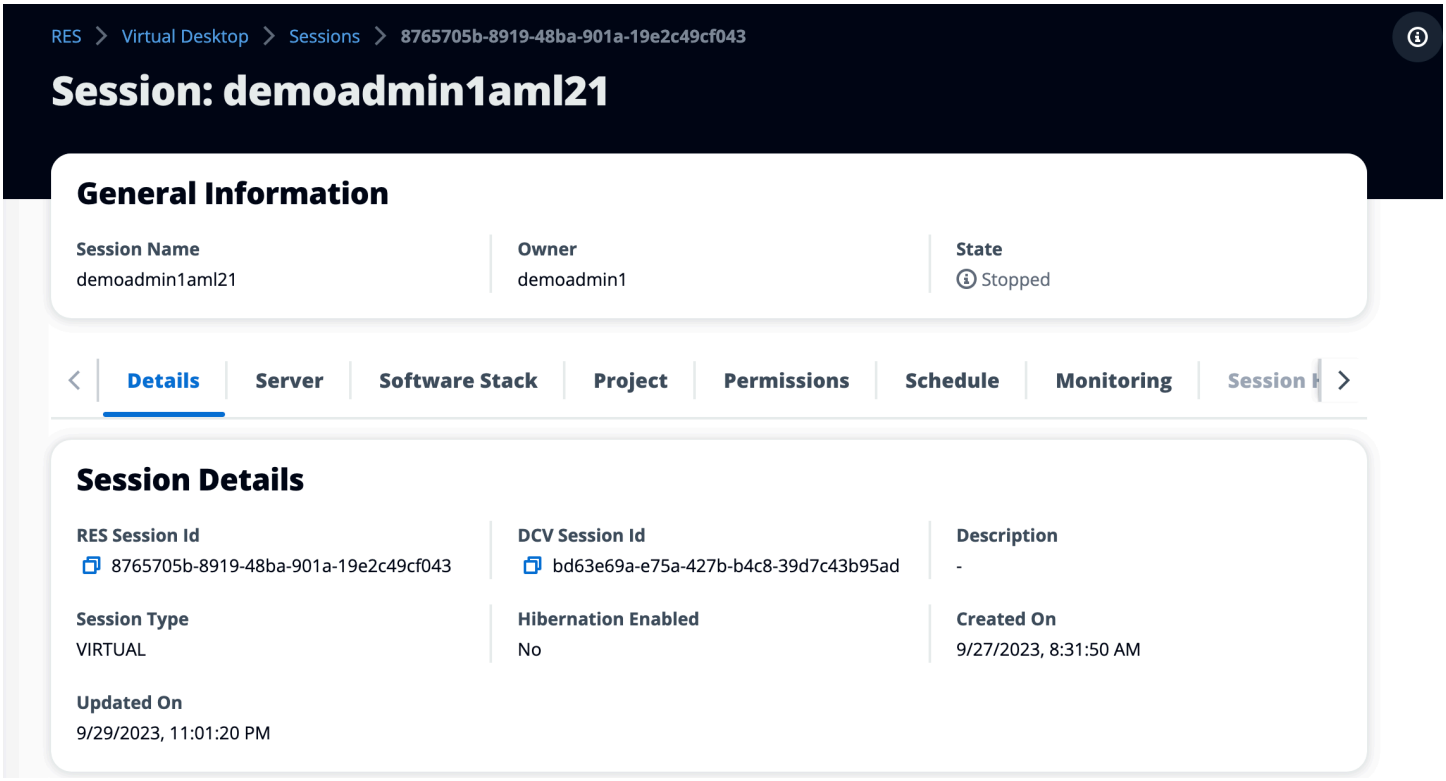
Virtual Desktop Size
Select a virtual desktop instance type

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

10

Einzelheiten der Sitzung

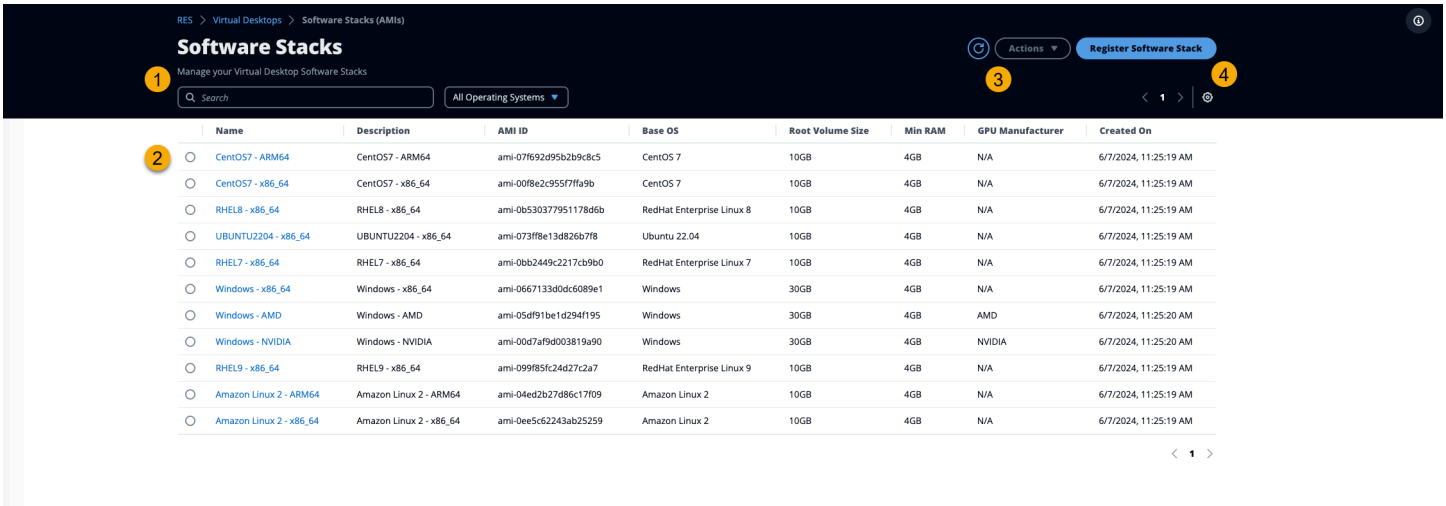
Wählen Sie in der Sitzungsliste den Sitzungsnamen aus, um die Sitzungsdetails anzuzeigen.



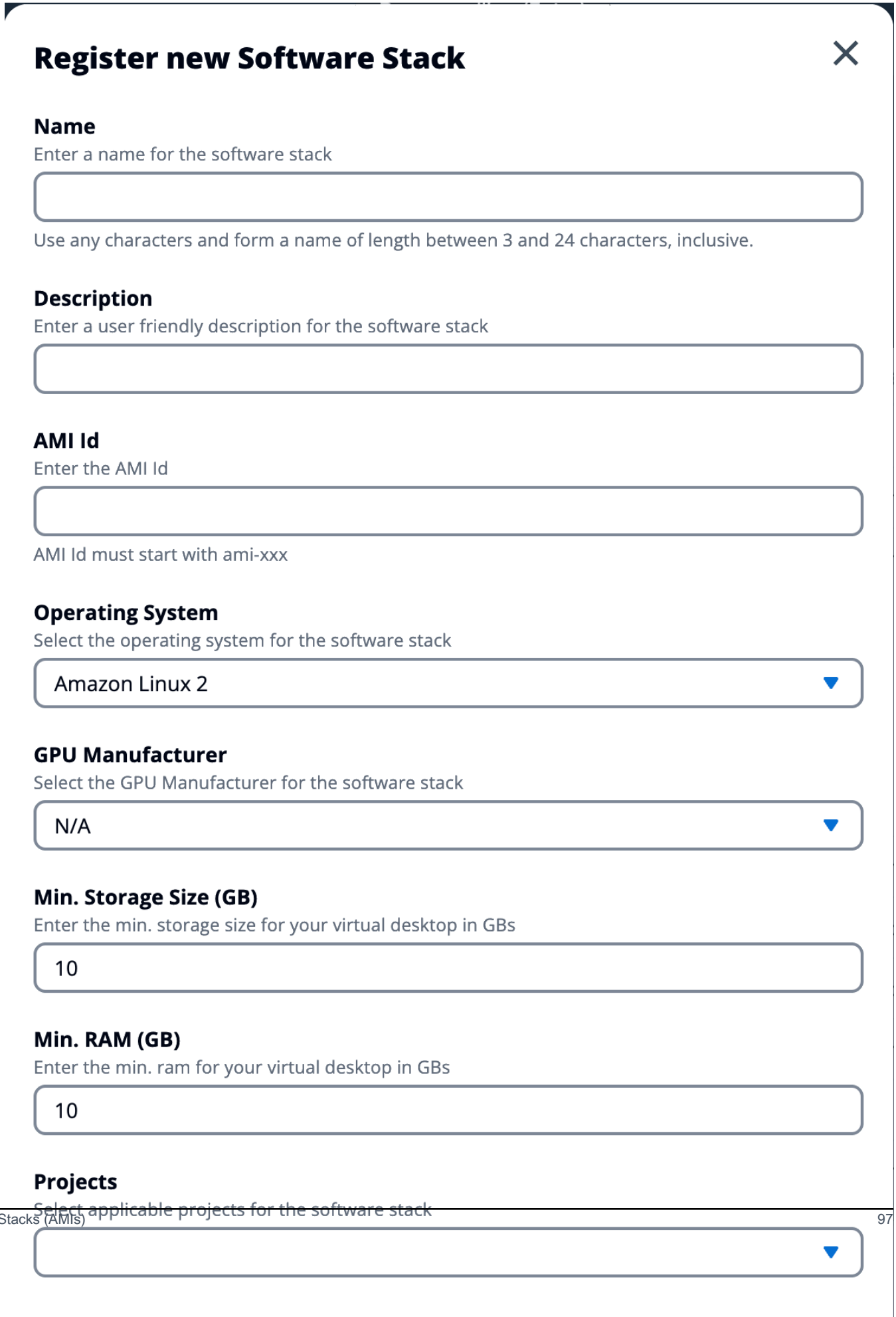
Software-Stacks (AMIs)

> **Note**
>
> Um den bereitgestellten CentSO7-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

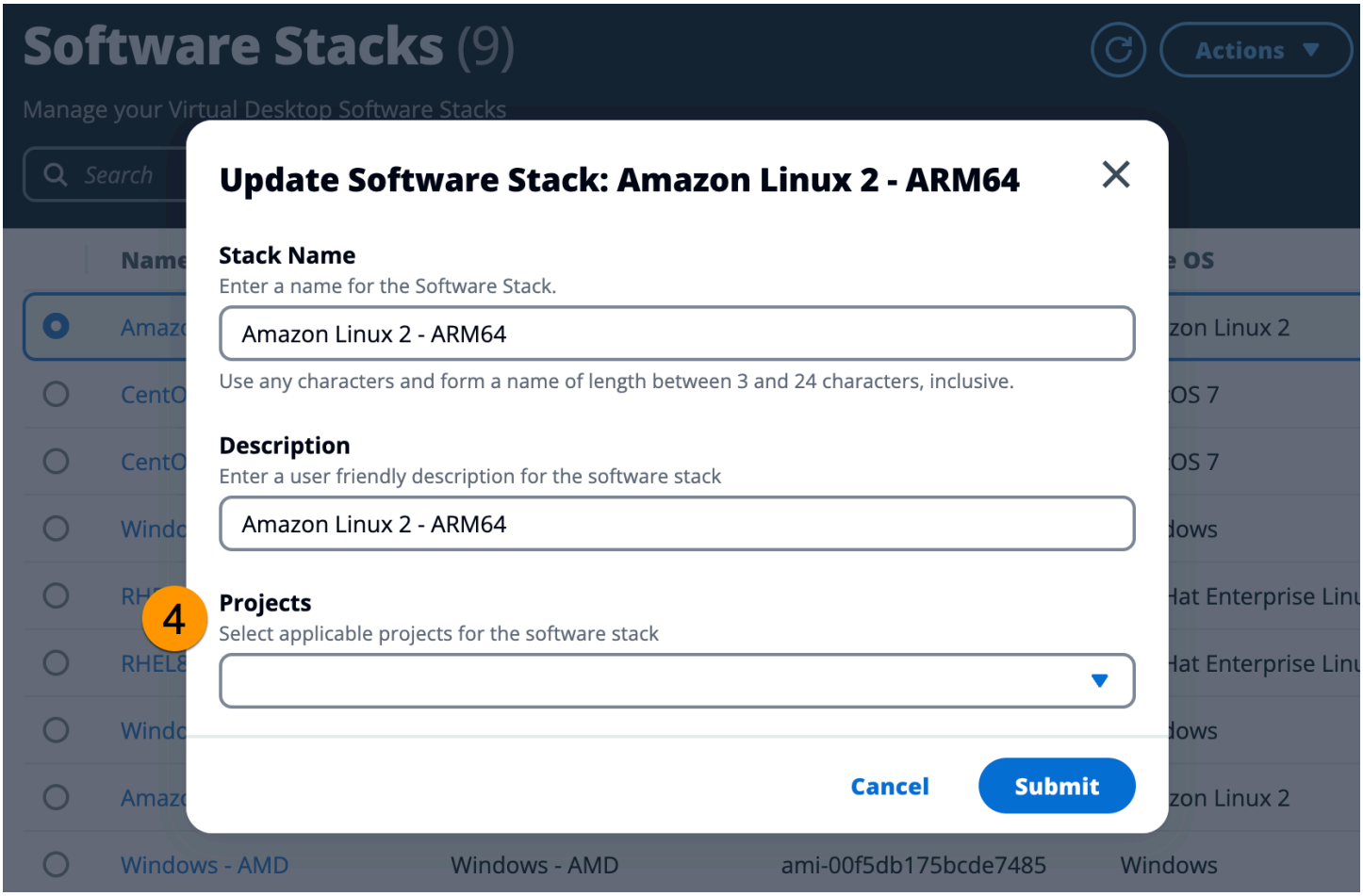
Weisen Sie einem Projekt einen Software-Stack zu

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.

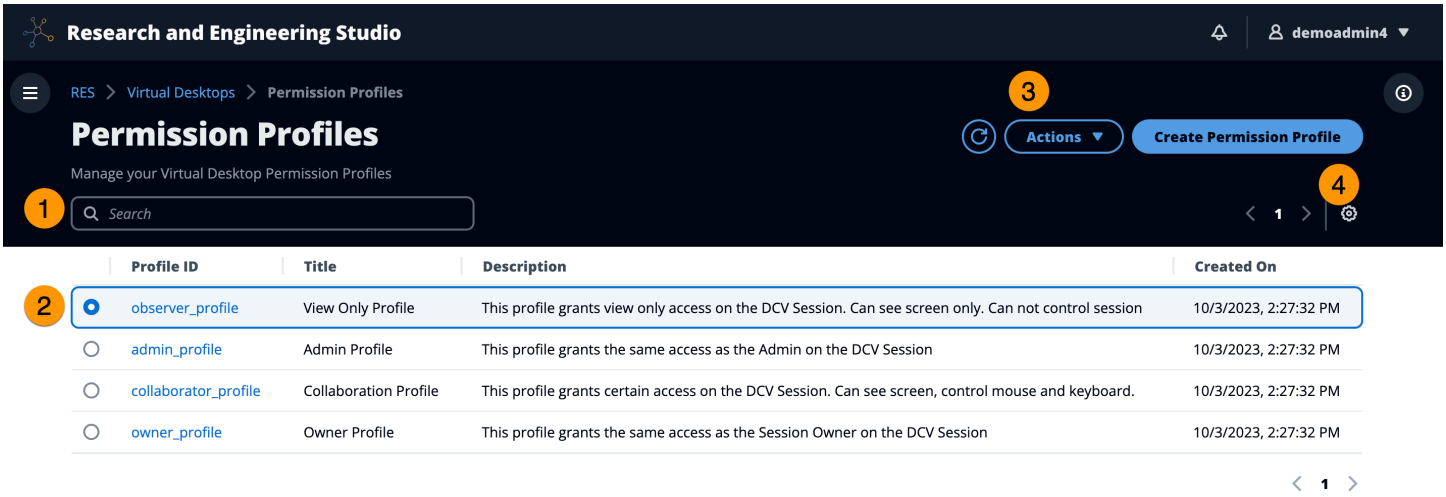


Details zum Software-Stack anzeigen

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.

Berechtigungsprofile

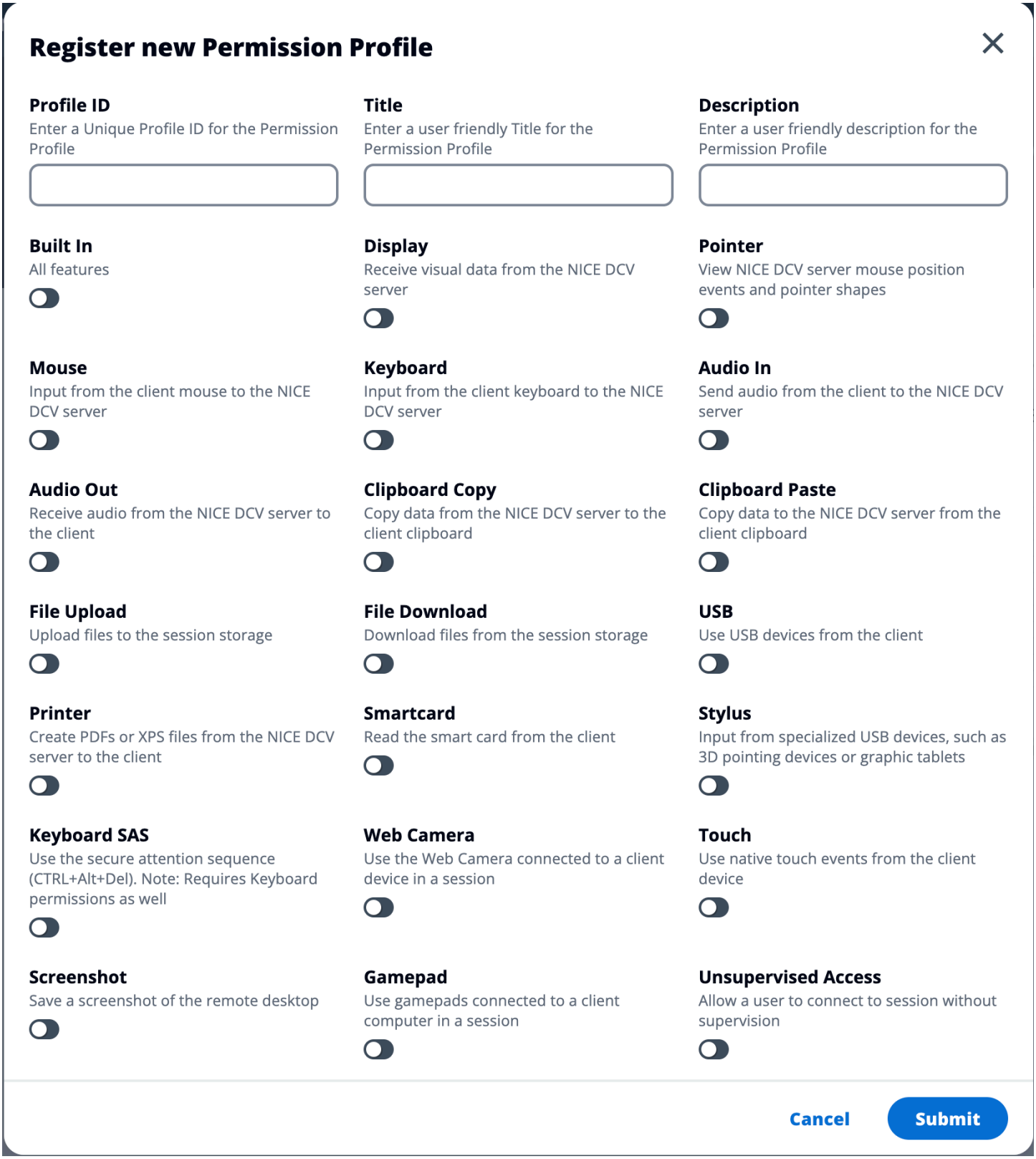
Verwenden Sie Berechtigungsprofile, um wiederverwendbare Profile für Berechtigungen zu erstellen und zu verwalten.



1. Suchen Sie nach einem Berechtigungsprofil.
2. Wählen Sie die Profil-ID, um Details anzuzeigen.
3. Wenn ein Profil ausgewählt ist, verwenden Sie das Aktionsmenü, um das Profil zu bearbeiten.
4. Wählen Sie „Berechtigungsprofil erstellen“, um ein neues Profil zu erstellen.

Erstellen Sie ein Berechtigungsprofil

1. Wählen Sie „Berechtigungsprofil erstellen“.
2. Geben Sie Details für das neue Profil ein und verwenden Sie die Berechtigungsschalter, um Berechtigungen für das Profil auszuwählen.
3. Wählen Sie Absenden aus.


Register new Permission Profile
Profile ID
Enter a Unique Profile ID for the Permission Profile
Title
Enter a user friendly Title for the Permission Profile
Description
Enter a user friendly description for the Permission Profile
Built In
All features
Display
Receive visual data from the NICE DCV server
Pointer
View NICE DCV server mouse position events and pointer shapes
Mouse
Input from the client mouse to the NICE DCV server
Keyboard
Input from the client keyboard to the NICE DCV server
Audio In
Send audio from the client to the NICE DCV server
Audio Out
Receive audio from the NICE DCV server to the client
Clipboard Copy
Copy data from the NICE DCV server to the client clipboard
Clipboard Paste
Copy data to the NICE DCV server from the client clipboard
File Upload
Upload files to the session storage
File Download
Download files from the session storage
USB
Use USB devices from the client
Printer
Create PDFs or XPS files from the NICE DCV server to the client
Smartcard
Read the smart card from the client
Stylus
Input from specialized USB devices, such as 3D pointing devices or graphic tablets
Keyboard SAS
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
Web Camera
Use the Web Camera connected to a client device in a session
Touch
Use native touch events from the client device
Screenshot
Save a screenshot of the remote desktop
Gamepad
Use gamepads connected to a client computer in a session
Unsupervised Access
Allow a user to connect to session without supervision
Cancel
Submit

Bearbeiten Sie ein Berechtigungsprofil

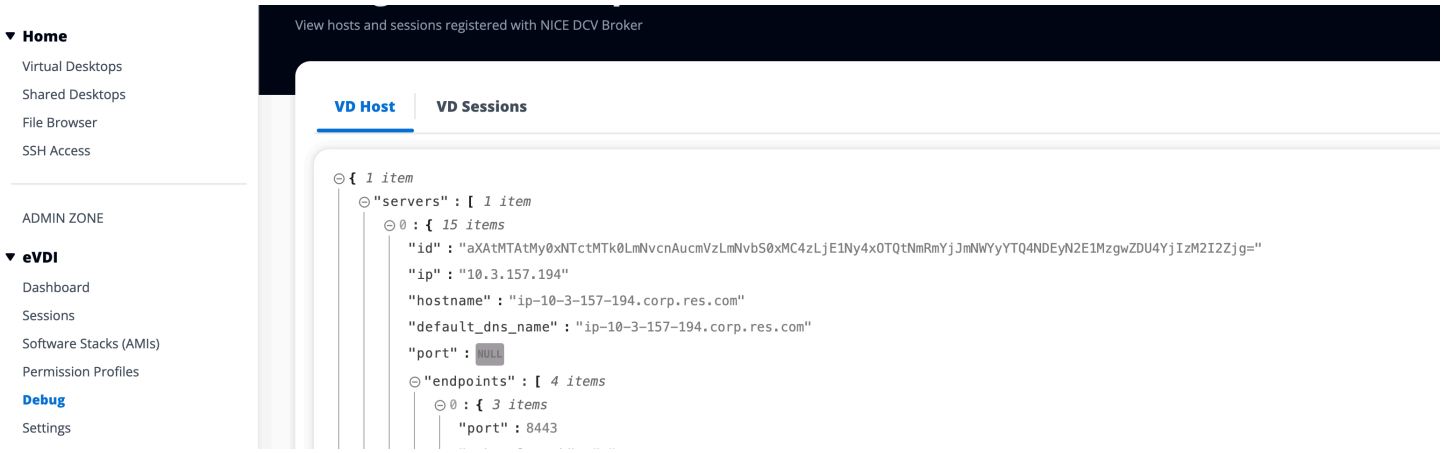
1. Wählen Sie auf der Seite „Berechtigungsprofile“ das Berechtigungsprofil aus, das Sie bearbeiten möchten.
2. Wählen Sie Aktionen.
3. Wählen Sie „Berechtigungsprofil bearbeiten“.
4. Bearbeiten Sie das Profil.
5. Wählen Sie Absenden aus.

Details zum Berechtigungsprofil anzeigen

Wählen Sie aus der Liste der Berechtigungsprofile die Profil-ID aus, um Details anzuzeigen. Auf der Detailseite können Sie auch Bearbeiten auswählen, um das Berechtigungsprofil 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.

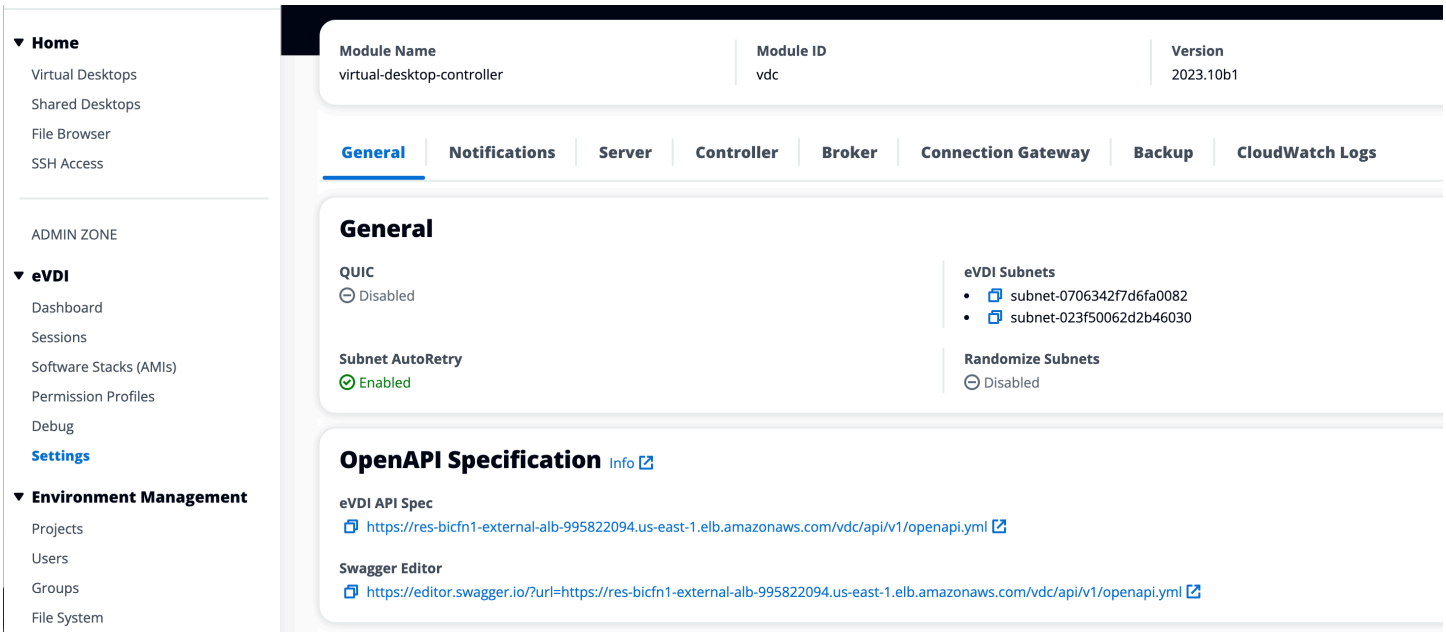


Desktop-Einstellungen

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

- Warnung vor Timeout bei Leerlauf
- Schwellenwert für die CPU-Auslastung
- Zulässige Sitzungen pro Benutzer



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
- Dateisysteme
- Umgebungsstatus

- Snapshot-Verwaltung
- Umgebungseinstellungen

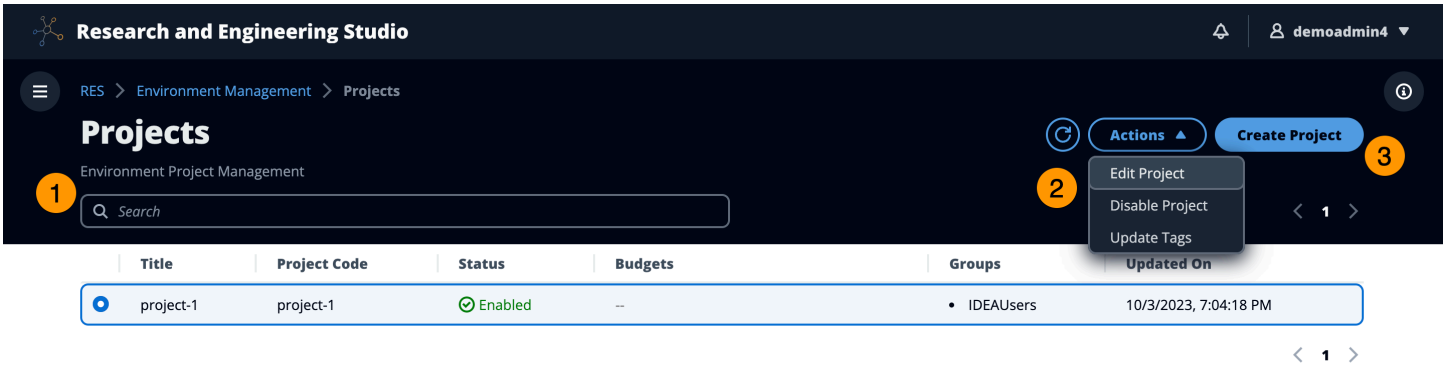
Projekte

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
- Fügen Sie Tags zu einem Projekt hinzu oder entfernen Sie sie
- 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.

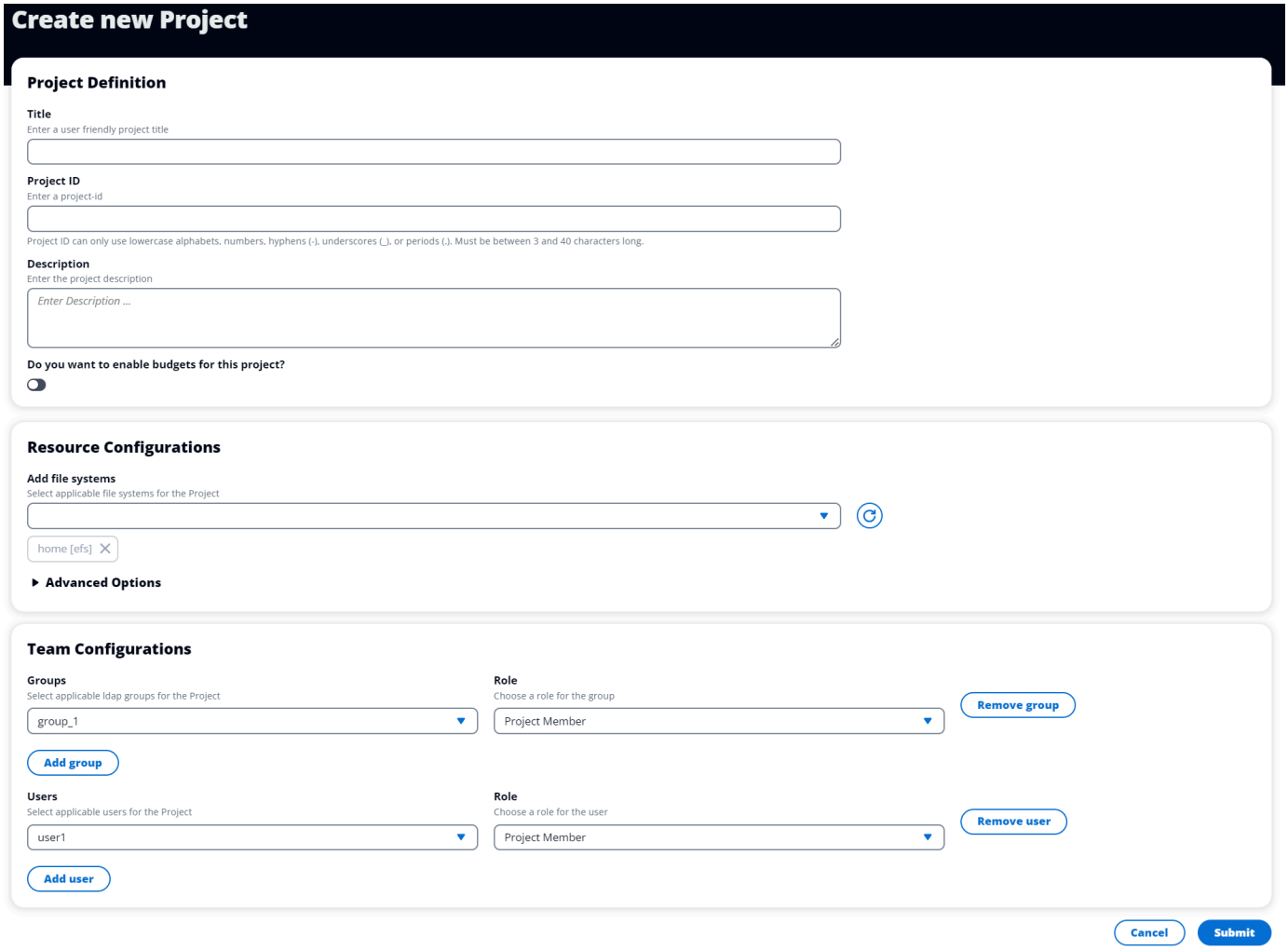
Erstellen eines Projekts

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.

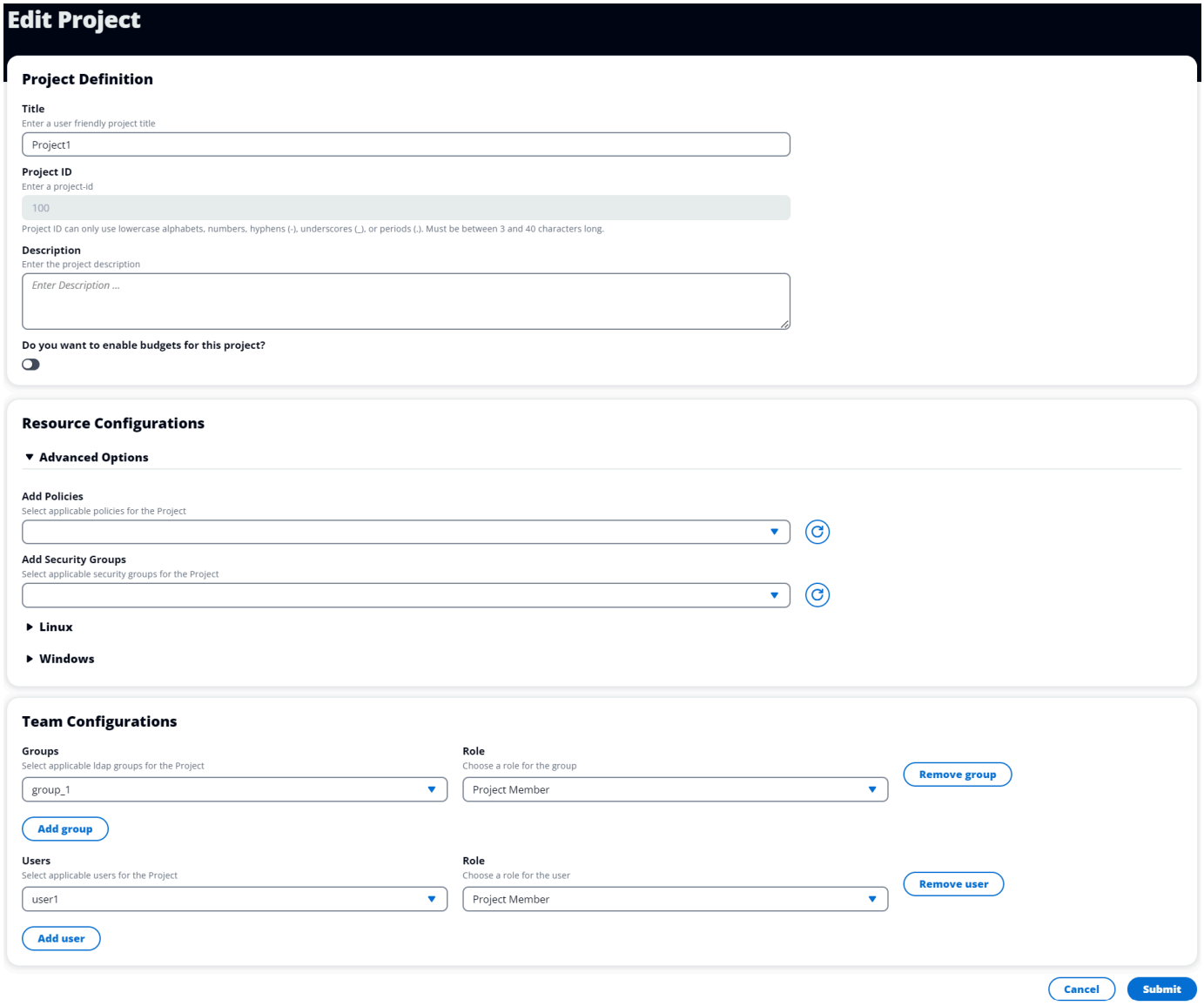
   > **Important**
   >
   > Die Projekt-ID kann nach der Erstellung nicht geändert werden.

   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 Benutzern und/oder Gruppen die entsprechende Rolle zu („Projektmitglied“ oder „Projekteigentümer“). Hier findest du Berechtigungen 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.



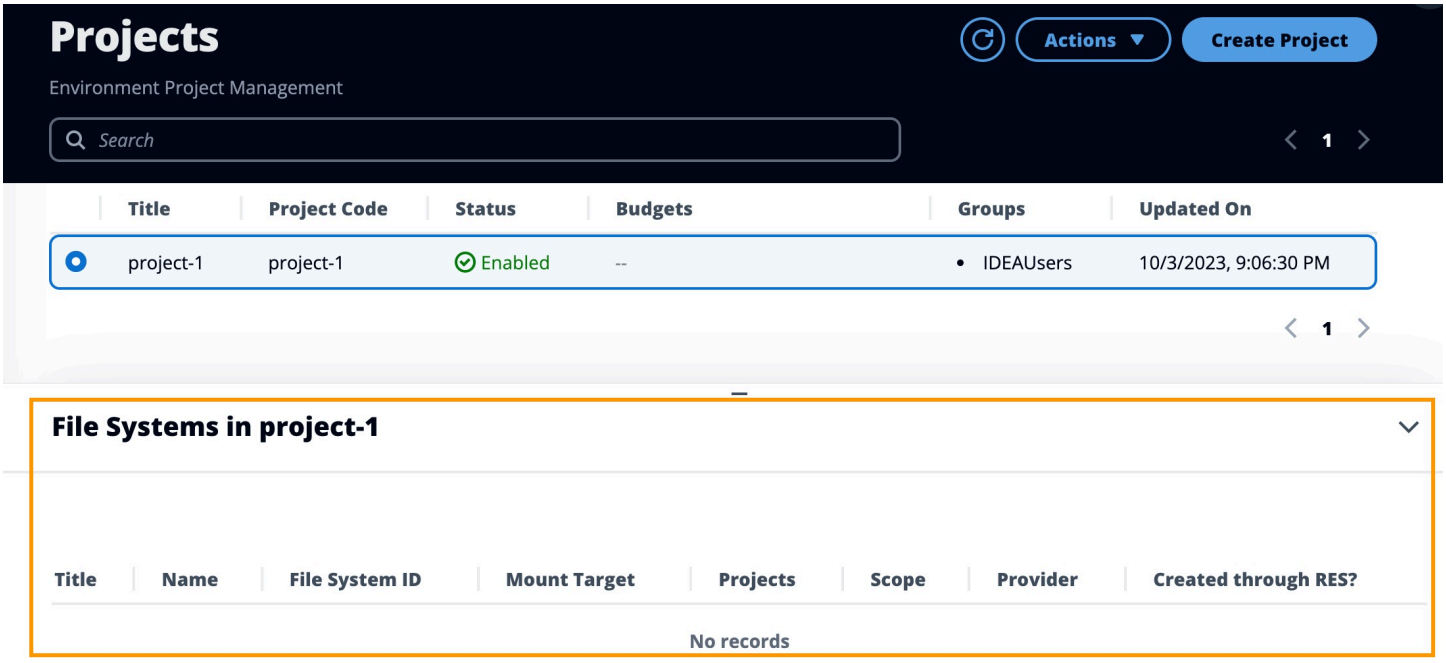
Fügen Sie Tags zu einem Projekt hinzu oder entfernen Sie sie

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.

Fügen Sie Richtlinien hinzu

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.

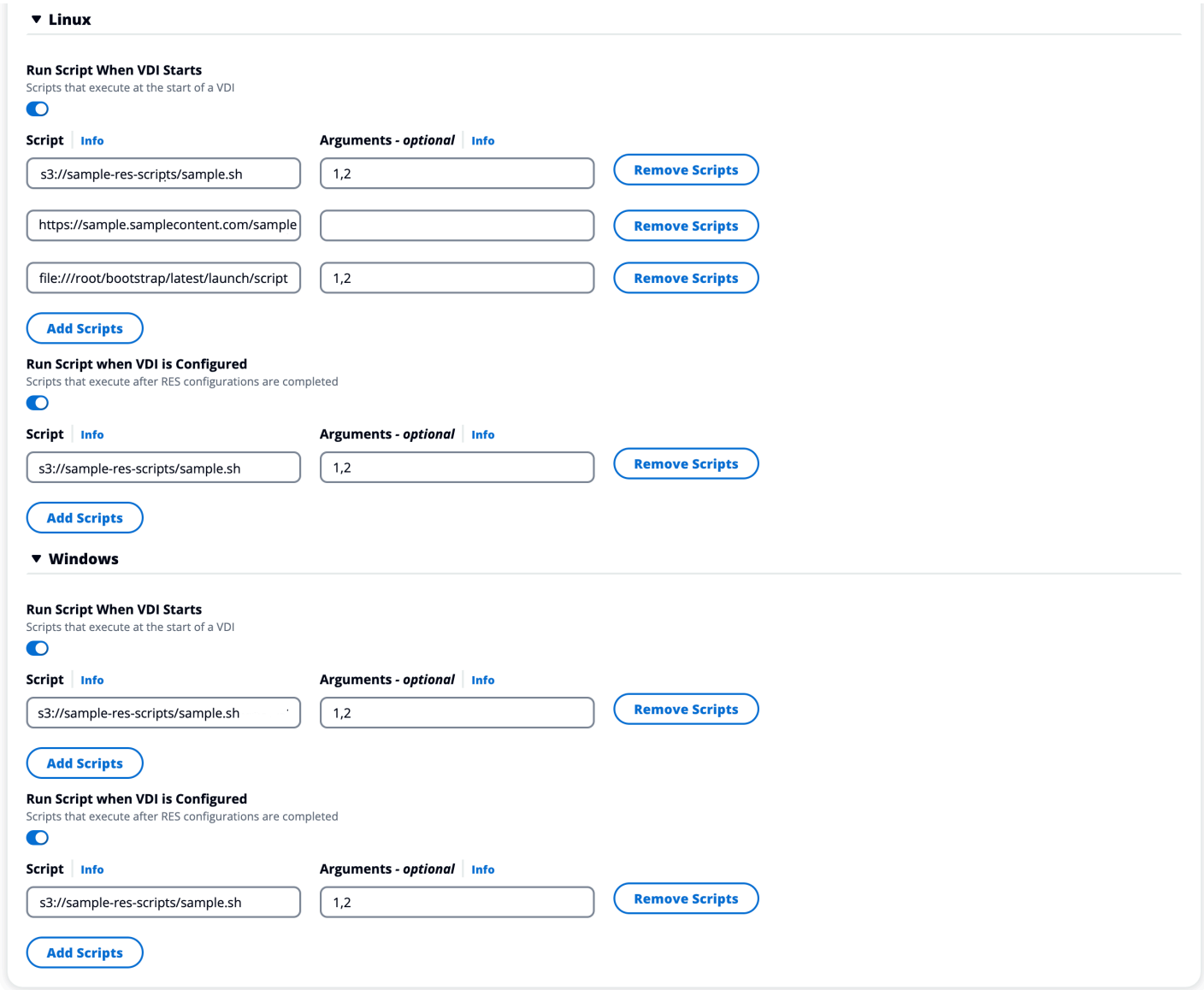
Führen Sie das Skript aus, wenn VDI konfiguriert ist

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/sample
Lokale Datei	Datei: ///user/scripts/example.sh

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

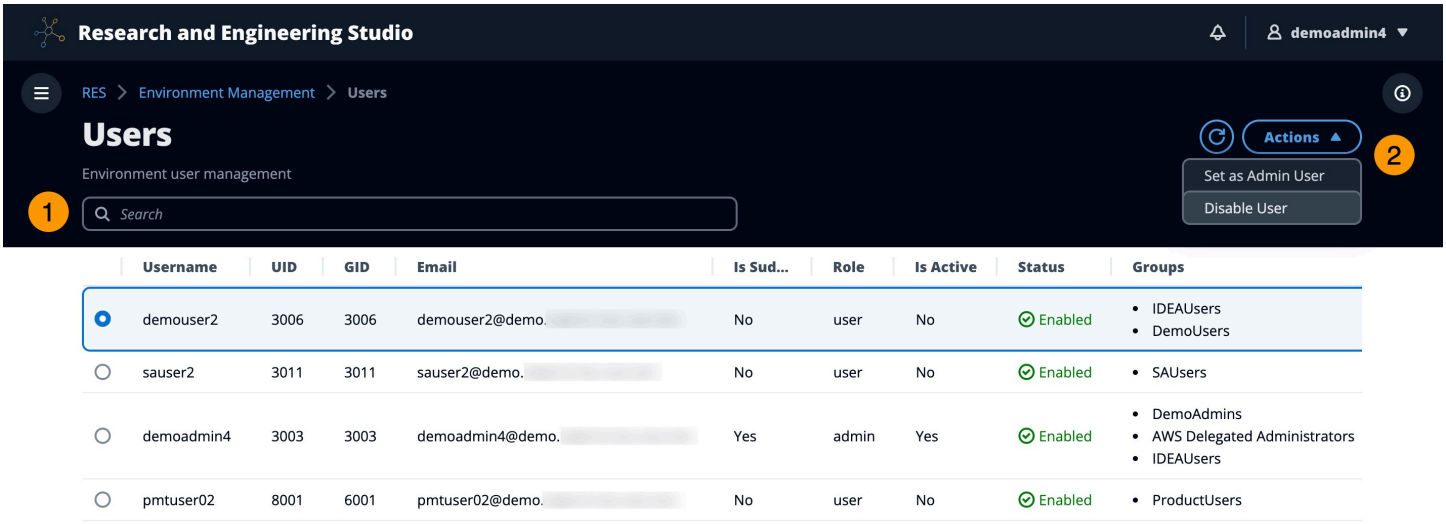


Beispiel für eine Projektkonfiguration

Benutzer

Alle Benutzer, die über Ihr 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.

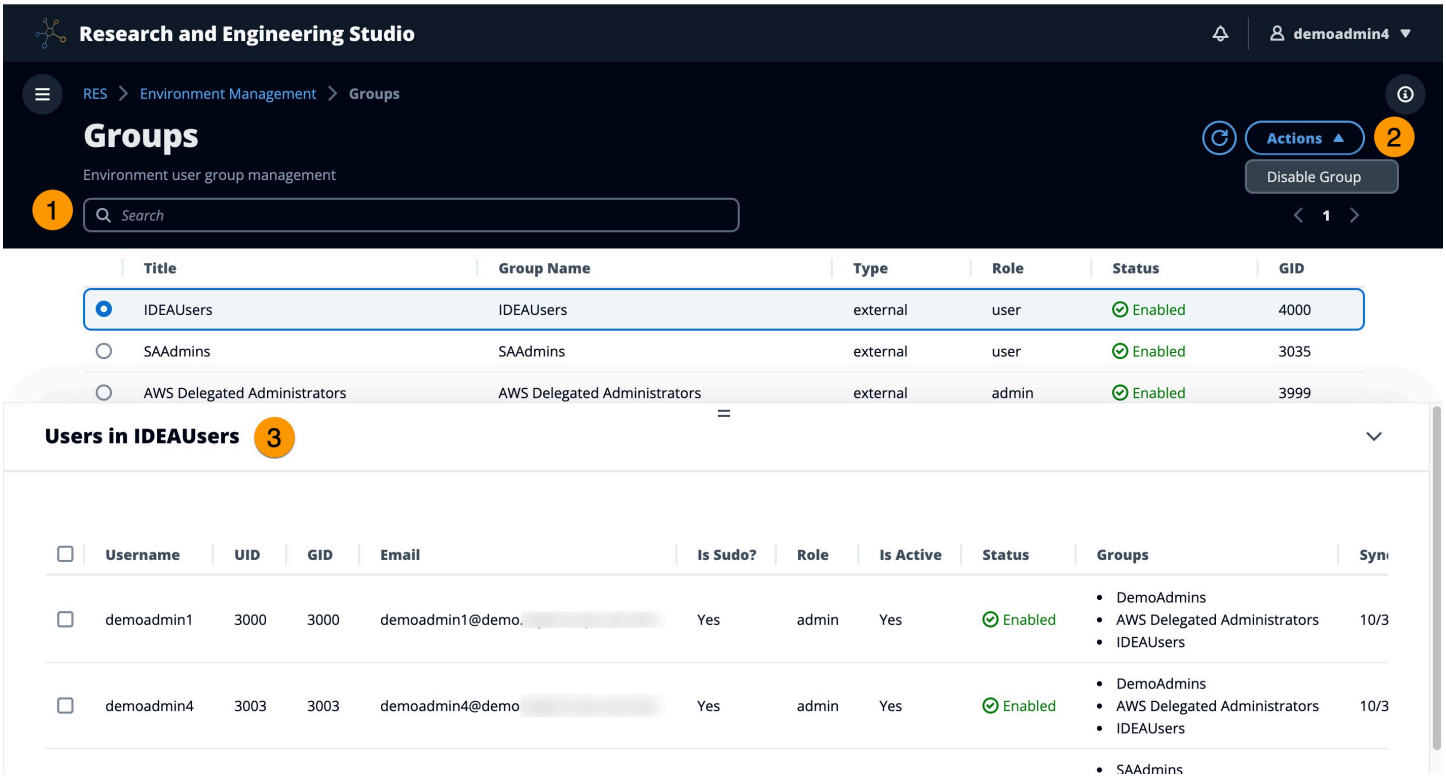


Auf der Benutzerseite können Sie:

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

Gruppen

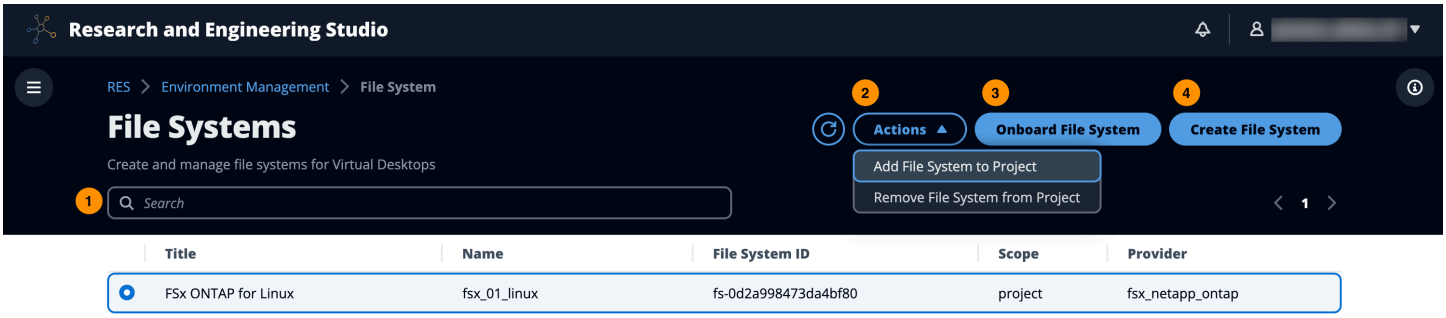
Alle Gruppen, die aus dem Active Directory synchronisiert wurden, werden auf der Gruppenseite angezeigt. Weitere Informationen zur Konfiguration und Verwaltung von Gruppen finden Sie unterLeitfaden zur Konfiguration.



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.

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. Geben Sie Subnetz-IDs von der VPC an. Sie finden die IDs auf 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

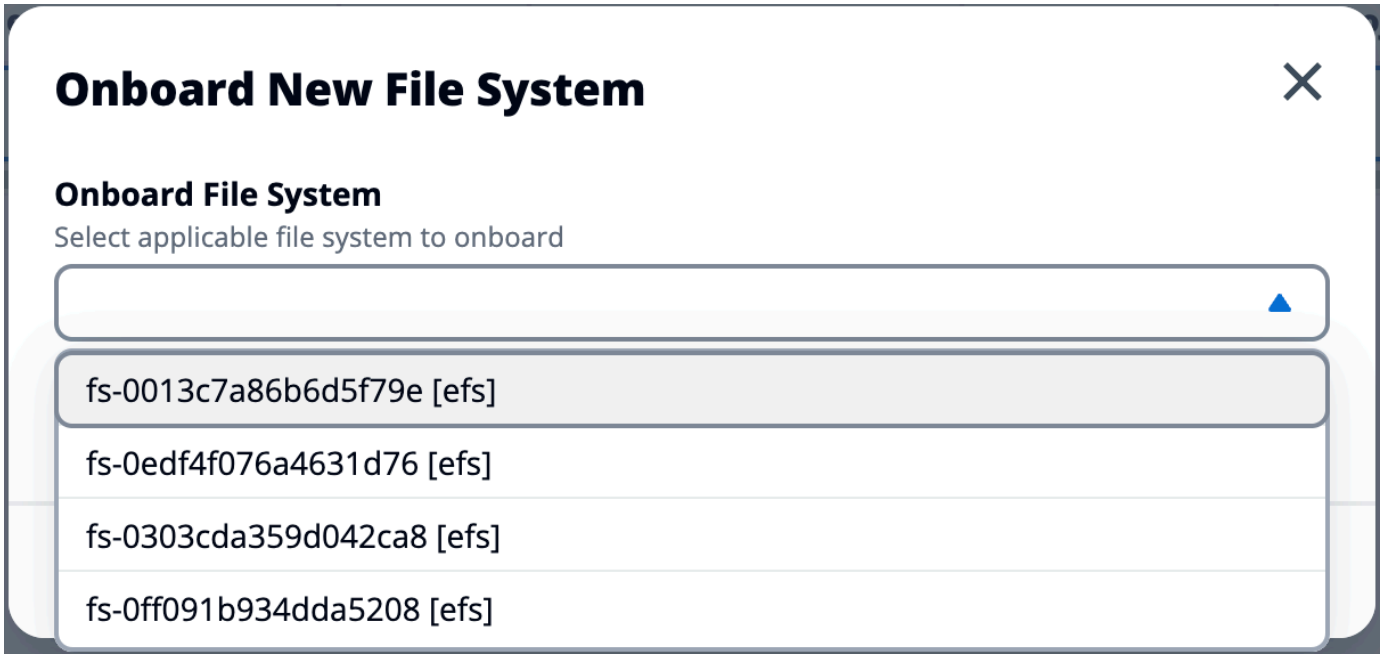
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

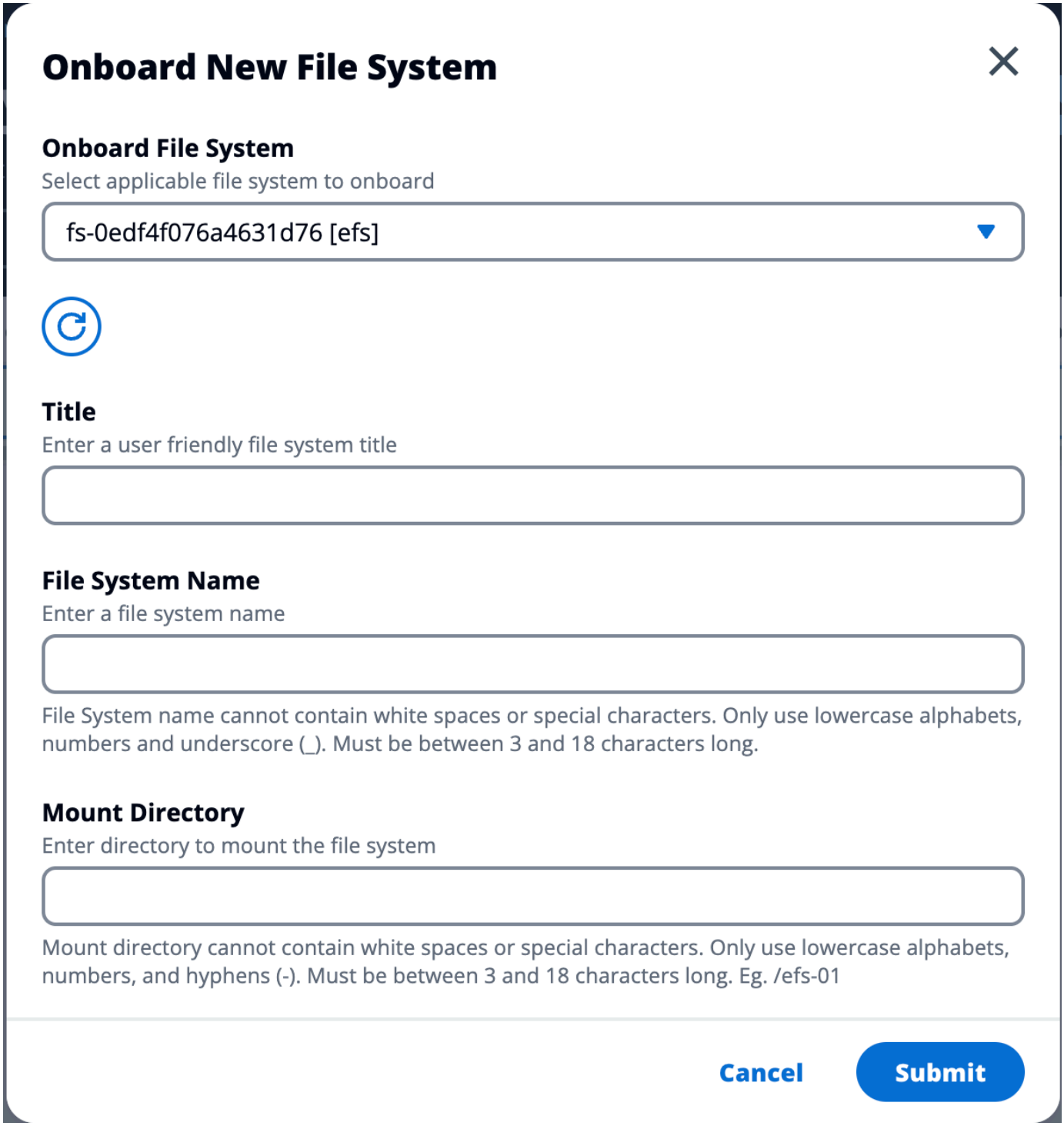
Enter directory to mount the file system

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.

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	2023.10	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

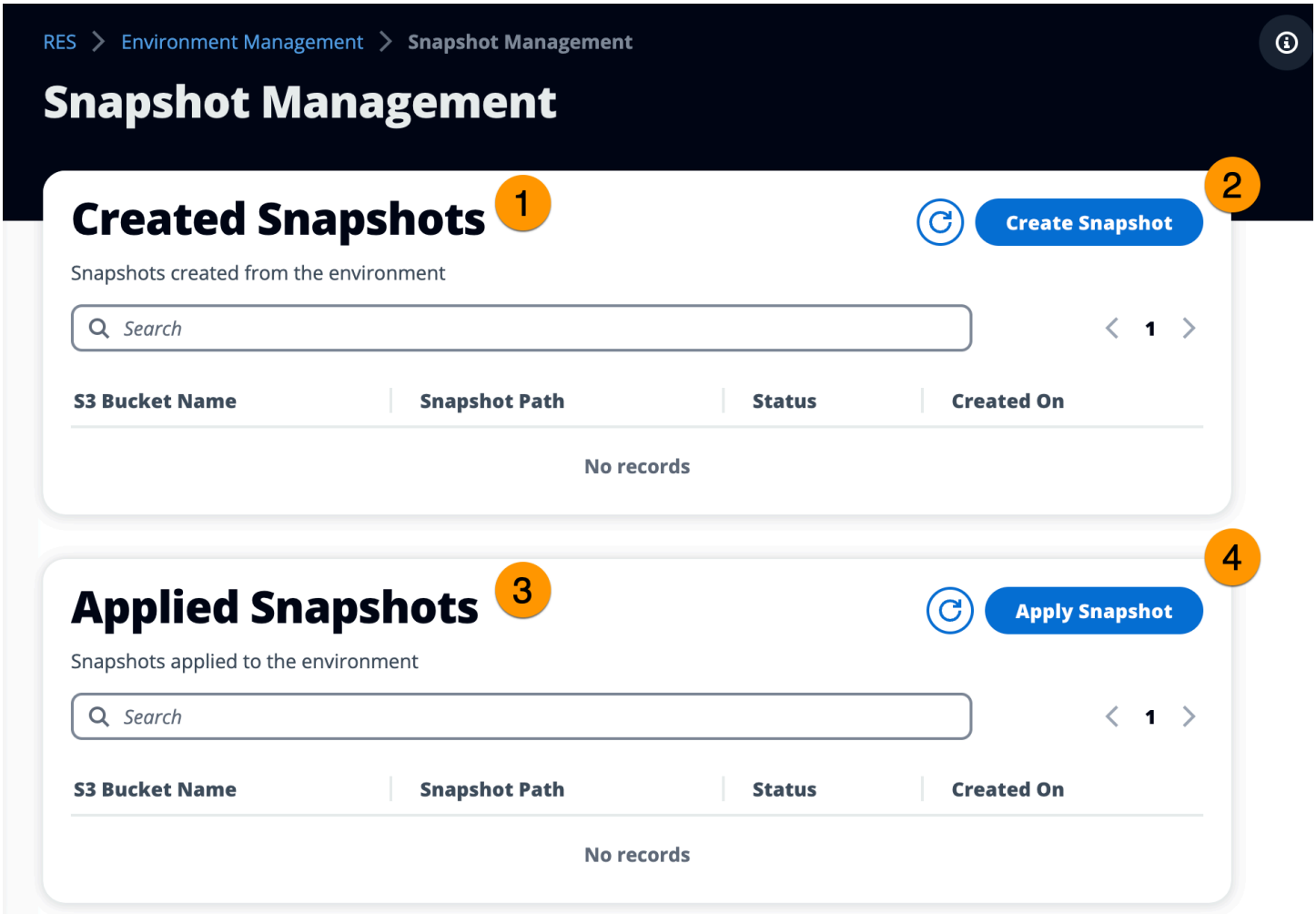
Infrastructure Hosts

Cluster hosts and status

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
   - RES_ENVIRONMENT_NAME
   - 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.

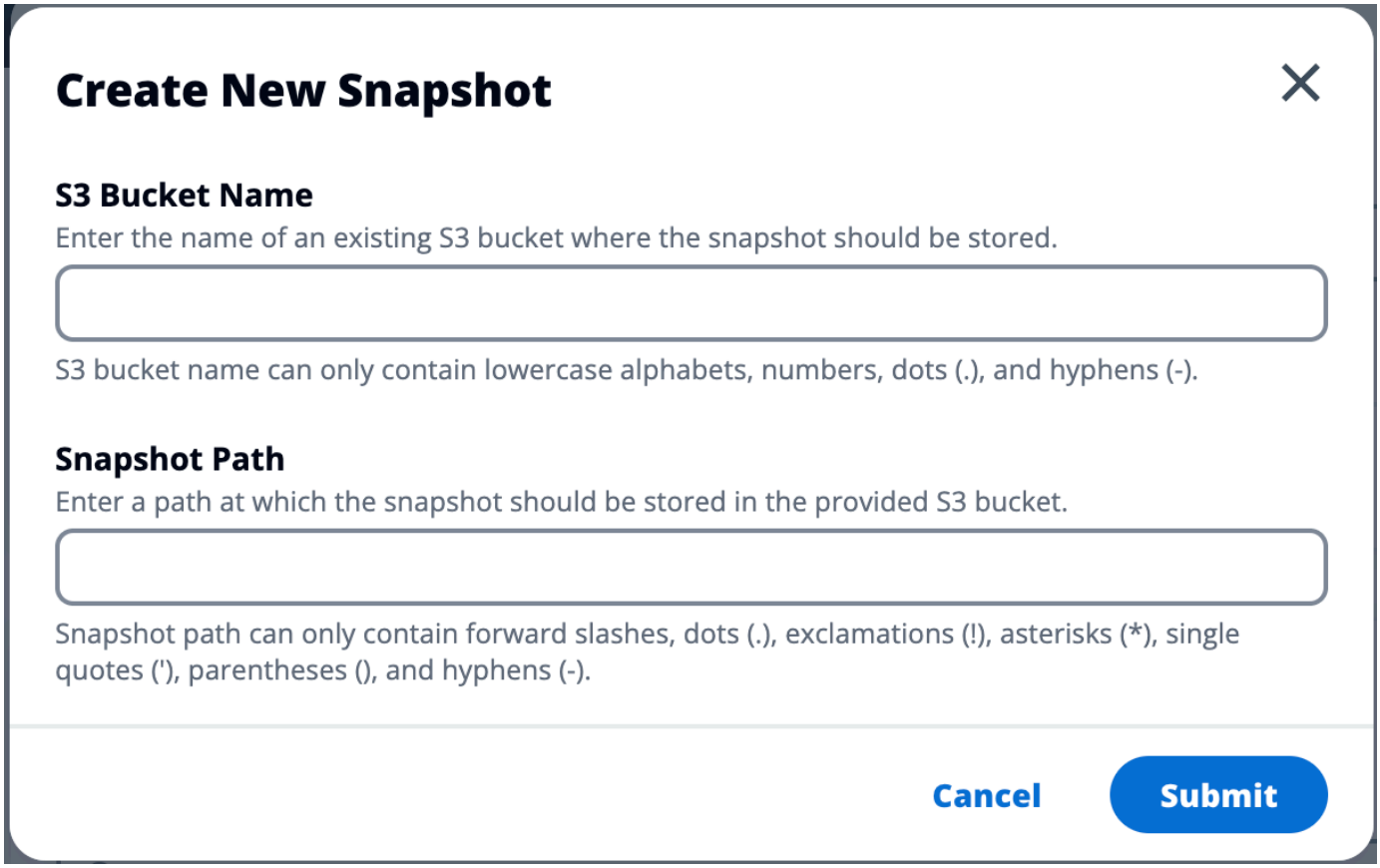
```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}: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. z. B. **`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:

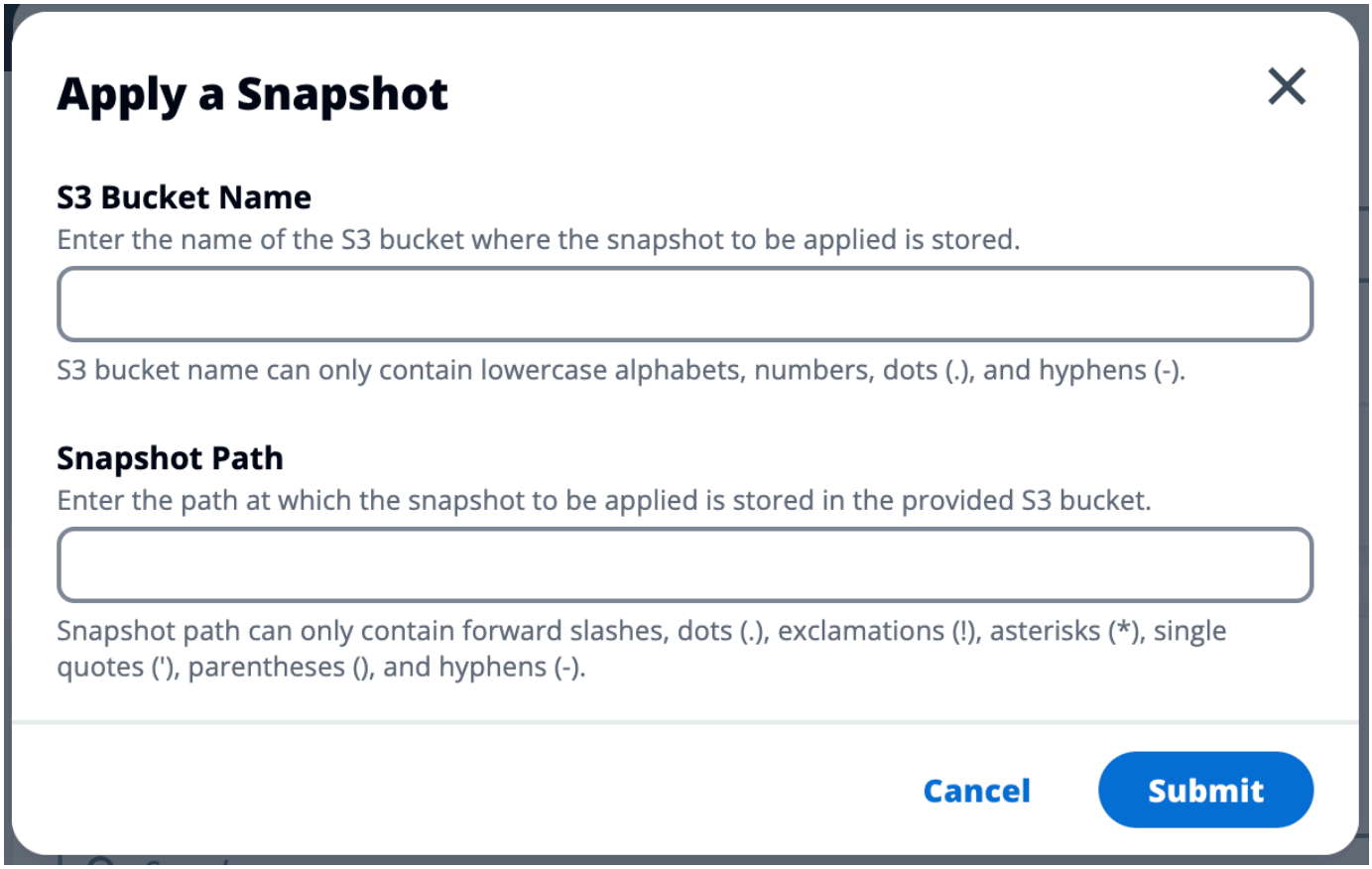
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKETNAME

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}: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

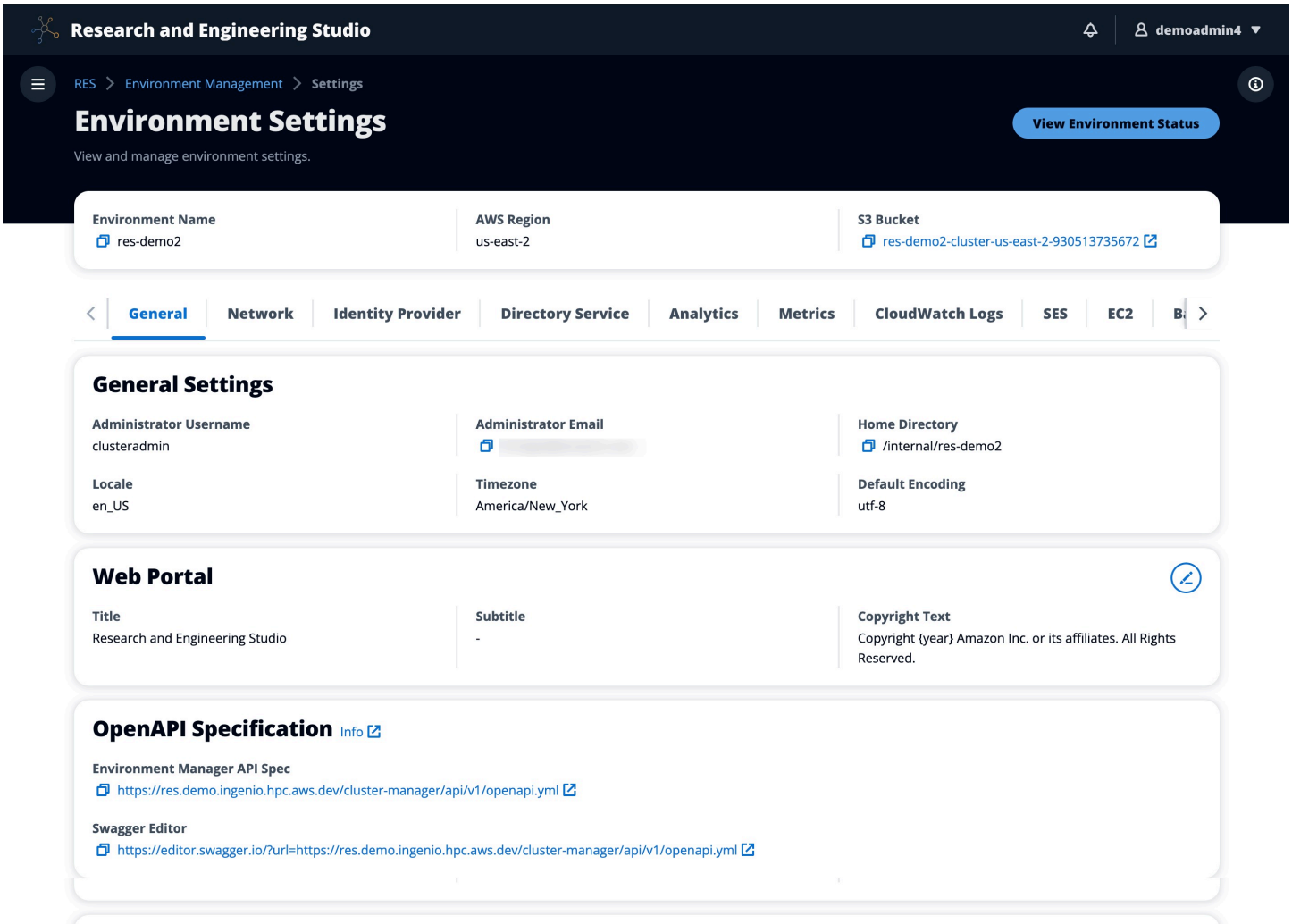
  Zeigt Informationen wie den Single Sign-On-Status an.

- Network (Netzwerk)

  Zeigt VPC-ID und Präfixlisten-IDs für den Zugriff an.

- Directory Service

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



Verwaltung von Secrets

Research and Engineering Studio wahrt 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 OAuth2-Client für Single Sign-On 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	✓	
<envname>-externes Zertifikat	Selbstsigniertes Zertifikat für die Domain	✓	
<envname>- internal-private-key	Privater Schlüssel für das selbstsig	✓	

Secret-Name	Beschreibung	RES generiert	Admin hat eingegeben
	nierte Zertifikat für die Domäne		
<envname>-internes Zertifikat	Selbstsigniertes Zertifikat für die Domain	✓	
<envname>-Verzeichnisdienst- ServiceAccountUsername			✓
<envname>-Verzeichnisdienst- ServiceAccountPassword			✓

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_secret_arn	Stack
directoryservice.root_username_secret_arn	
vdc.client_secret	Stack
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	Stack

Schlüssel	Quelle
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	

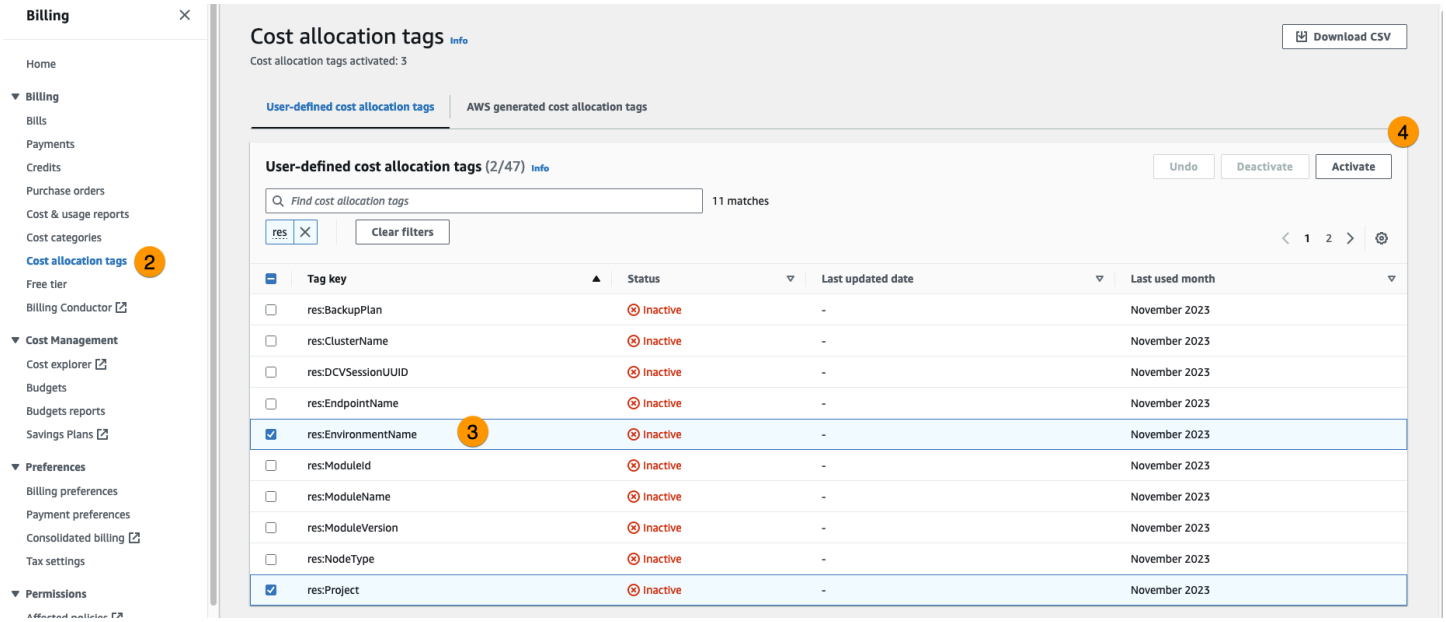
Kostenüberwachung und -kontrolle

> **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 jeweiligen Preisseite für die einzelnenthe section called “AWS -Services 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.

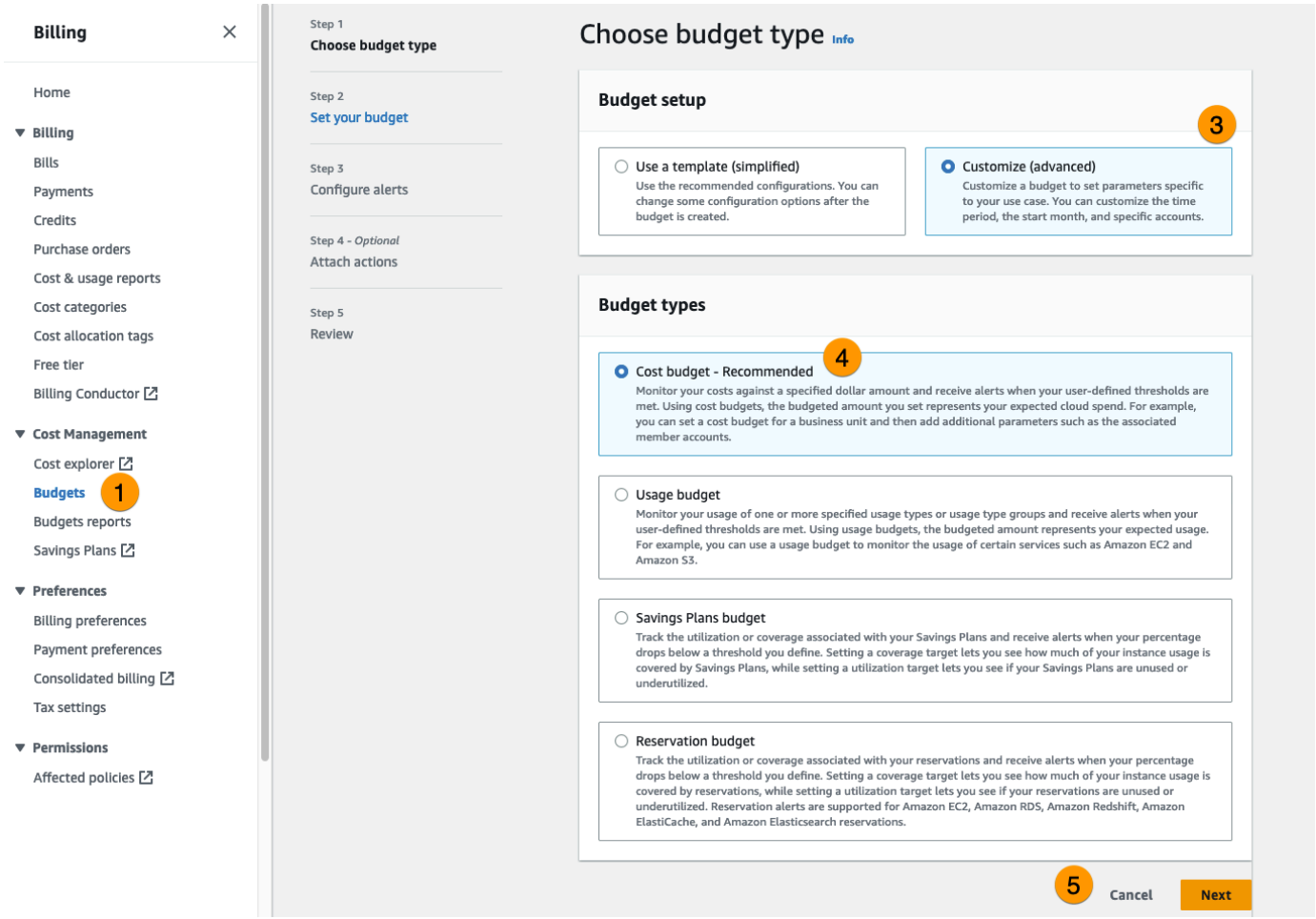
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Billing Konsole unter https://console.aws.amazon.com/billing/.
2. Wählen Sie Tags für die Kostenzuweisung aus.
3. Suchen Sie nach den `res:EnvironmentName` Tags `res:Project` und wählen Sie sie aus.
4. Wählen Sie Activate.



> **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 aus.
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.

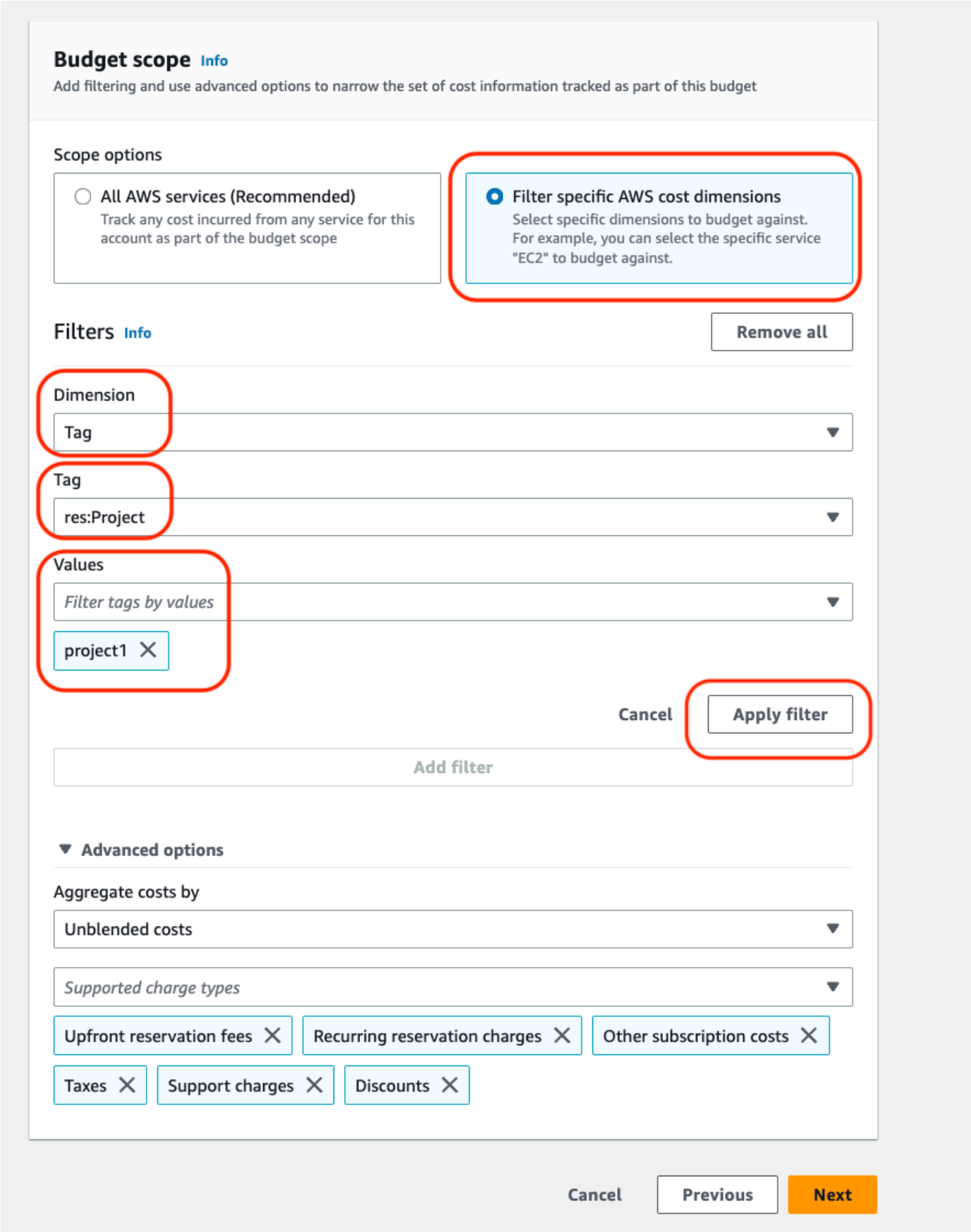


6. Geben Sie unter Details eine aussagekräftige Budgetbezeichnung für Ihr Budget ein, um es von anderen Budgets in Ihrem Konto zu unterscheiden. Zum Beispiel [EnvironmentName] - [ProjectName] - [BudgetName].
7. Geben Sie unter Budgetbetrag festlegen den für Ihr Projekt budgetierten Betrag ein.
8. Wählen 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.

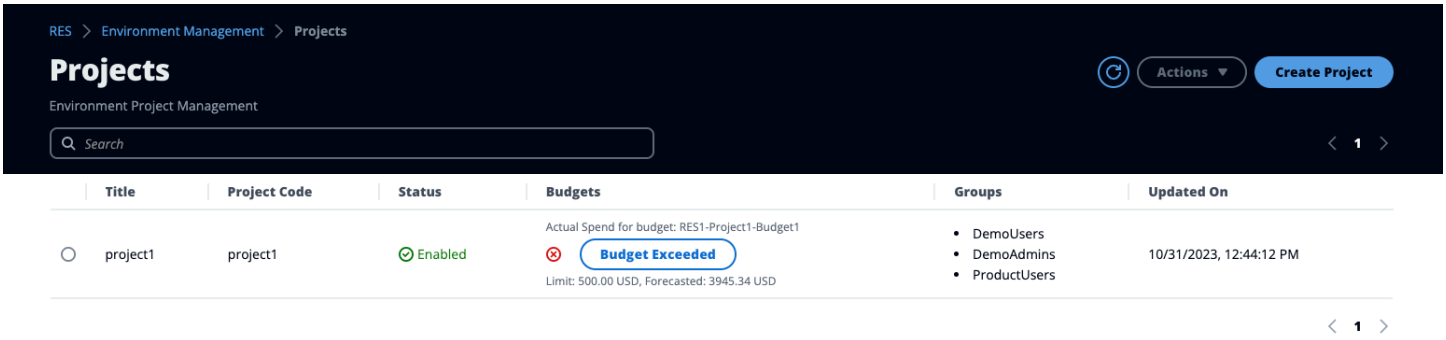
12. Wählen Sie unter Werte den Projektnamen aus.

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.

Berechtigungen

	Mitglied des Projekts	Eigentümer des Projekts	Globaler Administrator	Scope
Fügen Sie Benutzer als Projektmitglied/		X	X	Projektei gentümer: Projekte, die ihnen gehören

	Mitglied des Projekts	Eigentümer des Projekts	Globaler Administrator	Scope
Projekteigentümer hinzu				Globaler Administrator: Beliebiges Projekt
Fügen Sie Gruppen als Projektmitglied/ Projekteigentümer hinzu		X	X	Projekteigentümer: Projekte, die ihnen gehören Globaler Administrator: Beliebiges Projekt
Benutzer entfernen		X	X	Projekteigentümer: Projekte, die ihnen gehören Globaler Administrator: Beliebiges Projekt
Gruppen entfernen		X	X	Projekteigentümer: Projekte, die ihnen gehören Globaler Administrator: Beliebiges Projekt

	Mitglied des Projekts	Eigentümer des Projekts	Globaler Administrator	Scope
Starten/Stoppen von VDI-Instanzen	X	X	X	Projektmitglied/ Projekteigentümer: VDI-Instanzen, deren Eigentümer sie sind, wenn sie Teil eines Projekts sind. Globaler Administrator: Alle VDI-Instanzen.

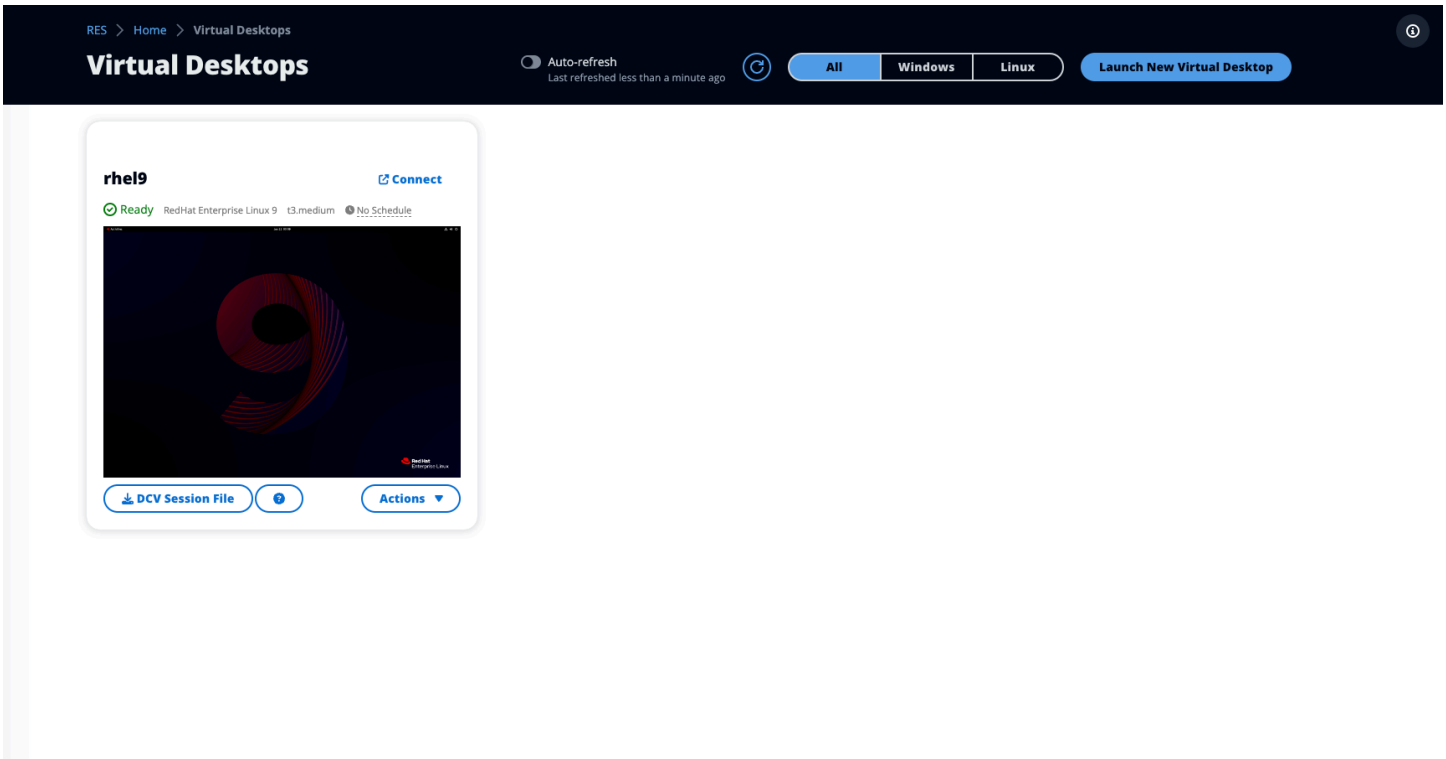
Benutze das Produkt

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

Themen

Virtuelle Desktops

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



Unterstützte Betriebssysteme

> **Note**
>
> CentOS 7 soll derzeit end-of-life am 30.06.2024 erscheinen. Research and Engineering Studio Version 2024.06 wird die letzte Version sein, die CentOS 7 unterstützt.

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

- Amazon Linux 2 (x86 und ARM64)
- CentOS 7 (x86 und ARM64)
- RHEL 7 (x86), 8 (x86) und 9 (x86)
- 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.

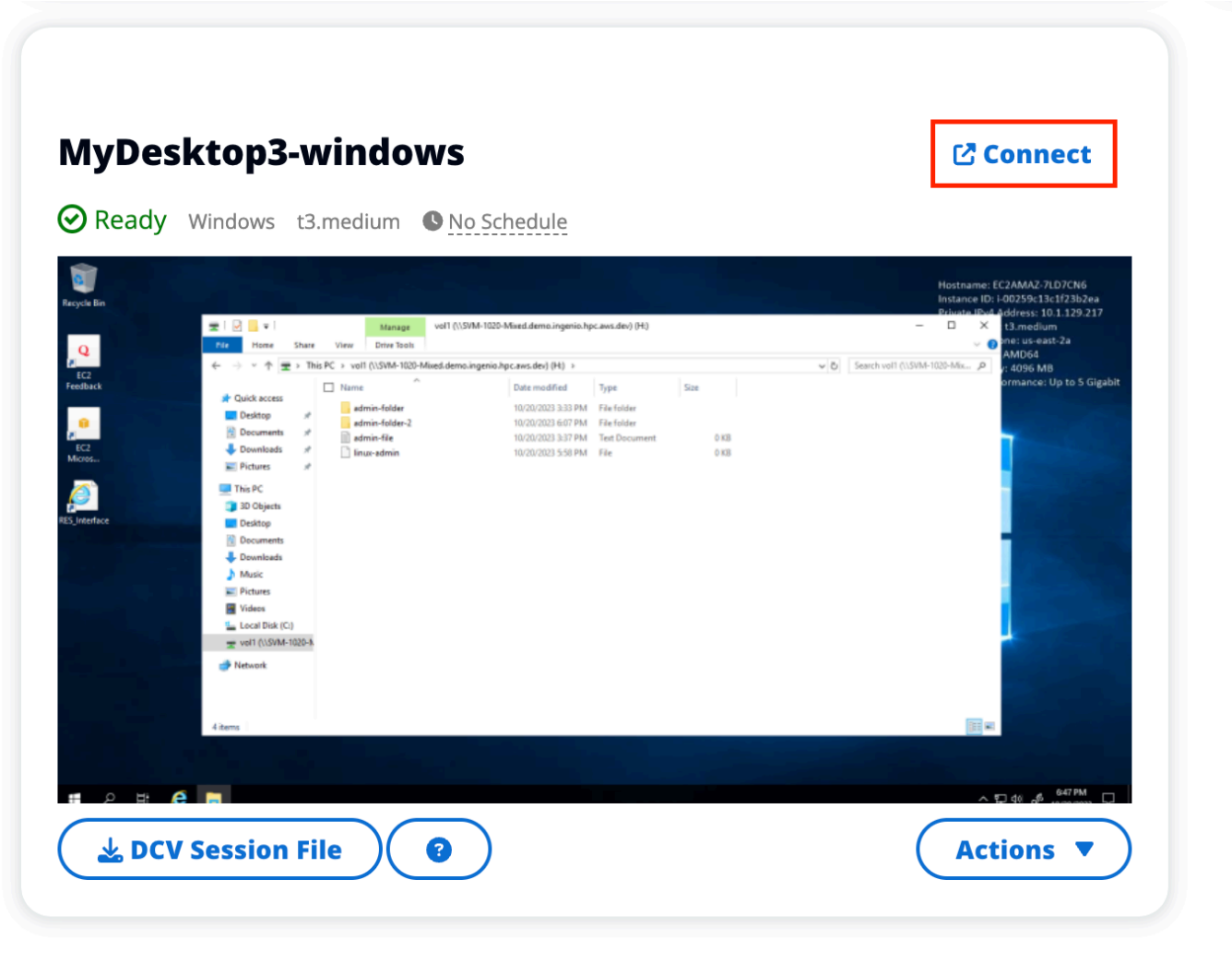
Greifen Sie auf Ihren Desktop zu

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.

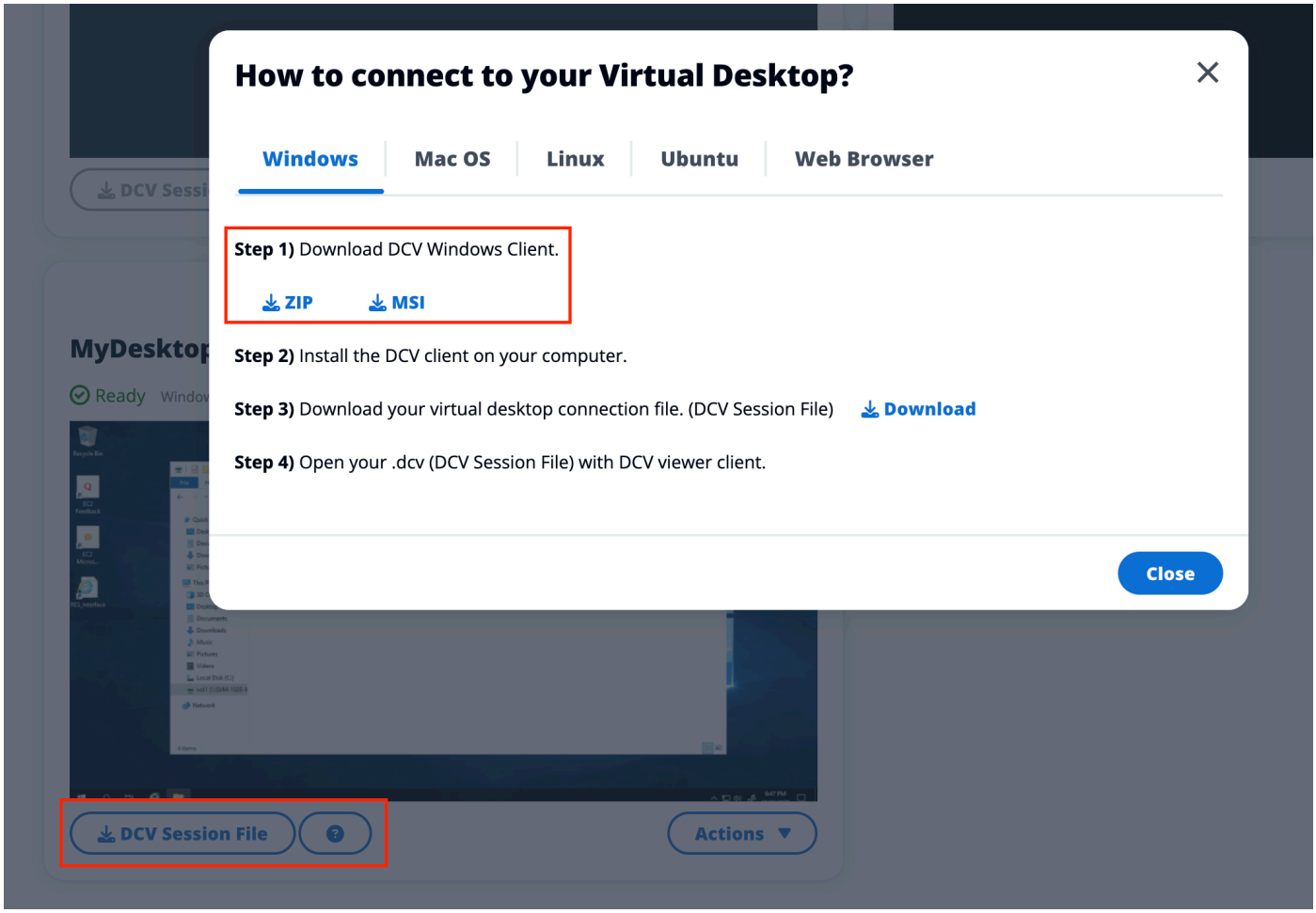
- Wählen Sie Connect oder wählen Sie das Vorschaubild, um direkt über Ihren Browser auf Ihren Desktop zuzugreifen.



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.

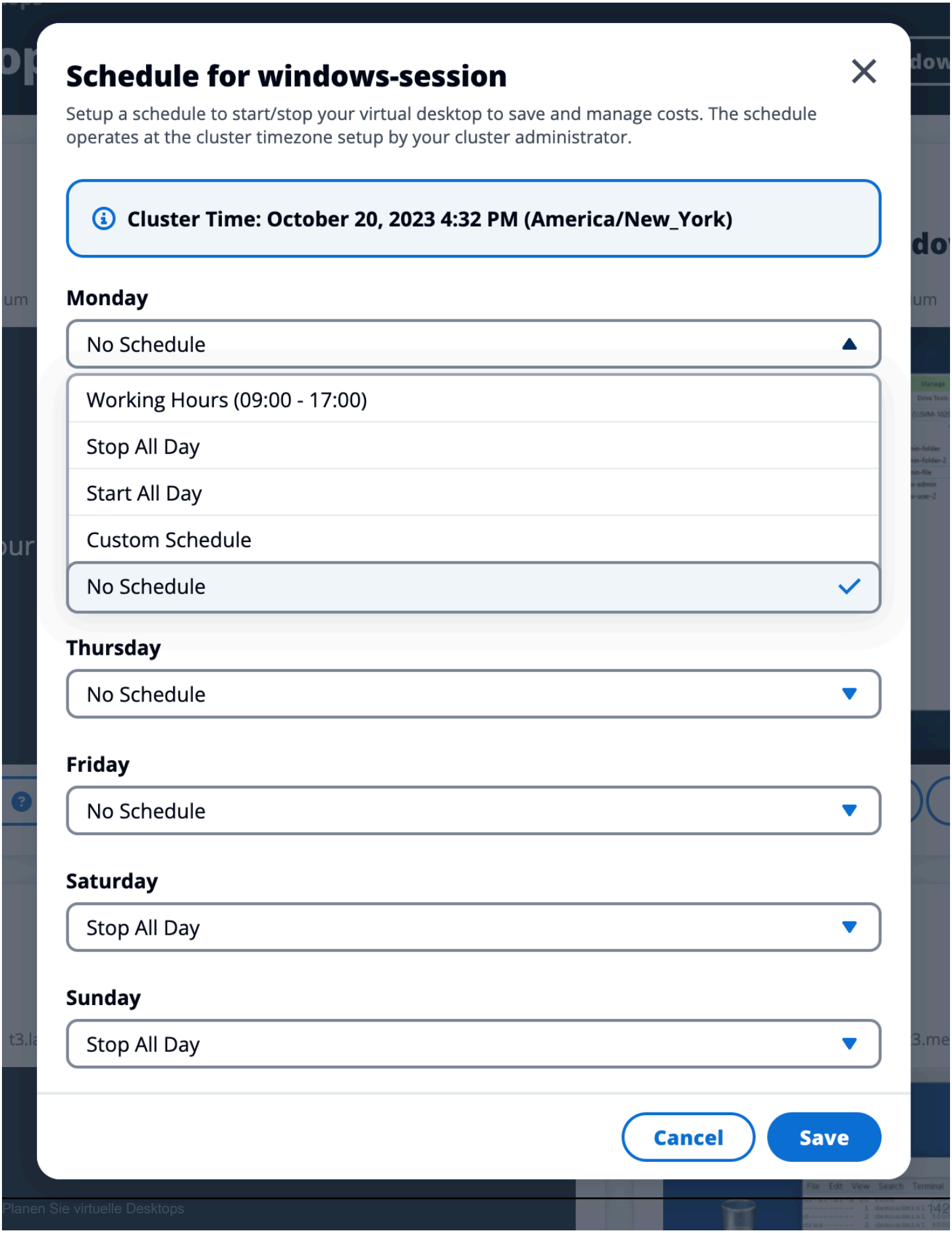
Sitzungsinformationen abrufen

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

Virtuelle Desktops planen

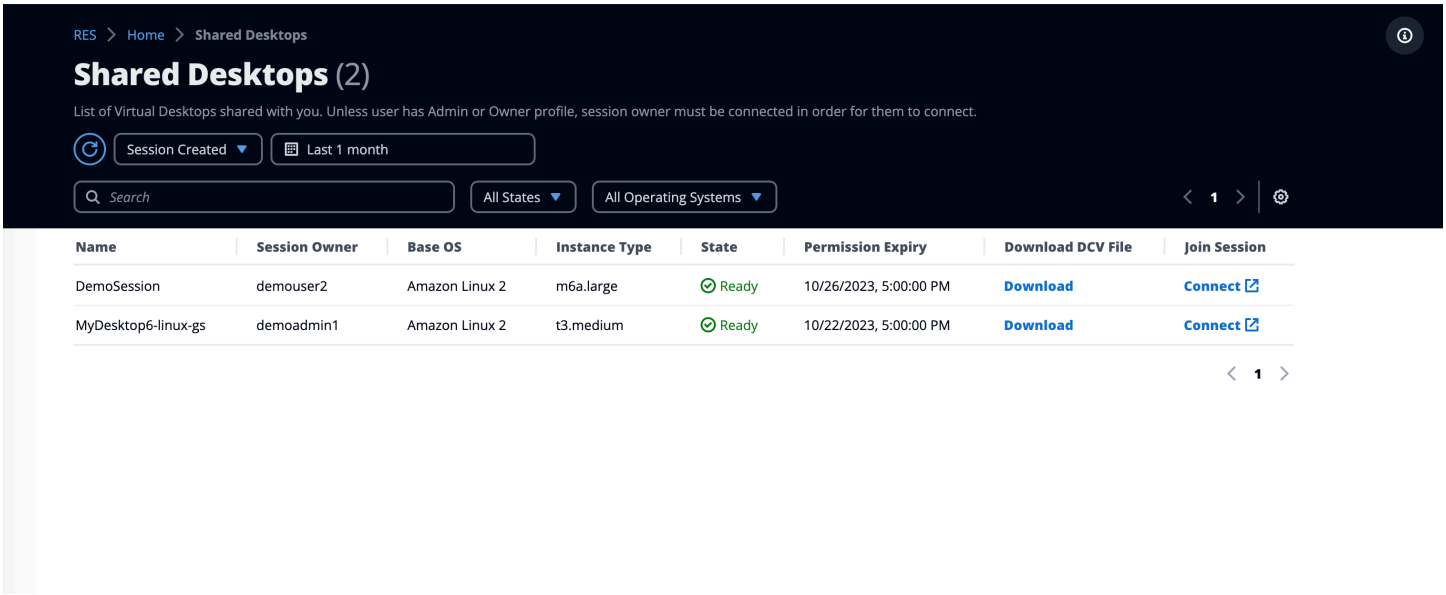
Standardmäßig haben virtuelle Desktops keinen Zeitplan und bleiben aktiv, bis Sie die Sitzung beenden oder beenden. Desktops werden auch angehalten, wenn sie inaktiv sind, um versehentliche Stopps zu verhindern. Ein Ruhezustand liegt vor, wenn keine aktive Verbindung besteht und die CPU-Auslastung mindestens 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

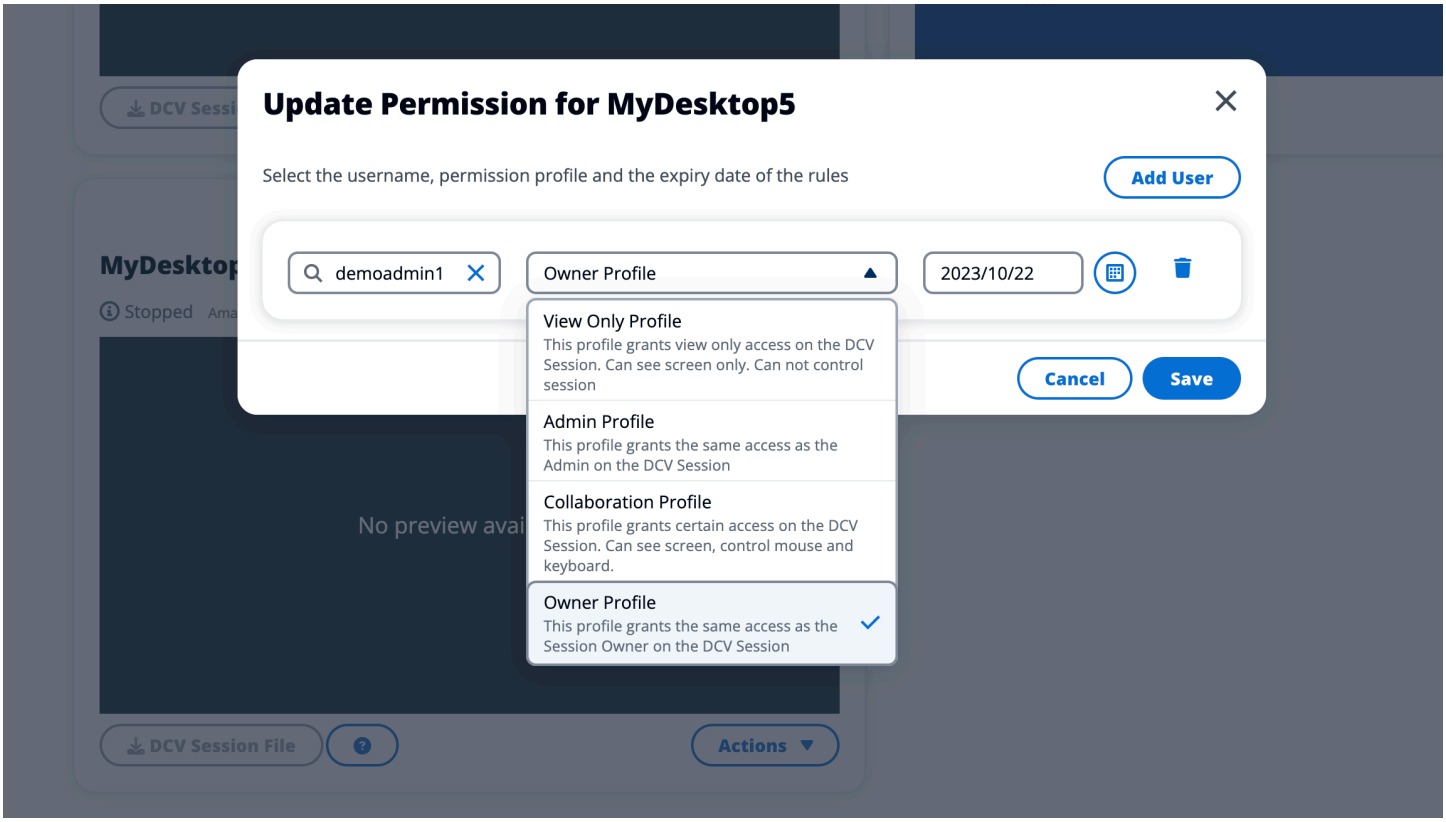
Auf Shared Desktops können Sie die Desktops sehen, die für Sie freigegeben wurden. Um eine Verbindung zu einem Desktop herzustellen, muss auch der Sitzungsbesitzer verbunden sein, es sei denn, Sie sind Administrator oder Besitzer.



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.



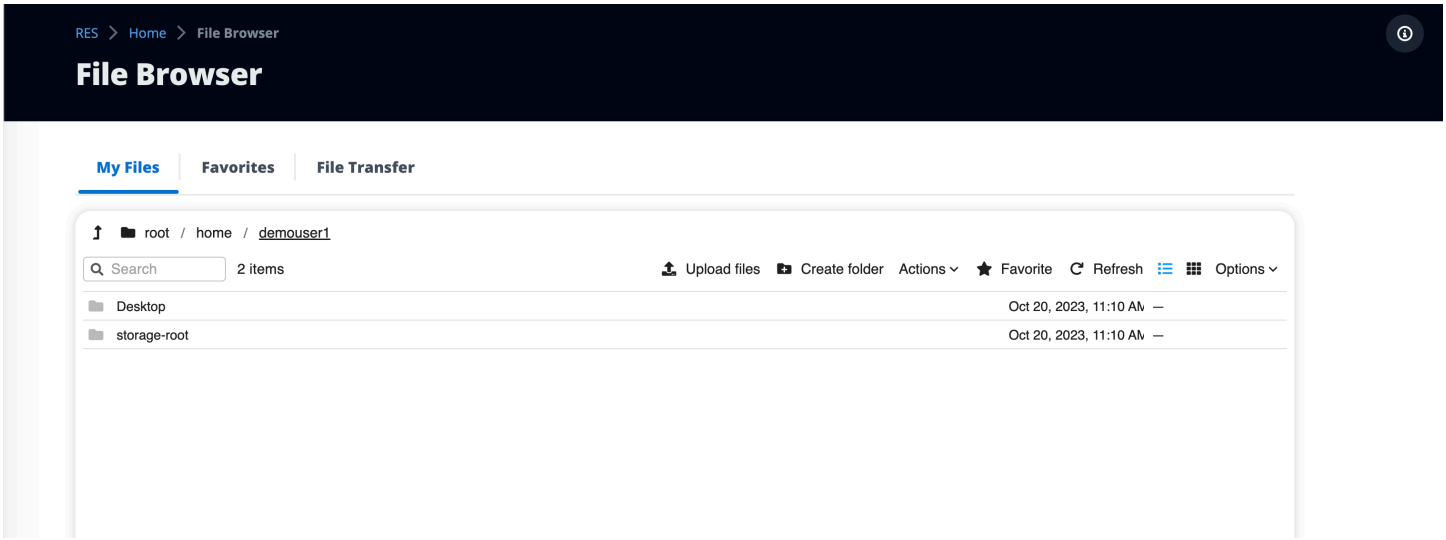
Weitere Informationen zu Berechtigungen finden Sie unterthe section called “Berechtigungsprofile”.

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 for 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

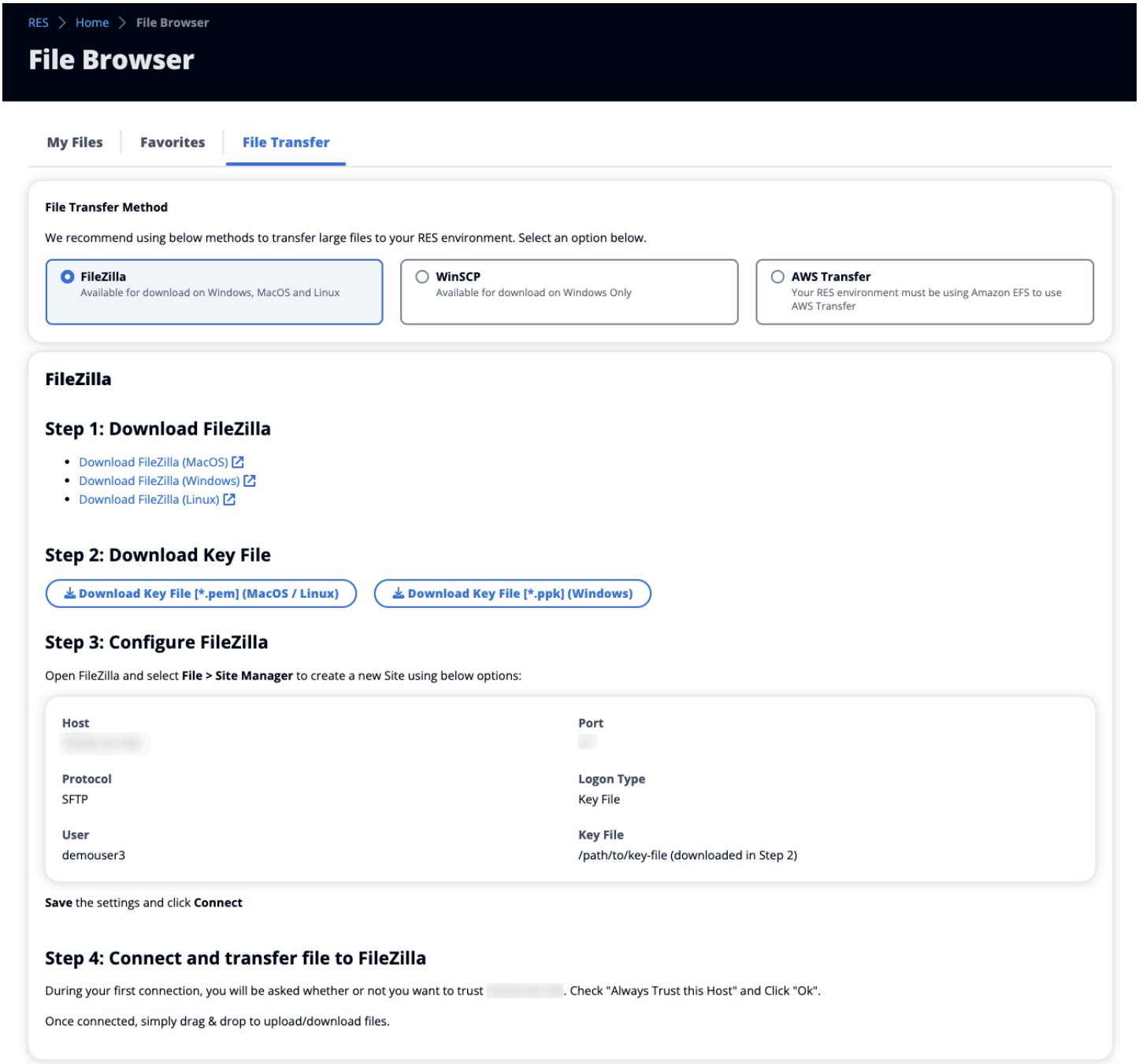
Sie können den Inhalt textbasierter Dateien im Webportal bearbeiten.

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

Dieses Dokument enthält Informationen zur Überwachung des Systems und zur Behebung bestimmter Probleme, die auftreten können. Wenn Sie die Lösung für ein Problem nicht finden können, finden Sie möglicherweise weitere Themen zur Problembehandlung unter GitHub.

Themen

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“

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 Stapel erfolgreich erstellt wurden

Wenn nach der erfolgreichen AWS CloudFormation Erstellung 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 Amazon EC2 EC2-Konsole nach Hinweisen auf wechselnde Instances.

   Wenn es Amazon EC2 EC2-Instances gibt, deren `<envname>` Präfix als beendet erscheint und dann durch eine neue Instance ersetzt wird, 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 befindet sich im ausgefallenen Zustand”, um das Problem zu lösen.

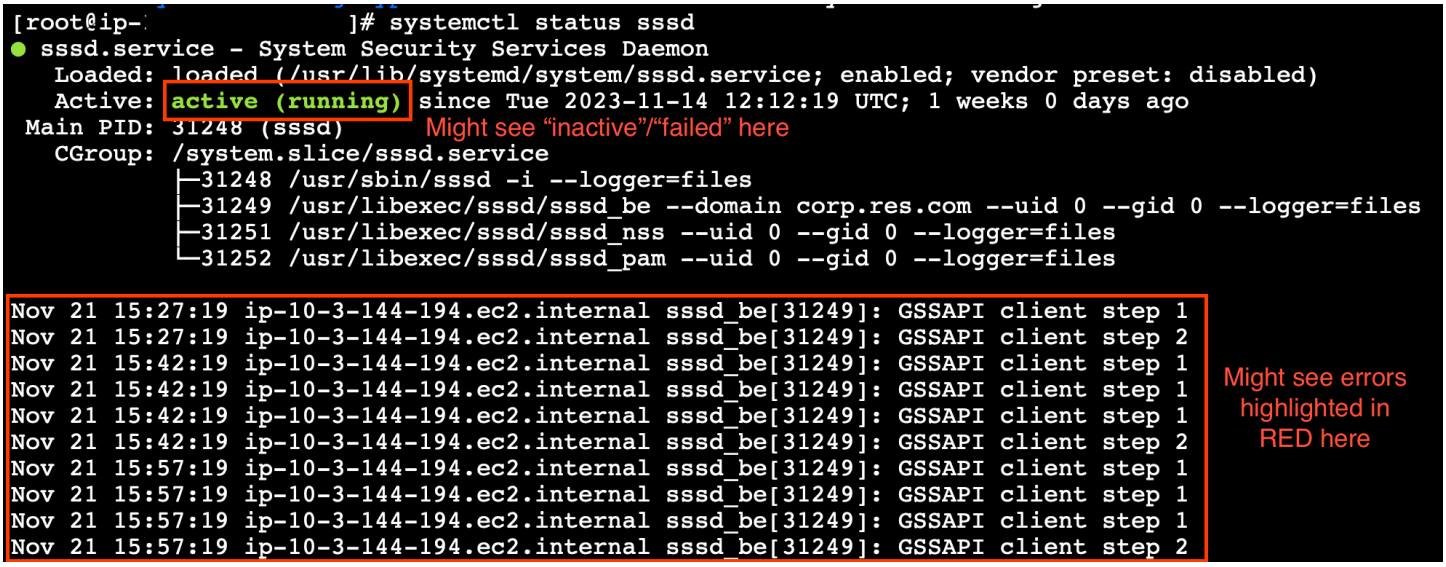
Instanzen laufen oder der VDC-Controller befindet sich im ausgefallenen Zustand

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.



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 sein.

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 die folgenden Elemente 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. Löschen Sie nach dem Aktualisieren der Tabelle 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.

Hauptursache 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. Um das Passwort in Secrets Manager zurückzusetzen:

   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.

5. Wenn der Wert aktualisiert wurde, 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 Amazon EC2 EC2-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 Amazon EC2 EC2-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 Amazon EC2-Patches während der Bereitstellung nach dem Start der Instance unerwartet ausgeführt wurden.

```
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 im SSM RunCommand /Automation-Ausführungsverlauf, ob die Ausführung eines SSM-Dokuments, das sich auf das Patchen bezieht, mit dem Start einer Instanz übereinstimmt.
3. Überprüfen Sie in den Protokolldateien für die Amazon EC2 EC2-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 einer Fehlkonfiguration auf. Informationen zum Einrichten 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 dem Identitätsmanagement finden Sie in den folgenden Themen zur Fehlerbehebung:

Themen

- Wenn ich mich bei der Umgebung anmelde, kehre ich sofort zur Anmeldeseite zurück
- Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden
- Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES
- Benutzer beim Erstellen einer Sitzung nicht verfügbar
- Größenbeschränkung überschritten Fehler im CloudWatch Cluster-Manager-Protokoll

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 Protokolle der Controller-Instance und überprüfen Sie die Konfigurationseinstellungen auf Fehler.

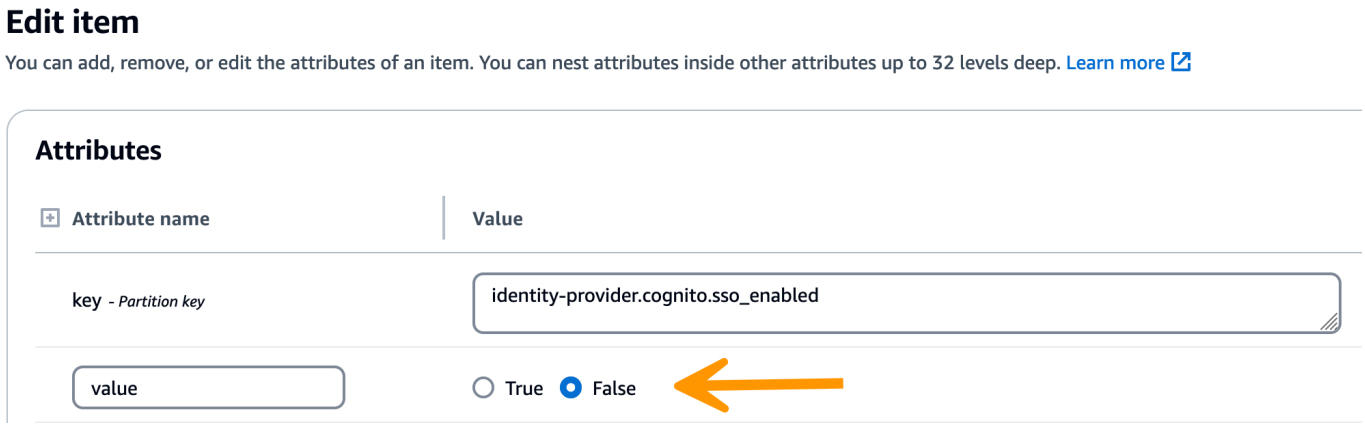
So überprüfen Sie die Protokolle:

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Suchen Sie unter Protokollgruppen die Gruppe mit dem Namen `/<environment-name>/cluster-manager`.
3. Öffnen Sie die Protokollgruppe, um nach Fehlern in den Protokollstreams zu suchen.

So überprüfen Sie die Konfigurationseinstellungen:

1. Öffnen Sie die DynamoDB-Konsole unter https://console.aws.amazon.com/dynamodb/.

2. Suchen Sie in Tabellen die Tabelle mit dem Namen `<environment-name>.cluster-settings`.
3. Öffnen Sie die Tabelle und wählen Sie Tabellenelemente erkunden aus.
4. Erweitern Sie den Filterabschnitt und geben Sie die folgenden Variablen ein:
   - Attributname – Schlüssel
   - Bedingung – enthält
   - Wert – sso
5. Wählen Sie Ausführen aus.
6. Überprüfen Sie in der zurückgegebenen Zeichenfolge, ob 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 das SSO neu zu konfigurieren.

Fehler „Benutzer nicht gefunden“ beim Versuch, sich anzumelden

Wenn Sie bei der Anmeldung bei der RES-Schnittstelle die Fehlermeldung „Benutzer nicht gefunden“ erhalten, ist der Benutzer in Active Directory, aber nicht in RES vorhanden. Wenn Sie den Benutzer kürzlich zu AD hinzugefügt haben, werden er möglicherweise nicht mit RES synchronisiert. RES synchronisiert stündlich, sodass Sie möglicherweise warten und überprüfen müssen, ob der Benutzer nach der nächsten Synchronisierung hinzugefügt wurde. Um sofort zu synchronisieren, führen Sie die Schritte unter austhe section called “Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES”.

Wenn der Benutzer in RES vorhanden ist:

1. Stellen Sie sicher, dass die Attributzuordnung korrekt konfiguriert ist. Weitere Informationen finden Sie unter the section called “Konfiguration Ihres Identitätsanbieters für Single Sign-On (SSO)”.
2. Stellen Sie sicher, dass der SAML-Betreff und die SAML-E-Mail der E-Mail-Adresse des Benutzers zugeordnet sind.

Benutzer wurde in Active Directory hinzugefügt, fehlt aber in RES

Wenn Sie dem Active Directory einen Benutzer hinzugefügt haben, dieser jedoch in RES fehlt, muss die AD-Synchronisierung ausgelöst werden. Die AD-Synchronisierung wird stündlich von einer Lambda-Funktion ausgeführt, um AD-Einträge in die RES-Umgebung zu importieren. Gelegentlich kommt es nach dem Hinzufügen neuer Benutzer oder Gruppen zu einer Verzögerung, bis der nächste Synchronisierungsprozess ausgeführt wird. Sie können die Synchronisierung manuell über den Amazon Simple Queue Service starten.

Initiieren Sie den Synchronisierungsprozess manuell:

1. Öffnen Sie die Amazon-SQS-Konsole unter https://console.aws.amazon.com/sqs/.
2. Wählen Sie unter Warteschlangen aus`<environment-name>-cluster-manager-tasks.fifo`.
3. Wählen Sie Nachrichten senden und empfangen.
4. Geben Sie für Nachrichtentext Folgendes ein:

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

5. Geben Sie für Nachrichtengruppen-ID Folgendes ein: **`adsync.sync-from-ad`**
6. Geben Sie für Nachrichtendeduplizierungs-ID eine zufällige alphanumerische Zeichenfolge ein. Dieser Eintrag muss sich innerhalb von fünf Minuten von allen Aufrufen unterscheiden, sonst wird die Anforderung ignoriert.

Benutzer beim Erstellen einer Sitzung nicht verfügbar

Wenn Sie Administrator sind, der eine Sitzung erstellt, 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.

Größenbeschränkung überschritten Fehler 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 ldap-Suchergebnislimit Ihres IDP.

Hinweise

Jede Amazon EC2 EC2-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 Amazon EC2 EC2-Instances ohne RDP und ohne RDP-Lizenzen ermöglicht. Wenn zusätzliche Remote Desktop Services-Lizenzen benötigt werden, sollten Remote Desktop-Benutzer-CALs von Microsoft oder einem Microsoft-Lizenzhändler erworben werden. CALs für Remote-Desktop-Benutzer mit aktiver Software Assurance haben die Vorteile von License Mobility und können in AWS standardmäßige (gemeinsam genutzte) Mandantenumgebungen übertragen werden. Informationen zur Bereitstellung 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 The Apache Software Foundation erhältlich ist.

Revisionen

Weitere Informationen finden Sie in der Datei CHANGELOG.md im Repository. GitHub

Datum	Änderung
November 2023	Erstversion
Dezember 2023	GovCloud Wegbeschreibungen und Vorlagen hinzugefügt
Januar 2024	Version 2024.01 veröffentlichen
Februar 2024	Veröffentlichungsversion 2024.01.01 — aktualisierte Bereitstellungsvorlage
März 2024	Weitere Themen zur Problembehandlung, Aufbewahrung von CloudWatch Protokollen, Deinstallation von Nebenversionen
April 2024	Release-Version 2024.04 — RES-fähige AMIs und Vorlagen für den Projektstart
Juni 2024	• Veröffentlichungsversion 2024.06 — Ubuntu-Unterstützung, Rechte des Projektinhabers. • Benutzerhandbuch: hinzugefügt Erstellen Sie eine Demo-Umgebung

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.