aws

Guida per l'utente

Studio di ricerca e ingegneria

Studio di ricerca e ingegneria: Guida per l'utente

Table of Contents

Panoramica

Research and Engineering Studio (RES) è un prodotto open source AWS supportato che consente agli amministratori IT di fornire un portale web su cui scienziati e ingegneri possono eseguire carichi di lavoro di calcolo tecnico. AWS RES offre agli utenti un unico pannello di controllo per avviare desktop virtuali sicuri per condurre ricerche scientifiche, progettazione di prodotti, simulazioni ingegneristiche o carichi di lavoro di analisi dei dati. Gli utenti possono connettersi al portale RES utilizzando le proprie credenziali aziendali esistenti e lavorare su progetti individuali o collaborativi.

Gli amministratori possono creare spazi di collaborazione virtuali denominati progetti per un insieme specifico di utenti per accedere a risorse condivise e collaborare. Gli amministratori possono creare i propri stack di software applicativi (AMI) e consentire agli utenti RES di avviare desktop virtuali Windows o Linux e consentire l'accesso ai dati del progetto tramite file system condivisi. Gli amministratori possono assegnare stack software e file system e limitare l'accesso solo a quegli utenti del progetto. Gli amministratori possono utilizzare la telemetria integrata per monitorare l'utilizzo dell'ambiente e risolvere i problemi degli utenti. Possono anche impostare budget per singoli progetti per evitare un consumo eccessivo di risorse. Poiché il prodotto è open source, i clienti possono anche personalizzare l'esperienza utente del portale RES in base alle proprie esigenze.

RES è disponibile senza costi aggiuntivi e si pagano solo le AWS risorse necessarie per eseguire le applicazioni.

Questa guida fornisce una panoramica di Research and Engineering Studio on AWS, della sua architettura e dei suoi componenti di riferimento, considerazioni per la pianificazione della distribuzione e i passaggi di configurazione per la distribuzione di RES su Amazon Web Services (AWS) Cloud.

Funzionalità e vantaggi

Research and Engineering Studio on AWS offre le seguenti funzionalità:

Interfaccia utente basata sul Web

RES fornisce un portale basato sul Web che amministratori, ricercatori e ingegneri possono utilizzare per accedere e gestire i propri spazi di lavoro di ricerca e ingegneria. Gli scienziati e gli ingegneri non hanno bisogno di un'esperienza in ambito cloud Account AWS per utilizzare RES.

Configurazione basata su progetti

Utilizza i progetti per definire le autorizzazioni di accesso, allocare risorse e gestire i budget per una serie di attività o attività. Assegna stack software specifici (sistemi operativi e applicazioni approvate) e risorse di archiviazione a un progetto per garantire coerenza e conformità. Monitora e gestisci la spesa in base al progetto.

Strumenti di collaborazione

Scienziati e ingegneri possono invitare altri membri del loro progetto a collaborare con loro, impostando i livelli di autorizzazione che desiderano che i colleghi abbiano. Queste persone possono accedere a RES per connettersi a quei desktop.

Integrazione con l'infrastruttura di gestione delle identità esistente

Effettua l'integrazione con l'infrastruttura esistente di gestione delle identità e dei servizi di directory per consentire la connessione al portale RES con l'identità aziendale esistente di un utente e assegnare le autorizzazioni ai progetti utilizzando le appartenenze di utenti e gruppi esistenti.

Archiviazione persistente e accesso ai dati condivisi

Per fornire agli utenti l'accesso ai dati condivisi tra sessioni di desktop virtuali, connettiti ai file system esistenti o crea nuovi file system all'interno di RES. I servizi di storage supportati includono Amazon Elastic File System per desktop Linux e Amazon FSx NetApp per ONTAP per desktop Windows e Linux.

Monitoraggio e reportistica

Utilizza la dashboard di analisi per monitorare l'utilizzo delle risorse, ad esempio tipi di istanze, stack software e tipi di sistemi operativi. La dashboard fornisce anche una suddivisione dell'utilizzo delle risorse per progetto per la rendicontazione.

Gestione del budget e dei costi

Collegati Budget AWS ai tuoi progetti RES per monitorare i costi di ogni progetto. Se superi il budget, puoi limitare l'avvio delle sessioni VDI.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questo prodotto:

Browser di file

Un file browser è una parte dell'interfaccia utente RES in cui gli utenti attualmente connessi possono visualizzare il proprio file system.

File system

Il file system funge da contenitore per i dati del progetto (spesso denominati set di dati). Fornisce una soluzione di archiviazione entro i confini del progetto e migliora la collaborazione e il controllo dell'accesso ai dati.

Amministratore globale

Un delegato amministrativo con accesso alle risorse RES condivise in un ambiente RES. L'ambito e le autorizzazioni riguardano più progetti. Possono creare o modificare progetti e assegnare i proprietari dei progetti. Possono delegare o assegnare autorizzazioni ai proprietari e ai membri del progetto. A volte la stessa persona funge da amministratore RES a seconda delle dimensioni dell'organizzazione.

Progetto

Un progetto è una partizione logica all'interno dell'applicazione che funge da confine distinto per i dati e le risorse di elaborazione, garantendo la governance del flusso di dati e impedendo la condivisione di dati e host VDI tra progetti.

Autorizzazioni basate sul progetto

Le autorizzazioni basate sul progetto descrivono una partizione logica di dati e host VDI in un sistema in cui possono esistere più progetti. L'accesso di un utente ai dati e agli host VDI all'interno di un progetto è determinato dai ruoli associati. A un utente deve essere assegnato l'accesso (o l'appartenenza al progetto) per ogni progetto a cui richiede l'accesso. In caso contrario, un utente non sarà in grado di accedere ai dati del progetto e ai VDI se non gli è stata concessa l'iscrizione.

Membro del progetto

Un utente finale di risorse RES (VDI, storage, ecc.). L'ambito e le autorizzazioni sono limitati ai progetti a cui sono assegnati. Non possono delegare o assegnare alcuna autorizzazione.

Proprietario del progetto

Un delegato amministrativo con accesso e proprietà su un progetto specifico. L'ambito e le autorizzazioni sono limitati ai progetti di cui sono proprietari. Possono assegnare autorizzazioni ai membri del progetto nei progetti di loro proprietà.

Pila di software

Gli stack software sono Amazon Machine Images (AMI) con metadati specifici per RES basati su qualsiasi sistema operativo che un utente ha scelto di fornire per il proprio host VDI.

Host VDI

Gli host VDI (Virtual Desktop Instance) consentono ai membri del progetto di accedere a dati e ambienti di calcolo specifici del progetto, garantendo aree di lavoro sicure e isolate.

Per un riferimento generale dei AWS termini, consulta il AWS glossario nella Guida generale.AWS

Panoramica dell'architettura

Questa sezione fornisce un diagramma di architettura per i componenti distribuiti con questo prodotto.

Diagramma architetturale

La distribuzione di questo prodotto con i parametri predefiniti distribuisce i seguenti componenti nel tuo. Account AWS

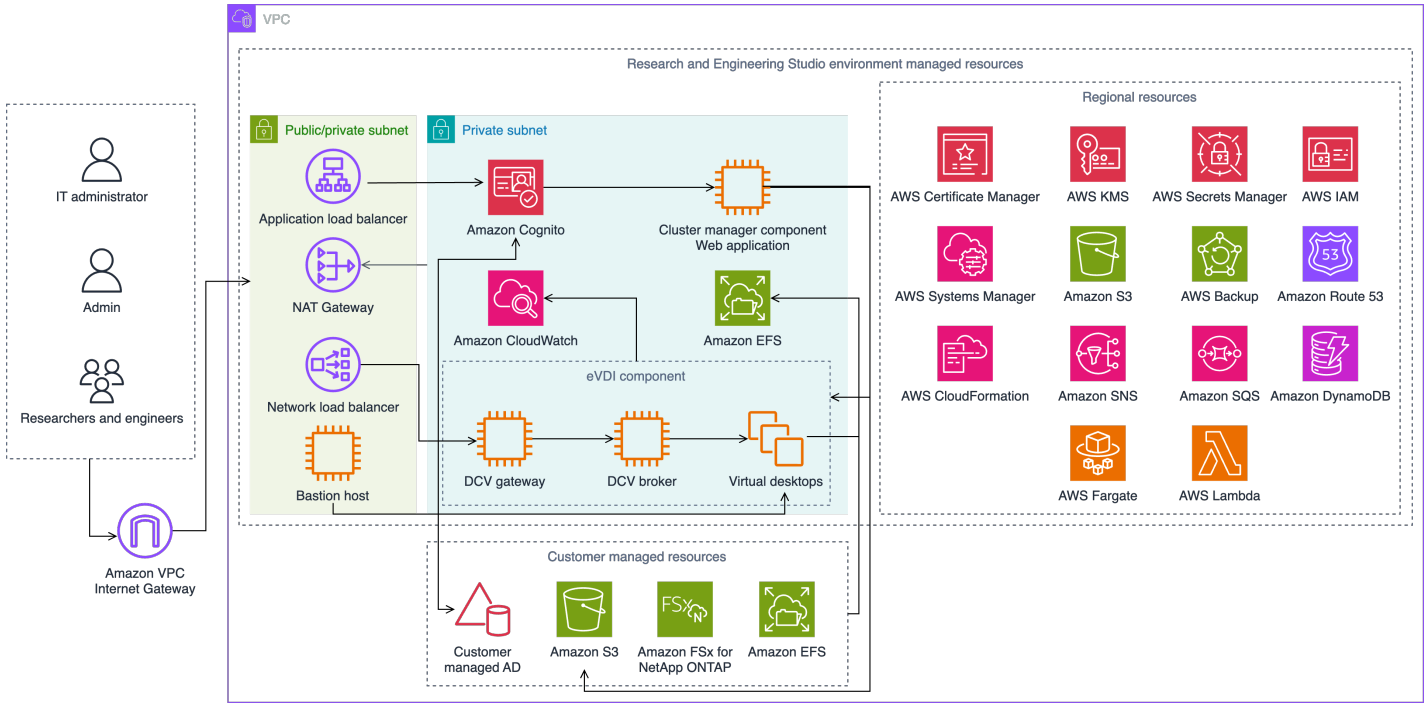


Figura 1: Studio di ricerca e ingegneria sull'AWSarchitettura

> **Note**
>
> AWS CloudFormationle risorse vengono create a partire da AWS Cloud Development Kit (AWS CDK) costrutti.

Il flusso di processo di alto livello per i componenti del prodotto distribuiti con il AWS CloudFormation modello è il seguente:

1. RES installa componenti per il portale web e:

a. Componente Engineering Virtual Desktop (eVDI) per carichi di lavoro interattivi

b. Componente metriche

   Amazon CloudWatch riceve i parametri dai componenti eVDI.

c. Componente Bastion Host

   Gli amministratori possono connettersi al componente bastion host utilizzando SSH per gestire l'infrastruttura sottostante.

2. RES installa componenti in sottoreti private dietro un gateway NAT. Gli amministratori accedono alle sottoreti private tramite l'Application Load Balancer (ALB) o il componente Bastion Host.
3. Amazon DynamoDB memorizza la configurazione dell'ambiente.
4. AWS Certificate Manager(ACM) genera e archivia un certificato pubblico per l'Application Load Balancer (ALB).

> **Note**
>
> Ti consigliamo di AWS Certificate Manager utilizzarlo per generare un certificato affidabile per il tuo dominio.

5. Amazon Elastic File System (EFS) ospita il `/home` file system predefinito montato su tutti gli host di infrastruttura applicabili e le sessioni eVDI Linux.
6. RES utilizza Amazon Cognito per creare un utente bootstrap iniziale chiamato clusteradmin e invia credenziali temporanee all'indirizzo e-mail fornito durante l'installazione. L'amministratore del cluster deve modificare la password al primo accesso.
7. Amazon Cognito si integra con Active Directory e con le identità degli utenti della tua organizzazione per la gestione delle autorizzazioni.
8. Le zone di sicurezza consentono agli amministratori di limitare l'accesso a componenti specifici del prodotto in base alle autorizzazioni.

AWSservizi inclusi in questo prodotto

Servizio AWS	Descrizione
Amazon Elastic Compute Cloud	Nucleo. Fornisce i servizi di elaborazione sottostanti per creare desktop virtuali con il sistema operativo e lo stack software scelti.
Elastic Load Balancing	Nucleo. Gli host Bastion, cluster-manager e VDI vengono creati nei gruppi di Auto Scaling dietro il sistema di bilanciamento del carico. ELB bilancia il traffico proveniente dal portale web tra gli host RES.
Amazon Virtual Private Cloud	Nucleo. Tutti i componenti principali del prodotto vengono creati all'interno del tuo VPC.
Amazon Cognito	Nucleo. Gestisce le identità e l'autenticazione degli utenti. Gli utenti di Active Directory vengono mappati su utenti e gruppi di Amazon Cognito per autenticare i livelli di accesso.
Amazon Elastic File System	Nucleo. Fornisce il `/home` file system per il browser di file e gli host VDI, nonché per i file system esterni condivisi.
Amazon DynamoDB	Nucleo. Memorizza dati di configurazione come utenti, gruppi, progetti, file system e impostazi oni dei componenti.
AWS Systems Manager	Nucleo. Memorizza i documenti per l'esecuzi one di comandi per la gestione delle sessioni VDI.
AWS Lambda	Nucleo. Supporta funzionalità del prodotto come l'aggiornamento delle impostazioni all'interno della tabella DynamoDB, l'avvio dei flussi di lavoro di sincronizzazione con Active

Servizio AWS	Descrizione
	Directory e l'aggiornamento dell'elenco dei prefissi.
Amazon CloudWatch	Supporto. Fornisce parametri e registri delle attività per tutti gli host Amazon EC2 e le funzioni Lambda.
Amazon Simple Storage Service	Supporto. Memorizza i file binari delle applicazioni per il bootstrap e la configurazione dell'host.
AWS Key Management Service	Supporto. Utilizzato per la crittografia a riposo con code Amazon SQS, tabelle DynamoDB e argomenti Amazon SNS.
AWS Secrets Manager	Supporto. Memorizza le credenziali degli account di servizio in Active Directory e i certificati autofirmati per VDI.
AWS CloudFormation	Supporto. Fornisce un meccanismo di distribuzione per il prodotto.
AWS Identity and Access Management	Supporto. Limita il livello di accesso per gli host.
Amazon Route 53	Supporto. Crea una zona ospitata privata per risolvere il load balancer interno e il nome di dominio dell'host bastion.
Amazon Simple Queue Service	Supporto. Crea code di attività per supportare esecuzioni asincrone.
Amazon Simple Notification Service	Supporto. Supporta il modello di abbonamento alla pubblicazione tra componenti VDI come il controller e gli host.
AWS Fargate	Supporto. Installa, aggiorna ed elimina gli ambienti utilizzando le attività di Fargate.

Servizio AWS	Descrizione
Gateway di file Amazon FSx	Facoltativo. Fornisce un file system condiviso esterno.
Amazon FSx per ONTAP NetApp	Facoltativo. Fornisce un file system condiviso esterno.
AWS Certificate Manager	Facoltativo. Genera un certificato affidabile per il tuo dominio personalizzato.
AWS Backup	Facoltativo. Offre funzionalità di backup per host Amazon EC2, file system e DynamoDB.

Crea un ambiente demo

Segui i passaggi di questa sezione per provare Research and Engineering Studio su. AWS Questa demo implementa un ambiente non di produzione con un set minimo di parametri utilizzando il modello di stack di ambiente AWS demo di Research and Engineering Studio. Utilizza un server Keycloak per SSO.

Tieni presente che dopo aver distribuito lo stack, devi seguire i passaggi riportati di Fasi successive alla distribuzione seguito per configurare gli utenti nell'ambiente prima di effettuare l'accesso.

Crea uno stack dimostrativo con un clic

Questo AWS CloudFormation stack crea tutti i componenti richiesti da Research and Engineering Studio.

Tempo di implementazione: ~90 minuti

Prerequisiti

Argomenti

- Crea un file Account AWS con un utente amministrativo
- Crea una coppia di chiavi SSH Amazon EC2
- Aumentare le quote di servizio

Crea un file Account AWS con un utente amministrativo

Devi avere un account Account AWS con un utente amministrativo:

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Crea una coppia di chiavi SSH Amazon EC2

Se non disponi di una coppia di chiavi SSH Amazon EC2, dovrai crearne una. Per ulteriori informazioni, consulta Create a key pair using Amazon EC2 nella Amazon EC2 User Guide.

Aumentare le quote di servizio

Consigliamo di aumentare le quote di servizio per:

- Amazon VPC
  - Aumenta la quota di indirizzi IP elastici per gateway NAT da cinque a otto
  - Aumentate il numero di gateway NAT per zona di disponibilità da cinque a dieci
- Amazon EC2
  - Aumentare gli IP elastici EC2-VPC da cinque a dieci

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate. Per ulteriori informazioni, consulta the section called “Quote per i AWS servizi relativi a questo prodotto”.

Crea risorse e parametri di input

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Assicurati di essere nel tuo account amministratore.

2. Avvia il modello nella console.
3. In Parametri, esamina i parametri di questo modello di prodotto e modificali se necessario.

Parametro	Predefinito	Descrizione
EnvironmentName	`< res-demo >`	Un nome univoco assegnato all'ambiente RES che inizia

Parametro	Predefinito	Descrizione
		con res- e non più lungo di 11 caratteri.
AdministratorEmail		L'indirizzo e-mail dell'utente che completa la configura zione del prodotto. Questo utente funge anche da utente inaffidabile in caso di errore di integrazione Single Sign-On con Active Directory.
KeyPair		La key pair utilizzata per connettersi agli host dell'infr astruttura.
ClientIPCIDR	<0.0.0.0/0>	Filtro per indirizzi IP che limita la connessione al sistema. È possibile aggiornare il file ClientIpCidr dopo la distribuzione.
InboundPrefixList		(Facoltativo) Fornisci un elenco di prefissi gestito per gli IP autorizzati ad accedere direttamente all'interfaccia utente Web e a SSH nell'host bastion.

Fasi successive alla distribuzione

1. Reimposta le password degli utenti`AWS Directory Service`: lo stack demo crea quattro utenti con nomi utente che puoi usare:`admin1`,`user1`, `admin2` e. `user2`

   a. Vai alla console Directory Service.

   b. Seleziona l'ID della directory per il tuo ambiente. È possibile ottenere l'ID della directory dall'output dello `<StackName>*DirectoryService*` stack.
   c. Dal menu a discesa Azione in alto a destra, seleziona Reimposta la password dell'utente.
   d. Per tutti gli utenti che desideri utilizzare, inserisci il nome utente e digita la password che desideri avere e seleziona Reimposta password.
2. Dopo aver reimpostato le password degli utenti, dovrai attendere che Research and Engineering Studio sincronizzi gli utenti nell'ambiente. Research and Engineering Studio sincronizza gli utenti ogni ora alle xx.00. Puoi attendere che ciò accada o seguire i passaggi elencati in Utente aggiunto in Active Directory, ma mancante in RES per sincronizzare immediatamente gli utenti.

La tua implementazione è ora pronta. Usa EnvironmentUrl quello che hai ricevuto nell'e-mail per accedere all'interfaccia utente oppure puoi anche ottenere lo stesso URL dall'output dello stack distribuito. Ora puoi accedere all'ambiente Research and Engineering Studio con l'utente e la password per cui hai reimpostato la password in Active Directory.

Pianifica la tua implementazione

Costo

Research and Engineering Studio on AWS è disponibile senza costi aggiuntivi e si pagano solo le risorse necessarie per eseguire le applicazioni. AWS Per ulteriori informazioni, consulta AWSservizi inclusi in questo prodotto.

> **Note**
>
> L'utente è responsabile del costo dei AWS servizi utilizzati durante l'esecuzione di questo prodotto.
> Ti consigliamo di creare un budget AWS Cost Explorerper aiutarti a gestire i costi. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi di ogni AWS servizio utilizzato in questo prodotto.

Sicurezza

Quando crei sistemi sull' AWS infrastruttura, le responsabilità in materia di sicurezza vengono condivise tra te e AWS te. Questo modello di responsabilità condivisa riduce il carico operativo perché AWS gestisce, gestisce e controlla i componenti, tra cui il sistema operativo host, il livello di virtualizzazione e la sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla AWS sicurezza, visita Cloud AWS Sicurezza.

Ruoli IAM

AWS Identity and Access Management I ruoli (IAM) consentono ai clienti di assegnare policy e autorizzazioni di accesso granulari a servizi e utenti su. Cloud AWS Questo prodotto crea ruoli IAM che garantiscono alle AWS Lambda funzioni del prodotto e alle istanze Amazon EC2 l'accesso per creare risorse regionali.

RES supporta politiche basate sull'identità all'interno di IAM. Una volta implementato, RES crea politiche per definire l'autorizzazione e l'accesso dell'amministratore. L'amministratore che implementa il prodotto crea e gestisce gli utenti finali e i responsabili di progetto all'interno del cliente esistente Active Directory integrato con RES. Per ulteriori informazioni, consulta Creating IAM policies nella AWS Identity and Access Management User Guide.

L'amministratore dell'organizzazione può gestire l'accesso degli utenti con una directory attiva. Quando gli utenti finali accedono all'interfaccia utente RES, RES si autentica con Amazon Cognito.

Gruppi di sicurezza

I gruppi di sicurezza creati in questo prodotto sono progettati per controllare e isolare il traffico di rete tra le funzioni Lambda, le istanze EC2, le istanze CSR dei file system e gli endpoint VPN remoti. Ti consigliamo di esaminare i gruppi di sicurezza e di limitare ulteriormente l'accesso, se necessario, una volta distribuito il prodotto.

Crittografia dei dati

Per impostazione predefinita, Research and Engineering Studio on AWS (RES) crittografa i dati dei clienti inattivi e in transito utilizzando una chiave di proprietà di RES. Quando si implementa RES, è possibile specificare un. AWS KMS key RES utilizza le tue credenziali per concedere l'accesso alle chiavi. Se fornite la proprietà e la gestione di un cliente AWS KMS key, i dati inattivi del cliente verranno crittografati utilizzando tale chiave.

RES crittografa i dati dei clienti in transito utilizzando SSL/TLS. Richiediamo TLS 1.2, ma consigliamo TLS 1.3.

Supportato Regioni AWS

Questo prodotto utilizza servizi che al momento non sono tutti disponibili Regioni AWS. È necessario avviare questo prodotto in un Regione AWS luogo in cui tutti i servizi siano disponibili. Per la disponibilità più aggiornata dei AWS servizi per regione, consulta l'elenco di Regione AWS tutti i servizi.

Research and Engineering Studio on AWS è supportato nei seguenti casi Regioni AWS:

Nome Regione	
Stati Uniti orientali (Ohio)	Canada (Centrale)
Stati Uniti orientali (Virginia settentrionale)	Europa (Francoforte)
Stati Uniti occidentali (California settentrionale)	Europa (Irlanda)
US West (Oregon)	Europa (Londra)

Nome Regione	
Asia Pacifico (Mumbai)	Europa (Milano)
Asia Pacifico (Seoul)	Europa (Parigi)
Asia Pacifico (Singapore)	Israele (Tel Aviv)
Asia Pacifico (Sydney)	AWS GovCloud (Stati Uniti occidentali)
Asia Pacifico (Tokyo)	

Quote

Le service quotas (o quote di servizio), a cui si fa riferimento anche come limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l' Account AWS.

Quote per i AWS servizi relativi a questo prodotto

Assicurati di disporre di una quota sufficiente per ciascuno dei servizi implementati in questo prodotto. Per ulteriori informazioni, consulta Service Quotas di AWS.

Per questo prodotto, consigliamo di aumentare le quote per i seguenti servizi:

- Amazon Virtual Private Cloud
- Amazon EC2

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di incremento dei limiti.

AWS CloudFormation quote

Hai delle AWS CloudFormation quote di cui dovresti essere a conoscenza quando avvii lo stack di questo prodotto. Account AWS Comprendendo queste quote, è possibile evitare errori di limitazione che impedirebbero di implementare correttamente questo prodotto. Per ulteriori informazioni, consulta le AWS CloudFormation quote nella Guida per l'AWS CloudFormation utente.

Pianificazione della resilienza

Il prodotto implementa un'infrastruttura predefinita con il numero e la dimensione minimi di istanze Amazon EC2 per far funzionare il sistema. Per migliorare la resilienza negli ambienti di produzione su larga scala, consigliamo di aumentare le impostazioni di capacità minima predefinite all'interno dei gruppi di Auto Scaling (ASG) dell'infrastruttura. L'aumento del valore da un'istanza a due istanze offre il vantaggio di più zone di disponibilità (AZ) e riduce il tempo necessario per ripristinare la funzionalità del sistema in caso di perdita imprevista dei dati.

Le impostazioni ASG possono essere personalizzate all'interno della console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/. Per impostazione predefinita, il prodotto crea quattro ASG con ogni nome che termina con. `-asg` È possibile modificare i valori minimi e desiderati impostando un valore appropriato per l'ambiente di produzione. Scegliete il gruppo che desiderate modificare, quindi scegliete Azioni e Modifica. Per ulteriori informazioni sugli ASG, consulta Ridimensionare le dimensioni del gruppo Auto Scaling nella Guida per l'utente di Amazon EC2 Auto Scaling.

Implementa il prodotto

> **Note**
>
> Questo prodotto utilizza AWS CloudFormation modelli e stack per automatizzarne l'implementazione. I CloudFormation modelli descrivono le AWS risorse incluse in questo prodotto e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nei modelli.

Prima di lanciare il prodotto, esaminate i costi, l'architettura, la sicurezza di rete e altre considerazioni discusse in precedenza in questa guida.

Argomenti

Prerequisiti

Argomenti

Crea un messaggio Account AWS con un utente amministrativo

È necessario disporre di un account Account AWS con un utente amministrativo:

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Crea una coppia di chiavi SSH Amazon EC2

Se non disponi di una coppia di chiavi SSH Amazon EC2, dovrai crearne una. Per ulteriori informazioni, consulta Create a key pair using Amazon EC2 nella Amazon EC2 User Guide.

Aumentare le quote di servizio

Consigliamo di aumentare le quote di servizio per:

- Amazon VPC
  - Aumentare la quota di indirizzi IP elastici per gateway NAT da cinque a otto
  - Aumentate il numero di gateway NAT per zona di disponibilità da cinque a dieci
- Amazon EC2
  - Aumentare gli IP elastici EC2-VPC da cinque a dieci

Il tuo AWS account ha delle quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate. Per ulteriori informazioni, consulta the section called “Quote per i AWS servizi relativi a questo prodotto”.

Crea un dominio pubblico (opzionale)

Ti consigliamo di utilizzare un dominio personalizzato per il prodotto in modo da avere un URL intuitivo. Dovrai registrare un dominio utilizzando Amazon Route 53 o un altro provider e importare un certificato per il dominio che utilizza AWS Certificate Manager. Se disponi già di un dominio pubblico e di un certificato, puoi saltare questo passaggio.

1. Segui le istruzioni per registrare un dominio con Route53. Dovresti ricevere un'email di conferma.
2. Recupera la zona ospitata per il tuo dominio. Questa viene creata automaticamente da Route53.
    a. Apri la console Route53.
    b. Scegli Zone ospitate dalla barra di navigazione a sinistra.
    c. Apri la zona ospitata creata per il tuo nome di dominio e copia l'ID della zona ospitata.
3. Apri AWS Certificate Manager e segui questi passaggi per richiedere un certificato di dominio. Assicurati di trovarti nella regione in cui intendi implementare la soluzione.
4. Scegli Elenca certificati dalla navigazione e trova la tua richiesta di certificato. La richiesta dovrebbe essere in sospeso.
5. Scegli l'ID del certificato per aprire la richiesta.
6. Dalla sezione Domini, scegli Crea record in Route53. L'elaborazione della richiesta richiederà circa dieci minuti.
7. Una volta emesso il certificato, copia l'ARN dalla sezione Stato del certificato.

Crea dominio (GovCloud solo)

Se effettui la distribuzione nella regione AWS GovCloud (Stati Uniti occidentali), dovrai completare questi passaggi preliminari.

1. Distribuisci lo AWS CloudFormation stack di certificati nell' AWS account con partizione commerciale in cui è stato creato il dominio ospitato pubblico.
2. Dai Certificate CloudFormation Outputs, trova e annota il simbolo e. `CertificateARN` `PrivateKeySecretARN`
3. Nell'account della GovCloud partizione, crea un segreto con il valore dell'`CertificateARN`output. Nota il nuovo ARN segreto e aggiungi due tag al segreto in modo da `vdc-gateway` poter accedere al valore segreto:
    a. res: = ModuleName virtual-desktop-controller

b. res: EnvironmentName = [nome dell'ambiente] (potrebbe essere res-demo.)

4. Nell'account della GovCloud partizione, crea un segreto con il valore dell'output. `PrivateKeySecretArn` Nota il nuovo ARN segreto e aggiungi due tag al segreto in modo da `vdc-gateway` poter accedere al valore segreto:

   a. res: = ModuleName virtual-desktop-controller

   b. res: EnvironmentName = [nome dell'ambiente] (potrebbe essere res-demo.)

Fornisci risorse esterne

Quando installi Research and Engineering Studio su AWS, il prodotto utilizzerà risorse esterne di cui avrai bisogno. RES si aspetta che tali risorse esistano al momento dell'implementazione.

- Rete (VPC, sottoreti pubbliche e private)

  Qui verranno eseguite le istanze EC2 utilizzate per ospitare l'ambiente, Active Directory (AD) e lo storage condiviso.

- Archiviazione (Amazon EFS)

  I volumi di storage contengono i file e i dati necessari per l'infrastruttura desktop virtuale (VDI).

- Servizio di directory ()AWS Directory Service for Microsoft Active Directory

  Il servizio di directory autentica gli utenti nelle pagine di ambiente.

- Un segreto che contiene la password dell'account del servizio

  Research and Engineering Studio accede ai segreti forniti dall'utente, inclusa la password dell'account del servizio, utilizzando AWS Secrets Manager.

> **Tip**
>
> Se stai implementando un ambiente demo e non disponi di queste risorse esterne, puoi utilizzare le ricette AWS High Performance Compute per generare le risorse esterne. Consulta la sezione seguente per distribuire Crea risorse esterne le risorse nel tuo account. Per le distribuzioni dimostrative nella regione AWS GovCloud (Stati Uniti occidentali), dovrai completare i passaggi preliminari indicati in. Crea dominio (GovCloud solo)

Configura LDAPS nel tuo ambiente (opzionale)

Se si prevede di utilizzare la comunicazione LDAPS nel proprio ambiente, è necessario completare questi passaggi per creare e allegare certificati al controller di dominio AWS Managed Microsoft AD (AD) per fornire la comunicazione tra AD e RES.

1. Segui i passaggi forniti in Come abilitare LDAPS lato server per il tuo. AWS Managed Microsoft AD Puoi saltare questo passaggio se hai già abilitato LDAPS.
2. Dopo aver verificato che LDAPS è configurato su AD, esporta il certificato AD:

   a. Vai al tuo server Active Directory.

   b. Apri PowerShell come amministratore.

   c. Esegui `certmgr.msc` per aprire l'elenco dei certificati.

   d. Apri l'elenco dei certificati aprendo prima Trusted Root Certification Authorities e poi Certificati.

   e. Seleziona e tieni premuto (o fai clic con il pulsante destro del mouse) sul certificato con lo stesso nome del server AD e scegli Tutte le attività, quindi Esporta.

   f. Scegli X.509 con codifica Base-64 (.CER) e scegli Avanti.

   g. Seleziona una directory, quindi scegli Avanti.
3. Crea un segreto in AWS Secrets Manager:

   Quando crei il tuo segreto nel Secrets Manager, seleziona Other type of secrets (Altro tipo di segreti) in secret type (Tipo di segreto) e incolla il certificato codificato PEM nel campo Plaintext (Testo normale).
4. Annotate l'ARN creato e inseritelo come `DomainTLSCertificateSecretARN` parametro in. the section called “Fase 1: Avviare il prodotto”

Configurazione di un VPC privato (opzionale)

L'implementazione di Research and Engineering Studio in un VPC isolato offre una maggiore sicurezza per soddisfare i requisiti di conformità e governance dell'organizzazione. Tuttavia, l'implementazione standard di RES si basa sull'accesso a Internet per l'installazione delle dipendenze. Per installare RES in un VPC privato, è necessario soddisfare i seguenti prerequisiti:

Argomenti

- Preparazione di Amazon Machine Images (AMI)

- Configurazione degli endpoint VPC
- Connect ai servizi senza endpoint VPC
- Imposta i parametri di distribuzione di un VPC privato

Preparazione di Amazon Machine Images (AMI)

1. Scarica le dipendenze. Per l'implementazione in un VPC isolato, l'infrastruttura RES richiede la disponibilità di dipendenze senza l'accesso pubblico a Internet.
2. Crea un ruolo IAM con accesso in sola lettura e identità affidabile di Amazon S3 come Amazon EC2.

    a. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.

    b. Da Ruoli, scegli Crea ruolo.

    c. Nella pagina Seleziona entità attendibile:

    - In Tipo di entità affidabile, scegli Servizio AWS.
    - Per Caso d'uso in Servizio o caso d'uso, seleziona EC2 e scegli Avanti.

    d. In Aggiungi autorizzazioni, seleziona le seguenti politiche di autorizzazione, quindi scegli Avanti:

    - Amazon S3 ReadOnlyAccess
    - Amazon SSM ManagedInstanceCore
    - EC2 InstanceProfileForImageBuilder

    e. Aggiungi un nome e una descrizione del ruolo, quindi scegli Crea ruolo.
3. Crea il componente EC2 image builder:

    a. Apri la console EC2 Image Builder https://console.aws.amazon.com/imagebuilder all'indirizzo.

    b. In Risorse salvate, scegli Componenti e scegli Crea componente.

    c. Nella pagina Crea componente, inserisci i seguenti dettagli:

    - Per Tipo di componente, scegli Costruisci.
    - Per i dettagli del componente, scegli:

Parametro	Inserimento utente
Sistema operativo (OS) di immagine	Linux
Versioni del sistema operativo compatibili	Amazon Linux 2
Nome componente	Scegli un nome come: *< research-and-engineering-studio - infrastructure>*
Versione del componente	Consigliamo di iniziare con 1.0.0.
Descrizione	Inserimento utente opzionale.

d. Nella pagina Crea componente, scegli Definisci il contenuto del documento.

i. Prima di inserire il contenuto del documento di definizione, è necessario un URI del file per il file tar.gz. Carica il file tar.gz fornito da RES in un bucket Amazon S3 e copia l'URI del file dalle proprietà del bucket.

ii. Immetti i seguenti dati:

> **Note**
>
> `AddEnvironmentVariables`è facoltativo e puoi rimuoverlo se non hai bisogno di variabili di ambiente personalizzate negli host dell'infrastruttura. Se si stanno `http_proxy` configurando variabili di `https_proxy` ambiente, i `no_proxy` parametri sono necessari per impedire all'istanza di utilizzare il proxy per interrogare localhost, gli indirizzi IP dei metadati dell'istanza e i servizi che supportano gli endpoint VPC.

```
#  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. Scegli Crea componente.

4. Crea una ricetta di immagini Image Builder.

   a. Nella pagina Crea ricetta, inserisci quanto segue:

Sezione	Parametro	Inserimento utente
Dettagli della ricetta	Nome	Immettete un nome appropriato, ad esempio res-recipe-linux-x 86.
	Versione	Immettete una versione, che in genere inizia con 1.0.0.
	Descrizione	Aggiungi una descrizione opzionale.
Immagine di base	Seleziona l'immagine	Seleziona immagini gestite.
	SISTEMA OPERATIVO	Amazon Linux
	Origine dell'immagine	Avvio rapido (gestito da Amazon)
	Nome dell'immagine	Amazon Linux 2 x86
	Opzioni di controllo automatico delle versioni	Usa l'ultima versione del sistema operativo disponibile.
Configurazione dell'istanza	–	Mantieni tutto nelle impostazioni predefinite e assicurati che Rimuovi l'agente SSM dopo l'esecuzione della pipeline non sia selezionato.
Directory di lavoro	Percorso della directory di lavoro	/root/bootstrap/res_dependencies

Sezione	Parametro	Inserimento utente
Componenti	Costruisci componenti	Cerca e seleziona quanto segue: • Gestito da Amazon: -2-linux aws-cli-version • Gestito da Amazon: amazon-cloudwatch-agent-linux • Di tua proprietà: componente Amazon EC2 creato in precedenz a. Inserisci il tuo Account AWS ID e la tua corrente Regione AWS nei campi.
	Componenti di test	Cerca e seleziona: • Gestito da Amazon: simple-boot-test-linux

b. Scegli Crea ricetta.

5. Crea la configurazione dell'infrastruttura Image Builder.

a. In Risorse salvate, scegli Configurazioni dell'infrastruttura.

b. Scegli Crea configurazione dell'infrastruttura.

c. Nella pagina Crea configurazione dell'infrastruttura, inserisci quanto segue:

Sezione	Parametro	Inserimento utente
Generale	Nome	Immettere un nome appropriato, ad esempio res-infra-linux-x 86.
	Descrizione	Aggiungi una descrizione opzionale.

Sezione	Parametro	Inserimento utente
	Ruolo IAM	Seleziona il ruolo IAM creato in precedenza.
AWS infrastruttura	Tipo di istanza	Scegli t3.medium.

	VPC, sottorete e gruppi di sicurezza	Seleziona un'opzione che consenta l'accesso a Internet e al bucket Amazon S3. Se devi creare un gruppo di sicurezza , puoi crearne uno dalla console Amazon EC2 con i seguenti input:
		• VPC: seleziona lo stesso VPC utilizzato per la configurazione dell'infr astruttura. Questo VPC deve avere accesso a Internet.
		• Regola in entrata:
		  • Tipo: SSH
		  • Source (Origine): personalizzata
		  • Blocco CIDR: 0.0.0.0/0

d. Scegli Crea configurazione dell'infrastruttura.

6. Crea una nuova pipeline EC2 Image Builder:

a. Vai a Image pipelines e scegli Crea pipeline di immagini.

b. Nella pagina Specificare i dettagli della pipeline, immettete quanto segue e scegliete Avanti:

- Nome della tubazione e descrizione opzionale
- Per Programma di costruzione, imposta un programma o scegli Manuale se desideri avviare manualmente il processo di cottura AMI.

c. Nella pagina Scegli la ricetta, scegli Usa ricetta esistente e inserisci il nome della ricetta creato in precedenza. Seleziona Successivo.

d. Nella pagina Definisci il processo dell'immagine, seleziona i flussi di lavoro predefiniti e scegli Avanti.

e. Nella pagina Definisci la configurazione dell'infrastruttura, scegli Usa la configurazione dell'infrastruttura esistente e inserisci il nome della configurazione dell'infrastruttura creata in precedenza. Seleziona Successivo.

f. Nella pagina Definisci le impostazioni di distribuzione, considera quanto segue per le tue selezioni:

- L'immagine di output deve risiedere nella stessa regione dell'ambiente RES distribuito, in modo che RES possa avviare correttamente le istanze host dell'infrastruttura da essa. Utilizzando le impostazioni predefinite del servizio, l'immagine di output verrà creata nella regione in cui viene utilizzato il servizio EC2 Image Builder.
- Se desideri implementare RES in più regioni, puoi scegliere Crea nuove impostazioni di distribuzione e aggiungervi altre regioni.

g. Controlla le tue selezioni e scegli Crea pipeline.

7. Esegui la pipeline EC2 Image Builder:

a. Da Image pipelines, trova e seleziona la pipeline che hai creato.

b. Scegli Azioni e scegli Esegui pipeline.

La pipeline può impiegare da 45 minuti a un'ora per creare un'immagine AMI.

8. Annota l'ID AMI per l'AMI generato e usalo come input per il parametro InfrastructureHost AMI inthe section called “Fase 1: Avviare il prodotto”.

Configurazione degli endpoint VPC

Per implementare RES e avviare desktop virtuali, Servizi AWS richiedi l'accesso alla tua sottorete privata. È necessario configurare gli endpoint VPC per fornire l'accesso richiesto e sarà necessario ripetere questi passaggi per ogni endpoint.

1. Se gli endpoint non sono stati configurati in precedenza, segui le istruzioni fornite in Accesso e Servizio AWS utilizzo di un endpoint VPC di interfaccia.
2. Seleziona una sottorete privata in ciascuna delle due zone di disponibilità.

Servizio AWS	Nome servizio
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*.cloudformation
Amazon CloudWatch	com.amazonaws.*region*.monitoring
CloudWatch Registri Amazon	com.amazonaws.*region*.logs
Amazon DynamoDB	com.amazonaws. *region* .dynamodb (richiede un endpoint gateway)
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
Flusso di dati Amazon Kinesis	com.amazonaws.*region*.kinesis-streams
Amazon S3	com.amazonaws. *region* .s3 (richiede un endpoint gateway creato per impostazione predefinita in RES).
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
Amazon SES	com.amazonaws. *region* .email-smtp (non supportato nelle seguenti zone di disponibilità: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 e cac1-az4.)

Servizio AWS	Nome servizio
AWS Security Token Service	com.amazonaws.*region*.sts
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssmmessages

Connect ai servizi senza endpoint VPC

Per l'integrazione con servizi che non supportano gli endpoint VPC, puoi configurare un server proxy in una sottorete pubblica del tuo VPC. Segui questi passaggi per creare un server proxy con l'accesso minimo necessario per una distribuzione di Research and Engineering Studio utilizzando AWS Identity Center come provider di identità.

1. Avvia un'istanza Linux nella sottorete pubblica del VPC che utilizzerai per la distribuzione RES.
   - Famiglia Linux: Amazon Linux 2 o Amazon Linux 3
   - Architettura: x86
   - Tipo di istanza: t2.micro o versione successiva
   - Gruppo di sicurezza: TCP sulla porta 3128 da 0.0.0.0/0
2. Connect all'istanza per configurare un server proxy.
   a. Apri la connessione http.
   b. Consenti la connessione ai seguenti domini da tutte le sottoreti pertinenti:
      - .amazonaws.com (per servizi generici) AWS
      - .amazoncognito.com (per Amazon Cognito)
      - .awsapps.com (per Identity Center)
      - .signin.aws (per Identity Center)
      - . amazonaws-us-gov.com (per Gov Cloud)

c. Nega tutte le altre connessioni.

d. Attiva e avvia il server proxy.

e. Annota la PORTA su cui il server proxy ascolta.

3. Configura la tabella delle rotte per consentire l'accesso al server proxy.

   a. Vai alla tua console VPC e identifica le tabelle di routing per le sottoreti che utilizzerai per gli host dell'infrastruttura e gli host VDI.

   b. Modifica la tabella di routing per consentire a tutte le connessioni in entrata di accedere all'istanza del server proxy creata nei passaggi precedenti.

   c. Fate questa operazione per le tabelle di routing per tutte le sottoreti (senza accesso a Internet) che intendete utilizzare per l'infrastruttura/VDI.

4. Modifica il gruppo di sicurezza dell'istanza EC2 del server proxy e assicurati che consenta le connessioni TCP in entrata sulla PORTA su cui il server proxy è in ascolto.

Imposta i parametri di distribuzione di un VPC privato

Inthe section called “Fase 1: Avviare il prodotto”, è necessario inserire determinati parametri nel AWS CloudFormation modello. Assicurati di impostare i seguenti parametri come indicato per una corretta implementazione nel VPC privato che hai appena configurato.

Parametro	Input
InfrastructureHostAMI	Utilizza l'ID AMI dell'infrastruttura creato inthe section called “Preparazione di Amazon Machine Images (AMI)”.
IsLoadBalancerInternetFacing	Impostato su false.
LoadBalancerSubnets	Scegli sottoreti private senza accesso a Internet.
InfrastructureHostSubnets	Scegli sottoreti private senza accesso a Internet.
VdiSubnets	Scegli sottoreti private senza accesso a Internet.

Parametro	Input
ClientIP	Puoi scegliere il tuo VPC CIDR per consentire l'accesso a tutti gli indirizzi IP VPC.

Crea risorse esterne

Questo CloudFormation stack crea certificati di rete, di archiviazione, di Active Directory e di dominio (se PortalDomainName viene fornito un). È necessario disporre di queste risorse esterne per distribuire il prodotto.

È possibile scaricare il modello di ricette prima della distribuzione.

Tempo di implementazione: circa 40-90 minuti

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Assicurati di essere nel tuo account amministratore.

2. Avvia il modello nella console.

   Se stai distribuendo nella regione AWS GovCloud (Stati Uniti occidentali), avvia il modello nell'account di GovCloud partizione.

3. Immettete i parametri del modello:

Parametro	Predefinito	Descrizione
DomainName	`corp.res.com`	Dominio utilizzato per Active Directory. Il valore predefinito viene fornito nel `LDIF` file che configura gli utenti bootstrap. Se desideri utilizzare gli utenti predefiniti, lascia il valore come predefinito. Per modificare

Parametro	Predefinito	Descrizione
		il valore, aggiorna e fornisci un `LDIF` file separato. Non è necessario che corrispon da al dominio utilizzato per Active Directory.
SubDomain (GovCloud solo)		Questo parametro è facoltati vo per le regioni commercia li, ma obbligatorio per GovCloud le regioni. Se fornisci un SubDomain, il parametro avrà il prefisso DomainName fornito. Il nome di dominio Active Directory fornito diventerà un sottodominio.
AdminPassword		La password per l'amminis tratore di Active Directory (nome utente`Admin`). Questo utente viene creato in Active Directory per la fase iniziale di bootstrap e non viene utilizzato dopo. Nota: la password per questo utente deve soddisfare i requisiti di complessità della password per Active Directory.

Parametro	Predefinito	Descrizione
ServiceAccountPassword		Password utilizzata per creare un account di servizio (`ReadOnlyUser `). Questo account viene utilizzato per la sincronizzazione. Importante: a partire dalla versione 2024.06 di Research and Engineering Studio è necessario fornire un ARN segreto che contenga la password in chiaro per. ServiceAccount Nota: la password per questo utente deve soddisfare i requisiti di complessità della password per Active Directory.
Coppia di chiavi		Connette le istanze amministrative utilizzando un client SSH. Nota:AWS Systems Manager Session Manager può essere utilizzato anche per connettersi alle istanze.

Parametro	Predefinito	Descrizione
LDIFS3Path	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	Il percorso Amazon S3 di un file LDIF importato durante la fase di avvio della configurazione di Active Directory. Per ulteriori informazioni, vedere LDIF Support. Il parametro viene precompilato con un file che crea un numero di utenti in Active Directory. Per visualizzare il file, consultate il file res.ldif disponibile in. GitHub
ClientIpCidr		L'indirizzo IP da cui accederai al sito. Ad esempio, puoi selezionare il tuo indirizzo IP e `[IPADDRESS]/32` utilizzarlo per consentire l'accesso solo dal tuo host. È possibile aggiornarlo dopo la distribuzione.
ClientPrefixList		Immettere un elenco di prefissi per fornire l'accesso ai nodi di gestione di Active Directory. Per informazioni sulla creazione di un elenco di prefissi gestiti, consulta Utilizzare gli elenchi di prefissi gestiti dal cliente.

Parametro	Predefinito	Descrizione
EnvironmentName	`res-[environment name]`	Se fornito, questo parametro `PortalDomainName` viene utilizzato per aggiungere tag ai segreti generati in modo che possano essere utilizzati all'interno dell'ambiente. Questo deve corrispondere al `EnvironmentName` parametro utilizzato durante la creazione dello stack RES. Se stai implementando più ambienti nel tuo account, questo dovrà essere unico.
PortalDomainName		Per le GovCloud distribuzioni, non inserire questo parametro. I certificati e i segreti sono stati creati manualmente durante i prerequisiti. Il nome di dominio in Amazon Route 53 per l'account. Se viene fornito, verranno generati e caricati un certificato pubblico e un file chiave AWS Secrets Manager. Se hai il tuo dominio e i tuoi certificati, questo parametro `EnvironmentName` può essere lasciato vuoto.

4. Riconosci tutte le caselle di controllo in Capacità e scegli Crea stack.

Fase 1: Avviare il prodotto

Segui le step-by-step istruzioni in questa sezione per configurare e distribuire il prodotto nel tuo account.

Tempo di implementazione: circa 60 minuti

È possibile scaricare il CloudFormation modello per questo prodotto prima di distribuirlo.

Se stai distribuendo in AWS GovCloud (Stati Uniti occidentali), usa questo modello.

res-stack: utilizza questo modello per avviare il prodotto e tutti i componenti associati. La configurazione predefinita implementa lo stack principale RES e le risorse di autenticazione, frontend e backend.

> **Note**
>
> AWS CloudFormation le risorse vengono create da AWS Cloud Development Kit (AWS CDK) costrutti ().AWS CDK

Il AWS CloudFormation modello implementa Research and Engineering Studio AWS in. Cloud AWSÈ necessario soddisfare i prerequisiti prima di avviare lo stack.

1. Accedi AWS Management Console e apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Avvia il modello.

   Per implementarlo in AWS GovCloud (Stati Uniti occidentali), avvia questo modello.
3. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare la soluzione in un'altra Regione AWS, utilizza il selettore della regione nella barra di navigazione della console.

   > **Note**
   >
   > Questo prodotto utilizza il servizio Amazon Cognito, che al momento non è disponibile in tutti. Regioni AWSÈ necessario avviare questo prodotto in un Regione AWS luogo in cui Amazon Cognito è disponibile. Per la disponibilità più aggiornata per regione, consulta l'elenco di Regione AWS tutti i servizi.

4. In Parametri, esamina i parametri per questo modello di prodotto e modificali se necessario. Se hai distribuito risorse esterne automatizzate, puoi trovare questi parametri nella scheda Output dello stack di risorse esterne.

Parametro	Predefinito	Descrizione
EnvironmentName	*< res-demo >*	Un nome univoco assegnato all'ambiente RES che inizia con res- e non più lungo di 11 caratteri.
AdministratorEmail		L'indirizzo e-mail dell'utente che completa la configura zione del prodotto. Questo utente funge anche da utente Break-Glass in caso di errore di integrazione Single Sign-On di Active Directory.
InfrastructureHostAMI	ami- *[solo numeri o lettere]*	(Facoltativo) È possibile fornire un ID AMI personali zzato da utilizzare per tutti gli host dell'infrastruttura. Il sistema operativo di base attualmente supportato è Amazon Linux 2. Per ulteriori informazioni, consulta Configurazione delle AMI pronte per RESS.
SSH KeyPair		La key pair utilizzata per connettersi agli host dell'infr astruttura.

Parametro	Predefinito	Descrizione
ClientIP	*x.x.x .0/24 o x.x.x .0/32*	Filtro per indirizzi IP che limita la connessione al sistema. È possibile aggiornare il file ClientIpCidr dopo la distribuzione.
ClientPrefixList		(Facoltativo) Fornisci un elenco di prefissi gestito per gli IP autorizzati ad accedere direttamente all'interfaccia utente Web e a SSH nell'host bastion.
IAM PermissionBoundary		(Facoltativo) È possibile fornire un ARN di policy gestito che verrà allegato come limite di autorizza zione a tutti i ruoli creati in RES. Per ulteriori informazi oni, consulta Impostazione di limiti di autorizzazione personalizzati.
VpcId		IP per il VPC in cui verranno avviate le istanze.
IsLoadBalancerInternetFacin g		Seleziona true per implement are il sistema di bilanciam ento del carico con accesso a Internet (richiede sottoreti pubbliche per il bilanciam ento del carico). Per le distribuzioni che richiedon o un accesso limitato a Internet, seleziona false.

Parametro	Predefinito	Descrizione
LoadBalancerSubnets		Seleziona almeno due sottoreti in diverse zone di disponibilità in cui verranno avviati i sistemi di bilanciam ento del carico. Per le implementazioni che richiedono un accesso limitato a Internet, scegli sottoreti private. Per le implementazioni che richiedono l'accesso a Internet, scegli sottoreti pubbliche. Se più di due sono state create dallo stack di rete esterno, seleziona tutte quelle create.
InfrastructureHostSubnets		Seleziona almeno due sottoreti private in diverse zone di disponibilità in cui verranno avviati gli host dell'infrastruttura. Se più di due sono state create dallo stack di rete esterno, seleziona tutte quelle create.
VdiSubnets		Seleziona almeno due sottoreti private in diverse zone di disponibilità in cui verranno avviate le istanze VDI. Se più di due sono state create dallo stack di rete esterno, seleziona tutte quelle create.

Parametro	Predefinito	Descrizione
ActiveDirectoryName	*corp.res.com*	Dominio per l'Active Directory. Non è necessario che corrisponda al nome di dominio del portale.
ANNUNCIO ShortName	*corp*	Il nome breve per Active Directory. Viene anche chiamato nome NetBIOS.
Base LDAP	***DC=corp,DC=res,DC=com***	Un percorso LDAP verso la base all'interno della gerarchia LDAP.
URI di connessione LDAP		Un singolo percorso ldap:// che può essere raggiunto dal server host di Active Directory. Se hai distribuito le risorse esterne automatizzate con il dominio AD predefinito, puoi usare ldap: //corp.res.com.
ServiceAccountUserName	ServiceAccount	Nome utente per un account di servizio utilizzato per connettersi ad AD. Questo account deve avere accesso per creare computer all'interno di ComputerSOU.
ServiceAccountPasswordSecretArn		Fornisci un ARN segreto che contenga la password in testo semplice per. ServiceAccount

Parametro	Predefinito	Descrizione
UserSOU		Unità organizzativa all'interno di AD per gli utenti che effettueranno la sincronizzazione.
Gruppi OU		Unità organizzativa all'interno di AD per i gruppi che verranno sincronizzati.
SudoerSou		Unità organizzativa all'interno di AD for global sudoers.
SudoersGroupName	Amministratori RESS	Nome del gruppo che contiene tutti gli utenti con accesso sudoer sulle istanze al momento dell'installazione e accesso come amministratore su RES.
Computer (OU)		Unità organizzativa all'interno di AD a cui le istanze si uniranno.
Dominio TLS ARN CertificateSecret		(Facoltativo) Fornisci un ARN segreto del certificato TLS di dominio per abilitare la comunicazione TLS con AD.

Parametro	Predefinito	Descrizione
EnableLdapIDMapping		Determina se i numeri UID e GID vengono generati da SSSD o se vengono utilizzati i numeri forniti dall'AD. Impostare su True per utilizzare UID e GID generati da SSSD o su False per utilizzare UID e GID forniti dall'AD. Nella maggior parte dei casi questo parametro deve essere impostato su True.
Disabilita AdJoin	False	Per evitare che gli host Linux entrino a far parte del dominio della directory, impostate True. Altrimenti, lascia l'impostazione predefinita False.
ServiceAccountUserDN		Fornisci il nome distinto (DN) dell'utente dell'account di servizio in Directory.
SharedHomeFilesystemID		Un ID EFS da utilizzare per il file system home condiviso per gli host VDI Linux.
CustomDomainNamefor WebApp		(Facoltativo) Sottodominio utilizzato dal portale web per fornire collegamenti alla parte web del sistema.

Parametro	Predefinito	Descrizione
CustomDomainNameforVDI		(Facoltativo) Sottodominio utilizzato dal portale Web per fornire collegamenti per la parte VDI del sistema.
Certificato ACM AR NforWebApp		(Facoltativo) Quando si utilizza la configurazione predefinita, il prodotto ospita l'applicazione Web con il dominio amazonaws.com. Puoi ospitare i servizi relativi al prodotto nell'ambito del tuo dominio. Se hai distribui to risorse esterne automatiz zate, queste sono state generate per te e le informazi oni sono disponibili negli Output dello stack res-bi. Se devi generare un certifica to per la tua applicazione web, consulta. Guida alla configurazione
CertificateSecretARN per VDI		(Facoltativo) Questo segreto ARN archivia il certifica to pubblico per il certifica to pubblico del tuo portale web. Se imposti un nome di dominio del portale per le tue risorse esterne automatiz zate, puoi trovare questo valore nella scheda Output dello stack res-bi.

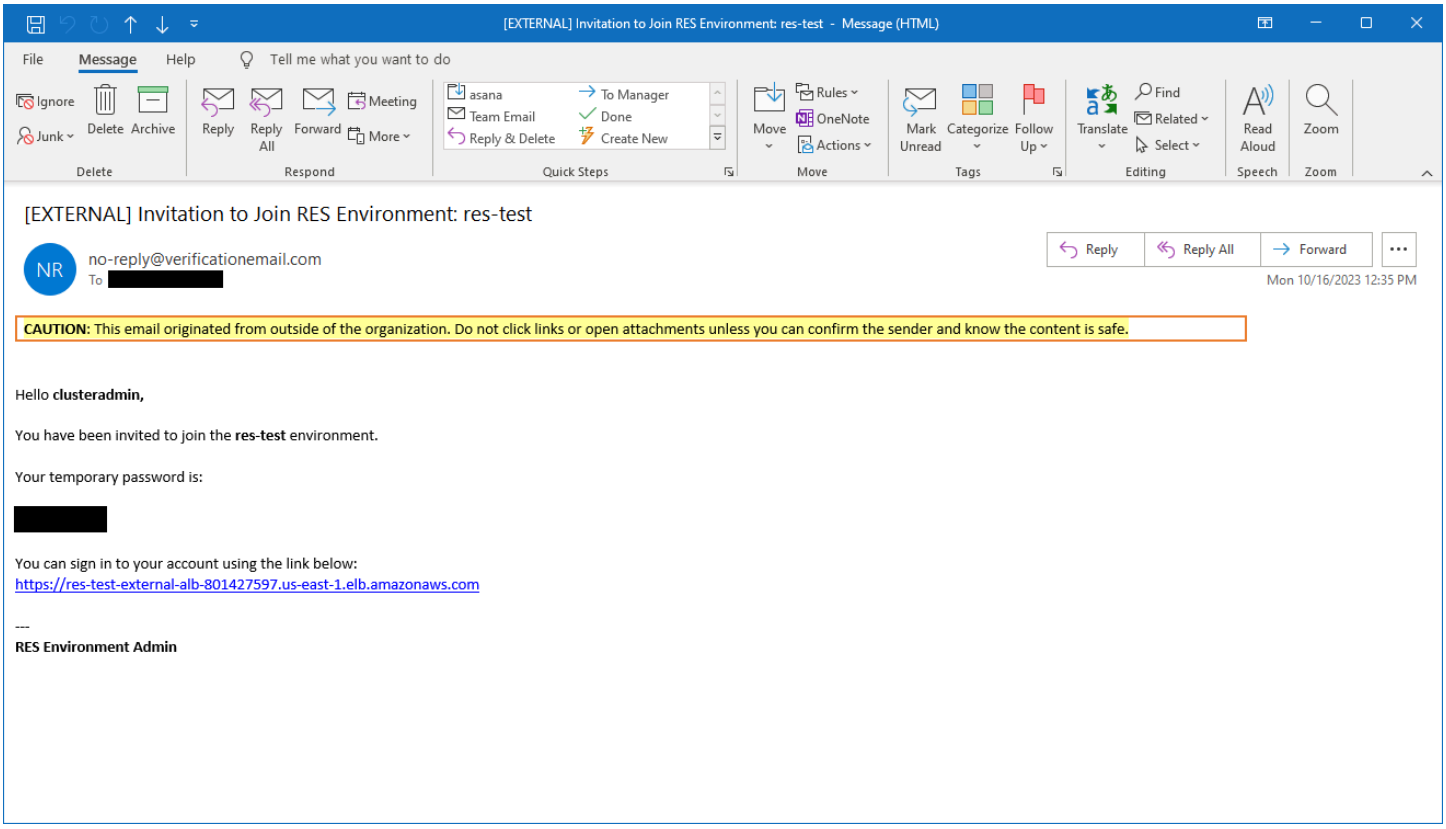
Parametro	Predefinito	Descrizione
PrivateKeySecretARN per VDI		(Facoltativo) Questo segreto ARN memorizza la chiave privata per il certificato del tuo portale web. Se imposti un nome di dominio del portale per le tue risorse esterne automatizzate, puoi trovare questo valore nella scheda Output dello stack res-bi.

5. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 60 minuti.

Passaggio 2: accedi per la prima volta

Una volta che lo stack di prodotti sarà stato distribuito nel tuo account, riceverai un'email con le tue credenziali. Usa l'URL per accedere al tuo account e configurare l'area di lavoro per altri utenti.



Dopo aver effettuato l'accesso per la prima volta, puoi configurare le impostazioni nel portale web per connetterti al provider SSO. Per informazioni sulla configurazione post-implementazione, consulta. Guida alla configurazione

Aggiorna il prodotto

Research and Engineering Studio (RES) offre due metodi per aggiornare il prodotto, che dipendono dal fatto che l'aggiornamento della versione sia principale o secondario.

RES utilizza uno schema di versioni basato sulla data. Una versione principale utilizza l'anno e il mese, mentre una versione secondaria aggiunge un numero di sequenza quando necessario. Ad esempio, la versione 2024.01 è stata rilasciata a gennaio 2024 come versione principale; la versione 2024.01.01 era un aggiornamento secondario di quella versione.

Argomenti

Principali aggiornamenti delle versioni

Research and Engineering Studio utilizza le istantanee per supportare la migrazione da un ambiente RES precedente a quello più recente senza perdere le impostazioni dell'ambiente. È inoltre possibile utilizzare questo processo per testare e verificare gli aggiornamenti dell'ambiente prima dell'onboarding degli utenti.

Per aggiornare l'ambiente con l'ultima versione di RES:

1. Crea un'istantanea del tuo ambiente attuale. Per informazioni, consulta the section called “Creazione di una snapshot”.
2. Ridistribuisci RES con la nuova versione. Per informazioni, consulta the section called “Fase 1: Avviare il prodotto”.
3. Applica l'istantanea all'ambiente aggiornato. Per informazioni, consulta the section called “Applicare un'istantanea”.
4. Verifica che tutti i dati siano stati migrati correttamente nel nuovo ambiente.

Aggiornamenti di versione minori

Per gli aggiornamenti delle versioni minori di RES, non è richiesta una nuova installazione. È possibile aggiornare lo stack RES esistente aggiornando il relativo AWS CloudFormation modello.

Controlla la versione del tuo attuale ambiente RES AWS CloudFormation prima di distribuire l'aggiornamento. Puoi trovare il numero di versione all'inizio del modello.

Ad esempio: `"Description": "RES_2024.1"`

Per effettuare un aggiornamento secondario della versione:

1. Scarica il AWS CloudFormation modello più recente inthe section called “Fase 1: Avviare il prodotto”.
2. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
3. Da Stacks, trova e seleziona lo stack principale. Dovrebbe apparire come. *<stack-name>*
4. Scegli Aggiorna.
5. Scegli Sostituisci il modello corrente.
6. Come Template source (Origine modello), scegliere Upload a template file (Carica un file di modello).
7. Scegli il file e carica il modello che hai scaricato.
8. In Specificare i dettagli dello stack, scegli Avanti. Non è necessario aggiornare i parametri.
9. In Configura le opzioni dello stack, scegli Avanti.
10. In Revisione<stack-name>, scegli Invia.

Disinstalla il prodotto

È possibile disinstallare Research and Engineering Studio sul prodotto da o utilizzando il. AWS AWS Management Console AWS Command Line InterfaceÈ necessario eliminare manualmente i bucket Amazon Simple Storage Service (Amazon S3) creati da questo prodotto. Questo prodotto non elimina automaticamente < EnvironmentName >- shared-storage-security-group nel caso in cui siano stati memorizzati dati da conservare.

Usando il AWS Management Console

1. Accedi alla console AWS CloudFormation.
2. Nella pagina Stacks, seleziona lo stack di installazione di questo prodotto.
3. Scegli Elimina.

Usando AWS Command Line Interface

Determina se AWS Command Line Interface (AWS CLI) è disponibile nel tuo ambiente. Per le istruzioni di installazione, consultate Cosa si trova AWS Command Line Interface nella Guida AWS CLI per l'utente. Dopo aver verificato che AWS CLI sia disponibile e configurato per l'account amministratore nella regione in cui è stato distribuito il prodotto, esegui il comando seguente.

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

Eliminazione del shared-storage-security-group

> **Warning**
>
> Il prodotto mantiene questo file system per impostazione predefinita per proteggere dalla perdita involontaria dei dati. Se si sceglie di eliminare il gruppo di sicurezza e i file system associati, tutti i dati conservati all'interno di tali sistemi verranno eliminati definitivamente. Consigliamo di eseguire il backup dei dati o di riassegnarli a un nuovo gruppo di sicurezza.

1. Accedi AWS Management Console e apri la console Amazon EFS all'indirizzo https://console.aws.amazon.com/efs/.
2. Elimina tutti i file system associati a <RES-stack-name>-shared-storage-security-group. In alternativa, è possibile riassegnare questi file system a un altro gruppo di sicurezza per conservare i dati.
3. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
4. Elimina il <RES-stack-name>-shared-storage-security-group.

Eliminazione dei bucket Amazon S3

Questo prodotto è configurato per conservare il bucket Amazon S3 creato dal prodotto (per la distribuzione in una regione opzionale) se decidi di eliminare lo stack per evitare AWS CloudFormation la perdita accidentale di dati. Dopo aver disinstallato il prodotto, puoi eliminare manualmente questo bucket S3 se non hai bisogno di conservare i dati. Segui questi passaggi per eliminare il bucket Amazon S3.

1. Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Scegli Bucket dal pannello di navigazione.
3. Individua i `stack-name` bucket S3.
4. Seleziona ogni bucket Amazon S3, quindi scegli Empty. Devi svuotare ogni bucket.
5. Seleziona il bucket S3 e scegli Elimina.

Per eliminare i bucket S3 utilizzando AWS CLI, esegui il seguente comando:

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

> **Note**
>
> Il `--force` comando svuota il bucket del suo contenuto.

Guida alla configurazione

Questa guida alla configurazione fornisce istruzioni post-implementazione per un pubblico tecnico su come personalizzare e integrare ulteriormente il prodotto con Research and Engineering Studio. AWS

Argomenti

Gestione di utenti e gruppi

Research and Engineering Studio può utilizzare qualsiasi provider di identità conforme a SAML 2.0. Se hai distribuito RES utilizzando risorse esterne o prevedi di utilizzare IAM Identity Center, vedi. the section called “Configurazione dell'SSO con IAM Identity Center” Se disponi di un provider di identità personale conforme a SAML 2.0, consulta. the section called “Configurazione del provider di identità per il Single Sign-On (SSO)”

Argomenti

Configurazione dell'SSO con IAM Identity Center

Se non disponi già di un centro di identità collegato all'Active Directory gestita, inizia conthe section called “Configura un centro di identità”. Se hai già un centro di identità collegato all'Active Directory gestita, inizia conthe section called “Connect a un centro di identità”.

> **Note**
>
> Se stai effettuando la distribuzione nella regione AWS GovCloud (Stati Uniti occidentali), configura l'SSO nell'account di AWS GovCloud (US) partizione in cui hai distribuito Research and Engineering Studio.

Fase 1: configurare un centro di identità

Attivazione del centro di identità

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Apri l'Identity Center.
3. Scegli Abilita .
4. Scegli Abilita con AWS Organizations.
5. Scegli Continua.

> **Note**
>
> Assicurati di trovarti nella stessa regione in cui hai la tua Active Directory gestita.

Connessione del centro di identità all'Active Directory gestita

Dopo aver abilitato il centro di identità, completa questi passaggi di configurazione consigliati:

1. Dalla navigazione, scegli Impostazioni.
2. In Origine dell'identità, scegli Azioni e scegli Cambia origine identità.
3. In Directory esistenti, seleziona la tua directory.
4. Seleziona Successivo.
5. Controlla le modifiche e inseriscile **`ACCEPT`** nella casella di conferma.
6. Scegli Cambia fonte di identità.

Sincronizzazione di utenti e gruppi con il centro identità

Una volta the section called “Connessione del centro di identità all'Active Directory gestita” completate le modifiche, dovrebbe apparire un banner verde.

1. Nel banner di conferma, scegli Avvia configurazione guidata.
2. Da Configura le mappature degli attributi, scegli Avanti.
3. Nella sezione Utente, inserisci gli utenti che desideri sincronizzare.
4. Scegli Aggiungi.
5. Seleziona Successivo.
6. Controlla le modifiche e scegli Salva configurazione.
7. Il processo di sincronizzazione potrebbe richiedere alcuni minuti. Se ricevi un messaggio di avviso relativo alla mancata sincronizzazione degli utenti, scegli Riprendi sincronizzazione.

Abilitare gli utenti

1. Dal menu, scegli Utenti.
2. Scegli gli utenti per i quali desideri abilitare l'accesso.
3. Scegli Abilita l'accesso utente.

Fase 2: Connect a un centro di identità

Configurazione dell'applicazione in Identity Center

1. Accedi a AWS Management Console e apri IAM Identity Center all'indirizzo https://console.aws.amazon.com/singlesignon/.
2. Selezionare Applications (Applicazioni).
3. Scegli Aggiungi applicazione.
4. In Preferenze di configurazione, scegli Ho un'applicazione che voglio configurare.
5. In Tipo di applicazione, scegli SAML 2.0.
6. Seleziona Successivo.
7. Inserisci il nome visualizzato e la descrizione che desideri utilizzare.
8. In Metadati IAM Identity Center, copia il link per il file di metadati IAM Identity Center SAML. Ne avrai bisogno per configurare l'SSO con il portale RES.

9. In Proprietà dell'applicazione, inserisci l'URL di avvio dell'applicazione. Ad esempio, < your-portal-domain >/sso.
10. In Application ACS URL, inserite l'URL di reindirizzamento dal portale RES. Per trovarlo:
    a. In Gestione dell'ambiente, scegli Impostazioni generali.
    b. Scegli la scheda Identity provider.
    c. In Single Sign-On, troverai l'URL di reindirizzamento SAML.
11. In Application SAML Audience, inserisci l'URN di Amazon Cognito. Per creare l'urna:
    a. Dal portale RES, apri Impostazioni generali.
    b. Una volta aperta la scheda Identity provider, individua l'ID del pool di utenti.
    c. Aggiungi l'ID del pool di utenti a questa stringa:

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

12. Scegli Invia.

Configurazione delle mappature degli attributi per l'applicazione

1. Dall'Identity Center, apri i dettagli dell'applicazione creata.
2. Scegli Azioni e scegli Modifica mappature degli attributi.
3. In Oggetto, inserisci $ {user:email}.
4. In Formato, scegli EmailAddress.
5. Scegli Aggiungi nuova mappatura degli attributi.
6. In Attributo utente nell'applicazione, inserisci l'email.
7. In Maps to this string value o user attribute in IAM Identity Center, inserisci $ {user:email}.
8. In Formato, inserisci unspecified.
9. Seleziona Salvataggio delle modifiche.

Aggiungere utenti all'applicazione in Identity Center

1. Da Identity Center, apri Utenti assegnati per l'applicazione creata e scegli Assegna utenti.
2. Seleziona gli utenti a cui desideri assegnare l'accesso all'applicazione.
3. Scegliere Assign users (Assegna utenti).

Configurazione dell'SSO all'interno dell'ambiente RES

1. Dall'ambiente Research and Engineering Studio, apri Impostazioni generali in Gestione dell'ambiente.
2. Apri la scheda Identity provider.
3. In Single Sign-On, scegli il pulsante di modifica accanto a Stato.
4. Completa il modulo con le seguenti informazioni:
   a. Scegli SAML.
   b. In Nome del fornitore, inserisci un nome intuitivo.
   c. Seleziona Inserisci l'URL dell'endpoint del documento di metadati.
   d. Inserisci l'URL che hai copiato durante the section called “Configurazione dell'applicazione in Identity Center”
   e. In Attributo email del fornitore, inserisci l'email.
   f. Scegli Invia.
5. Aggiorna la pagina e verifica che lo stato sia visualizzato come abilitato.

Configurazione del provider di identità per il Single Sign-On (SSO)

Research and Engineering Studio si integra con qualsiasi provider di identità SAML 2.0 per autenticare l'accesso degli utenti al portale RES. Questi passaggi forniscono indicazioni per l'integrazione con il provider di identità SAML 2.0 scelto. Se intendi utilizzare IAM Identity Center, consultathe section called “Configurazione dell'SSO con IAM Identity Center”.

> **Note**
>
> L'e-mail dell'utente deve corrispondere nell'asserzione IDP SAML e in Active Directory. Dovrai connettere il tuo provider di identità con Active Directory e sincronizzare periodicamente gli utenti.

Argomenti

- Configura il tuo provider di identità
- Configura RES per utilizzare il tuo provider di identità
- Configurazione del provider di identità in un ambiente non di produzione

- Eseguire il debug dei problemi di SAML IdP

Configura il tuo provider di identità

Questa sezione illustra i passaggi per configurare il tuo provider di identità con le informazioni del pool di utenti RES Amazon Cognito.

1. RES presuppone che tu disponga di un AD (AWS Managed AD o un AD autofornito) con identità utente autorizzate ad accedere al portale e ai progetti RES. Collega il tuo AD al tuo provider di servizi di identità e sincronizza le identità degli utenti. Consulta la documentazione del tuo provider di identità per scoprire come connettere AD e sincronizzare le identità degli utenti. Ad esempio, vedi Utilizzo di Active Directory come fonte di identità nella Guida per l'AWS IAM Identity Center utente.
2. Configura un'applicazione SAML 2.0 per RES nel tuo provider di identità (IdP). Questa configurazione richiede i seguenti parametri:
   - URL di reindirizzamento SAML: l'URL utilizzato dal tuo IdP per inviare la risposta SAML 2.0 al provider di servizi.

     > **Note**
     >
     > A seconda dell'IdP, l'URL di reindirizzamento SAML potrebbe avere un nome diverso:
     >
     > - URL dell'applicazione
     > - URL dell'Assertion Consumer Service (ACS)
     > - URL vincolante POST ACS

     Per ottenere l'URL

     1. Accedi a RES come amministratore o amministratore del cluster.
     2. Vai a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
     3. Scegli SAML Redirect URL.

   - URI SAML Audience: l'ID univoco dell'entità di audience SAML sul lato del fornitore di servizi.

> **Note**
>
> A seconda dell'IdP, l'URI SAML Audience potrebbe avere un nome diverso:
>
> - ClientID
> - Applicazione SAML Audience
> - ID dell'entità SP

Fornisci l'input nel seguente formato.

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

Per trovare il tuo URI SAML Audience

1. Accedi a RES come amministratore o amministratore del cluster.
2. Vai a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
3. Scegli User Pool Id.

3. L'asserzione SAML pubblicata su RES deve avere i seguenti campi/affermazioni impostati sull'indirizzo e-mail dell'utente:
   - Oggetto o NameID SAML
   - Posta elettronica SAML
4. Il tuo IdP aggiunge campi/attestazioni all'asserzione SAML, in base alla configurazione. RES richiede questi campi. La maggior parte dei provider compila automaticamente questi campi per impostazione predefinita. Fai riferimento ai seguenti input e valori dei campi se devi configurarli.

   - AudienceRestriction— Impostato su. `urn:amazon:cognito:sp:user-pool-id` Sostituiscilo *`user-pool-id`*con l'ID del tuo pool di utenti Amazon Cognito.

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

   - Risposta: imposta su`InResponseTo`. `https://user-pool-domain/saml2/idpresponse` Sostituiscilo *`user-pool-domain`*con il nome di dominio del tuo pool di utenti Amazon Cognito.

```
<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— Imposta `Recipient` sull'`saml2/idpresponse`endpoint del pool di utenti e sull'`InResponseTo`ID della richiesta SAML originale.

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

- AuthnStatement— Configura come segue:

```
<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. Se la tua applicazione SAML ha un campo URL di disconnessione, impostalo su:. <*domain-url*>`/saml2/logout`

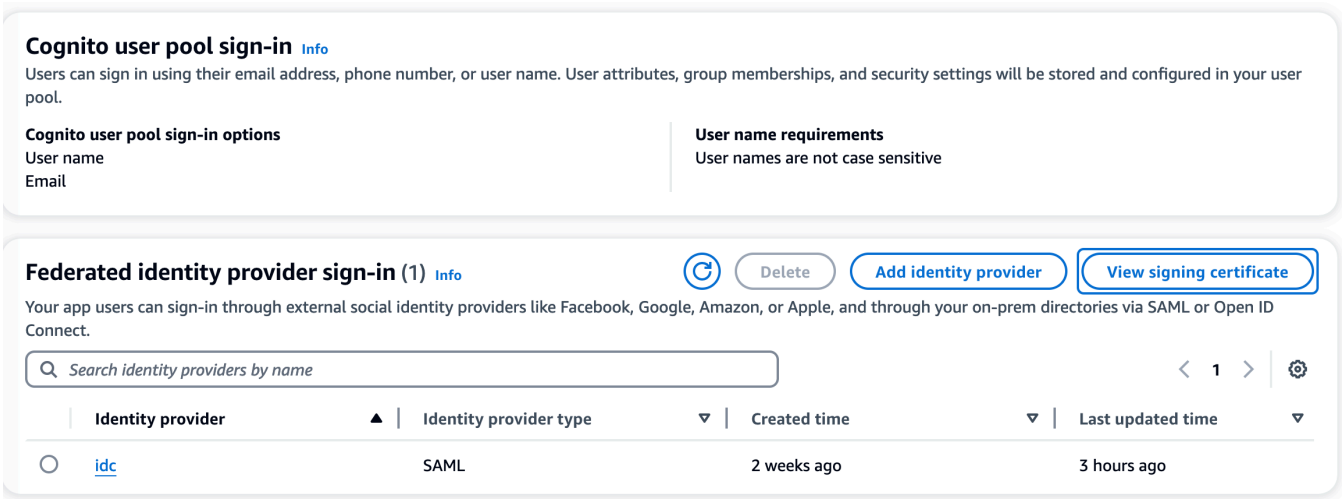
   Per ottenere l'URL del dominio

   1. Accedi a RES come amministratore o amministratore del cluster.
   2. Vai a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
   3. Scegli l'URL del dominio.

6. Se il tuo IdP accetta un certificato di firma per stabilire un rapporto di fiducia con Amazon Cognito, scarica il certificato di firma Amazon Cognito e caricalo nel tuo IdP.

   Per ottenere il certificato di firma

   1. Apri la console Amazon Cognito nella Guida introduttiva a AWS Management Console
   2. Seleziona il tuo pool di utenti. Il tuo pool di utenti dovrebbe essereres-*<environment name>*-user-pool.
   3. Scegli la scheda Sign-in experience (Esperienza di accesso).
   4. Nella sezione di accesso al Federated Identity Provider, scegli Visualizza certificato di firma.



   Puoi utilizzare questo certificato per configurare Active Directory IDP, aggiungere un `relying party trust` e abilitare il supporto SAML su questo relying party.

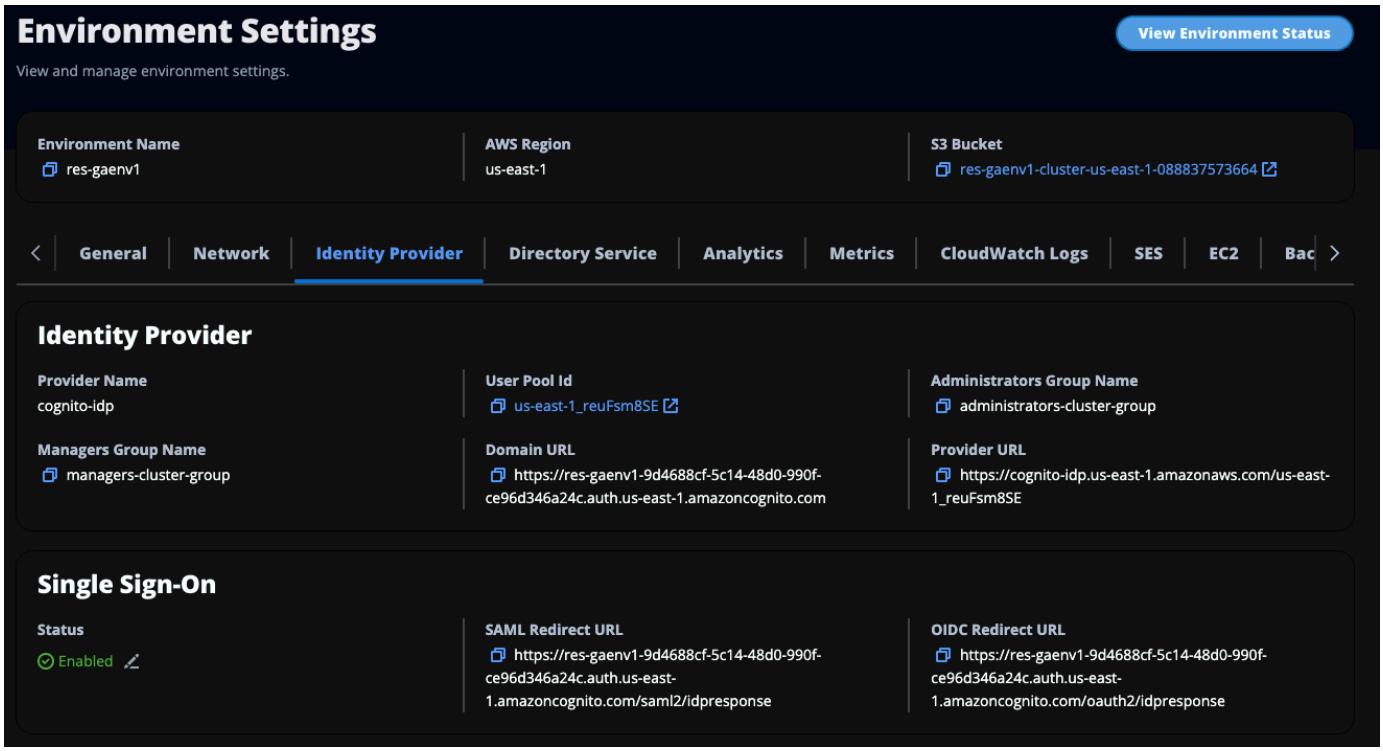
   > **Note**
   >
   > Questo non si applica a Keycloak e IDC.

5. Una volta completata la configurazione dell'applicazione, scarica l'XML o l'URL dei metadati dell'applicazione SAML 2.0. Lo utilizzerai nella sezione successiva.

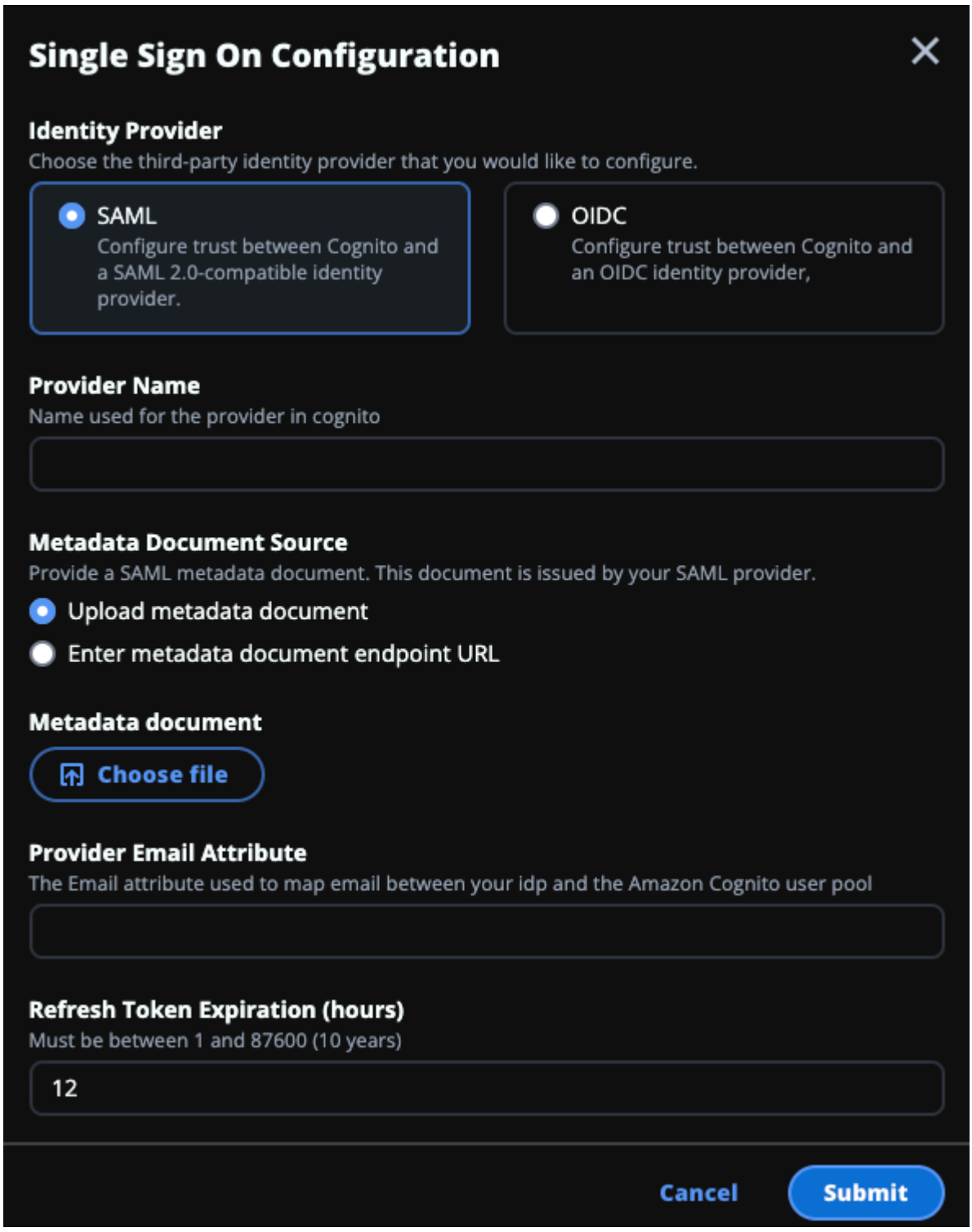
Configura RES per utilizzare il tuo provider di identità

Per completare la configurazione Single Sign-On per RES

1. Accedi a RES come amministratore o amministratore del cluster.
2. Vai a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.



3. In Single Sign-On, scegli l'icona di modifica accanto all'indicatore di stato per aprire la pagina di configurazione Single Sign-On.



a. Per Identity Provider, scegli SAML.

b. Per Provider Name, inserisci un nome univoco per il tuo provider di identità.

> **Note**
>
> I seguenti nomi non sono consentiti:
>
> - Cognito
> - IdentityCenter

c. In Origine documento di metadati, scegli l'opzione appropriata e carica il documento XML con metadati o fornisci l'URL dal provider di identità.

d. Per Provider Email Attribute, inserisci il valore di testo. `email`

e. Scegli Invia.

4. Ricarica la pagina delle impostazioni dell'ambiente. Il Single Sign-On è abilitato se la configurazione è corretta.

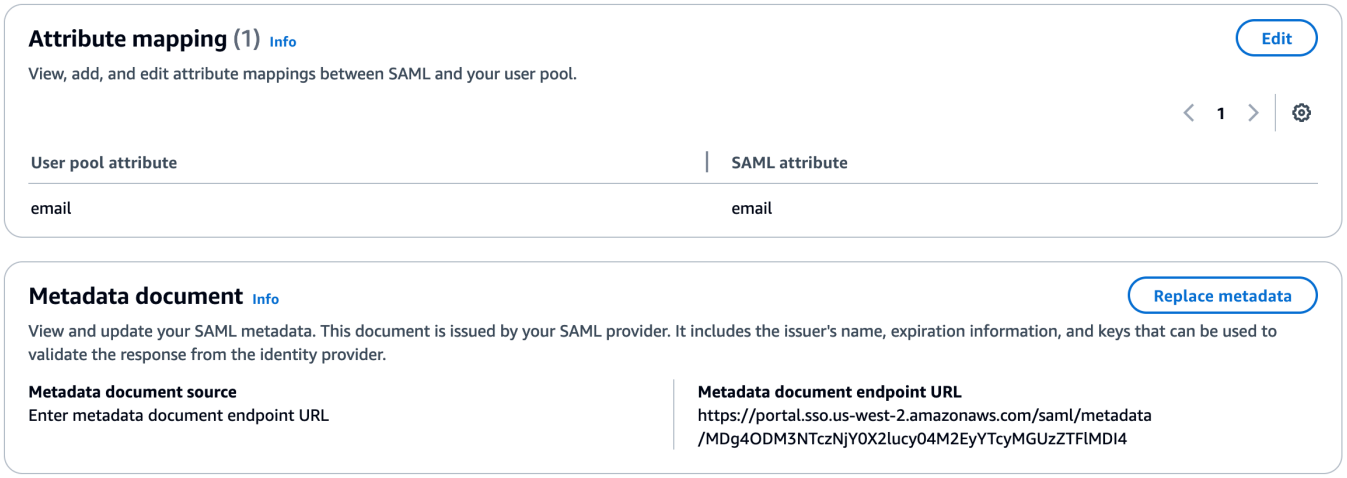
Configurazione del provider di identità in un ambiente non di produzione

Se hai utilizzato le risorse esterne fornite per creare un ambiente RES non di produzione e hai configurato IAM Identity Center come provider di identità, potresti voler configurare un provider di identità diverso come Okta. Il modulo di abilitazione RES SSO richiede tre parametri di configurazione:

1. Nome del provider: non può essere modificato
2. Documento o URL di metadati: può essere modificato
3. Attributo email del provider: può essere modificato

Per modificare il documento di metadati e l'attributo email del provider, procedi come segue:

1. Passa alla console Amazon Cognito.
2. Dalla navigazione, scegli Pool di utenti.
3. Scegli il tuo pool di utenti per visualizzare la panoramica del pool di utenti.
4. Dalla scheda Esperienza di accesso, accedi a Federated Identity Provider e apri il provider di identità configurato.
5. In genere, ti verrà richiesto solo di modificare i metadati e di lasciare invariata la mappatura degli attributi. Per aggiornare la mappatura degli attributi, scegliete Modifica. Per aggiornare il documento di metadati, scegliete Sostituisci metadati.



6. Se hai modificato la mappatura degli attributi, dovrai aggiornare la `<environment name>.cluster-settings` tabella in DynamoDB.

   a. Apri la console DynamoDB e scegli Tabelle dalla navigazione.

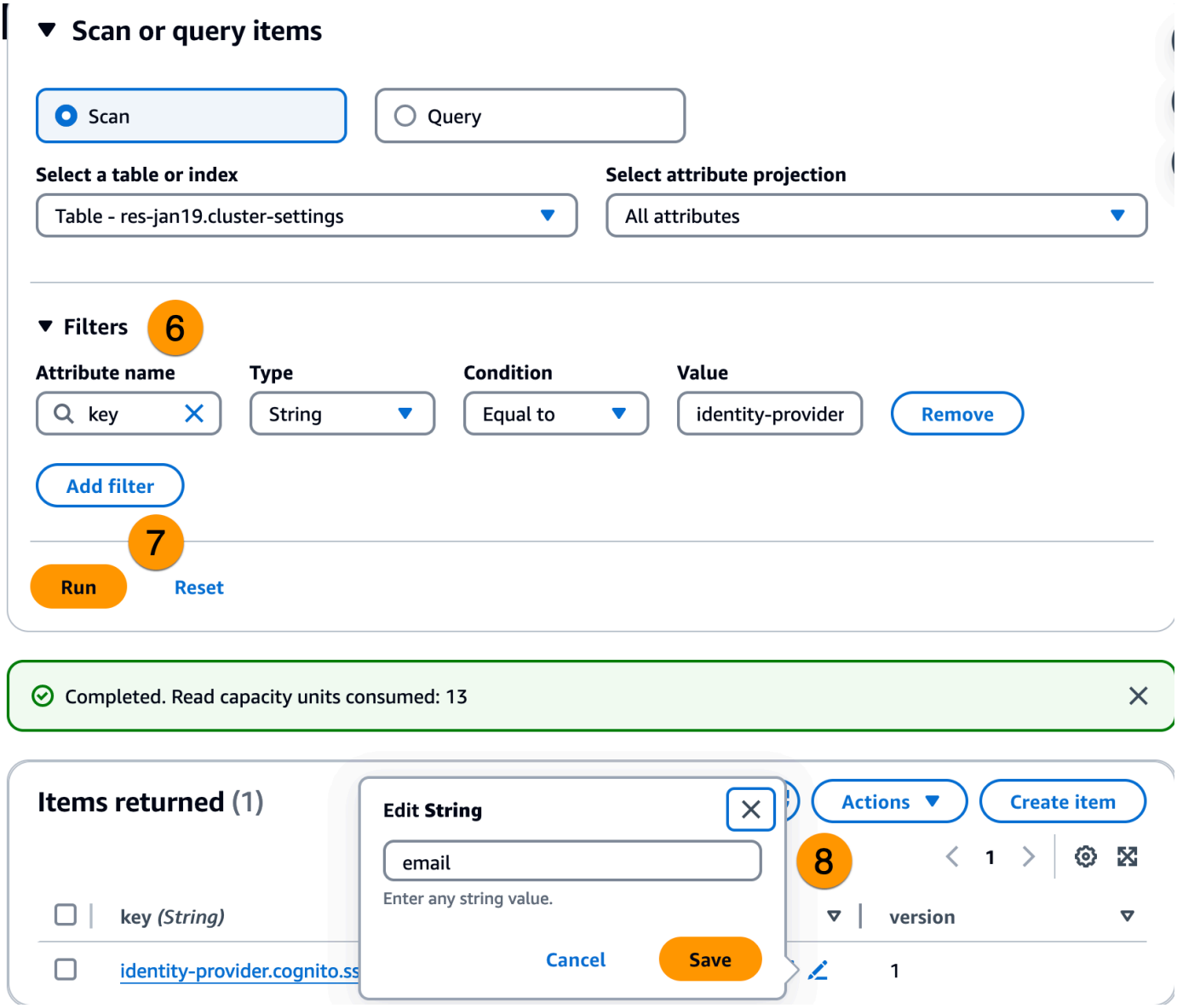
   b. Trova e seleziona la `<environment name>.cluster-settings` tabella e dal menu Azioni scegli Esplora gli elementi.

   c. In Elementi di scansione o interrogazione, vai su Filtri e inserisci i seguenti parametri:

      - Nome dell'attributo: `key`
      - Valore — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Seleziona Esegui.

7. In Articoli restituiti, trova la `identity-provider.cognito.sso_idp_provider_email_attribute` stringa e scegli Modifica per modificare la stringa in modo che corrisponda alle modifiche apportate in Amazon Cognito.



Eseguire il debug dei problemi di SAML IdP

SAML-Tracer: puoi utilizzare questa estensione per il browser Chrome per tenere traccia delle richieste SAML e controllare i valori delle asserzioni SAML. Per ulteriori informazioni, consulta SAML-Tracer nel Chrome Web Store.

Strumenti per sviluppatori SAML: OneLogin forniscono strumenti che puoi utilizzare per decodificare il valore codificato SAML e controllare i campi obbligatori nell'asserzione SAML. Per ulteriori informazioni, consulta Base 64 Decode + Inflate sul sito Web. OneLogin

Amazon CloudWatch Logs: puoi controllare i tuoi log RES in CloudWatch Logs per eventuali errori o avvisi. I tuoi log si trovano in un gruppo di log con il formato del nome. `res-environment-name/cluster-manager`

Documentazione di Amazon Cognito: per ulteriori informazioni sull'integrazione SAML con Amazon Cognito, consulta Aggiungere provider di identità SAML a un pool di utenti nella Amazon Cognito Developer Guide.

Impostazione delle password per gli utenti

1. Dalla AWS Directory Service console, seleziona la directory per lo stack creato.
2. Nel menu Azioni, scegli Reimposta la password utente.
3. Scegli l'utente e inserisci una nuova password.
4. Scegli Reimposta password.

Creazione di sottodomini

Se si utilizza un dominio personalizzato, sarà necessario configurare i sottodomini per supportare le parti Web e VDI del portale.

> **Note**
>
> Se state eseguendo la distribuzione nella regione AWS GovCloud (Stati Uniti occidentali), configurate l'applicazione Web e i sottodomini VDI nell'account di partizione commerciale che ospita la zona di hosting pubblico del dominio.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Trova il dominio che hai creato e scegli Crea record.
3. Inserisci web come nome del record.
4. Scegli CNAME come tipo di record.
5. Per Value, inserisci il link che hai ricevuto nell'email iniziale.
6. Scegli Crea record.
7. Per creare un record per il VDC, recupera l'indirizzo NLB.

a. Accedere AWS Management Console e aprire la console all'indirizzo https://console.aws.amazon.com/cloudformation. AWS CloudFormation
b. Scegli `<environment-name>-vdc`.
c. Scegli Risorse e apri`<environmentname>-vdc-external-nlb`.
d. Copia il nome DNS dal NLB.

8. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
9. Trova il tuo dominio e scegli Crea record.
10. In Nome del record, inserisci`vdc`.
11. In Record type (Tipo di record), seleziona CNAME.
12. Per l'NLB, inserisci il DNS.
13. Scegli Crea record.

Crea un certificato ACM

Per impostazione predefinita, RES ospita il portale Web con un sistema di bilanciamento del carico delle applicazioni utilizzando il dominio amazonaws.com. Per utilizzare il tuo dominio, dovrai configurare un certificato SSL/TLS pubblico fornito da te o richiesto da (ACM). AWS Certificate Manager Se utilizzi ACM, riceverai un nome di AWS risorsa che dovrai fornire come parametro per crittografare il canale SSL/TLS tra il client e l'host dei servizi web.

> **Tip**
>
> Se stai distribuendo il pacchetto demo di risorse esterne, dovrai inserire il dominio prescelto `PortalDomainName` quando distribuisci lo stack di risorse esterne. the section called “Crea risorse esterne”

Per creare un certificato per domini personalizzati:

1. Dalla console, apri AWS Certificate Managerper richiedere un certificato pubblico. Se stai distribuendo in AWS GovCloud (Stati Uniti occidentali), crea il certificato nel tuo account di GovCloud partizione.
2. Scegli Richiedi un certificato pubblico e scegli Avanti.

3. In Nomi di dominio, richiedi un certificato per entrambi `*.PortalDomainName` e`PortalDomainName`.
4. In Metodo di convalida, scegli Convalida DNS.
5. Scegli Richiedi.
6. Dall'elenco dei certificati, apri i certificati richiesti. Lo stato di ogni certificato sarà In attesa di convalida.

> **Note**
>
> Se non vedi i tuoi certificati, aggiorna l'elenco.

7. Esegui una di queste operazioni:
   - Distribuzione commerciale: dai dettagli del certificato per ogni certificato richiesto, scegli Crea record in Route 53. Lo stato del certificato dovrebbe cambiare in Emesso.
   - GovCloud distribuzione: se stai distribuendo in AWS GovCloud (Stati Uniti occidentali), copia la chiave e il valore CNAME. Dall'account di partizione commerciale, utilizza i valori per creare un nuovo record nella Public Hosted Zone. Lo stato del certificato dovrebbe cambiare in Emesso.
8. Copia il nuovo ARN del certificato da immettere come parametro per. `ACMCertificateARNforWebApp`

CloudWatch Registri Amazon

Research and Engineering Studio crea i seguenti gruppi di log CloudWatch durante l'installazione. Vedi la tabella seguente per le conservazioni predefinite:

CloudWatch Gruppi di log	Retention
/aws/lambda/ < >-cluster-endpoints installation-stack-name	Non scadono mai
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	Non scadono mai
/aws/lambda/ < >-cluster-settings installation-stack-name	Non scadono mai

CloudWatch Gruppi di log	Retention
/aws/lambda/ < >-oauth-credentials installation-stack-name	Non scadono mai
/aws/lambda/ < >- installation-stack-name self-signed-certificate	Non scadono mai
/aws/lambda/ < >- installation-stack-name update-cluster-prefix-list	Non scadono mai
/aws/lambda/ < >- installation-stack-name vdc-scheduled-event-transformer	Non scadono mai
/aws/lambda/ < >- -client-scope installation-stack-name vdc-update-cluster-manager	Non scadono mai
/< >/cluster-manager installation-stack-name	3 mesi
/< installation-stack-name >/vdc/controllore	3 mesi
/< >/vdc/dv-broker installation-stack-name	3 mesi
/< >/vdc/ installation-stack-name dcv-connection-gateway	3 mesi

Se desideri modificare la conservazione predefinita per un gruppo di log, puoi andare alla CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/ e seguire le istruzioni per modificare la conservazione dei dati di registro in CloudWatch Logs.

Impostazione di limiti di autorizzazione personalizzati

A partire dalla versione 2024.04, puoi facoltativamente modificare i ruoli creati da RES aggiungendo limiti di autorizzazione personalizzati. Un limite di autorizzazione personalizzato può essere definito come parte dell' AWS CloudFormation installazione RES fornendo l'ARN del limite di autorizzazione come parte del parametro IAM. PermissionBoundary Nessun limite di autorizzazione viene impostato su alcun ruolo RES se questo parametro viene lasciato vuoto. Di seguito è riportato l'elenco delle

azioni che i ruoli RES richiedono per operare. Assicurati che qualsiasi limite di autorizzazione che intendi utilizzare in modo esplicito consenta le seguenti azioni:

```
[
    {
        "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:*"
        ]
    }
]
```

Configurazione delle AMI pronte per RESS

Con le AMI pronte per RESS, puoi preinstallare le dipendenze RES per le istanze di desktop virtuali (VDI) sulle tue AMI personalizzate. L'uso delle AMI pronte per RESS migliora i tempi di avvio delle istanze VDI utilizzando le immagini predefinite. Utilizzando EC2 Image Builder, puoi creare e registrare le tue AMI come nuovi stack software. Per ulteriori informazioni su Image Builder, vedere la Guida per l'utente di Image Builder.

Prima di iniziare, è necessario distribuire la versione più recente di RES.

Argomenti

Prepara il ruolo IAM per accedere all'ambiente RES

Per accedere al servizio di ambiente RES da EC2 Image Builder, è necessario creare o modificare un ruolo IAM chiamato RES-EC2. InstanceProfileForImageBuilder Per informazioni sulla configurazione di un ruolo IAM da utilizzare in Image Builder, AWS Identity and Access Management consulta (IAM) nella Guida per l'utente di Image Builder.

Il tuo ruolo richiede:

- Le relazioni affidabili includono il servizio Amazon EC2
- Politiche AmazonSSM ManagedInstanceCore ed EC2 InstanceProfileForImageBuilder
- Policy RES personalizzata con accesso limitato a DynamoDB e Amazon S3 all'ambiente RES distribuito

  (Questa politica può essere un documento di policy gestito dal cliente o un documento di policy in linea con il cliente).

Entità di relazione affidabile:

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

Politica RES:

```
{
    "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/*"
        }
    ]
```

```
}
```

Crea il componente EC2 Image Builder

Segui le istruzioni per creare un componente utilizzando la console Image Builder nella Guida per l'utente di Image Builder.

Inserisci i dettagli del componente:

1. Per Tipo, scegli Costruisci.
2. Per il sistema operativo (OS) Image, scegli Linux o Windows.
3. Per Nome componente, inserisci un nome significativo, ad esempio**`research-and-engineering-studio-vdi-<operating-system>`**.
4. Inserisci il numero di versione del componente e, facoltativamente, aggiungi una descrizione.
5. Per il documento di definizione, inserisci il seguente file di definizione. Se si verificano errori, il file YAML è sensibile allo spazio ed è la causa più probabile.

   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. Crea eventuali tag opzionali e scegli Crea componente.

Prepara la tua ricetta per EC2 Image Builder

> **Note**
>
> L'arrivo di CentOS 7 è attualmente previsto per il end-of-life 30/06/2024. La versione 2024.06 di Research and Engineering Studio sarà l'ultima versione a supportare CentOS 7.

Una ricetta di EC2 Image Builder definisce l'immagine di base da utilizzare come punto di partenza per creare una nuova immagine, insieme al set di componenti che aggiungi per personalizzare l'immagine e verificare che tutto funzioni come previsto. È necessario creare o modificare una ricetta per costruire l'AMI di destinazione con le dipendenze software RES necessarie. Per ulteriori informazioni sulle ricette, consulta Gestire le ricette.

RES supporta i seguenti sistemi operativi di immagini:

- Amazon Linux 2 (x86 e ARM64)
- CentOS 7 (x86 e ARM64)
- RHEL 7 (x86), 8 (x86) e 9 (x86)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Apri la console EC2 Image Builder https://console.aws.amazon.com/imagebuilder all'indirizzo.
2. In Risorse salvate, scegli Ricette di immagini.
3. Scegli Crea ricetta di immagine.
4. Inserisci un nome univoco e un numero di versione.
5. Scegliete un'immagine di base supportata da RES.

6. In Configurazione dell'istanza, installa un agente SSM se non è preinstallato. Inserisci le informazioni in Dati utente e qualsiasi altro dato utente necessario.

   > **Note**
   >
   > Per informazioni su come installare un agente SSM, consulta:
   >
   > - Installazione manuale dell'agente SSM su istanze EC2 per Linux
   > - Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Windows Server

7. Per le ricette basate su Linux, aggiungi il componente di `aws-cli-version-2-linux` compilazione gestito da Amazon alla ricetta. Gli script di installazione RES utilizzano il AWS CLI per fornire l'accesso VDI ai valori di configurazione per le impostazioni del cluster DynamoDB. Windows non richiede questo componente.
8. Aggiungi il componente EC2 Image Builder creato per il tuo ambiente Linux o Windows e inserisci i valori dei parametri richiesti. I seguenti parametri sono input obbligatori: AWSAccountID, RESEnvName, RES e RESEnvRegion. EnvReleaseVersion

   > **Important**
   >
   > Per gli ambienti Linux, è necessario aggiungere questi componenti in ordine con il componente `aws-cli-version-2-linux` build aggiunto per primo.

9. (Consigliato) Aggiungi il componente di `simple-boot-test-<linux-or-windows>` test gestito da Amazon per verificare che l'AMI possa essere avviata. Questa è una raccomandazione minima. È possibile selezionare altri componenti di test che soddisfino le proprie esigenze.
10. Completa le sezioni opzionali, se necessario, aggiungi gli altri componenti desiderati e scegli Crea ricetta.

Modify a recipe

Se disponi di una ricetta EC2 Image Builder esistente, puoi utilizzarla aggiungendo i seguenti componenti:

1. Per le ricette basate su Linux, aggiungi il componente di `aws-cli-version-2-linux` compilazione gestito da Amazon alla ricetta. Gli script di installazione RES utilizzano il

AWS CLI per fornire l'accesso VDI ai valori di configurazione per le impostazioni del cluster DynamoDB. Windows non richiede questo componente.

2. Aggiungi il componente EC2 Image Builder creato per il tuo ambiente Linux o Windows e inserisci i valori dei parametri richiesti. I seguenti parametri sono input obbligatori: AWSAccountID, RESEnvName, RES e RESEnvRegion. EnvReleaseVersion

> **Important**
>
> Per gli ambienti Linux, è necessario aggiungere questi componenti in ordine con il componente `aws-cli-version-2-linux` build aggiunto per primo.

3. Completa le sezioni opzionali, se necessario, aggiungi gli altri componenti desiderati e scegli Crea ricetta.

Configurazione dell'infrastruttura EC2 Image Builder

Puoi utilizzare le configurazioni dell'infrastruttura per specificare l'infrastruttura Amazon EC2 utilizzata da Image Builder per creare e testare la tua immagine Image Builder. Per l'utilizzo con RES, puoi scegliere di creare una nuova configurazione dell'infrastruttura o utilizzarne una esistente.

- Per creare una nuova configurazione dell'infrastruttura, consulta Creare una configurazione dell'infrastruttura.
- Per utilizzare una configurazione dell'infrastruttura esistente, aggiorna una configurazione dell'infrastruttura.

Per configurare l'infrastruttura Image Builder:

1. Per il ruolo IAM, inserisci il ruolo in cui hai configurato in the section called “Prepara il ruolo IAM per accedere all'ambiente RES” precedenza.
2. Per Tipo di istanza, scegli un tipo con almeno 4 GB di memoria e che supporti l'architettura AMI di base scelta. Vedi i tipi di istanze Amazon EC2.
3. Per VPC, sottorete e gruppi di sicurezza, è necessario consentire l'accesso a Internet per scaricare i pacchetti software. È inoltre necessario consentire l'accesso alla tabella `cluster-settings` DynamoDB e al bucket cluster Amazon S3 dell'ambiente RES.

Configurazione della pipeline di immagini di Image Builder

La pipeline di immagini di Image Builder assembla l'immagine di base, i componenti per la creazione e il test, la configurazione dell'infrastruttura e le impostazioni di distribuzione. Per configurare una pipeline di immagini per le AMI pronte per RES-Ready, puoi scegliere di creare una nuova pipeline o utilizzarne una esistente. Per ulteriori informazioni, consulta Creare e aggiornare pipeline di immagini AMI nella Guida per l'utente di Image Builder.

Create a new Image Builder pipeline

1. Aprire la console Image Builder all'indirizzo. https://console.aws.amazon.com/imagebuilder
2. Dalla navigazione, scegli Image pipelines.
3. Scegli Crea pipeline di immagini.
4. Specificate i dettagli della pipeline inserendo un nome univoco, una descrizione opzionale, una pianificazione e una frequenza.
5. Per Scegli la ricetta, scegli Usa ricetta esistente e seleziona la ricetta creata inthe section called “Prepara la tua ricetta per EC2 Image Builder”. Verifica che i dettagli della ricetta siano corretti.
6. Per Definisci il processo di creazione dell'immagine, scegli il flusso di lavoro predefinito o personalizzato a seconda del caso d'uso. Nella maggior parte dei casi, i flussi di lavoro predefiniti sono sufficienti. Per ulteriori informazioni, consulta Configurare i flussi di lavoro di immagini per la pipeline EC2 Image Builder.
7. Per Definisci la configurazione dell'infrastruttura, scegli Scegli la configurazione dell'infrastruttura esistente e seleziona la configurazione dell'infrastruttura creata in. the section called “Configurazione dell'infrastruttura EC2 Image Builder” Verifica che i dettagli dell'infrastruttura siano corretti.
8. Per Definisci le impostazioni di distribuzione, scegli Crea impostazioni di distribuzione utilizzando i valori predefiniti del servizio. L'immagine di output deve risiedere nello stesso ambiente Regione AWS RES. Utilizzando le impostazioni predefinite del servizio, l'immagine verrà creata nella regione in cui viene utilizzato Image Builder.
9. Esamina i dettagli della pipeline e scegli Crea pipeline.

Modify an existing Image Builder pipeline

1. Per utilizzare una pipeline esistente, modifica i dettagli in modo da utilizzare la ricetta creata in. the section called “Prepara la tua ricetta per EC2 Image Builder”

2. Seleziona Salvataggio delle modifiche.

Esegui la pipeline di immagini di Image Builder

Per produrre l'immagine di output configurata, è necessario avviare la pipeline di immagini. Il processo di creazione può richiedere potenzialmente fino a un'ora a seconda del numero di componenti nella ricetta dell'immagine.

Per eseguire la pipeline di immagini:

1. Da Image pipelines, selezionate la pipeline creata in. the section called “Configurazione della pipeline di immagini di Image Builder”
2. Da Azioni, scegliete Esegui pipeline.

Registra un nuovo stack software in RES

1. Segui le istruzioni the section called “Stack software (AMI)” per registrare uno stack di software.
2. Per AMI ID, inserisci l'ID AMI dell'immagine di output incorporatathe section called “Esegui la pipeline di immagini di Image Builder”.

Guida per amministratori

Questa guida per amministratori fornisce istruzioni aggiuntive per un pubblico tecnico su come personalizzare e integrare ulteriormente il AWS prodotto con Research and Engineering Studio.

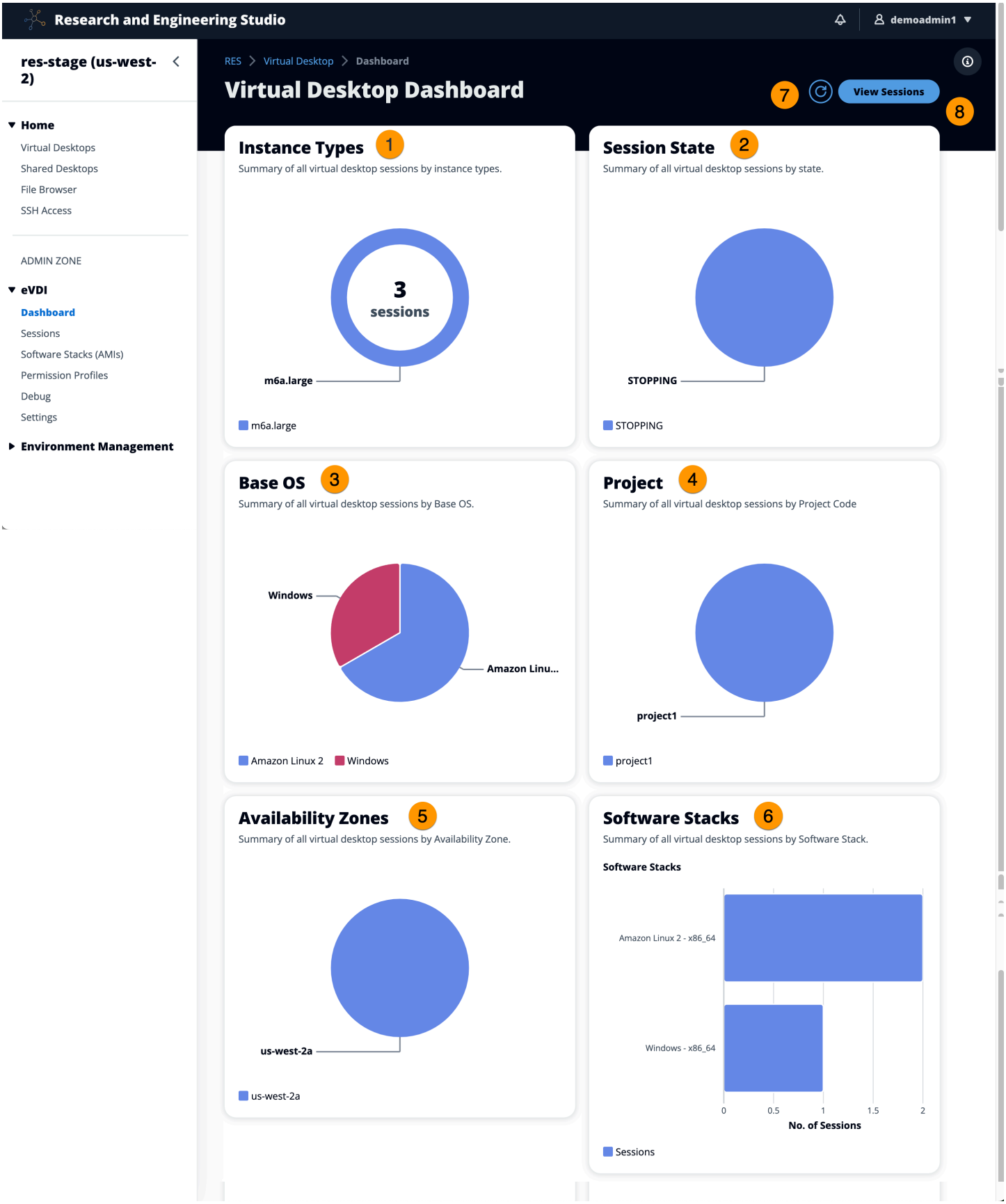
Argomenti

Gestione della sessione

La gestione delle sessioni offre un ambiente flessibile e interattivo per le sessioni di sviluppo e test. In qualità di utente amministrativo, puoi consentire agli utenti di creare e gestire sessioni interattive all'interno dei loro ambienti di progetto.

Argomenti

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

Il dashboard di gestione delle sessioni offre agli amministratori una rapida panoramica di:

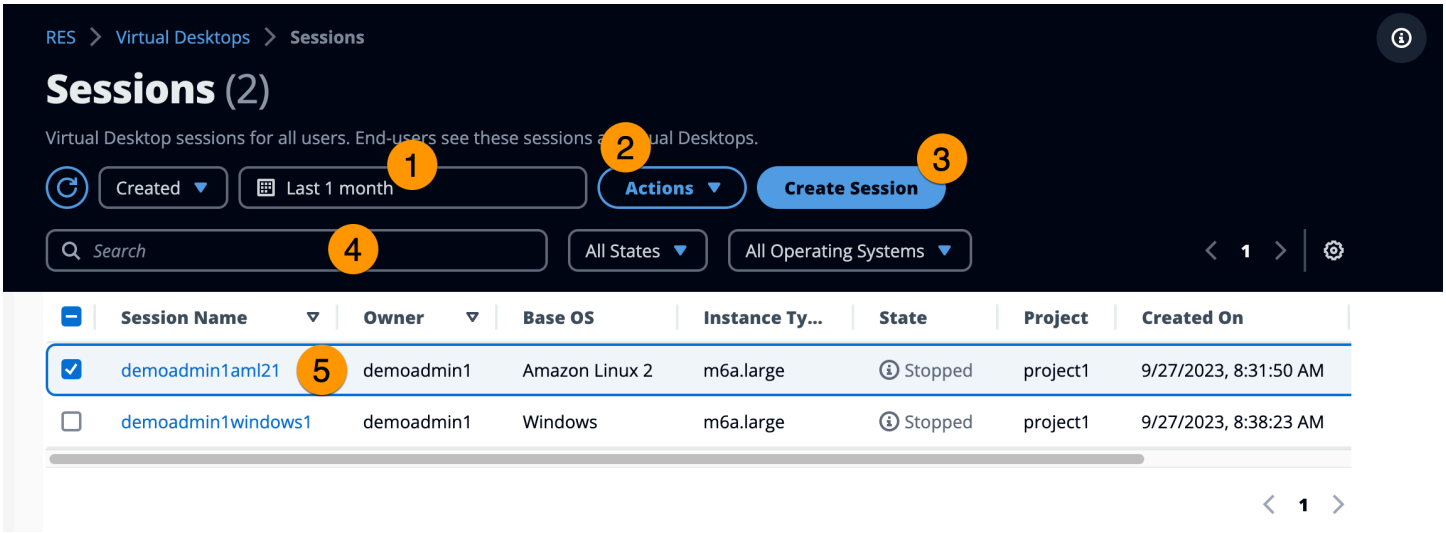
1. Tipi di istanza
2. Stati della sessione
3. Sistema operativo di base
4. Progetti
5. Zone di disponibilità
6. Pile di software

Inoltre, gli amministratori possono:

7. Aggiorna la dashboard per aggiornare le informazioni.
8. Scegli Visualizza sessioni per accedere a Sessioni.

Sessioni

Sessions mostra tutti i desktop virtuali creati in Research and Engineering Studio. Dalla pagina Sessioni, è possibile filtrare e visualizzare le informazioni sulla sessione o creare una nuova sessione.



1. Utilizza il menu per filtrare i risultati in base alle sessioni create o aggiornate entro un periodo di tempo specificato.
2. Seleziona una sessione e usa il menu Azioni per:
   a. Riprendere le sessioni

b. Arresta/ibernate le sessioni
c. Sessioni forzate di arresto/ibernazione
d. Termina sessione (e)
e. Interruzione forzata delle sessioni
f. Sessione (e) Health
g. Crea uno stack software

3. Scegli Crea sessione per creare una nuova sessione.
4. Cerca una sessione per nome e filtra per stato e sistema operativo.
5. Scegli il nome della sessione per visualizzare maggiori dettagli.

Crea una sessione

1. Scegli Crea sessione. Si apre la modalità Launch New Virtual Desktop.
2. Inserisci i dettagli per la nuova sessione.
3. Opzionale. Attiva Mostra opzioni avanzate per fornire dettagli aggiuntivi come l'ID di sottorete e il tipo di sessione DCV.
4. Scegli Invia.

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

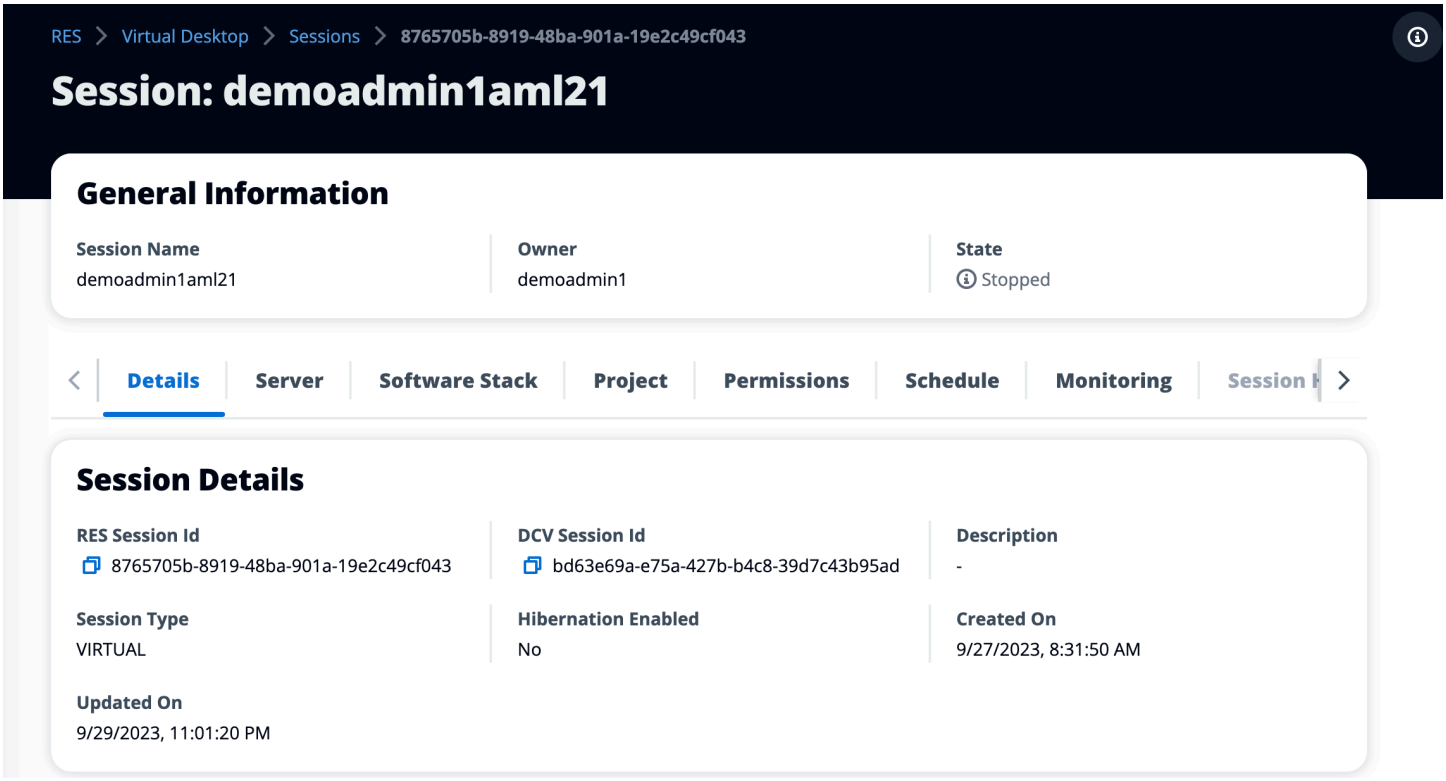
Storage Size (GB)

Enter the storage size for your virtual desktop in GBs

10

Dettagli della sessione

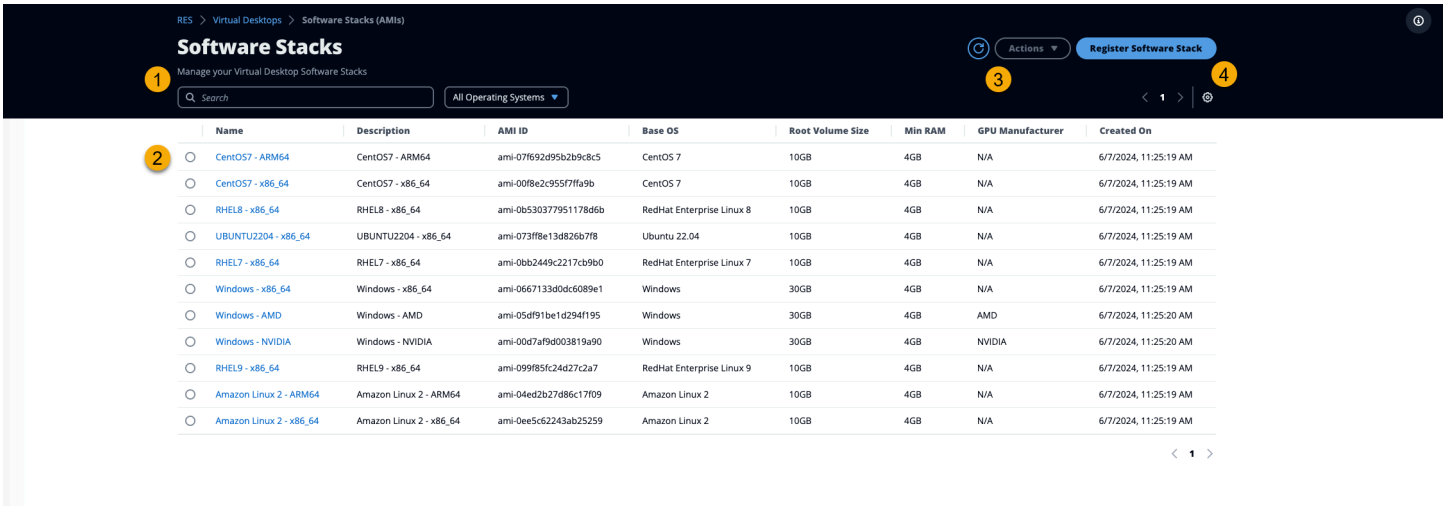
Dall'elenco Sessioni, scegli il nome della sessione per visualizzare i dettagli della sessione.



Software Stacks (AMI)

> **Note**
>
> Per eseguire lo stack software CentSO7 fornito AWS GovCloud (US), è necessario abbonarsi all'AMI interno Marketplace AWS utilizzando l'account standard collegato.

Dalla pagina Software Stacks, puoi configurare Amazon Machine Images (AMI) e gestire le AMI esistenti.



1. Per cercare uno stack software esistente, utilizza il menu a discesa del sistema operativo per filtrare per sistema operativo.
2. Scegli il nome di uno stack software per visualizzare i dettagli sullo stack.
3. Dopo aver selezionato uno stack di software, utilizzate il menu Azioni per modificare lo stack e assegnarlo a un progetto.
4. Il pulsante Register Software Stack consente di creare un nuovo stack:
    1. Scegli Register Software Stack.
    2. Inserisci i dettagli per il nuovo stack di software.
    3. Scegli Invia.

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

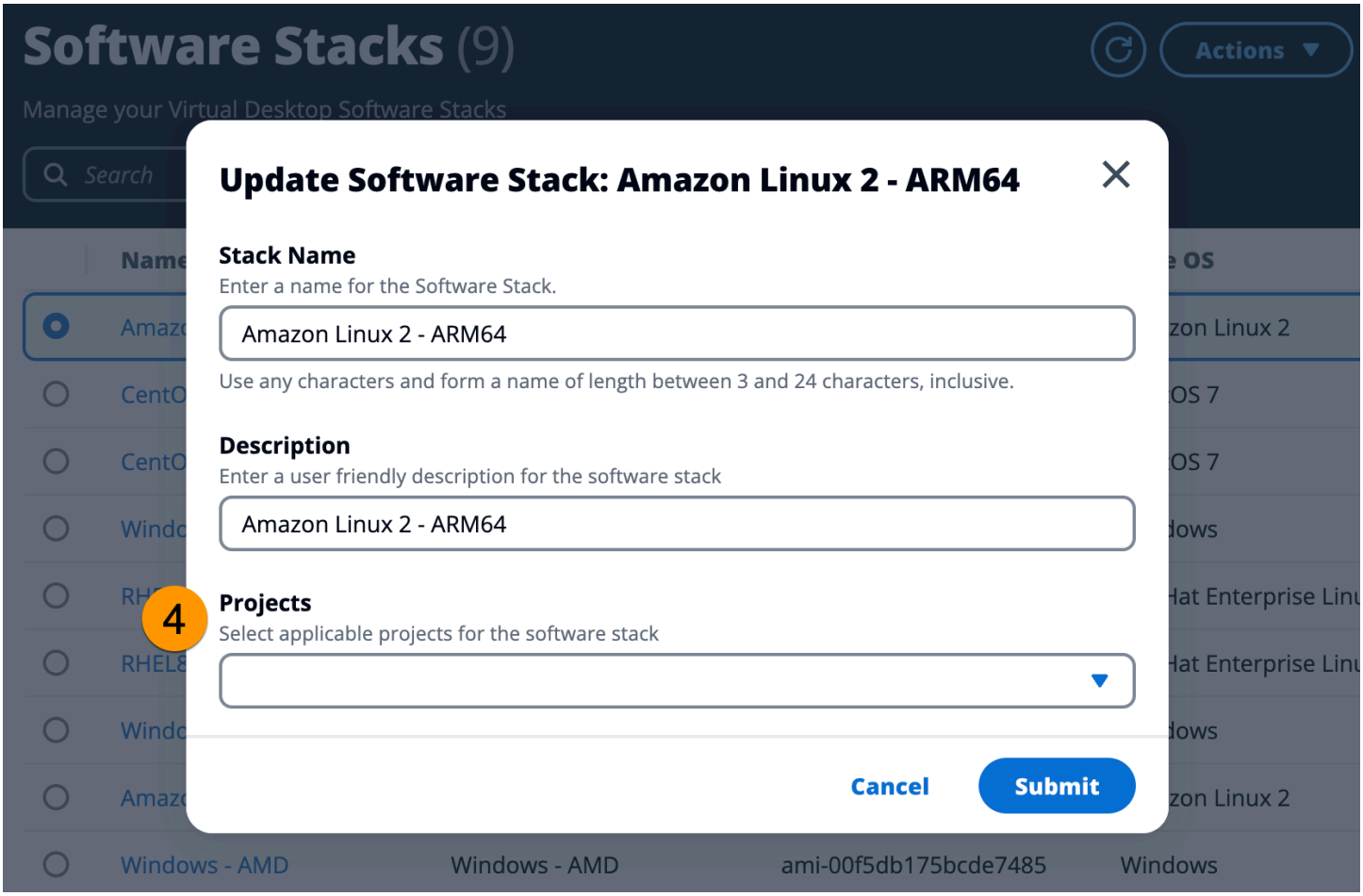
Assegna uno stack software a un progetto

Quando crei un nuovo stack software, puoi assegnare lo stack ai progetti. Se devi aggiungere lo stack a un progetto dopo la creazione iniziale, procedi come segue:

> **Note**
>
> Puoi assegnare stack software solo ai progetti di cui sei membro.

1. Seleziona lo stack software da aggiungere a un progetto dalla pagina Software Stacks.
2. Scegli Azioni.
3. Scegli Modifica.
4. Utilizza il menu a discesa Progetti per selezionare il progetto.
5. Scegli Invia.

Puoi anche modificare lo stack software dalla pagina dei dettagli dello stack.

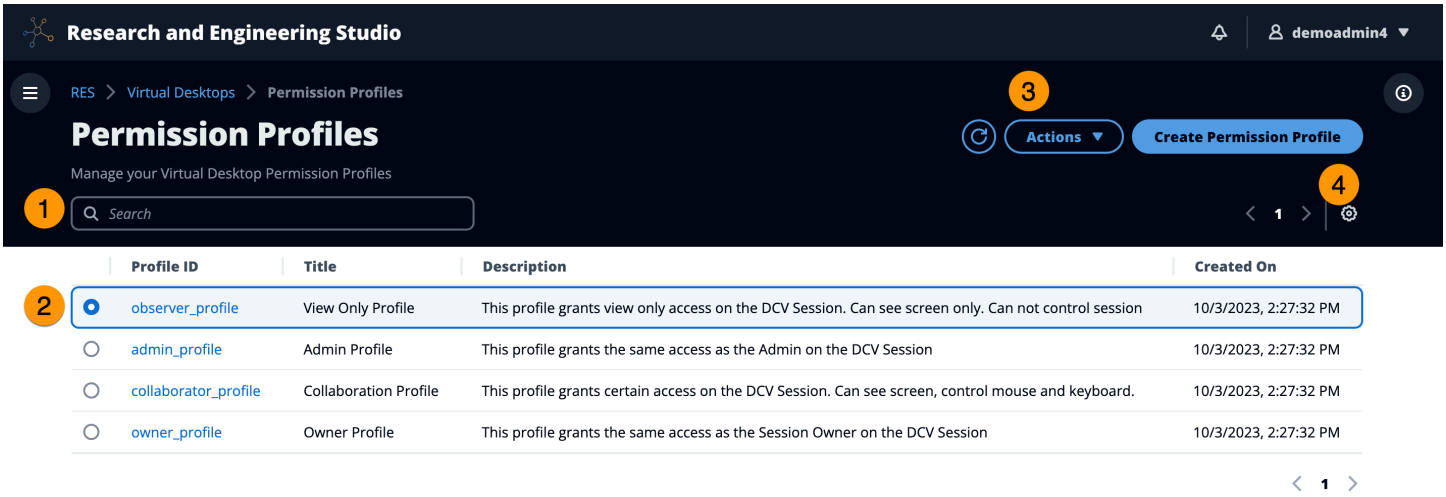


Visualizza i dettagli dello stack software

Dall'elenco Software Stacks, scegli il nome dello stack software per visualizzare i dettagli. Dalla pagina dei dettagli, puoi anche scegliere Modifica per modificare lo stack software.

Profili di autorizzazione

Utilizza i profili di autorizzazione per creare e gestire profili riutilizzabili per le autorizzazioni.



1. Cerca un profilo di autorizzazione.
2. Scegli l'ID del profilo per visualizzare i dettagli.
3. Quando viene selezionato un profilo, utilizza il menu Azioni per modificare il profilo.
4. Scegli Crea profilo di autorizzazione per creare un nuovo profilo.

Crea un profilo di autorizzazione

1. Scegli Crea profilo di autorizzazione.
2. Inserisci i dettagli per il nuovo profilo e usa gli interruttori di autorizzazione per selezionare le autorizzazioni per il profilo.
3. Scegli Invia.

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

Modifica un profilo di autorizzazione

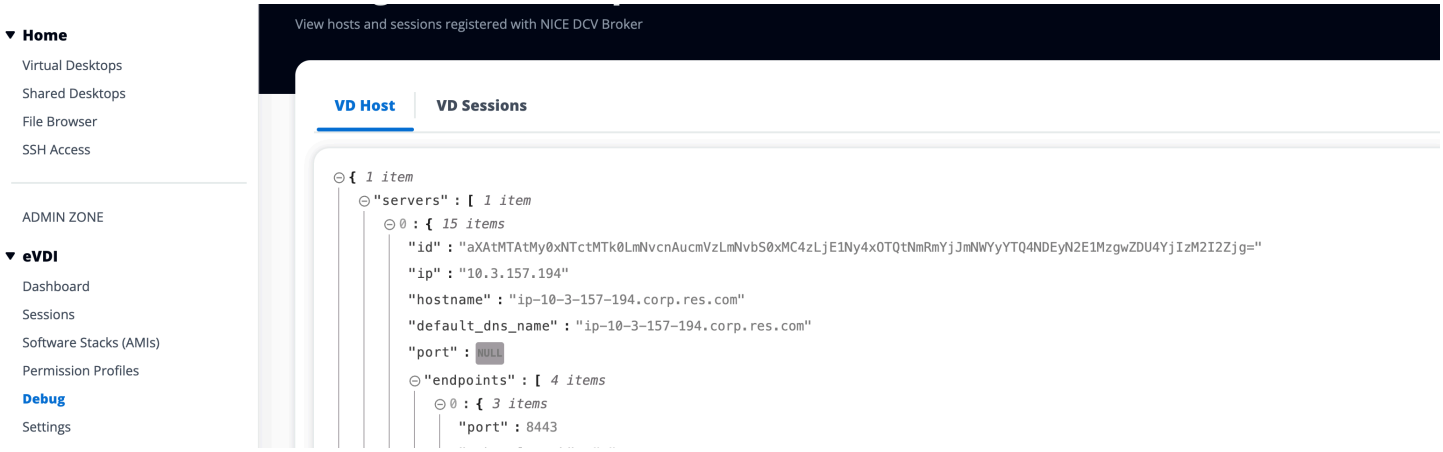
1. Seleziona il profilo di autorizzazione che devi modificare dalla pagina Profili di autorizzazione.
2. Scegli Azioni.
3. Scegli Modifica profilo di autorizzazione.
4. Modifica il profilo.
5. Scegli Invia.

Visualizza i dettagli del profilo di autorizzazione

Dall'elenco dei profili di autorizzazione, scegli l'ID del profilo per visualizzare i dettagli. Dalla pagina dei dettagli, puoi anche scegliere Modifica per modificare il profilo di autorizzazione.

Debug

Il pannello di debug mostra il traffico di messaggi associato ai desktop virtuali. È possibile utilizzare questo pannello per osservare l'attività tra gli host. La scheda VD Host mostra l'attività specifica dell'istanza e la scheda Sessioni VD mostra l'attività della sessione in corso.

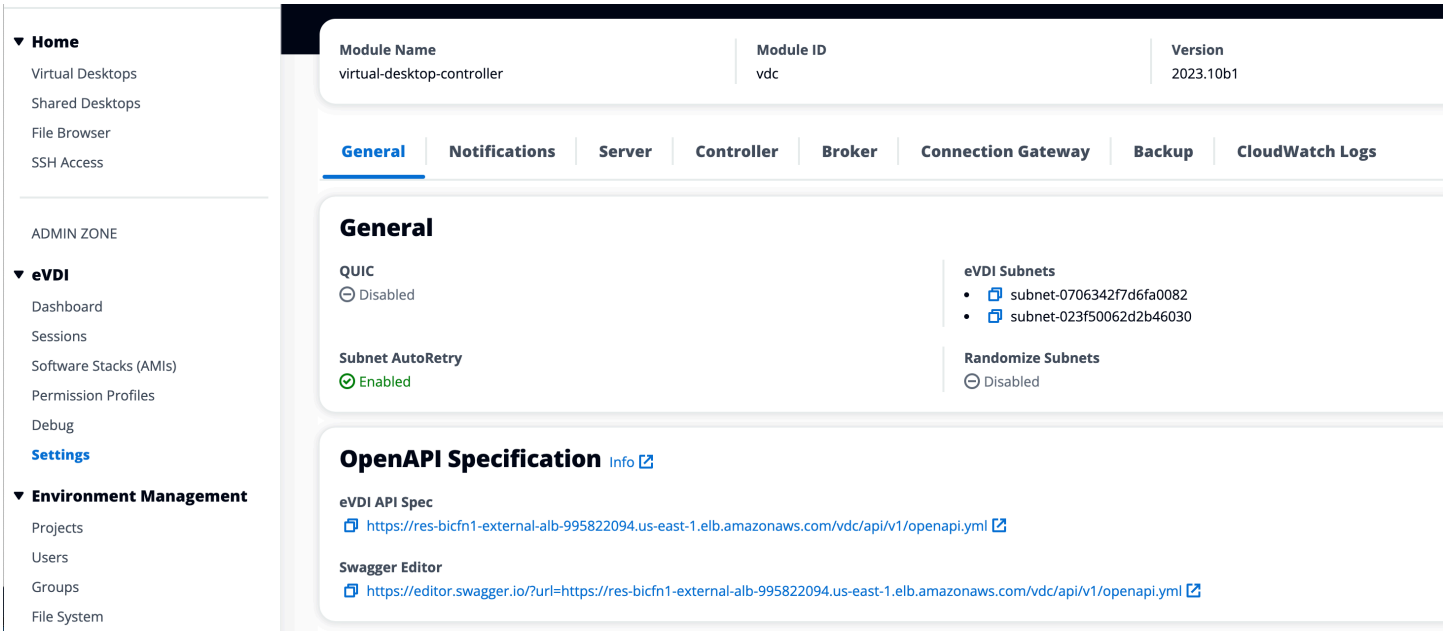


Impostazioni del desktop

È possibile utilizzare la pagina Impostazioni del desktop per configurare le risorse associate ai desktop virtuali. La scheda Server consente di accedere a impostazioni quali:

- Timeout di inattività della sessione DCV
- Avviso di timeout di inattività

- Soglia di utilizzo della CPU
- Sessioni consentite per utente



Gestione dell'ambiente

Dalla sezione Gestione ambientale di RES, gli utenti amministrativi possono creare e gestire ambienti isolati per i propri progetti di ricerca e ingegneria. Questi ambienti possono includere risorse di elaborazione, storage e altri componenti necessari, il tutto all'interno di un ambiente sicuro. Gli utenti possono configurare e personalizzare questi ambienti per soddisfare i requisiti specifici dei propri progetti, semplificando la sperimentazione, il test e l'iterazione delle soluzioni senza influire su altri progetti o ambienti.

Argomenti

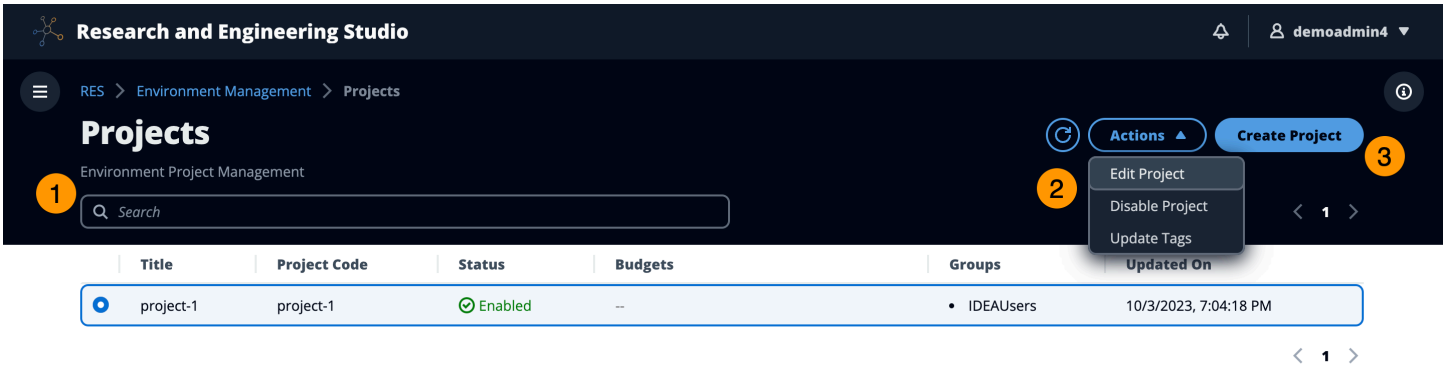
- Progetti
- Utenti
- Gruppi
- File system
- Stato dell'ambiente
- Gestione delle istantanee
- Impostazioni di ambiente

Progetti

I progetti costituiscono un limite per desktop virtuali, team e budget. Quando crei un progetto, ne definisci le impostazioni, come il nome, la descrizione e la configurazione dell'ambiente. I progetti includono in genere uno o più ambienti, che possono essere personalizzati per soddisfare i requisiti specifici del progetto, come il tipo e la dimensione delle risorse di elaborazione, lo stack software e la configurazione di rete.

Argomenti

Visualizza i progetti



La dashboard Progetti fornisce un elenco di progetti disponibili. Dalla dashboard Progetti, puoi:

1. Puoi utilizzare il campo di ricerca per trovare progetti.
2. Quando viene selezionato un progetto, puoi utilizzare il menu Azioni per:
   a. Modificare un progetto
   b. Disabilita o abilita un progetto
   c. Aggiorna i tag del progetto
3. Puoi scegliere Crea progetto per creare un nuovo progetto.

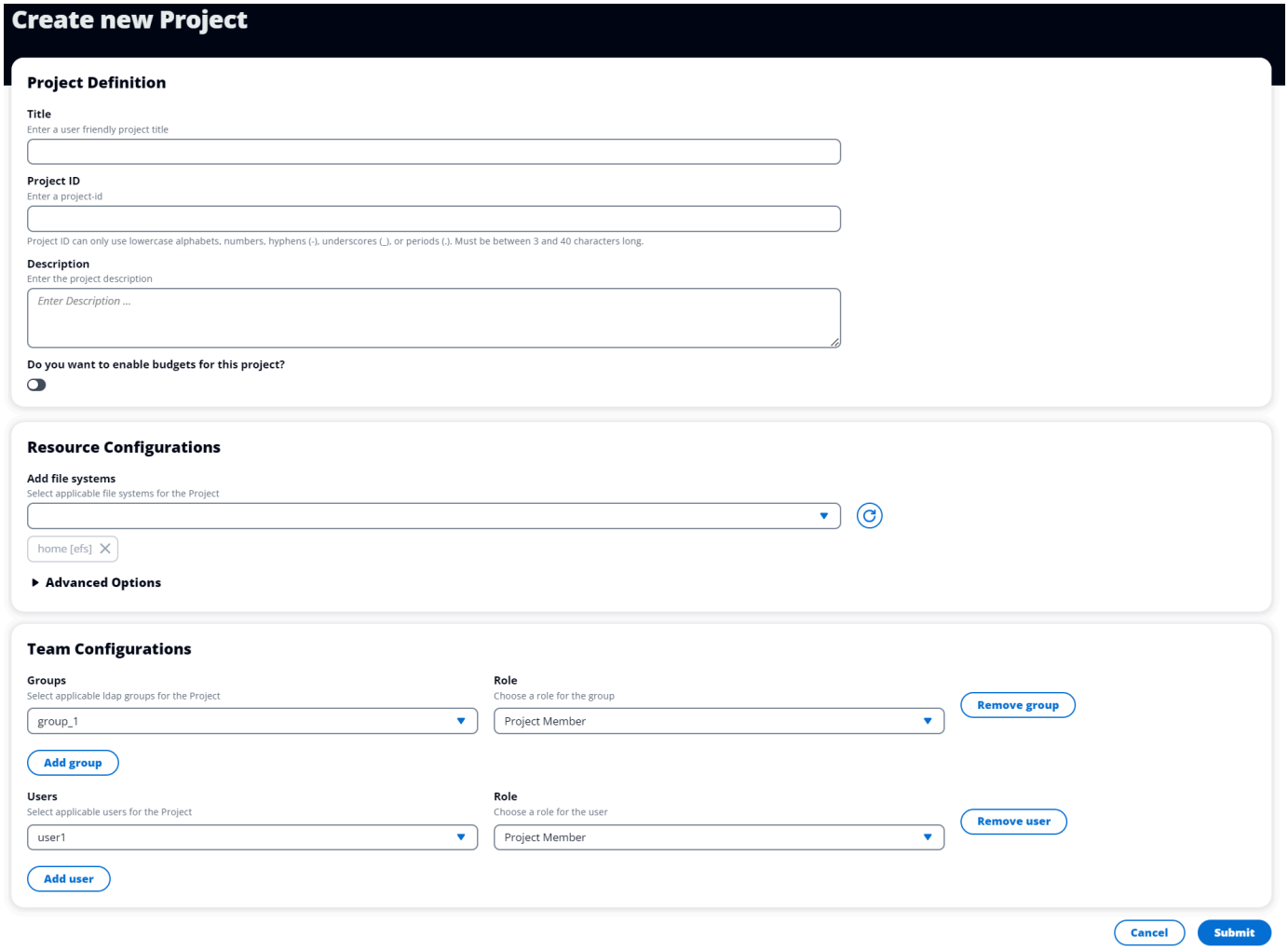
Crea un progetto

1. Scegli Crea progetto.
2. Inserisci i dettagli del progetto.

   L'ID del progetto è un tag di risorsa che può essere utilizzato per tenere traccia dell'allocazione dei costi in AWS Cost Explorer Service. Per ulteriori informazioni, vedere Attivazione dei tag di allocazione dei costi definiti dall'utente.

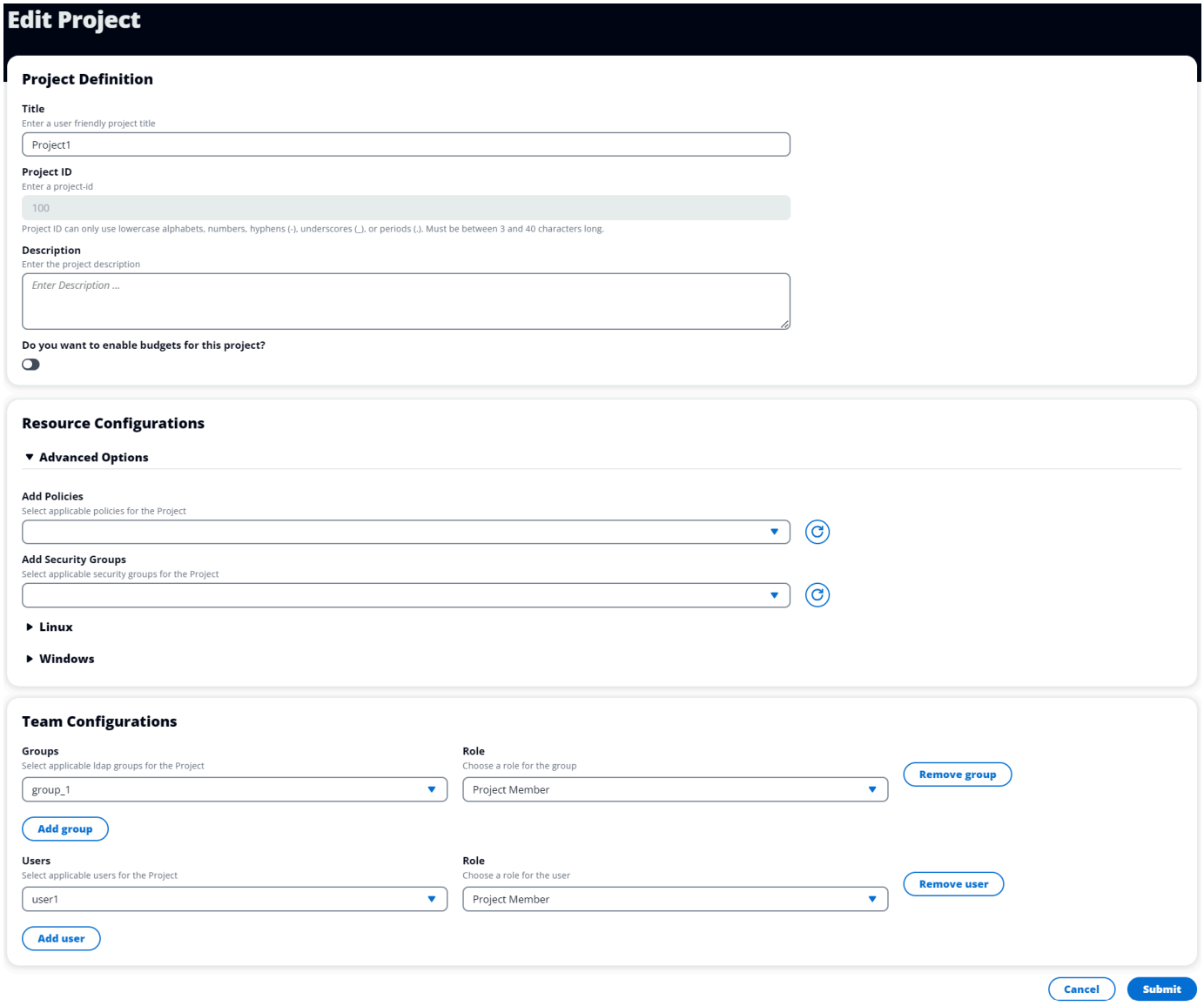
   > **Important**
   >
   > L'ID del progetto non può essere modificato dopo la creazione.

   Per informazioni sulle opzioni avanzate, vedereAggiungi un modello di lancio.
3. (Facoltativo) Attiva i budget per il progetto. Per ulteriori informazioni sui budget, consulta. Monitoraggio e controllo dei costi
4. Assegna agli utenti e/o ai gruppi il ruolo appropriato («Membro del progetto» o «Titolare del progetto»). Scopri Autorizzazioni le azioni che ogni ruolo può intraprendere.
5. Scegli Invia.



Modifica un progetto

1. Seleziona un progetto nell'elenco dei progetti.
2. Dal menu Azioni, scegli Modifica progetto.
3. Inserisci i tuoi aggiornamenti. Se intendi abilitare i budget, consulta Monitoraggio e controllo dei costi per ulteriori informazioni. Per informazioni sulle opzioni avanzate, consultaAggiungi un modello di lancio.
4. Scegli Invia.



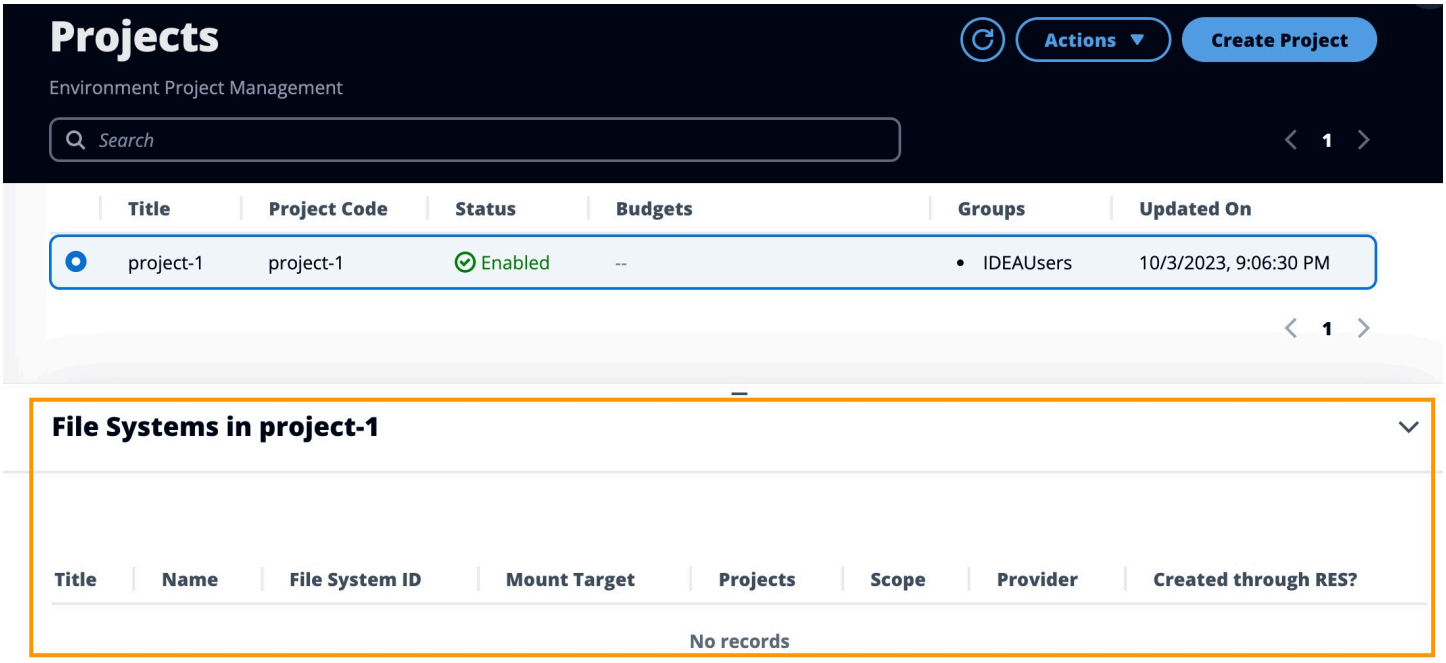
Aggiungere o rimuovere tag da un progetto

I tag di progetto assegneranno tag a tutte le istanze create nell'ambito di quel progetto.

1. Seleziona un progetto nell'elenco dei progetti.
2. Dal menu Azioni, scegli Aggiorna tag.
3. Scegli Aggiungi tag e inserisci un valore per Chiave.
4. Per rimuovere i tag, scegli Rimuovi accanto al tag che desideri rimuovere.

Visualizza i file system associati a un progetto

Quando viene selezionato un progetto, è possibile espandere il riquadro File system nella parte inferiore dello schermo per visualizzare i file system associati al progetto.



Aggiungi un modello di lancio

Quando crei o modifichi un progetto, puoi aggiungere modelli di lancio utilizzando le Opzioni avanzate all'interno della configurazione del progetto. I modelli di avvio forniscono configurazioni aggiuntive, come gruppi di sicurezza, policy IAM e script di avvio per tutte le istanze VDI all'interno del progetto.

Aggiungi politiche

Puoi aggiungere una policy IAM per controllare l'accesso VDI per tutte le istanze distribuite nell'ambito del tuo progetto. Per integrare una policy, contrassegna la policy con la seguente coppia chiave-valore:

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

Per ulteriori informazioni sui ruoli IAM, consulta Politiche e autorizzazioni in IAM.

Aggiunta di gruppi di sicurezza

Puoi aggiungere un gruppo di sicurezza per controllare i dati in uscita e in ingresso per tutte le istanze VDI del tuo progetto. Per integrare un gruppo di sicurezza, tagga il gruppo di sicurezza con la seguente coppia chiave-valore:

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

Per ulteriori informazioni sui gruppi di sicurezza, consulta Controlla il traffico verso AWS le tue risorse utilizzando i gruppi di sicurezza nella Amazon VPC User Guide.

Aggiungi script di avvio

È possibile aggiungere script di avvio che verranno avviati in tutte le sessioni VDI all'interno del progetto. RES supporta l'avvio degli script per Linux e Windows. Per l'avvio dello script, puoi scegliere tra:

Esegui script all'avvio di VDI

> Questa opzione avvia lo script all'inizio di un'istanza VDI prima dell'esecuzione di qualsiasi configurazione o installazione RES.

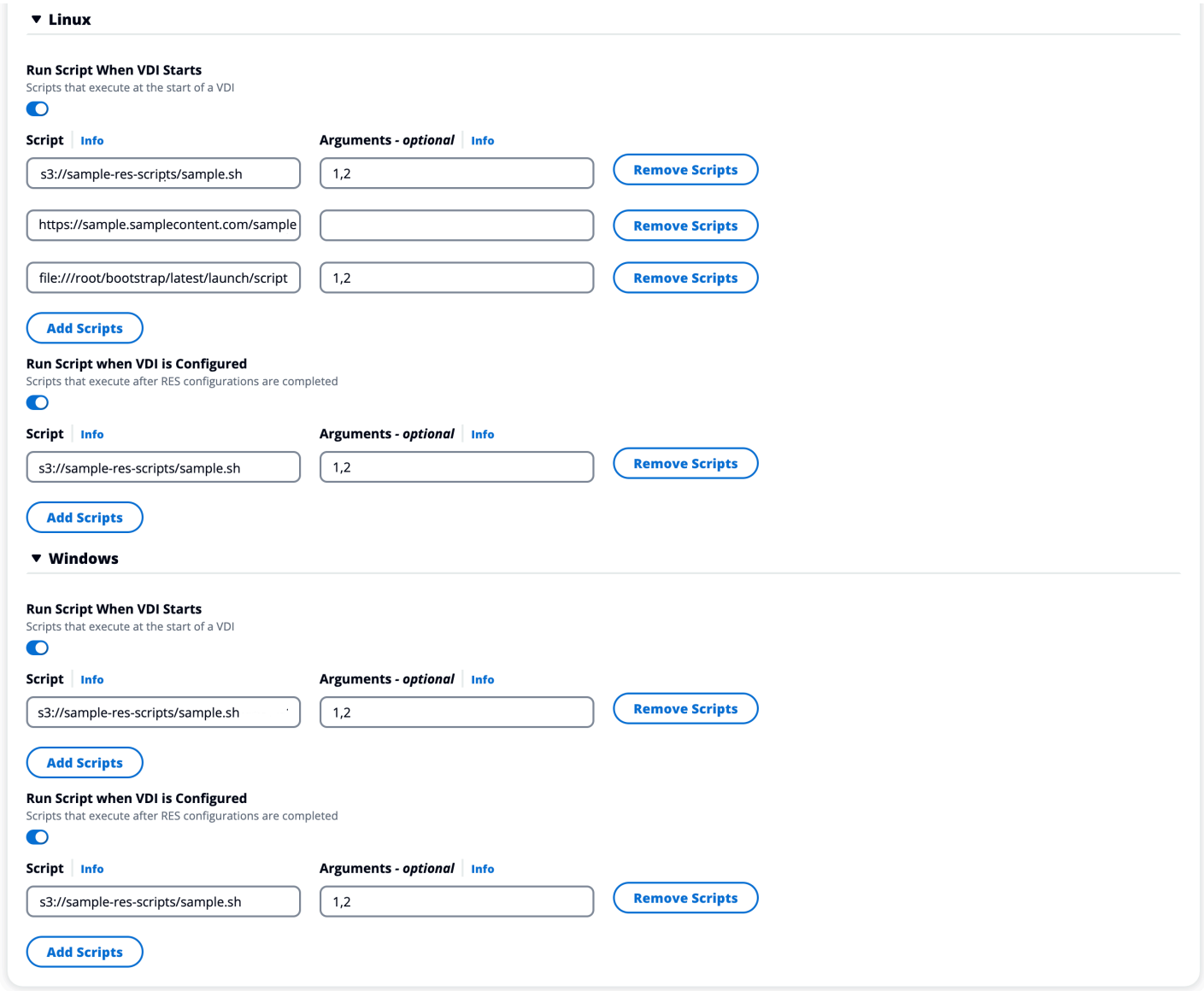
Esegui lo script quando VDI è configurato

> Questa opzione avvia lo script dopo il completamento delle configurazioni RES.

Gli script supportano le seguenti opzioni:

Configurazione degli script	Esempio
URI S3	s3://bucketname/script.sh
HTTPS URL (URL HTTPS)	https://sample.samplecontent.com/sample
File locale	file: ///user/scripts/example.sh

Per Argomenti, fornisci tutti gli argomenti separati da una virgola.

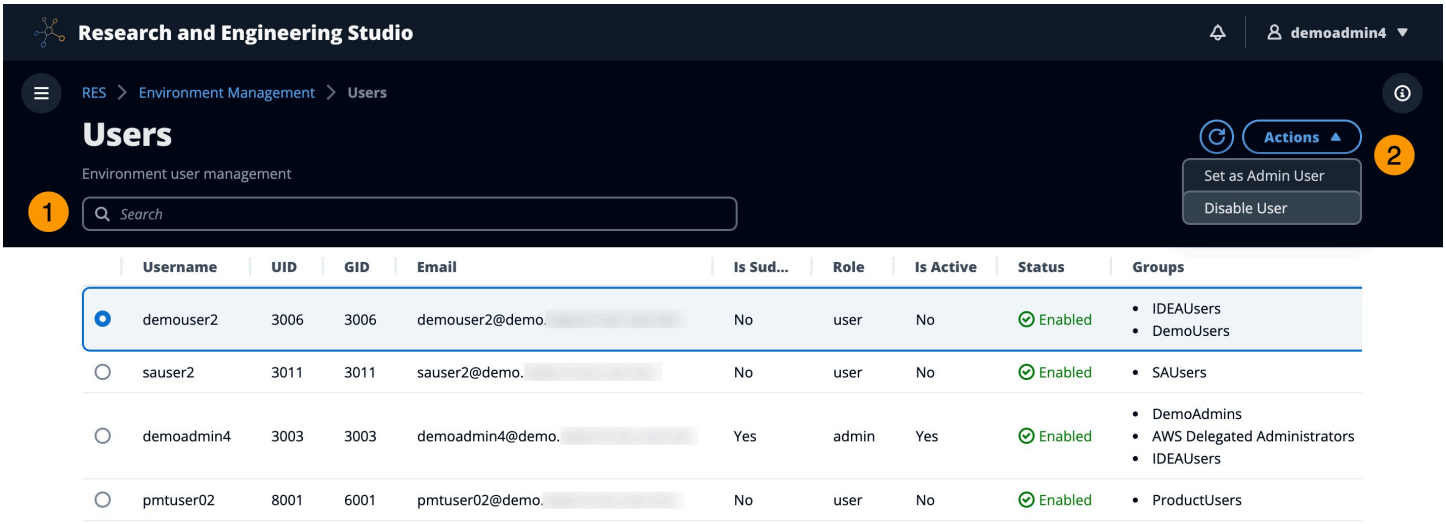


Esempio di configurazione di progetto

Utenti

Tutti gli utenti sincronizzati da Active Directory verranno visualizzati nella pagina Utenti. Gli utenti vengono sincronizzati dall'utente cluster-admin durante la configurazione del prodotto. Per ulteriori informazioni sulla configurazione iniziale dell'utente, consulta. Guida alla configurazione

> **Note**
>
> Gli amministratori possono creare sessioni solo per utenti attivi. Per impostazione predefinita, tutti gli utenti resteranno inattivi finché non accederanno all'ambiente del prodotto. Se un utente è inattivo, chiedigli di accedere prima di creare una sessione per lui.

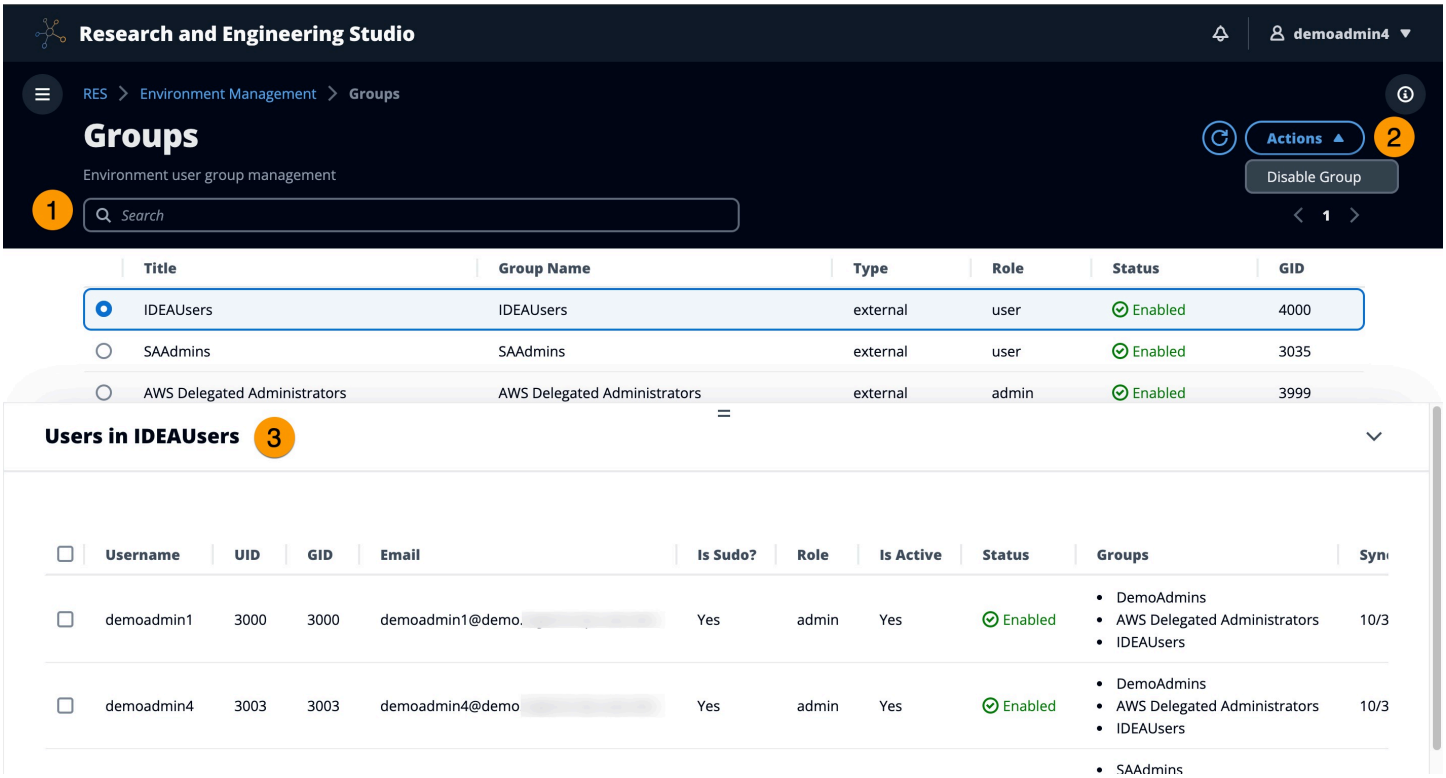


Dalla pagina Utenti, puoi:

1. Cerca gli utenti.
2. Quando è selezionato un nome utente, utilizza il menu Azioni per:
    a. Imposta come utente amministratore
    b. Disabilita utente

Gruppi

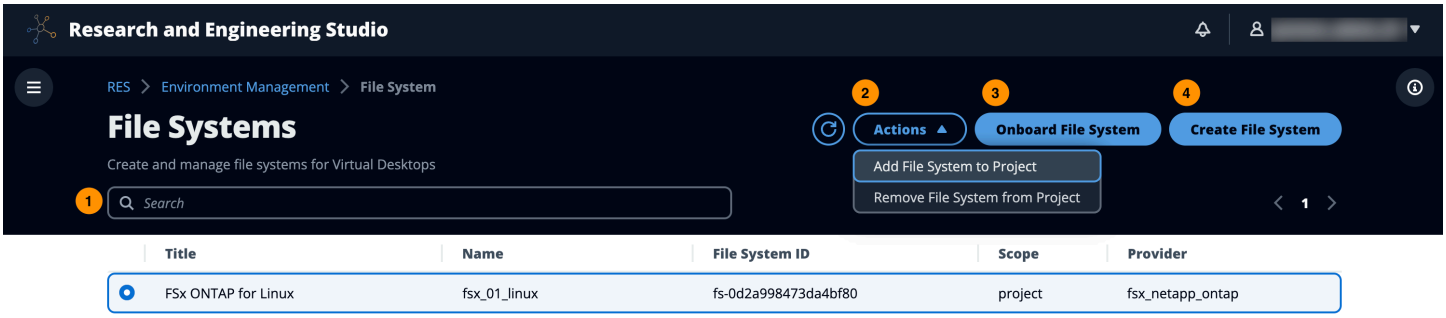
Tutti i gruppi sincronizzati da Active Directory vengono visualizzati nella pagina Gruppi. Per ulteriori informazioni sulla configurazione e la gestione dei gruppi, consultaGuida alla configurazione.



Dalla pagina Gruppi, puoi:

1. Cerca gruppi di utenti.
2. Quando è selezionato un gruppo di utenti, utilizzate il menu Azioni per disabilitare o abilitare un gruppo.
3. Quando è selezionato un gruppo di utenti, è possibile espandere il riquadro Utenti nella parte inferiore dello schermo per visualizzare gli utenti del gruppo.

File system



Dalla pagina File system è possibile:

1. Cercare i file system.
2. Quando è selezionato un file system, utilizzate il menu Azioni per:
    a. Aggiungere il file system a un progetto
    b. Rimuovere il file system da un progetto
3. Incorpora un nuovo file system.
4. Creare un file system.
5. Quando viene selezionato un file system, è possibile espandere il riquadro nella parte inferiore dello schermo per visualizzare i dettagli del file system.

Creare un file system

1. Scegliere Create File System (Crea file system).
2. Immettete i dettagli per il nuovo file system.
3. Fornisci gli ID di sottorete dal VPC. Puoi trovare gli ID nella scheda Gestione dell'ambiente > Impostazioni > Rete.
4. Scegli Invia.

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

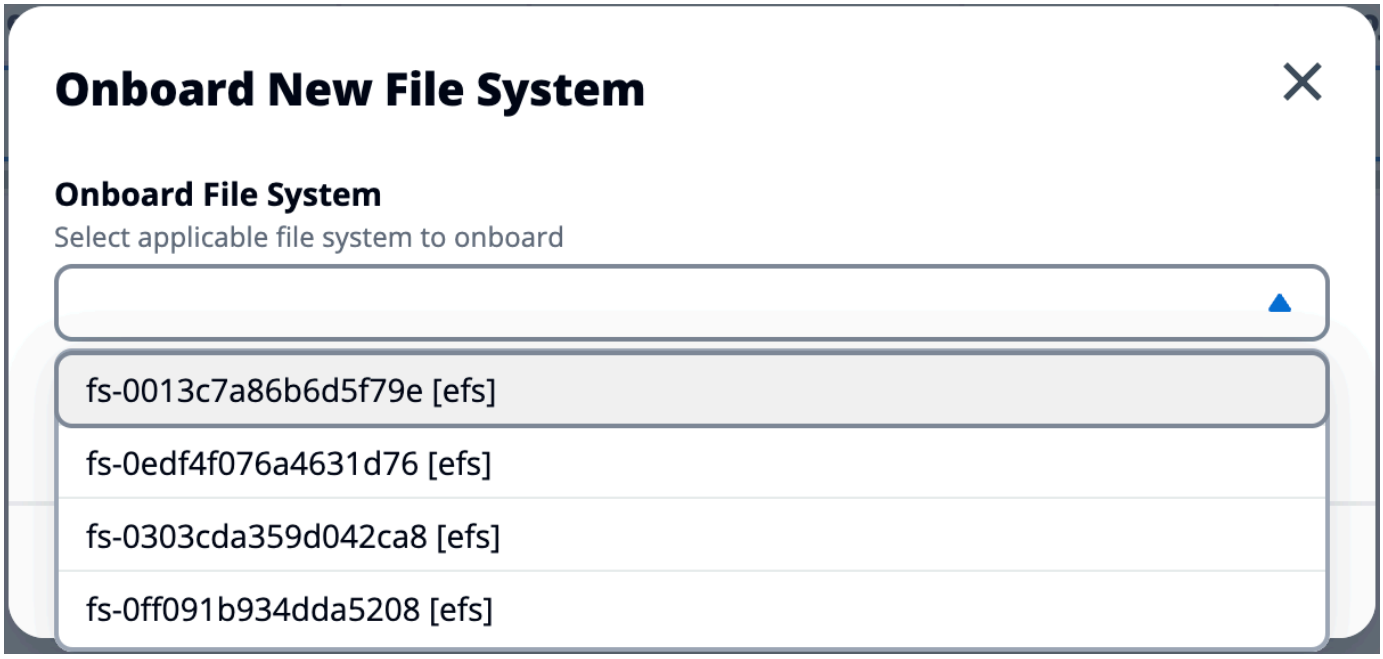
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

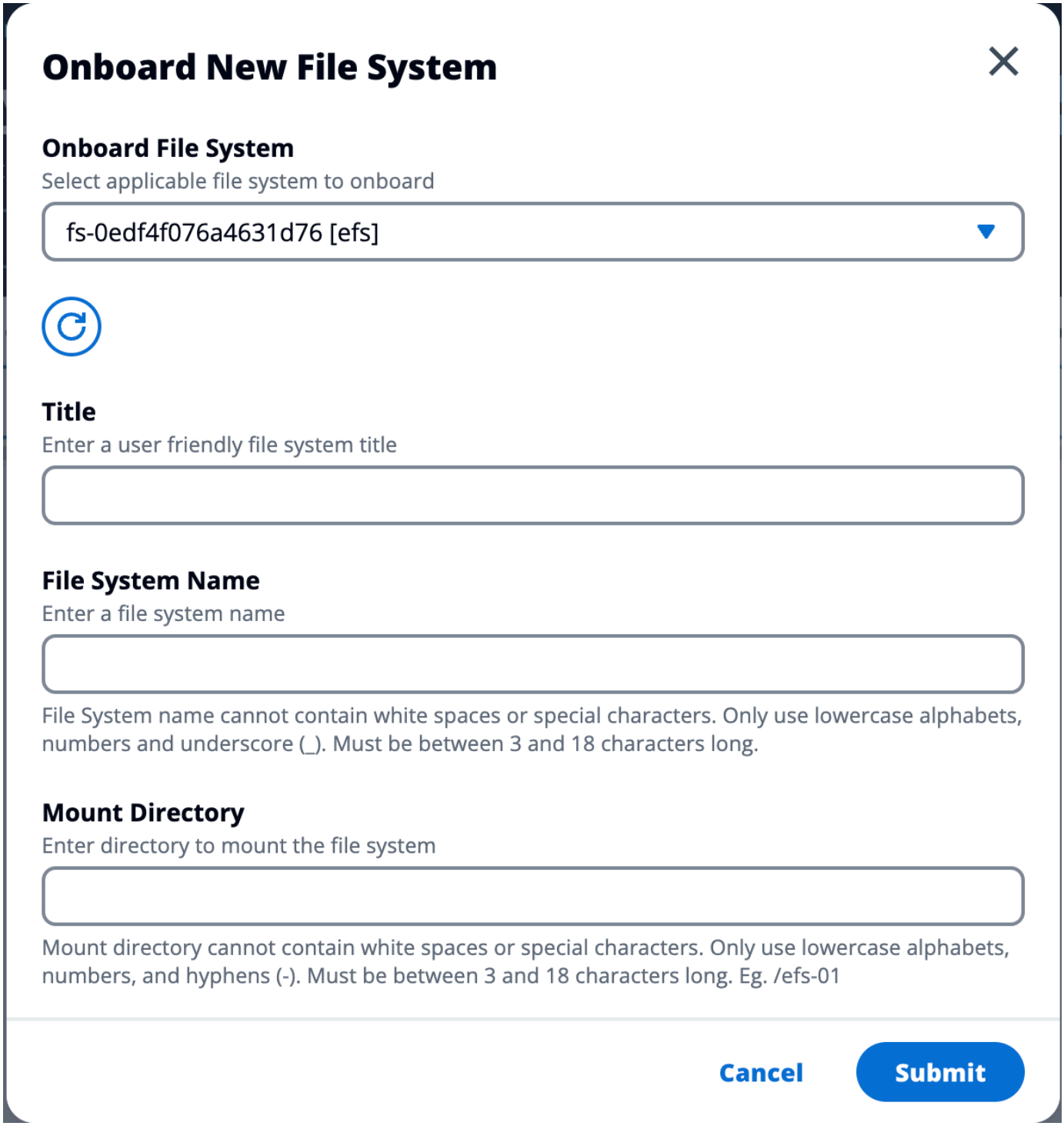
Enter directory to mount the file system

Incorpora un file system

1. Scegli Onboard File System.
2. Seleziona un file system dal menu a discesa. Il modale si espanderà con ulteriori inserimenti di dettagli.

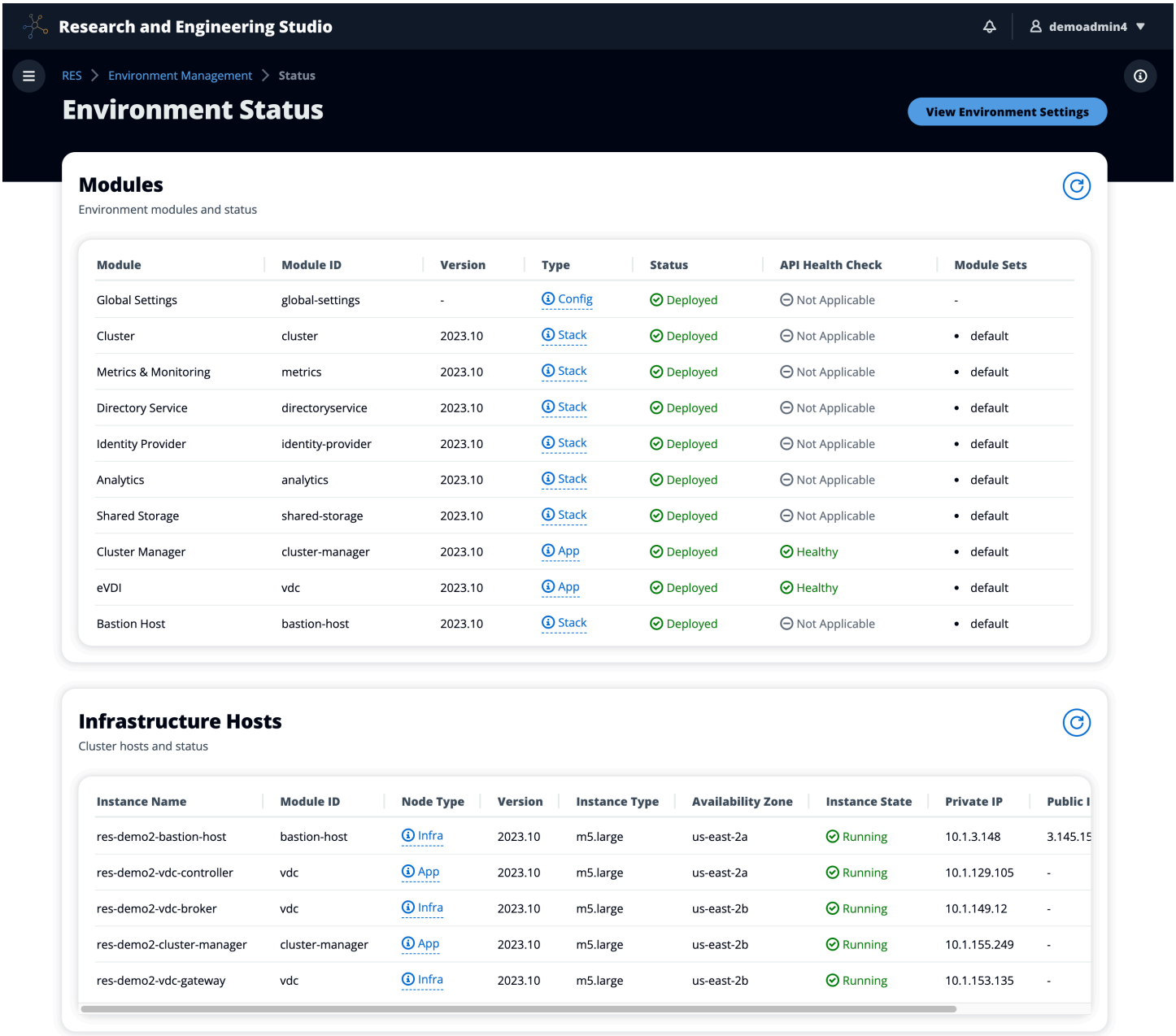


3. Inserisci i dettagli del file system.
4. Scegli Invia.



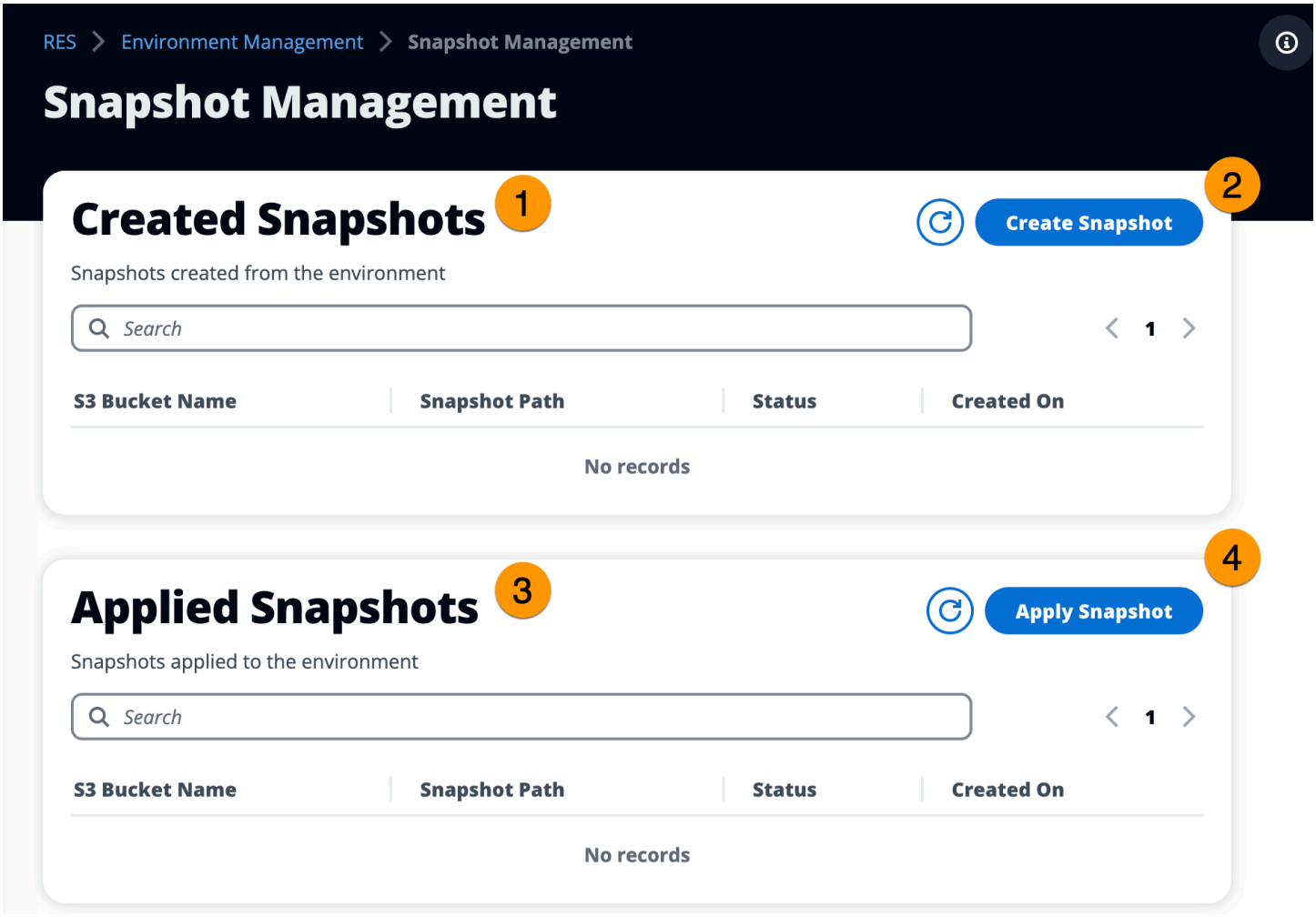
Stato dell'ambiente

La pagina Environment Status mostra il software e gli host distribuiti all'interno del prodotto. Include informazioni quali la versione del software, i nomi dei moduli e altre informazioni di sistema.



Gestione delle istantanee

La gestione delle istantanee semplifica il processo di salvataggio e migrazione dei dati tra ambienti, garantendo coerenza e precisione. Con le istantanee, è possibile salvare lo stato dell'ambiente e migrare i dati in un nuovo ambiente con lo stesso stato.



Dalla pagina di gestione delle istantanee, è possibile:

1. Visualizzare tutte le istantanee create e il relativo stato.
2. Crea un'istantanea. Prima di poter creare un'istantanea, è necessario creare un bucket con le autorizzazioni appropriate.
3. Visualizza tutte le istantanee applicate e il relativo stato.
4. Applica un'istantanea.

Creazione di una snapshot

Prima di poter creare uno snapshot, devi fornire a un bucket Amazon S3 le autorizzazioni necessarie. Per informazioni sulla creazione di un bucket, consulta Creazione di un bucket. Ti consigliamo di abilitare il controllo delle versioni del bucket e la registrazione degli accessi al server. Queste impostazioni possono essere abilitate dalla scheda Proprietà del bucket dopo il provisioning.

> **Note**
>
> Il ciclo di vita di questo bucket Amazon S3 non verrà gestito all'interno del prodotto. Dovrai gestire il ciclo di vita del bucket dalla console.

Per aggiungere autorizzazioni al bucket:

1. Scegli il bucket che hai creato dall'elenco dei bucket.
2. Scegli la scheda Autorizzazioni.
3. In Bucket Policy (Policy del bucket) scegliere Edit (Modifica).
4. Aggiungi la seguente dichiarazione alla policy del bucket. Sostituire questi valori con i propri valori:

   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - NOME_BUCKET S3_

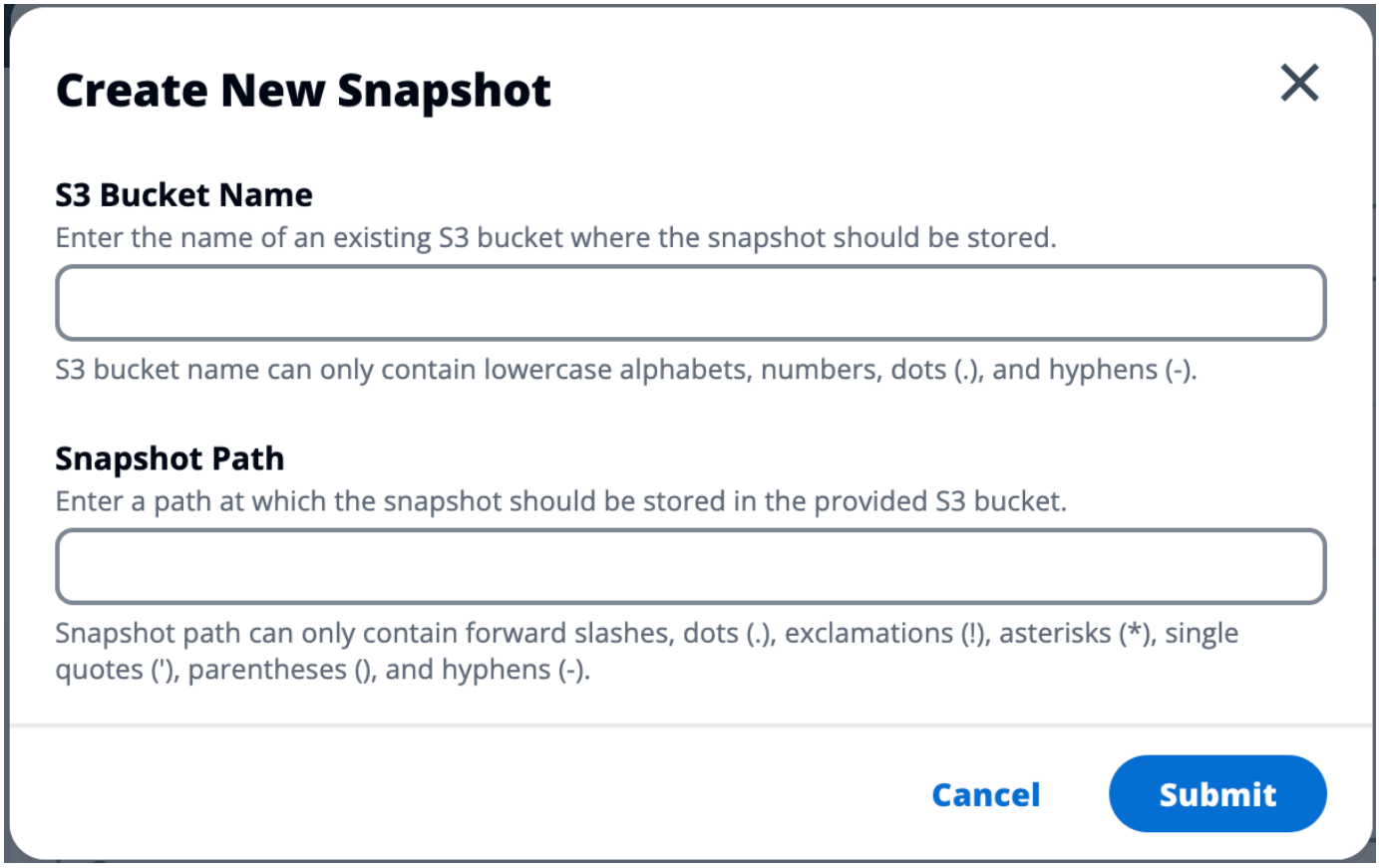
> **Important**
>
> Esistono stringhe di versione limitate supportate da. AWS Per ulteriori informazioni, consulta https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html

```
{
    "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": "*"
        }
    ]
}
```

Per creare l'istantanea:

1. Selezionare Create Snapshot (Crea snapshot).
2. Inserisci il nome del bucket Amazon S3 che hai creato.
3. Inserisci il percorso in cui desideri che lo snapshot venga archiviato all'interno del bucket. Ad esempio, **`october2023/23`**.
4. Scegli Invia.



5. Dopo cinque-dieci minuti, scegli Aggiorna nella pagina Istantanee per verificare lo stato. Un'istantanea non sarà valida finché lo stato non passerà da IN_PROGRESS a COMPLETED.

Applica un'istantanea

Dopo aver creato un'istantanea di un ambiente, è possibile applicarla a un nuovo ambiente per migrare i dati. Dovrai aggiungere una nuova policy al bucket che consenta all'ambiente di leggere l'istantanea.

L'applicazione di un'istantanea copia dati quali autorizzazioni utente, progetti, stack software, profili di autorizzazione e file system con le relative associazioni in un nuovo ambiente. Le sessioni utente non verranno replicate. Quando viene applicata, l'istantanea controlla le informazioni di base di ogni record di risorse per determinare se esiste già. Per i record duplicati, l'istantanea salta la creazione di risorse nel nuovo ambiente. Per i record simili, ad esempio che condividono un nome o una chiave, ma le altre informazioni di base sulle risorse variano, verrà creato un nuovo record con un nome e una chiave modificati utilizzando la seguente convenzione:. `RecordName_SnapshotRESVersion_ApplySnapshotID` `ApplySnapshotID`Sembra un timestamp e identifica ogni tentativo di applicare un'istantanea.

Durante l'applicazione dello snapshot, l'istantanea verifica la disponibilità delle risorse. La risorsa non disponibile per il nuovo ambiente non verrà creata. Per le risorse con una risorsa dipendente, l'istantanea verifica la disponibilità della risorsa dipendente. Se la risorsa dipendente non è disponibile, creerà la risorsa principale senza la risorsa dipendente.

Se il nuovo ambiente non è come previsto o non funziona, puoi controllare CloudWatch i log trovati nel gruppo di log `/res-<env-name>/cluster-manager` per i dettagli. Ogni registro avrà il tag [apply snapshot]. Dopo aver applicato un'istantanea, puoi controllarne lo stato dalla the section called “Gestione delle istantanee” pagina.

Per aggiungere autorizzazioni al bucket:

1. Scegli il bucket che hai creato dall'elenco dei bucket.
2. Scegli la scheda Autorizzazioni.
3. In Bucket Policy (Policy del bucket) scegliere Edit (Modifica).
4. Aggiungi la seguente dichiarazione alla policy del bucket. Sostituire questi valori con i propri valori:

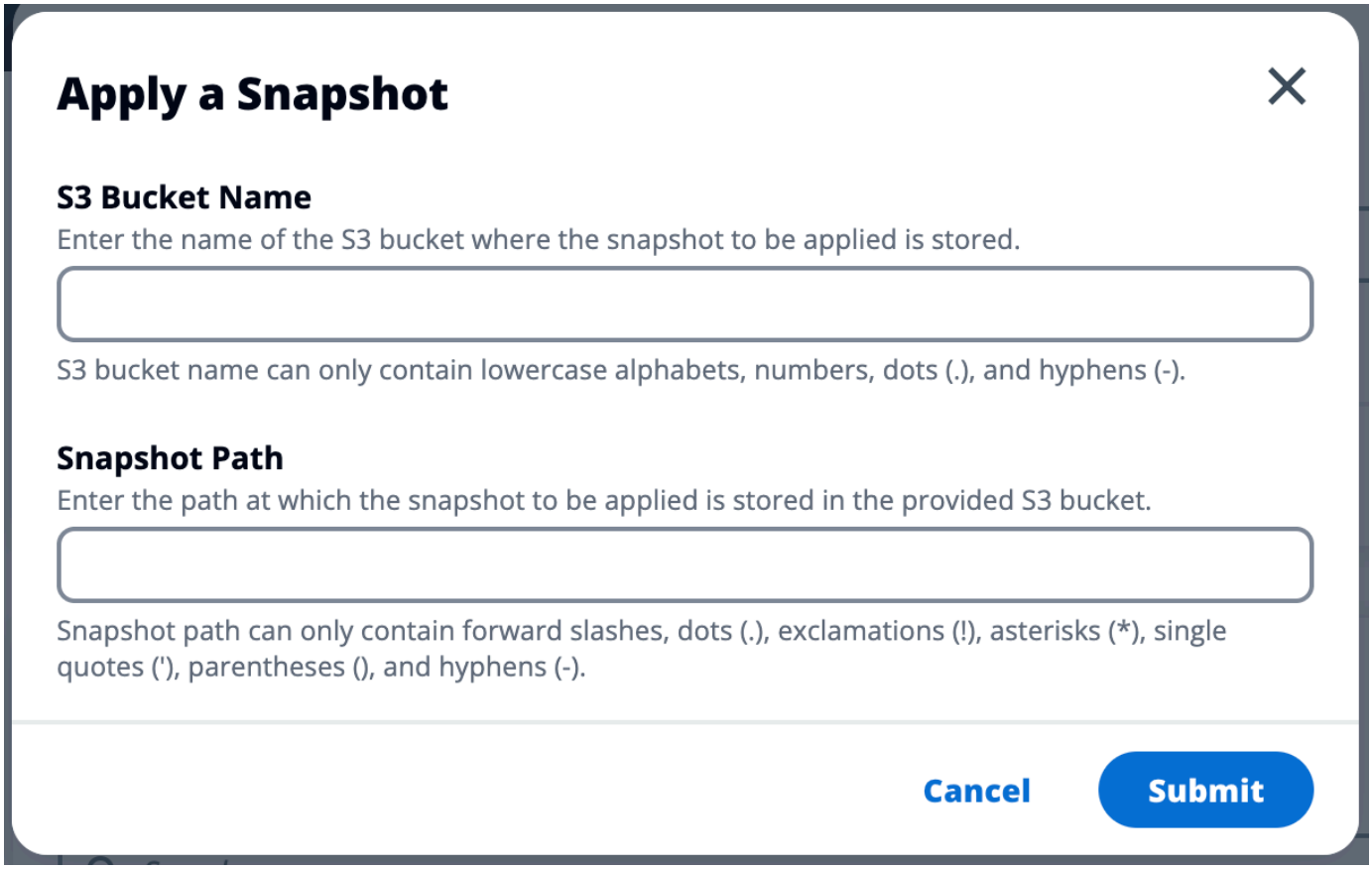
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - NOME_BUCKET S3_

```
{
    "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": "*"
        }
    ]
}
```

Per applicare l'istantanea:

1. Scegli Applica istantanea.
2. Inserisci il nome del bucket Amazon S3 contenente lo snapshot.
3. Inserisci il percorso del file dello snapshot all'interno del bucket.
4. Scegli Invia.



5. Dopo cinque-dieci minuti, scegli Aggiorna nella pagina di gestione delle istantanee per verificarne lo stato.

Impostazioni di ambiente

Le impostazioni di ambiente mostrano i dettagli di configurazione del prodotto, come:

- Generali

  Visualizza informazioni come il nome utente dell'amministratore e l'e-mail dell'utente che ha fornito il prodotto. È possibile modificare il titolo del portale Web e il testo del copyright.

- Provider di identità

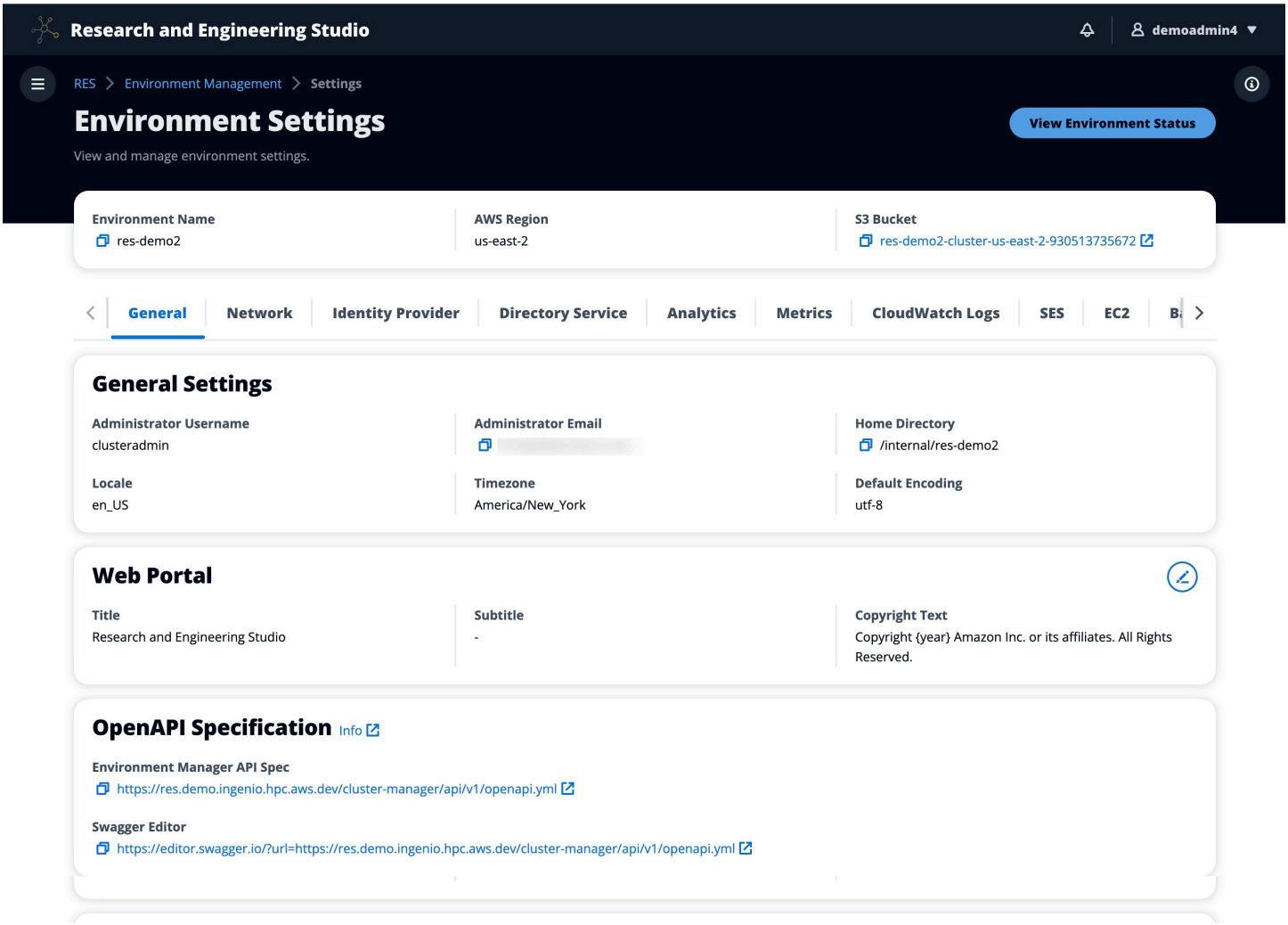
  Visualizza informazioni come lo stato del Single Sign-On.

- Rete

  Visualizza l'ID VPC, gli ID dell'elenco dei prefissi per l'accesso.

- Directory Service

Visualizza le impostazioni di Active Directory e l'ARN del gestore segreti degli account di servizio per nome utente e password.



Gestione dei segreti

Research and Engineering Studio conserva i seguenti segreti utilizzando AWS Secrets Manager. RES crea automaticamente i segreti durante la creazione dell'ambiente. I segreti immessi dall'amministratore durante la creazione dell'ambiente vengono immessi come parametri.

Nome segreto	Descrizione	RES generato	Amministratore inserito
<envname>- sso-client-secret	Segreto del client OAuth2 Single Sign-On per l'ambiente	✓	
<envname>- vdc-client-secret	- vdc ClientSecret	✓	
<envname>- vdc-client-id	- vdc ClientId	✓	
<envname>- -chiave vdc-gateway-certificate-private	Chiave privata del certificato autofirmato per il dominio	✓	
<envname>- vdc-gateway-certificate-certificate	Certificato autofirmato per dominio	✓	
<envname>- cluster-manager-client-secret	gestore di cluster ClientSecret	✓	
<envname>- cluster-manager-client-id	gestore di cluster ClientId	✓	
<envname>- external-private-key	Chiave privata del certificato autofirmato per il dominio	✓	
<envname>-certificato esterno	Certificato autofirmato per il dominio	✓	
<envname>- internal-private-key	Chiave privata del certificato autofirmato per il dominio	✓	

Nome segreto	Descrizione	RES generato	Amministratore inserito
<envname>-certificato interno	Certificato autofirmato per il dominio	✓	
<envname>-servizio di directory - ServiceAccountUsername			✓
<envname>- servizio di elenchi - ServiceAccountPassword			✓

I seguenti valori ARN segreti sono contenuti nella tabella <envname>-cluster-settings di DynamoDB:

Chiave	Origine
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
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	stack
directoryservice.root_password_secret_arn	

Chiave	Origine
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	stack
cluster-manager.client_secret	

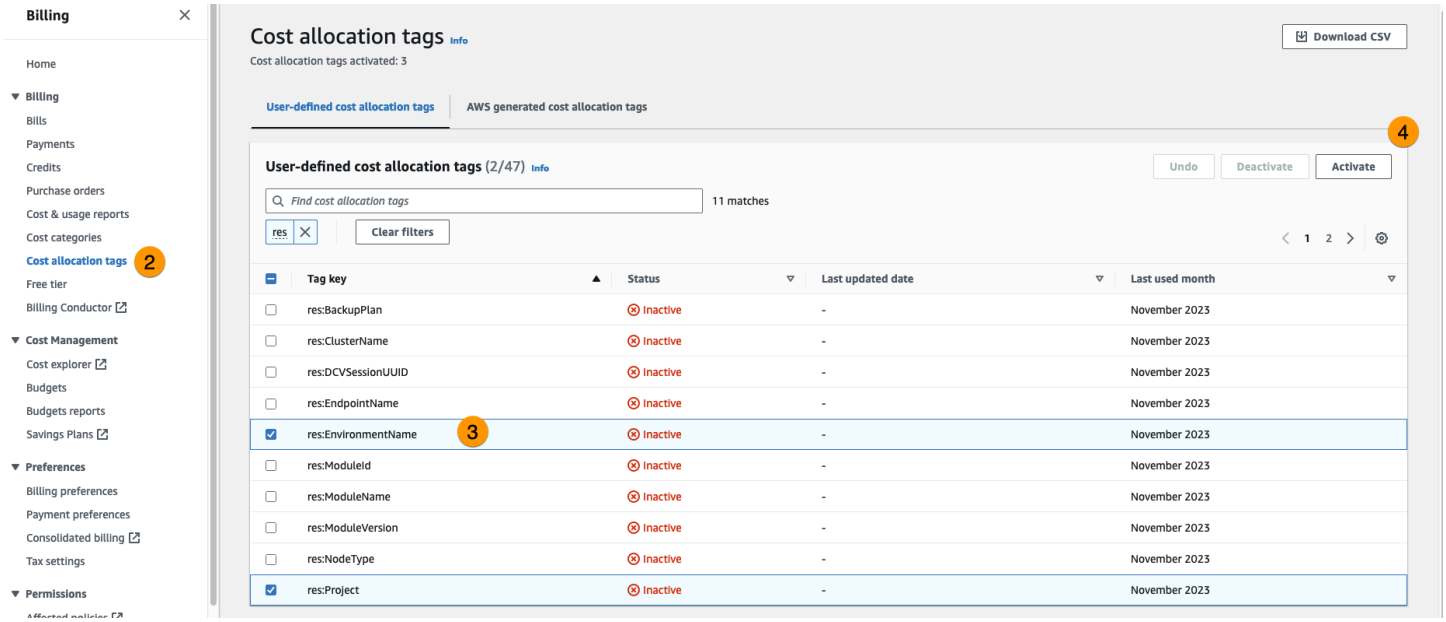
Monitoraggio e controllo dei costi

> **Note**
>
> L'associazione di progetti di Research and Engineering Studio a non Budget AWS è supportata in AWS GovCloud (US).

Ti consigliamo di creare un budget tramite AWS Cost Explorer per facilitare la gestione dei costi. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi per ciascuno deithe section called “AWSservizi inclusi in questo prodotto”.

Per facilitare il monitoraggio dei costi, puoi associare i progetti RES ai budget creati all'interno. Budget AWS Dovrai prima attivare i tag di ambiente all'interno dei tag di allocazione dei costi di fatturazione.

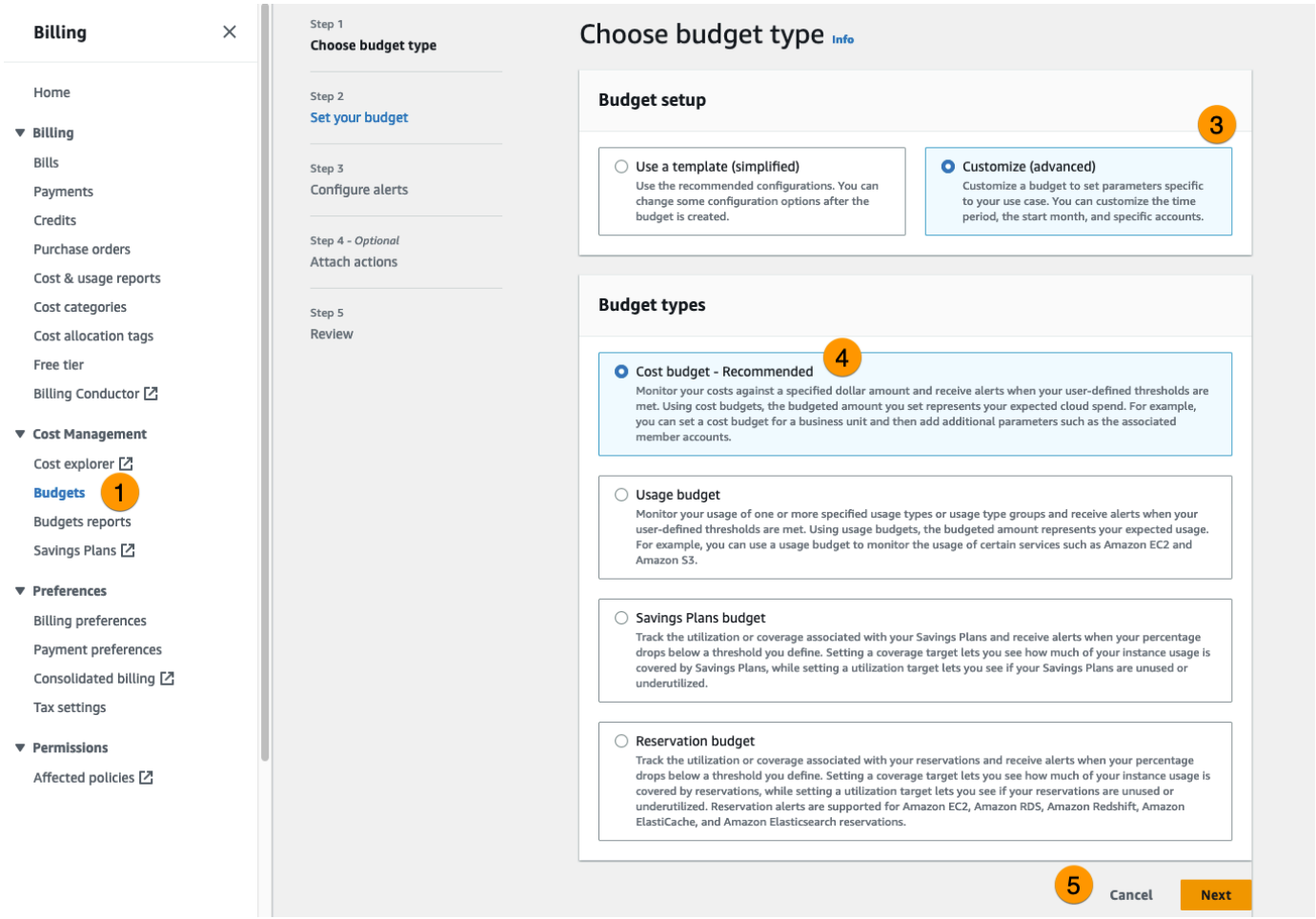
1. Accedi AWS Management Console e apri la AWS Billing console all'indirizzo https://console.aws.amazon.com/billing/.
2. Scegli i tag di allocazione dei costi.
3. Cerca e seleziona i `res:EnvironmentName` tag `res:Project` e.
4. Seleziona Activate (Attiva).



> **Note**
>
> La visualizzazione dei tag RES dopo la distribuzione può richiedere fino a un giorno.

Per creare un budget per le risorse RES:

1. Dalla console di fatturazione, scegli Budget.
2. Scegli Crea un budget.
3. In Configurazione del budget, scegli Personalizza (avanzato).
4. In Tipi di budget, scegli Budget di costo - Consigliato.
5. Seleziona Successivo.

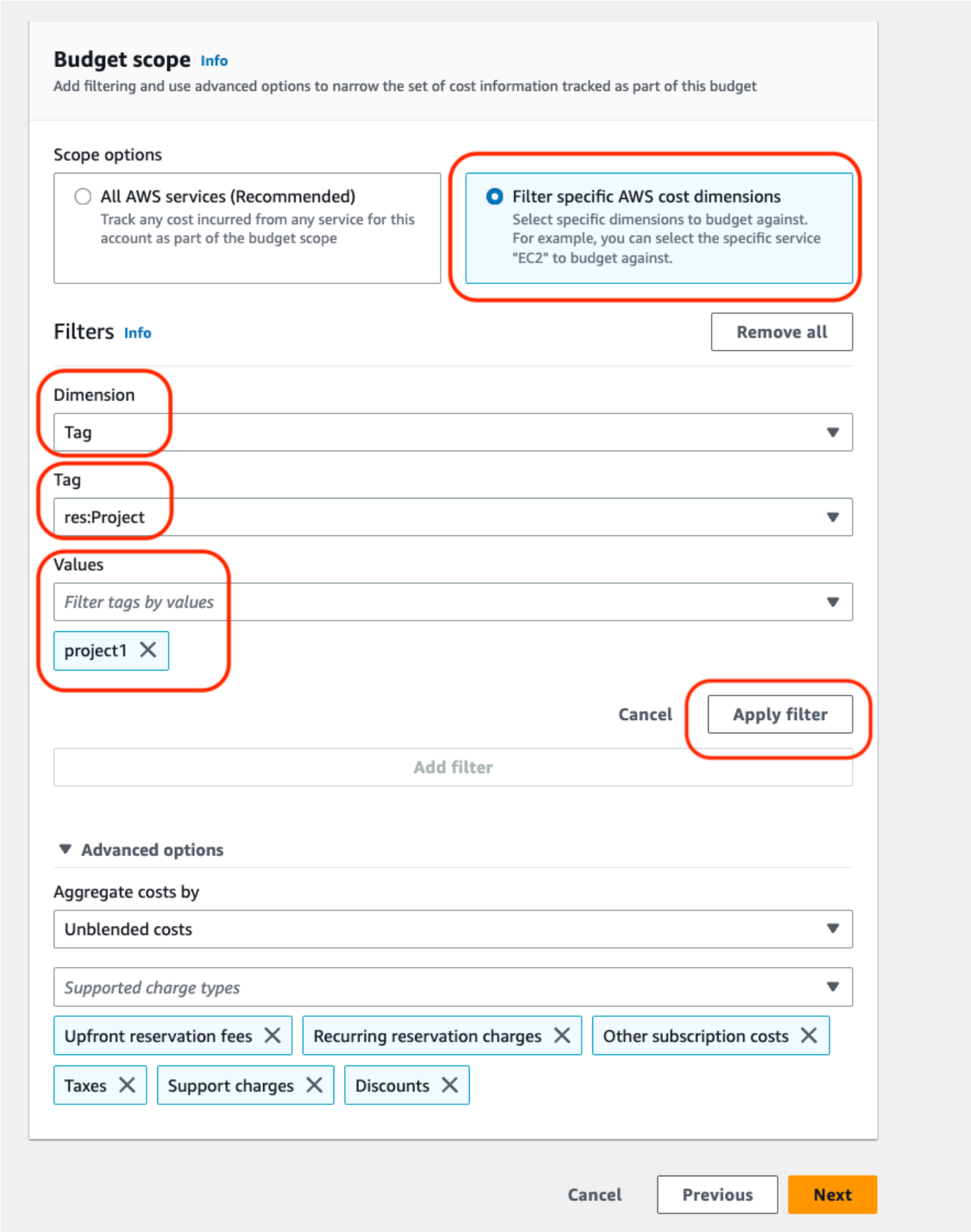


6. In Dettagli, inserisci un nome di budget significativo per il tuo budget per distinguerlo dagli altri budget del tuo account. Ad esempio, [EnvironmentName] - [ProjectName] - [BudgetName].
7. In Imposta l'importo del budget, inserisci l'importo previsto per il tuo progetto.
8. In Ambito del budget, scegli Filtra dimensioni di AWS costo specifiche.
9. Scegliere Add filter (Aggiungi filtro).
10. In Dimensione, scegli Tag.
11. In Tag, seleziona res:Project.

> **Note**
>
> Potrebbero essere necessari fino a due giorni prima che tag e valori diventino disponibili. Puoi creare un budget una volta che il nome del progetto sarà disponibile.

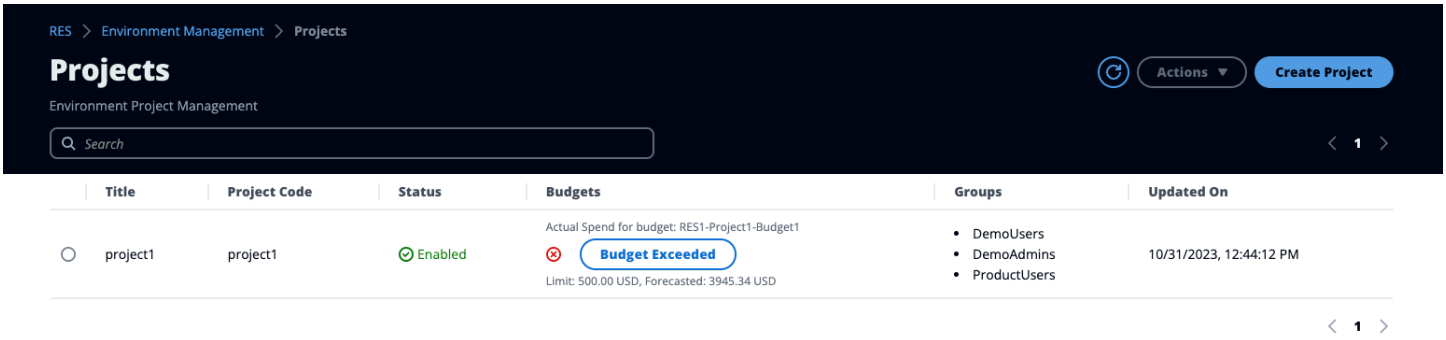
12. In Valori, seleziona il nome del progetto.
13. Scegli Applica filtro per allegare il filtro del progetto al budget.

14. Seleziona Successivo.


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. Opzionale. Aggiungi una soglia di avviso.
16. Seleziona Successivo.
17. Opzionale. Se è stato configurato un avviso, utilizza Allega azioni per configurare le azioni desiderate con l'avviso.
18. Seleziona Successivo.
19. Rivedi la configurazione del budget e conferma che il tag corretto sia stato impostato in Parametri di budget aggiuntivi.
20. Scegli Crea budget.

Ora che il budget è stato creato, puoi abilitarlo per i progetti. Per attivare i budget per un progetto, consultathe section called “Modificare un progetto”. L'avvio dei desktop virtuali verrà bloccato se il budget viene superato. Se il budget viene superato durante l'avvio di un desktop, il desktop continuerà a funzionare.



Se devi modificare il budget, torna alla console per modificare l'importo del budget. Potrebbero essere necessari fino a quindici minuti prima che la modifica abbia effetto in RES. In alternativa, puoi modificare un progetto per disattivare un budget.

Autorizzazioni

	Membro del progetto	Proprietario del progetto	Amministratore globale	Ambito
Aggiungi utenti come membro/ proprietario del progetto		X	X	Proprietario del progetto: progetti di cui è proprieta rio

	Membro del progetto	Proprietario del progetto	Amministratore globale	Ambito
				Amministratore globale: qualsiasi progetto
Aggiungi gruppi come membro/ proprietario del progetto		X	X	Proprietario del progetto: progetti di cui è proprietario Amministratore globale: qualsiasi progetto
Rimuovere gli utenti		X	X	Proprietario del progetto: progetti di cui è proprietario Amministratore globale: qualsiasi progetto
Rimozione di gruppi		X	X	Proprietario del progetto: progetti di cui è proprietario Amministratore globale: qualsiasi progetto

	Membro del progetto	Proprietario del progetto	Amministratore globale	Ambito
Avvia/interrompi le istanze VDI	X	X	X	Membro del progetto/ proprietario del progetto: istanze VDI di cui sono proprietari quando fanno parte di un progetto. Amministratore globale: qualsiasi istanza VDI.

Usa il prodotto

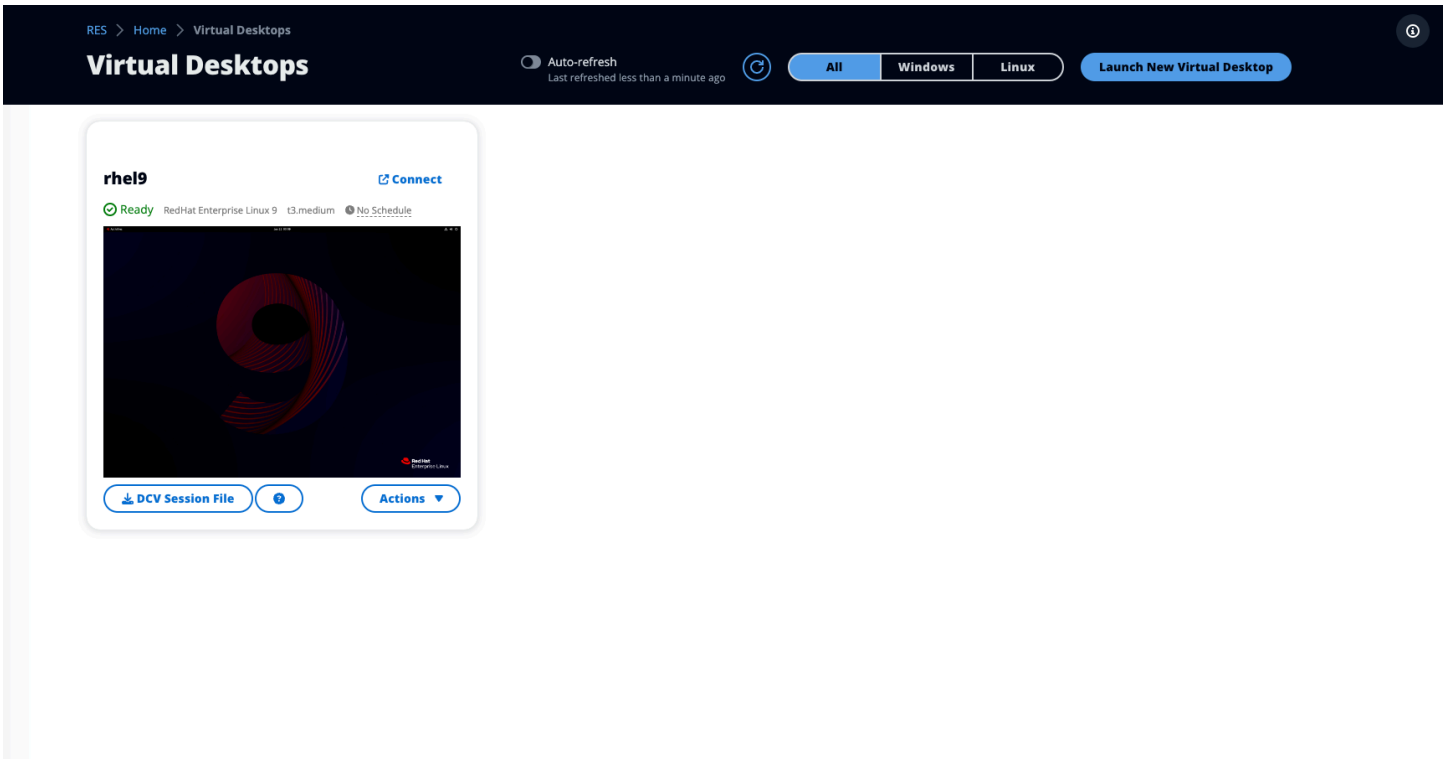
Questa sezione offre indicazioni agli utenti sull'utilizzo dei desktop virtuali per collaborare con altri utenti.

Argomenti

- Desktop virtuali
- Desktop condivisi
- Browser di file
- accesso SSH

Desktop virtuali

Il modulo VDI (Virtual Desktop Interface) consente agli utenti di creare e gestire desktop virtuali Windows o Linux su. AWS Gli utenti possono avviare istanze Amazon EC2 con gli strumenti e le applicazioni preferiti preinstallati e configurati.



Sistemi operativi supportati

> **Note**
>
> L'arrivo di CentOS 7 è attualmente previsto per il end-of-life 30/06/2024. La versione 2024.06 di Research and Engineering Studio sarà l'ultima versione a supportare CentOS 7.

RES attualmente supporta il lancio di desktop virtuali utilizzando i seguenti sistemi operativi:

- Amazon Linux 2 (x86 e ARM64)
- CentOS 7 (x86 e ARM64)
- RHEL 7 (x86), 8 (x86) e 9 (x86)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Avvia un nuovo desktop

1. Dal menu, scegli I miei desktop virtuali.
2. Scegli Avvia nuovo desktop virtuale.
3. Inserisci i dettagli del tuo nuovo desktop.
4. Scegli Invia.

Una nuova scheda con le informazioni sul desktop viene visualizzata immediatamente e il desktop sarà pronto per l'uso entro 10-15 minuti. Il tempo di avvio dipende dall'immagine selezionata. RES rileva le istanze della GPU e installa i driver pertinenti.

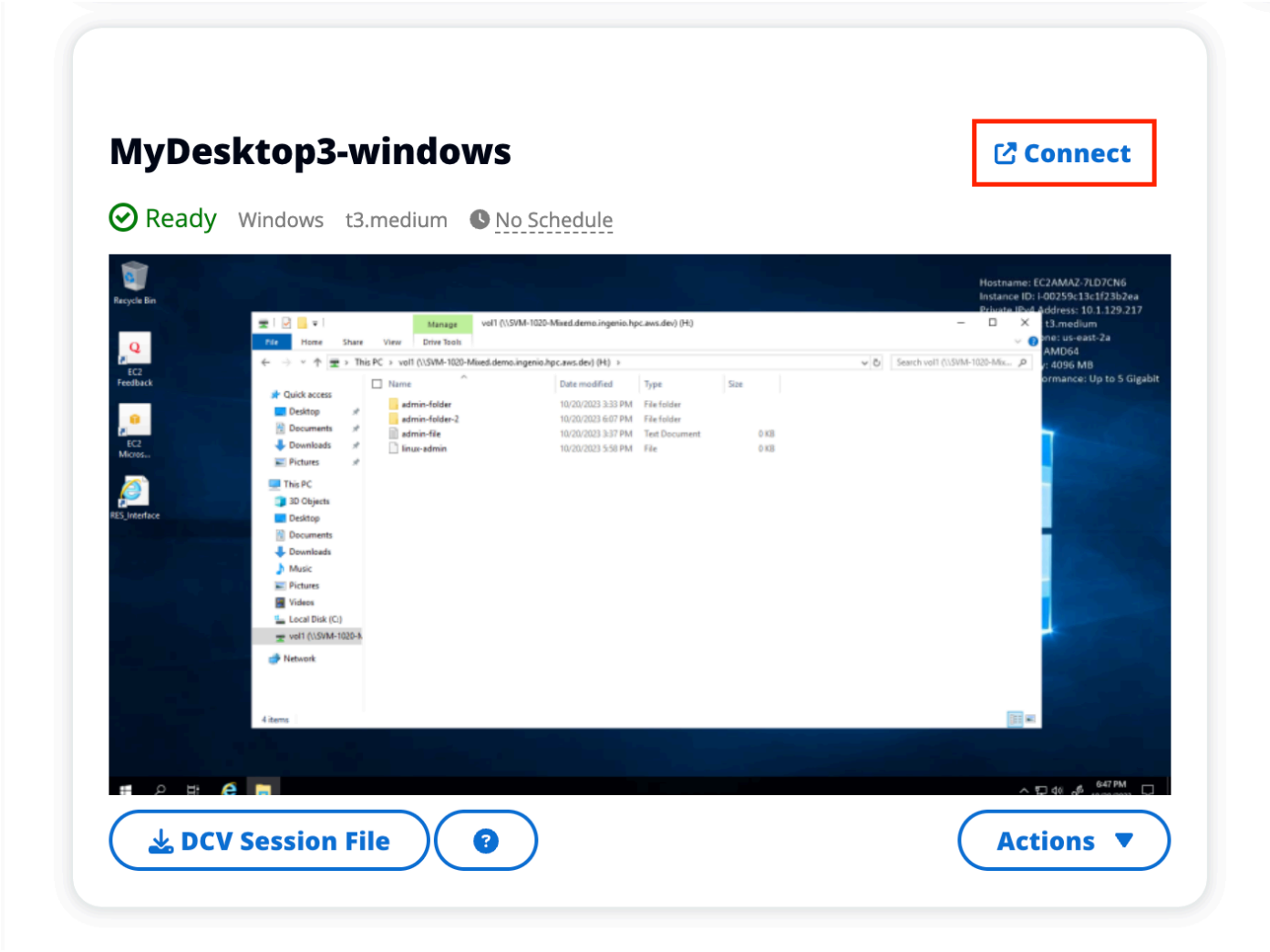
Accedi al tuo desktop

Per accedere a un desktop virtuale, scegli la scheda per il desktop e connettiti utilizzando un client Web o DCV.

Web connection

L'accesso al desktop tramite il browser Web è il metodo di connessione più semplice.

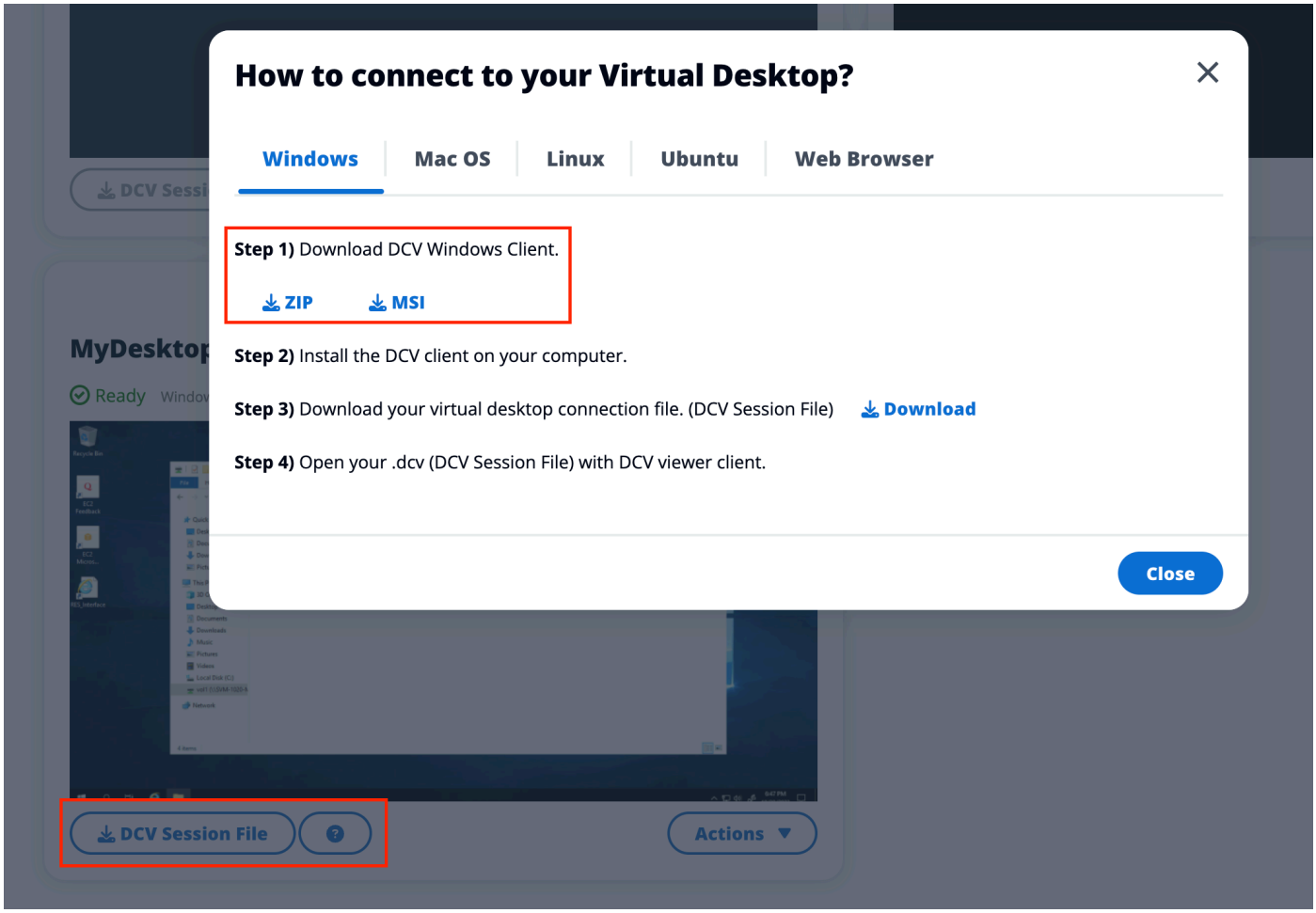
- Scegli Connect o scegli la miniatura per accedere al desktop direttamente tramite il browser.



DCV connection

L'accesso al desktop tramite un client DCV offre le migliori prestazioni. Per accedere tramite DCV:

1. Scegli DCV Session File per scaricare il. `dcv`file. Avrai bisogno di un client DCV installato sul tuo sistema.
2. Per le istruzioni di installazione, scegli il? icona.



Controlla lo stato del desktop

Per controllare lo stato del desktop:

1. Scegli Azioni.
2. Scegli Virtual Desktop State. Hai quattro stati tra cui scegliere:

   - Interrompi

     Una sessione interrotta non subirà alcuna perdita di dati ed è possibile riavviare una sessione interrotta in qualsiasi momento.

   - Riavviare

     Riavvia la sessione corrente.

   - Termina

Termina definitivamente una sessione. L'interruzione di una sessione può causare la perdita di dati se si utilizza l'archiviazione temporanea. È necessario eseguire il backup dei dati sul file system RES prima di terminare.

- Ibernazione

  Lo stato del desktop verrà salvato in memoria. Al riavvio del desktop, le applicazioni riprenderanno ma eventuali connessioni remote potrebbero andare perse. Non tutte le istanze supportano l'ibernazione e l'opzione è disponibile solo se è stata abilitata durante la creazione dell'istanza. Per verificare se l'istanza supporta questo stato, consulta Prerequisiti di ibernazione.

Modificare un desktop virtuale

È possibile aggiornare l'hardware del desktop virtuale o modificare il nome della sessione.

1. Prima di apportare modifiche alla dimensione dell'istanza, è necessario interrompere la sessione:
   a. Scegli Azioni.
   b. Scegli Virtual Desktop State.
   c. Scegli Stop (Arresta).

> **Note**
>
> Non è possibile aggiornare le dimensioni del desktop per le sessioni ibernate.

2. Dopo aver confermato che il desktop si è fermato, scegli Azioni, quindi scegli Aggiorna sessione.
3. Cambia il nome della sessione o scegli la dimensione del desktop che desideri.
4. Scegli Invia.
5. Una volta aggiornate le istanze, riavvia il desktop:
   a. Scegli Azioni.
   b. Scegli Virtual Desktop State.
   c. Scegli Avvia.

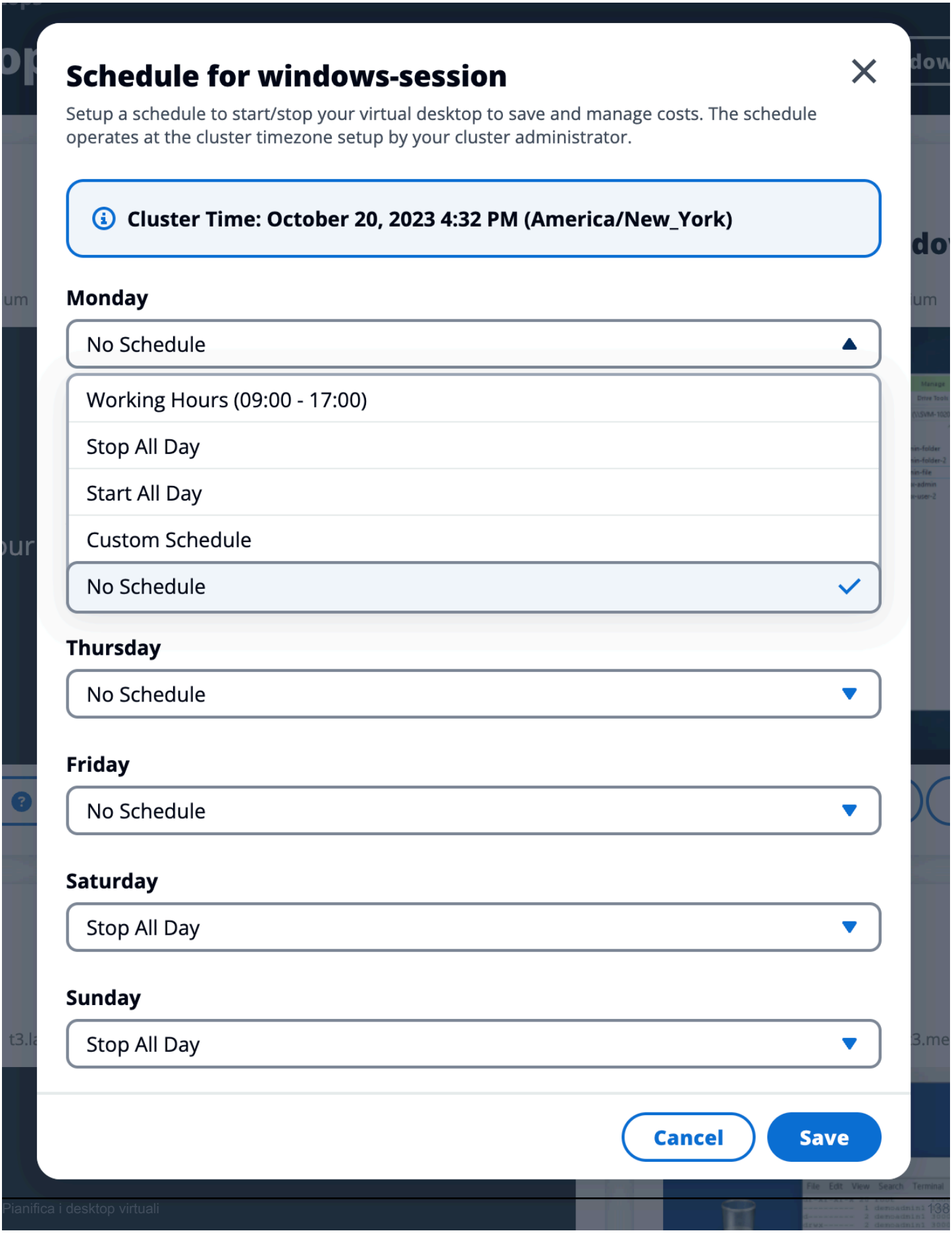
Recupera le informazioni sulla sessione

1. Scegli Azioni.
2. Scegli Mostra informazioni.

Pianifica i desktop virtuali

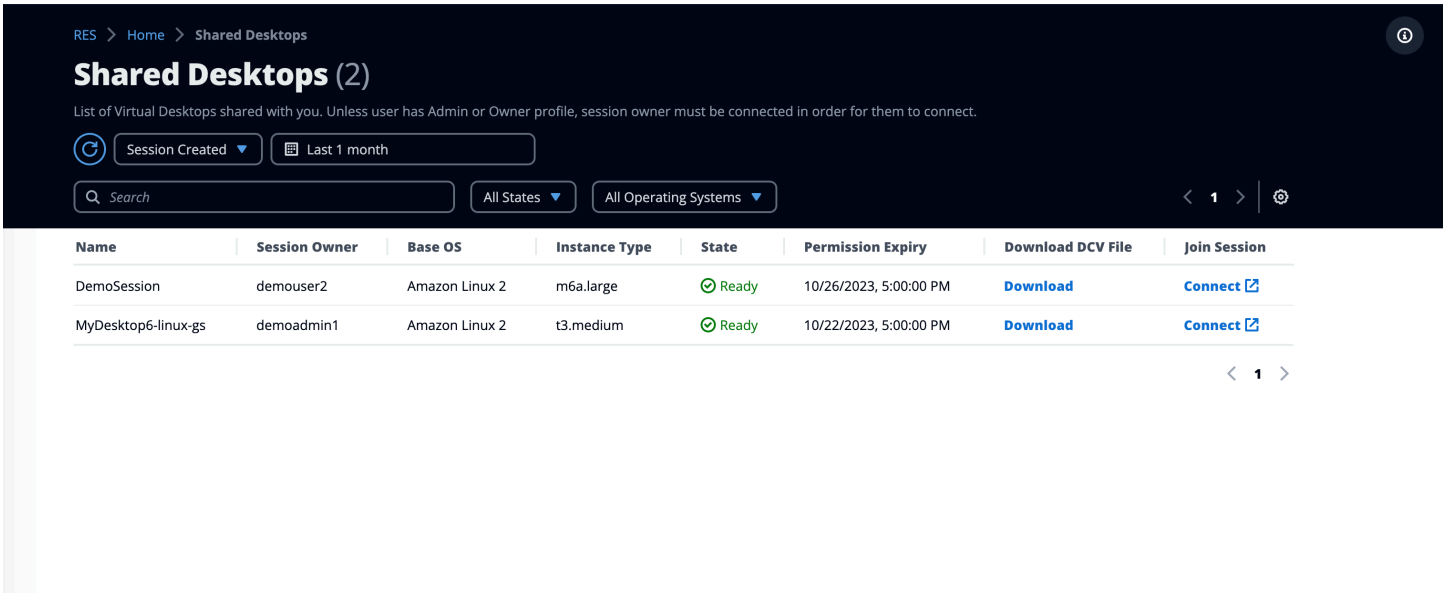
Per impostazione predefinita, i desktop virtuali non hanno una pianificazione e rimarranno attivi fino all'interruzione o alla fine della sessione. I desktop si arrestano anche se inattivi per evitare arresti accidentali. Lo stato di inattività è determinato dall'assenza di connessione attiva e dall'utilizzo della CPU inferiore al 15% per almeno 15 minuti. È possibile configurare una pianificazione per avviare e arrestare automaticamente il desktop.

1. Scegli Azioni.
2. Seleziona Schedule (Pianifica).
3. Imposta il tuo programma per ogni giorno.
4. Selezionare Salva.


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

Desktop condivisi

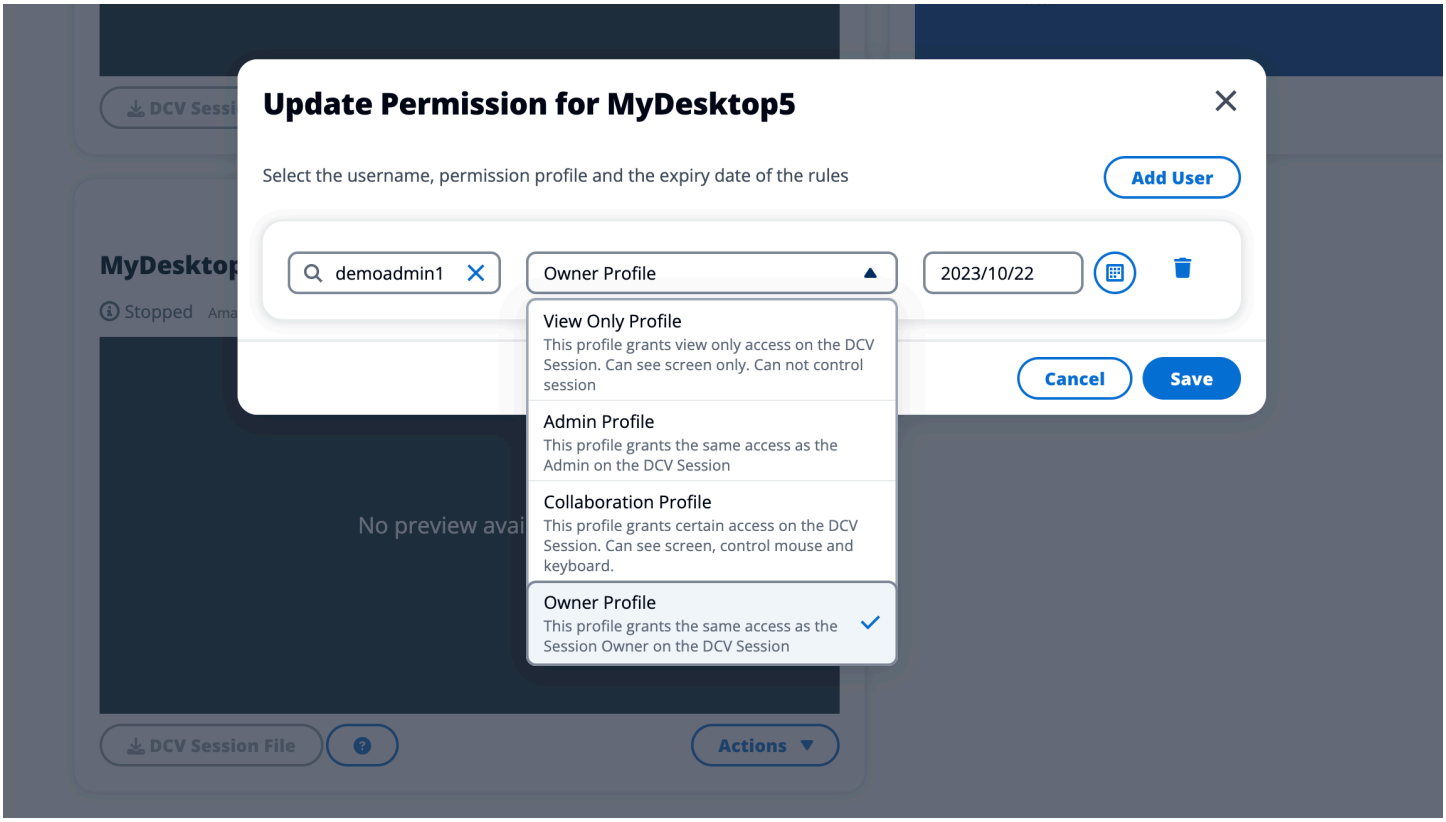
Sui desktop condivisi, puoi vedere i desktop che sono stati condivisi con te. Per connettersi a un desktop, deve essere connesso anche il proprietario della sessione, a meno che tu non sia un amministratore o un proprietario.



Durante la condivisione di una sessione, puoi configurare le autorizzazioni per i tuoi collaboratori. Ad esempio, puoi concedere l'accesso in sola lettura a un collega del team con cui collabori.

Condividi un desktop

1. Dalla sessione desktop, scegli Azioni.
2. Scegli Autorizzazioni di sessione.
3. Scegli l'utente e il livello di autorizzazione. Puoi anche impostare una scadenza.
4. Selezionare Salva.



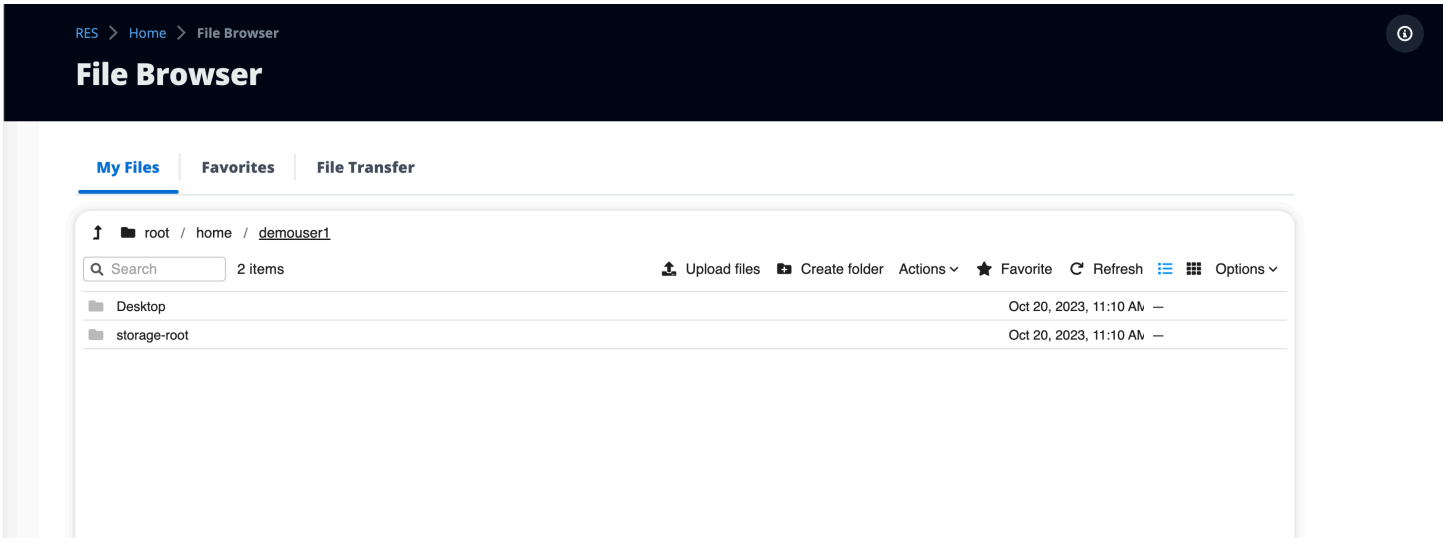
Per ulteriori informazioni sulle autorizzazioni, vedere. the section called “Profili di autorizzazione”

Accedere a un desktop condiviso

Da Shared Desktops, puoi visualizzare i desktop condivisi con te e connetterti a un'istanza. Puoi partecipare tramite browser web o DCV. Per connetterti, segui le istruzioni riportate inthe section called “Accedi al tuo desktop”.

Browser di file

Il file browser consente di accedere ai file system tramite il portale web. È possibile gestire tutti i file disponibili a cui si è autorizzati ad accedere sul filesystem sottostante. Lo storage di backend (Amazon EFS) è disponibile per tutti i nodi Linux. Per i nodi Linux e Windows, è disponibile FSx for ONTAP. L'aggiornamento dei file sul desktop virtuale equivale all'aggiornamento di un file tramite il terminale o il browser di file basato sul Web.



Carica file

1. Scegli Carica file.
2. Trascina i file o cerca i file da caricare.
3. Scegli Carica (n) file.

Elimina file

1. Seleziona i file che desideri eliminare.
2. Scegli Azioni.
3. Scegli Elimina file.

In alternativa, puoi anche fare clic con il pulsante destro del mouse su qualsiasi file o cartella e scegliere Elimina file.

Gestisci i preferiti

Per aggiungere file e cartelle importanti, puoi aggiungerli ai Preferiti.

1. Seleziona un file o una cartella.
2. Scegli Preferito.

In alternativa, puoi fare clic con il pulsante destro del mouse su qualsiasi file o cartella e scegliere Preferito.

> **Note**
>
> I preferiti vengono memorizzati nel browser locale. Se cambi browser o svuoti la cache, dovrai aggiungere nuovamente i preferiti.

Modifica i file

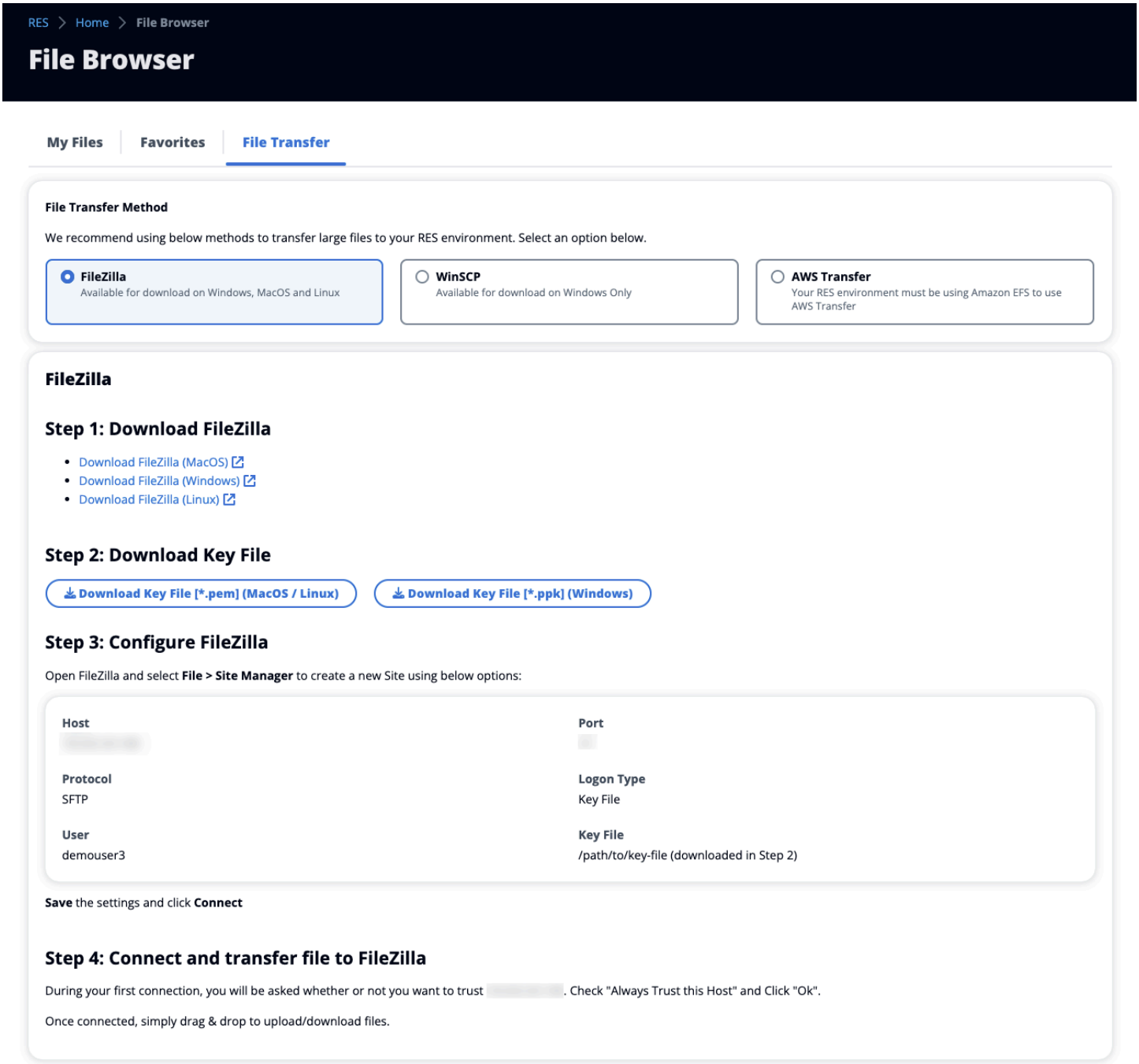
È possibile modificare il contenuto dei file di testo all'interno del portale web.

1. Scegliete il file che desiderate aggiornare. Si aprirà un modale con il contenuto del file.
2. Effettua gli aggiornamenti e scegli Salva.

Trasferimento dei file

Usa File Transfer per utilizzare applicazioni di trasferimento file esterne per trasferire file. È possibile selezionare una delle seguenti applicazioni e seguire le istruzioni visualizzate sullo schermo per trasferire i file.

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



accesso SSH

Per utilizzare SSH per accedere all'host bastion:

1. Dal menu RES, scegli l'accesso SSH.
2. Segui le istruzioni sullo schermo per utilizzare SSH o PuTTY per l'accesso.

Risoluzione dei problemi

Questo documento contiene informazioni su come monitorare il sistema e risolvere problemi specifici che possono verificarsi. Se non riesci a trovare la soluzione a un problema, potresti trovare altri argomenti sulla risoluzione dei problemi su. GitHub

Argomenti

Problemi di installazione

Argomenti

AWS CloudFormation lo stack non riesce a creare il messaggio «messaggio non riuscito WaitCondition ricevuto». Errore: Stati. TaskFailed»

Per identificare il problema, esamina il gruppo di CloudWatch log Amazon denominato`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. Se ci sono più gruppi di log con lo stesso nome, esamina il primo disponibile. Un messaggio di errore all'interno dei log fornirà ulteriori informazioni sul problema.

> **Note**
>
> Verificate che i valori dei parametri non abbiano spazi.

Notifica e-mail non ricevuta dopo che gli AWS CloudFormation stack sono stati creati correttamente

Se non è stato ricevuto un invito via e-mail dopo che è stato AWS CloudFormation creato correttamente, verifica quanto segue:

1. Conferma che il parametro dell'indirizzo email è stato inserito correttamente.

   Se l'indirizzo e-mail non è corretto o non è accessibile, elimina e ridistribuisci l'ambiente Research and Engineering Studio.
2. Controlla la console Amazon EC2 per le prove delle istanze cicliche.

   Se ci sono istanze Amazon EC2 con il `<envname>` prefisso che appare come terminato e poi vengono sostituite con una nuova istanza, potrebbe esserci un problema con la configurazione di rete o di Active Directory.
3. Se hai distribuito le ricette AWS High Performance Compute per creare le tue risorse esterne, verifica che il VPC, le sottoreti private e pubbliche e altri parametri selezionati siano stati creati dallo stack.

   Se uno qualsiasi dei parametri non è corretto, potrebbe essere necessario eliminare e ridistribuire l'ambiente RES. Per ulteriori informazioni, consulta Disinstalla il prodotto.
4. Se hai distribuito il prodotto con risorse esterne, verifica che la rete e Active Directory corrispondano alla configurazione prevista.

   È fondamentale confermare che le istanze dell'infrastruttura siano entrate correttamente in Active Directory. Prova i passaggi seguenti the section called “Istanze in ciclo o vdc-controller in stato di errore” per risolvere il problema.

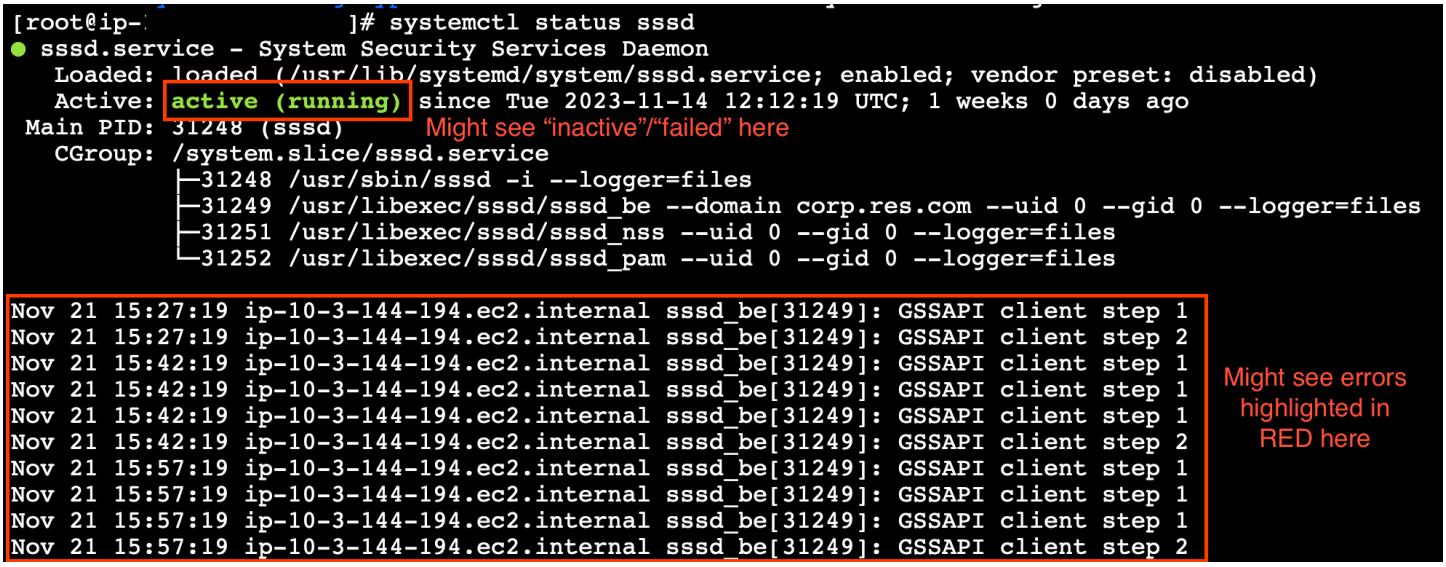
Istanze in ciclo o vdc-controller in stato di errore

La causa più probabile di questo problema è l'impossibilità per le risorse di connettersi o unirsi ad Active Directory.

Per verificare il problema:

1. Dalla riga di comando, avvia una sessione con SSM sull'istanza in esecuzione del vdc-controller.
2. Esegui `sudo su -`.
3. Esegui `systemctl status sssd`.

Se lo stato è inattivo, non riuscito o vengono visualizzati errori nei log, l'istanza non è riuscita a entrare in Active Directory.



Registro degli errori SSM

Per risolvere il problema:

- Dalla stessa istanza della riga di comando, `cat /root/bootstrap/logs/userdata.log` esegui per esaminare i log.

Il problema potrebbe essere una delle tre possibili cause principali.

Causa principale 1: dettagli di connessione LDAP immessi non corretti

Esamina i log. Se vedi quanto segue ripetuto più volte, significa che l'istanza non è riuscita a entrare in Active Directory.

```
+ 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. Verifica che i valori dei parametri per quanto segue siano stati inseriti correttamente durante la creazione dello stack RES.
   - directoryservice.ldap_connection_uri
   - directoryservice.ldap_base
   - directoryservice.users.ru
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - directoryservice.name
2. Aggiorna eventuali valori errati nella tabella DynamoDB. La tabella si trova nella console DynamoDB in Tabelle. Il nome della tabella dovrebbe essere. **`[stack name]`**`.cluster-settings`
3. Dopo aver aggiornato la tabella, elimina il gestore del cluster e il controller vdc che attualmente eseguono le istanze di ambiente. La scalabilità automatica avvierà nuove istanze utilizzando i valori più recenti della tabella DynamoDB.

Causa principale 2: nome utente inserito non corretto ServiceAccount

Se i log vengono restituiti`Insufficient permissions to modify computer account`, il ServiceAccount nome inserito durante la creazione dello stack potrebbe essere errato.

1. Dalla AWS console, apri Secrets Manager.
2. Cercare `directoryserviceServiceAccountUsername`. Il segreto dovrebbe essere**`[stack name]`**`-directoryservice-ServiceAccountUsername`.

3. Apri il segreto per visualizzare la pagina dei dettagli. In Valore segreto, scegli Recupera valore segreto e scegli Testo normale.
4. Se il valore è stato aggiornato, elimina le istanze cluster-manager e vdc-controller attualmente in esecuzione dell'ambiente. La scalabilità automatica avvierà nuove istanze utilizzando il valore più recente di Secrets Manager.

Causa principale 3: password inserita non corretta ServiceAccount

Se vengono visualizzati i log`Invalid credentials`, la ServiceAccount password inserita durante la creazione dello stack potrebbe essere errata.

1. Dalla AWS console, apri Secrets Manager.
2. Cercare `directoryserviceServiceAccountPassword`. Il segreto dovrebbe essere**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
3. Apri il segreto per visualizzare la pagina dei dettagli. In Valore segreto, scegli Recupera valore segreto e scegli Testo normale.
4. Se hai dimenticato la password o non sei sicuro che la password inserita sia corretta, puoi reimpostarla in Active Directory and Secrets Manager.
    a. Per reimpostare la password in: AWS Managed Microsoft AD
        i. Apri la AWS console e vai a AWS Directory Service.
        ii. Seleziona l'ID della directory RES e scegli Azioni.
        iii. Scegli Reimposta la password dell'utente.
        iv. Inserisci il ServiceAccount nome utente.
        v. Inserisci una nuova password e scegli Reimposta password.
    b. Per reimpostare la password in Secrets Manager:
        i. Apri la AWS console e vai a Secrets Manager.
        ii. Cercare `directoryserviceServiceAccountPassword`. Il segreto dovrebbe essere**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
        iii. Apri il segreto per visualizzare la pagina dei dettagli. In Valore segreto, scegli Recupera valore segreto e scegli Testo normale.
        iv. Scegli Modifica.
        v. Imposta una nuova password per l' ServiceAccount utente e scegli Salva.

5. Se il valore è stato aggiornato, elimina le istanze cluster-manager e vdc-controller attualmente in esecuzione dell'ambiente. La scalabilità automatica avvierà nuove istanze utilizzando il valore più recente.

Impossibile eliminare CloudFormation lo stack di ambiente a causa di un errore dell'oggetto dipendente

Se l'eliminazione dello **`[env-name]`**`-vdc` CloudFormation stack non riesce a causa di un errore dell'oggetto dipendente come il`vdcdcvhostsecuritygroup`, ciò potrebbe essere dovuto a un'istanza Amazon EC2 che è stata lanciata in una sottorete o in un gruppo di sicurezza creato da RES utilizzando la Console. AWS

Per risolvere il problema, trova e termina tutte le istanze Amazon EC2 avviate in questo modo. È quindi possibile riprendere l'eliminazione dell'ambiente.

Errore rilevato per il parametro del blocco CIDR durante la creazione dell'ambiente

Durante la creazione di un ambiente, viene visualizzato un errore per il parametro di blocco CIDR con uno stato di risposta di [FAILED].

Esempio di errore:

```
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.
```

Per risolvere il problema, il formato previsto è x.x.x.0/24 o x.x.x.0/32.

CloudFormation errore di creazione dello stack durante la creazione dell'ambiente

La creazione di un ambiente implica una serie di operazioni di creazione di risorse. In alcune regioni, può verificarsi un problema di capacità che impedisce la creazione di uno CloudFormation stack.

In tal caso, elimina l'ambiente e riprova a creare. In alternativa, puoi riprovare la creazione in un'altra regione.

La creazione dello stack di risorse esterne (demo) non riesce con CREATE_FAILED AdDomainAdminNode

Se la creazione dello stack dell'ambiente demo fallisce con il seguente errore, potrebbe essere dovuto all'applicazione di patch di Amazon EC2 imprevista durante il provisioning dopo il lancio dell'istanza.

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

Per determinare la causa dell'errore:

1. In SSM State Manager, controlla se l'applicazione delle patch è configurata e se è configurata per tutte le istanze.
2. Nella cronologia di esecuzione di SSM RunCommand /Automation, controlla se l'esecuzione di un documento SSM relativo all'applicazione di patch coincide con l'avvio di un'istanza.
3. Nei file di registro per le istanze Amazon EC2 dell'ambiente, esamina la registrazione dell'istanza locale per determinare se l'istanza è stata riavviata durante il provisioning.

Se il problema è stato causato dall'applicazione di patch, ritarda l'applicazione delle patch per le istanze RES di almeno 15 minuti dopo l'avvio.

Problemi di gestione delle identità

La maggior parte dei problemi con il Single Sign-On (SSO) e la gestione delle identità si verificano a causa di una configurazione errata. Per informazioni sulla configurazione SSO, consulta:

- the section called “Configurazione dell'SSO con IAM Identity Center”
- the section called “Configurazione del provider di identità per il Single Sign-On (SSO)”

Per risolvere altri problemi relativi alla gestione delle identità, consulta i seguenti argomenti di risoluzione dei problemi:

Argomenti

- Quando accedo all'ambiente, torno immediatamente alla pagina di accesso
- Errore «Utente non trovato» durante il tentativo di accesso

- Utente aggiunto in Active Directory, ma mancante in RES
- Utente non disponibile durante la creazione di una sessione
- Il limite di dimensione è stato superato (errore nel registro del gestore del CloudWatch cluster)

Quando accedo all'ambiente, torno immediatamente alla pagina di accesso

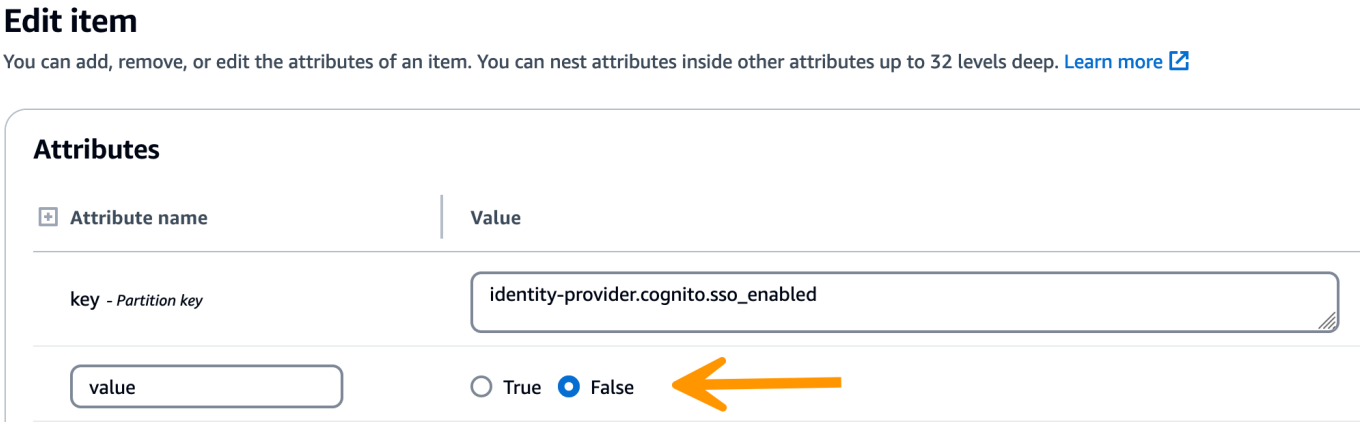
Questo problema si verifica quando l'integrazione SSO non è configurata correttamente. Per determinare il problema, controlla i registri delle istanze del controller e verifica la presenza di errori nelle impostazioni di configurazione.

Per controllare i log:

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Da Log groups, trova il gruppo denominato`/<environment-name>/cluster-manager`.
3. Apri il gruppo di log per cercare eventuali errori nei flussi di log.

Per verificare le impostazioni di configurazione:

1. Apri la console DynamoDB all'indirizzo https://console.aws.amazon.com/dynamodb/.
2. In Tabelle, trova la tabella denominata`<environment-name>.cluster-settings`.
3. Apri la tabella e scegli Esplora gli elementi della tabella.
4. Espandi la sezione dei filtri e inserisci le seguenti variabili:
   - Nome dell'attributo: chiave
   - Condizione: contiene
   - Valore: sso
5. Scegli Esegui.
6. Nella stringa restituita, verifica che i valori di configurazione SSO siano corretti. Se non sono corretti, modifica il valore della chiave sso_enabled su False.



7. Tornate all'interfaccia utente RES per riconfigurare l'SSO.

Errore «Utente non trovato» durante il tentativo di accesso

Se viene visualizzato l'errore «Utente non trovato» quando si accede all'interfaccia RES, l'utente è presente in Active Directory, ma non è presente in RES. Se hai aggiunto di recente l'utente ad AD, probabilmente non è sincronizzato con RES. RES si sincronizza ogni ora, quindi potrebbe essere necessario attendere e verificare che l'utente sia stato aggiunto dopo la sincronizzazione successiva. Per eseguire la sincronizzazione immediata, segui la procedura riportata di seguito. the section called “Utente aggiunto in Active Directory, ma mancante in RES”

Se l'utente è presente in RES:

1. Assicurati che la mappatura degli attributi sia configurata correttamente. Per ulteriori informazioni, consulta the section called “Configurazione del provider di identità per il Single Sign-On (SSO)”.
2. Assicurati che l'oggetto SAML e l'e-mail SAML corrispondano entrambi all'indirizzo e-mail dell'utente.

Utente aggiunto in Active Directory, ma mancante in RES

Se hai aggiunto un utente ad Active Directory ma non è presente in RES, è necessario attivare la sincronizzazione AD. La sincronizzazione AD viene eseguita ogni ora da una funzione Lambda per importare le voci AD nell'ambiente RES. Occasionalmente, dopo l'aggiunta di nuovi utenti o gruppi si verifica un ritardo fino all'esecuzione del processo di sincronizzazione successivo. Puoi avviare la sincronizzazione manualmente da Amazon Simple Queue Service.

Avvia il processo di sincronizzazione manualmente:

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/sqs/.
2. Da Queues, seleziona. `<environment-name>-cluster-manager-tasks.fifo`
3. Scegli Invia e ricevi messaggi.
4. Per il corpo del messaggio, inserisci:

   `{ "name": "adsync.sync-from-ad", "payload": {} }`
5. Per ID del gruppo di messaggi, inserisci: **`adsync.sync-from-ad`**
6. Per ID di deduplicazione dei messaggi, inserisci una stringa alfanumerica casuale. Questa voce deve essere diversa da tutte le chiamate effettuate entro cinque minuti, altrimenti la richiesta verrà ignorata.

Utente non disponibile durante la creazione di una sessione

Se sei un amministratore che crea una sessione, ma scopri che un utente che si trova in Active Directory non è disponibile durante la creazione di una sessione, potrebbe essere necessario accedere per la prima volta. Le sessioni possono essere create solo per utenti attivi. Gli utenti attivi devono accedere all'ambiente almeno una volta.

Il limite di dimensione è stato superato (errore nel registro del gestore del CloudWatch cluster)

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

Se si riceve questo errore nel registro del CloudWatch gestore del cluster, la ricerca ldap potrebbe aver restituito troppi record utente. Per risolvere questo problema, aumenta il limite dei risultati di ricerca ldap del tuo IDP.

Note

Ogni istanza Amazon EC2 viene fornita con due licenze Remote Desktop Services (Terminal Services) per scopi amministrativi. Queste informazioni sono disponibili per aiutarti a fornire queste licenze ai tuoi amministratori. Puoi anche utilizzare AWS Systems Manager Session Manager, che consente la connessione remota in istanze Amazon EC2 senza RDP e senza bisogno di licenze RDP. Se sono necessarie licenze aggiuntive di Remote Desktop Services, le CAL per utenti Remote Desktop devono essere acquistate da Microsoft o da un rivenditore di licenze Microsoft. Le licenze CAL per utenti di Desktop remoto con Software Assurance attiva offrono vantaggi in termini di mobilità delle licenze e possono essere trasferite in ambienti tenant AWS predefiniti (condivisi). Per informazioni sull'acquisto di licenze senza i vantaggi di Software Assurance o License Mobility, consulta questa sezione delle domande frequenti.

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le AWS attuali offerte e pratiche di prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. AWS le responsabilità nei confronti dei propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

Research and Engineering Studio on AWS è concesso in licenza secondo i termini della versione 2.0 della licenza Apache disponibile presso The Apache Software Foundation.

Revisioni

Per ulteriori informazioni, consultate il file ChangeLog.md nel repository. GitHub

Data	Modifica
Novembre 2023	Rilascio iniziale
Dicembre 2023	GovCloud indicazioni e modelli aggiunti
Gennaio 2024	Versione di rilascio 2024.01
Febbraio 2024	Versione di rilascio 2024.01.01: modello di distribuzione aggiornato
Marzo 2024	Argomenti aggiuntivi per la risoluzione dei problemi, conservazione dei CloudWatch log, disinstallazione delle versioni secondarie
aprile 2024	Versione 2024.04: AMI pronte per RES-ready e modelli di lancio di progetti
Giugno 2024	• Versione di rilascio 2024.06: supporto per Ubuntu, autorizzazioni del proprietario del progetto. • Guida per l'utente: aggiunta Crea un ambiente demo

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.