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 RESoffre 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 RES portale 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 gruppo specifico di utenti per accedere a risorse condivise e collaborare. Gli amministratori possono creare i propri stack di software applicativi (utilizzando Amazon Machine Images oAMIs) e consentire RES agli utenti 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 RES portale in base alle proprie esigenze.

RESè 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 RES per la distribuzione su Amazon Web Services (AWS) Cloud.

# Funzionalità e vantaggi

Research and Engineering Studio on AWS offre le seguenti funzionalità:

Interfaccia utente basata sul Web

RESfornisce 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 devono necessariamente disporre di competenze in ambito cloud Account AWS per poterle 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 le spese 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 per connettersi RES 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 RES portale 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'internoRES. I servizi di storage supportati includono Amazon Elastic File System per desktop Linux e Amazon FSx NetApp 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 RES progetti per monitorare i costi di ogni progetto. Se superi il budget, puoi limitare l'avvio delle VDI sessioni.

# Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di Research and Engineering Studio su AWS:

Browser di file

Un file browser è una parte dell'interfaccia RES utente 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 RES risorse condivise in un RES ambiente. 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 RES amministratore 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; ciò garantisce la governance del flusso di dati e impedisce la condivisione di dati e VDI host tra progetti.

Autorizzazioni basate sul progetto

Le autorizzazioni basate sui progetti descrivono una partizione logica di dati e VDI host in un sistema in cui possono esistere più progetti. L'accesso di un utente ai dati e agli VDI host 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 a VDIs quando non gli è stata concessa l'iscrizione.

Membro del progetto

Un utente finale di RES risorse (VDI, archiviazione, 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 RES specifici basati su qualsiasi sistema operativo che un utente ha scelto di fornire per il proprio host. VDI

VDIospita

Gli host di istanze desktop virtuali (VDI) consentono ai membri del progetto di accedere a dati e ambienti di calcolo specifici del progetto, garantendo spazi di lavoro sicuri e isolati.

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

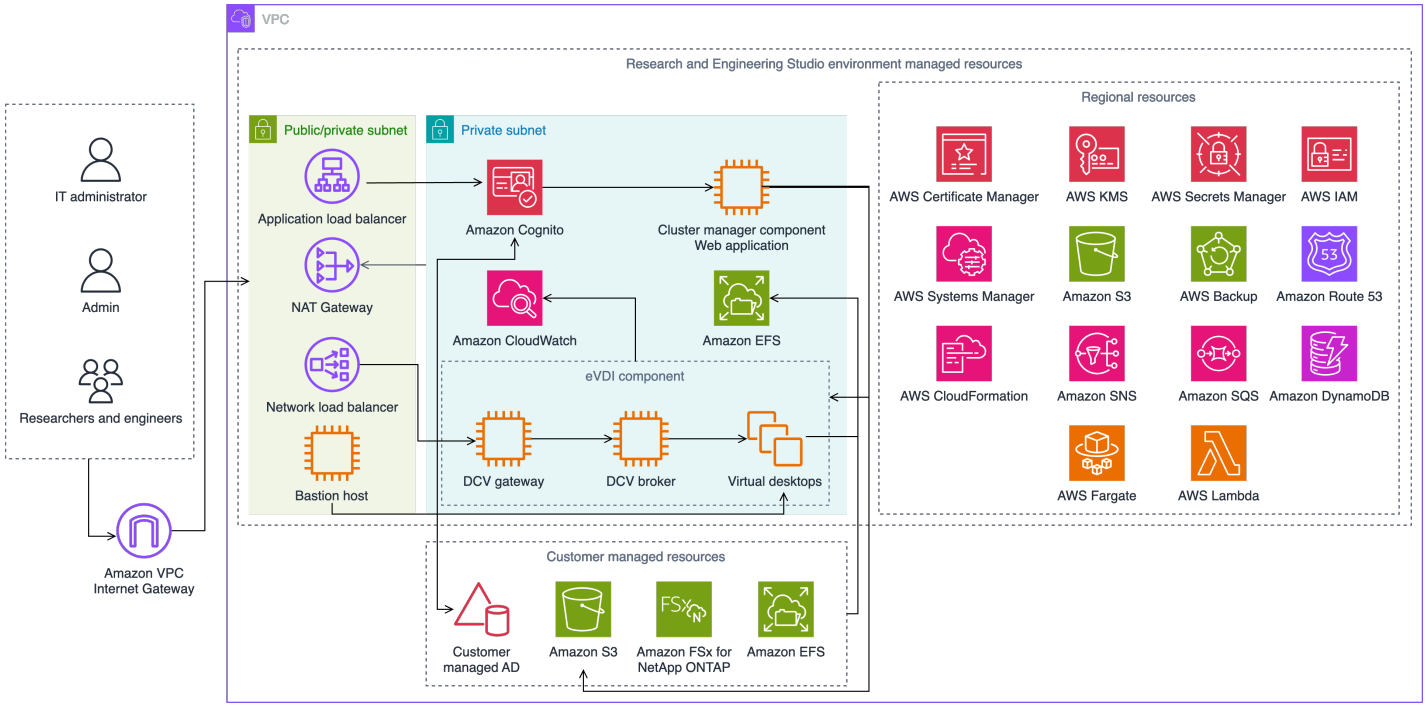



Figura 1: Studio di ricerca e ingegneria sull' AWS architettura

> **Note**
>
> AWS CloudFormation le risorse vengono create 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. RESinstalla 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 VDI componenti e.

c. Componente Bastion Host

   Gli amministratori possono utilizzare la connessione SSH al componente bastion host per gestire l'infrastruttura sottostante.

2. RESinstalla componenti in sottoreti private dietro un gateway. NAT Gli amministratori accedono alle sottoreti private tramite 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 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 e VDI Linux.
6. RESutilizza Amazon Cognito per creare un utente bootstrap iniziale chiamato 'clusteradmin' all'interno e invia credenziali temporanee all'indirizzo e-mail fornito durante l'installazione. Il 'clusteradmin' 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.

# AWS servizi inclusi in questo prodotto

| AWS servizio | Tipo | Descrizione |
| --- | --- | --- |
| Amazon Elastic Compute Cloud | Core | Fornisce i servizi di elaborazione sottostanti per creare desktop virtuali con il sistema |

| AWS servizio | Tipo | Descrizione |
| --- | --- | --- |
| | | operativo e lo stack software scelti. |
| Elastic Load Balancing | Core | Bastion, cluster-manager e VDI gli host vengono creati nei gruppi di Auto Scaling dietro il sistema di bilanciamento del carico. ELBbilancia il traffico proveniente dal portale web tra gli host. RES |
| Amazon Virtual Private Cloud | Core | Tutti i componenti principali del prodotto vengono creati all'interno del tuoVPC. |
| Amazon Cognito | Core | Gestisce le identità e l'autenti cazione degli utenti. Gli utenti di Active Directory vengono mappati su utenti e gruppi di Amazon Cognito per autentica re i livelli di accesso. |
| Amazon Elastic File System | Core | Fornisce il `/home` file system per il browser di file e VDI gli host, nonché per i file system esterni condivisi. |
| Amazon DynamoDB | Core | Memorizza dati di configura zione come utenti, gruppi, progetti, file system e impostazioni dei componenti. |
| AWS Systems Manager | Core | Memorizza i documenti per l'esecuzione di comandi per la gestione delle VDI sessioni. |

| AWS servizio | Tipo | Descrizione |
| --- | --- | --- |
| AWS Lambda | Core | Supporta funzionalità del prodotto come l'aggiorn amento delle impostazi oni all'interno della tabella DynamoDB, l'avvio dei flussi di lavoro di sincronizzazione con Active Directory e l'aggiorn amento dell'elenco dei prefissi. |
| Amazon CloudWatch | Supporta | Fornisce metriche e registri delle attività per tutti gli EC2 host Amazon e le funzioni Lambda. |
| Amazon Simple Storage Service | Supporta | Memorizza i file binari delle applicazioni per il bootstrap e la configurazione degli host. |
| AWS Key Management Service | Supporta | Utilizzato per la crittogra fia a riposo con SQS code Amazon, tabelle DynamoDB e argomenti Amazon. SNS |
| AWS Secrets Manager | Supporto | Archivia le credenziali degli account di servizio in Active Directory e i certificati autofirmati per. VDIs |
| AWS CloudFormation | Supporto | Fornisce un meccanismo di distribuzione per il prodotto. |
| AWS Identity and Access Management | Supportare | Limita il livello di accesso per gli host. |

| AWS servizio | Tipo | Descrizione |
| --- | --- | --- |
| Amazon Route 53 | Supportare | 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 pubblicaz ione tra VDI componenti come il controller e gli host. |
| AWS Fargate | Supporto | Installa, aggiorna ed elimina gli ambienti utilizzando le attività di Fargate. |
| Amazon FSx File Gateway | Facoltativo | Fornisce un file system condiviso esterno. |
| Amazon FSx per NetApp ONTAP | Facoltativo | Fornisce un file system condiviso esterno. |
| AWS Certificate Manager | Facoltativo | Genera un certificato affidabil e per il tuo dominio personali zzato. |
| AWS Backup | Facoltativo | Offre funzionalità di backup per EC2 host Amazon, 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 quanto Fasi successive alla distribuzione segue 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 EC2 SSH chiavi Amazon
- Aumenta 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 https://portal.aws.amazon.com/billing/registrazione.
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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

### Crea una coppia di EC2 SSH chiavi Amazon

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

### Aumenta le quote di servizio

Consigliamo di aumentare le quote di servizio per:

- Amazon VPC
  - Aumenta la quota di indirizzi IP elastici per NAT gateway da cinque a otto
  - Aumentate il numero di NAT gateway per zona di disponibilità da cinque a dieci
- Amazon EC2
  - Aumenta l'EC2VPCelastico IPs 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/cloudformazione.

   > **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'RESambiente che inizia con res-, non più lungo di |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| | | 11 caratteri e senza lettere maiuscole. |
| 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. |
| C lientIPCidr | <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 IPs consentire l'accesso diretto all'interfaccia utente web e l'accesso SSH all'host bastion. |

4. Seleziona Crea stack.

# 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 scegli 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 da 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

Questa sezione contiene informazioni su costi, sicurezza, aree supportate e quote che possono aiutarti a pianificare l'implementazione di Research and Engineering Studio su AWS.

## Costo

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

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili a Research and Engineering Studio on AWS, vedere AWS Servizi nell'ambito del programma di conformitàAWS .

- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio che utilizza. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Per capire come applicare il modello di responsabilità condivisa ai AWS servizi utilizzati da Research and Engineering Studio, consultaConsiderazioni sulla sicurezza per i servizi di questo prodotto. Per ulteriori informazioni sulla AWS sicurezza, visita Cloud AWS Sicurezza.

## IAMruoli

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

RESsupporta politiche basate sull'identità all'interno di. IAM Una volta distribuito, 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 con cui è integrato Active Directory. RES Per ulteriori informazioni, vedere Creazione IAM di politiche nella Guida per l'utente di AWS Identity and Access Management.

L'amministratore dell'organizzazione può gestire l'accesso degli utenti con una directory attiva. Quando gli utenti finali accedono all'interfaccia RES utente, si RES 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 istanzeEC2, le istanze CSR dei file system e gli endpoint remoti. VPN Si consiglia 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 RES proprietaria. Quando si esegue la distribuzioneRES, è possibile specificare un. AWS KMS key RESutilizza le tue credenziali per concedere l'accesso con chiave. Se fornisci la proprietà e la gestione di un cliente AWS KMS key, i dati inattivi del cliente verranno crittografati utilizzando quella chiave.

REScrittografa i dati dei clienti in transito utilizzandoSSL/TLS. Richiediamo TLS 1.2, ma consigliamo TLS 1.3.

## Considerazioni sulla sicurezza per i servizi di questo prodotto

Per informazioni più dettagliate sulle considerazioni sulla sicurezza per i servizi utilizzati da Research and Engineering Studio, segui i collegamenti in questa tabella:

| AWS informazioni sulla sicurezza del servizio | Tipo di servizio | Come viene utilizzato il servizio in RES |
|---|---|---|
| Amazon Elastic Compute Cloud | Core | Fornisce i servizi di elaborazione sottostanti per creare desktop virtuali con il sistema operativo e lo stack software scelti. |
| Elastic Load Balancing | Core | Bastion, cluster-manager e VDI gli host vengono creati nei gruppi di Auto Scaling dietro il sistema di bilanciamento del carico. ELBbilancia il traffico proveniente dal portale web tra gli host. RES |
| Amazon Virtual Private Cloud | Core | Tutti i componenti principali del prodotto vengono creati all'interno del tuoVPC. |
| Amazon Cognito | Core | 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 | Core | Fornisce il `/home` file system per il browser di file e VDI gli |

| AWS informazioni sulla sicurezza del servizio | Tipo di servizio | Come viene utilizzato il servizio in RES |
|---|---|---|
| | | host, nonché per i file system esterni condivisi. |
| Amazon DynamoDB | Core | Memorizza dati di configura zione come utenti, gruppi, progetti, file system e impostazioni dei componenti. |
| AWS Systems Manager | Core | Memorizza i documenti per l'esecuzione di comandi per la gestione delle VDI sessioni. |
| AWS Lambda | Core | Supporta funzionalità del prodotto come l'aggiorn amento delle impostazi oni all'interno della tabella DynamoDB, l'avvio dei flussi di lavoro di sincronizzazione con Active Directory e l'aggiorn amento dell'elenco dei prefissi. |
| Amazon CloudWatch | Supporta | Fornisce metriche e registri delle attività per tutti gli EC2 host Amazon e le funzioni Lambda. |
| Amazon Simple Storage Service | Supporta | Memorizza i file binari delle applicazioni per il bootstrap e la configurazione degli host. |
| AWS Key Management Service | Supporta | Utilizzato per la crittogra fia a riposo con SQS code Amazon, tabelle DynamoDB e argomenti Amazon. SNS |

| AWS informazioni sulla sicurezza del servizio | Tipo di servizio | Come viene utilizzato il servizio in RES |
|---|---|---|
| AWS Secrets Manager | Supportare | Archivia le credenziali degli account di servizio in Active Directory e i certificati autofirmati per. VDIs |
| AWS CloudFormation | Supporto | Fornisce un meccanismo di distribuzione per il prodotto. |
| AWS Identity and Access Management | Supportare | Limita il livello di accesso per gli host. |
| Amazon Route 53 | Supportare | Crea una zona ospitata privata per risolvere il load balancer interno e il nome di dominio dell'host bastion. |
| Amazon Simple Queue Service | Supportare | Crea code di attività per supportare esecuzioni asincrone. |
| Amazon Simple Notification Service | Supportare | Supporta il modello di abbonamento alla pubblicaz ione tra VDI componenti come il controller e gli host. |
| AWS Fargate | Supporto | Installa, aggiorna ed elimina gli ambienti utilizzando le attività di Fargate. |
| Amazon FSx File Gateway | Facoltativo | Fornisce un file system condiviso esterno. |
| Amazon FSx per NetApp ONTAP | Facoltativo | Fornisce un file system condiviso esterno. |

| AWS informazioni sulla sicurezza del servizio | Tipo di servizio | Come viene utilizzato il servizio in RES |
|---|---|---|
| AWS Certificate Manager | Facoltativo | Genera un certificato affidabile per il tuo dominio personalizzato. |
| AWS Backup | Facoltativo | Offre funzionalità di backup per EC2 host Amazon, file system e DynamoDB. |

# 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 di questo prodotto

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

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 EC2 istanze Amazon 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 dell'infrastruttura (). ASG 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.

ASGle impostazioni possono essere personalizzate all'interno della EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/. Per impostazione ASGs predefinita, il prodotto ne crea quattro con ogni nome che termina con`-asg`. È possibile modificare i valori minimi e desiderati impostando un valore appropriato per l'ambiente di produzione. Seleziona il gruppo che desideri modificare, quindi scegli Azioni e seleziona Modifica. Per ulteriori informazioniASGs, consulta Ridimensionare le dimensioni del gruppo Auto Scaling nella Amazon Auto EC2 Scaling User Guide.

# 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 | Regione | Versioni precedenti | Versione più recente (2024.10) |
|---|---|---|---|
| US East (N. Virginia) | us-east-1 | sì | sì |
| Stati Uniti orientali (Ohio) | us-east-2 | sì | sì |
| US West (N. Californi a) | us-west-1 | sì | sì |
| US West (Oregon) | us-west-2 | sì | sì |
| Asia Pacifico (Tokyo) | ap-northeast-1 | sì | sì |

| Nome Regione | Regione | Versioni precedenti | Versione più recente (2024.10) |
|---|---|---|---|
| Asia Pacifico (Seul) | ap-northeast-2 | sì | sì |
| Asia Pacific (Mumbai) | ap-south-1 | sì | sì |
| Asia Pacifico (Singapore) | ap-southeast-1 | sì | sì |
| Asia Pacifico (Sydney) | ap-southeast-2 | sì | sì |
| Canada (Central) | ca-central-1 | sì | sì |
| Europe (Frankfurt) | eu-central-1 | sì | sì |
| Europa (Milano) | eu-south-1 | sì | sì |
| Europa (Irlanda) | eu-west-1 | sì | sì |
| Europe (London) | eu-west-2 | sì | sì |
| Europe (Paris) | eu-west-3 | sì | sì |
| Europa (Stoccolma) | eu-north-1 | no | sì |
| Israele (Tel Aviv) | il-central-1 | sì | sì |
| AWS GovCloud (Stati Uniti occidentali) | us-gov-west-1 | sì | sì |

# 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

Devi avere un account Account AWS con un utente amministrativo:

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
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 best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

## Crea una coppia di EC2 SSH chiavi Amazon

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

## Aumenta le quote di servizio

Consigliamo di aumentare le quote di servizio per:

- Amazon VPC
  - Aumenta la quota di indirizzi IP elastici per NAT gateway da cinque a otto.
  - Aumenta il numero di NAT gateway per zona di disponibilità da cinque a dieci.
- Amazon EC2
  - Aumenta l'EC2VPCelastico IPs 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 Quote per i AWS servizi di questo prodotto.

## Crea un dominio pubblico (opzionale)

Ti consigliamo di utilizzare un dominio personalizzato per il prodotto in modo da avere un dominio intuitivoURL. 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, copialo ARNdalla sezione Stato del certificato.

## Crea dominio (GovCloud solo)

Se esegui la distribuzione nella regione AWS GovCloud (Stati Uniti occidentali) e utilizzi un dominio personalizzato per Research and Engineering Studio, dovrai completare questi passaggi preliminari.

1. Implementa lo AWS CloudFormation stack di certificati nell' AWS account della 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. Annota il nuovo segreto ARN 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` Annota il nuovo segreto ARN 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

Research and Engineering Studio on AWS prevede che al momento dell'implementazione siano disponibili le seguenti risorse esterne.

- Rete (VPCsottoreti pubbliche e sottoreti private)

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

- Archiviazione (AmazonEFS)

  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 nell'RESambiente.

- 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 LDAPS comunicazione 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 eRES.

1. Segui i passaggi forniti in Come abilitare il lato server LDAPS per il tuo. AWS Managed Microsoft AD Puoi saltare questo passaggio se lo hai già abilitato. LDAPS
2. Dopo aver verificato che LDAPS sia configurato sull'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. Seleziona X.509 con codifica Base-64 (. CER) e scegliete Avanti.
   g. Seleziona una directory, quindi scegli Avanti.
3. Crea un segreto in AWS Secrets Manager:

   Quando crei il tuo segreto in Secrets Manager, scegli Altro tipo di segreti in Tipo segreto e incolla il certificato PEM codificato nel campo Testo normale.
4. Annota il file ARN creato e inseriscilo come parametro in. `DomainTLSCertificateSecretARN` Fase 1: Avviare il prodotto

# Configura un account privato VPC (opzionale)

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

Argomenti

- Preparare le immagini delle macchine Amazon (AMIs)

- Configura gli VPC endpoint
- Connect ai servizi senza VPC endpoint
- Imposta i parametri di VPC distribuzione privata

## Preparare le immagini delle macchine Amazon (AMIs)

1. Scarica le dipendenze. Per essere implementata in un ambiente isolatoVPC, l'RESinfrastruttura richiede la disponibilità di dipendenze senza l'accesso pubblico a Internet.
2. Crea un IAM ruolo con l'accesso in sola lettura e l'identità affidabile di Amazon S3 come Amazon. EC2

    a. Apri la console all'IAMindirizzo. 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, scegli EC2e scegli Avanti.

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

    - Amazon S3 ReadOnlyAccess
    - Un mazonSSMManaged InstanceCore
    - EC2InstanceProfileForImageBuilder

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

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

    b. In Risorse salvate, scegliete Componenti e scegliete 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 | Inserisci 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 file URI per il file tar.gz. Carica il file tar.gz fornito RES da in un bucket Amazon S3 e copia il file URI 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 VPC gli endpoint.

```
#  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 l'opzione Rimuovi SSM agente dopo l'esecuzione della pipeline non sia selezionata. |
| Cartella di lavoro | Percorso della directory di lavoro | /root/bootstrap/res_dipendenze |

| Sezione | Parametro | Inserimento utente |
| --- | --- | --- |
| Componenti | Costruisci componenti | Cerca e seleziona quanto segue:<br>• Gestito da Amazon: -2-linux aws-cli-version<br>• Gestito da Amazon: amazon-cloudwatch-agent-linux<br>• Di tua proprietà: EC2 componente Amazon creato in precedenza. Inserisci il tuo Account AWS ID e la tua corrente Regione AWS nei campi. |
| | Componenti di test | Cerca e seleziona:<br>• 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 |
| --- | --- | --- |
| | IAMruolo | Seleziona il IAM ruolo 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 EC2 console Amazon con i seguenti input:<br>• VPC: Seleziona lo stesso VPC utilizzato per la configurazione dell'infr astruttura. Questo VPC deve avere accesso a Internet.<br>• Regola in entrata:<br>  • Tipo: SSH<br>  • Source (Origine): personalizzata<br>  • CIDRblocco: 0.0.0.0/0 |

d. Scegli Crea configurazione dell'infrastruttura.

6. Crea una nuova pipeline di 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 Pianificazione, imposta un programma o scegli Manuale se desideri avviare il processo di AMI cottura manualmente.

c. Nella pagina Scegli la ricetta, scegli Usa ricetta esistente e inserisci il nome della ricetta creato in precedenza. Scegli Next (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. Scegli Next (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'RESambiente distribuito, in modo da poter RES 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 EC2 servizio Image Builder.
- Se desideri eseguire la distribuzione RES in più regioni, puoi scegliere Crea nuove impostazioni di distribuzione e aggiungere altre regioni.

g. Controlla le tue selezioni e scegli Crea pipeline.

7. Esegui la EC2 pipeline di Image Builder:

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

b. Scegliete Azioni e selezionate Esegui pipeline.

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

8. Annotate l'AMIID del file generato AMI e usatelo come input per il InfrastructureHost AMI parametro inthe section called “Fase 1: Avviare il prodotto”.

## Configura gli VPC endpoint

Per distribuire RES e avviare desktop virtuali, Servizi AWS richiedi l'accesso alla tua sottorete privata. È necessario configurare gli VPC endpoint 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 di interfaccia. VPC
2. Seleziona una sottorete privata in ciascuna delle due zone di disponibilità.

| Servizio AWS | Nome servizio |
| --- | --- |
| Application Auto Scaling | com.amazonaws.*region*.scalabilità automatica delle applicazioni |
| AWS CloudFormation | com.amazonaws.*region*cloudformation. |
| Amazon CloudWatch | com.amazonaws.*region*.monitoraggio |
| CloudWatch Registri Amazon | com.amazonaws.*region*.registri |
| 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*.filesystem elastico |
| Elastic Load Balancing | com.amazonaws.*region*. bilanciamento elastico del carico |
| 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-stream |
| AWS Lambda | com.amazonaws.*region*.lambda |
| Amazon S3 | com.amazonaws.*region*.s3 (richiede un endpoint gateway creato per impostazione predefinita in.) RES<br><br>Sono necessari endpoint di interfaccia Amazon S3 aggiuntivi per il montaggio incrociato di bucket in un |

| Servizio AWS | Nome servizio |
| --- | --- |
| | ambiente isolato. Vedi Accesso agli endpoint dell'interfaccia Amazon Simple Storage Service. |
| AWS Secrets Manager | com.amazonaws.*region*. gestore dei segreti |
| 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.) |
| 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*messaggi.ec2 |
| | com.amazonaws.*region*.ssm |
| | com.amazonaws.*region*messaggi.ssm |

## Connect ai servizi senza VPC endpoint

Per l'integrazione con servizi che non supportano gli VPC endpoint, 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 che VPC utilizzerai per la RES distribuzione.
   - 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 a partire dalla versione 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. Nota PORT su quale server viene ascoltato il proxy.

3. Configura la tabella di routing per consentire l'accesso al server proxy.

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

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. Fatelo per le tabelle di routing per tutte le sottoreti (senza accesso a Internet) che userete per Infrastructure/. VDIs

4. Modifica il gruppo di sicurezza dell'EC2istanza del server proxy e assicurati che consenta le TCP connessioni in entrata PORT sulla quale il server proxy è in ascolto.

## Imposta i parametri di VPC distribuzione privata

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 eseguire correttamente la distribuzione nel file privato VPC che hai appena configurato.

| Parametro | Input |
| --- | --- |
| InfrastructureHostAMI | Utilizza l'AMIID dell'infrastruttura creato inthe section called “Preparare le immagini delle macchine Amazon (AMIs)”. |

| Parametro | Input |
| --- | --- |
| 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. |
| ClientIP | Puoi scegliere di consentire l'accesso VPC CIDR a tutti gli VPC indirizzi IP. |

## Crea risorse esterne

Questo CloudFormation stack crea certificati di rete, storage, active directory e dominio (se PortalDomainName viene fornito a). 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 /cloudformazione.

   > **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. Inserisci 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 il valore, aggiorna e fornisci un `LDIF` file separato. Non è necessario che corrisponda al dominio utilizzato per Active Directory. |
| SubDomain (GovCloud solo) | | Questo parametro è facoltativo per le regioni commerciali, ma obbligatorio per GovCloud le regioni.<br><br>Se fornisci un SubDomain, il parametro avrà il prefisso DomainName fornito. Il nome di dominio Active Directory fornito diventerà un sottodominio. |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| AdminPassword | | La password per l'amministratore di Active Directory (nome utente`Admin`). Questo utente viene creato in Active Directory per la fase iniziale di bootstrap e non viene utilizzato dopo.<br><br>Importante: il formato di questo campo può essere (1) una password in testo semplice o (2) il formato ARN di un AWS Secret formattato come coppia chiave/valore. `{"password":"somepassword"}`<br><br>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.<br><br>Importante: il formato di questo campo può essere (1) una password in testo semplice o (2) il formato ARN di un AWS segreto formattato come coppia chiave/valore. `{"password":"somepassword"}`<br><br>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 SSH client.<br><br>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 LDIF file importato durante la fase di avvio della configurazione di Active Directory. Per ulteriori informazioni, consulta LDIFSupport. Il parametro viene precompilato con un file che crea un numero di utenti in Active Directory.<br><br>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 RES stack. 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.<br>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 RES principale 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 / cloudformazione. https://console.aws.amazon.com
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'RESambiente che inizia con res-, non più lungo di 11 caratteri e senza lettere maiuscole. |
| 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-*[numbers or letters only]* | (Facoltativo) È possibile fornire un AMI ID 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 Configura RES -ready AMIs. |
| SSHKeyPair | | La key pair utilizzata per connettersi agli host dell'infr astruttura. |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| ClientIP | *x.x.x*.0/24 oppure *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 IPs consentire l'accesso diretto all'interfaccia utente web e l'accesso SSH all'host bastion. |
| IAMPermissionBoundary | | (Facoltativo) Puoi fornire una policy gestita ARN che verrà allegata come limite di autorizzazione a tutti i ruoli creati in. RES Per ulteriori informazioni, consulta Impostazione di limiti di autorizzazione personalizzati. |
| VpcId | | ID per le istanze VPC in cui verranno avviate. |
| IsLoadBalancerInternetFacing | | Seleziona true per implementare il sistema di bilanciamento del carico con accesso a Internet (richiede sottoreti pubbliche per il bilanciamento del carico). Per le distribuzioni che richiedono 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 bilanciamento del carico. Per le implementazioni che richiedono un accesso limitato a Internet, seleziona sottoreti private. Per le distribuzioni che richiedono l'accesso a Internet, seleziona 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 VDI istanze. 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. |
| ADShortName | *corp* | Il nome breve per Active Directory. Viene anche chiamato BIOS nome di rete. |
| LDAPBase | ***DC=corp,DC=res,DC=com*** | Un LDAP percorso verso la base all'interno della LDAP gerarchia. |
| LDAPConnectionURI | | 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. |
| ServiceAccountCredentialsSecretArn | | Fornisci un segreto ARN che contiene il nome utente e la password per l'utente di Active Directory, formattato come coppia nome ServiceAccount utente:password chiave/valore. |
| Utenti: OU | | Unità organizzativa all'interno di AD per gli utenti che effettueranno la sincronizzazione. |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| Gruppi OU | | Unità organizzativa all'interno di AD per i gruppi che verranno sincronizzati. |
| SudoersGroupName | RESAdministrators | 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. |
| D omainTLSCertificate Segreto ARN | | (Facoltativo) Fornisci un TLS certificato di dominio segreto ARN per abilitare TLS la comunicazione con AD. |
| EnableLdapIDMapping | | Determina se UID e GID i numeri vengono generati da SSSD o se vengono utilizzati i numeri forniti da AD. Imposta su True per utilizzare i dati SSSD generati UID e GID su False per utilizzare UID e GID forniti dall'AD. Nella maggior parte dei casi questo parametro deve essere impostato su True. |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| D isableADJoin | False | Per evitare che gli host Linux entrino a far parte del dominio della directory , impostate True. Altriment i, lascia l'impostazione predefinita False. |
| ServiceAccountUserDN | | Fornisci il nome distinto (DN) dell'utente dell'account di servizio in Directory. |
| SharedHomeFilesystemID | | Un EFS ID da utilizzare per il file system home condiviso per gli host Linux. VDI |
| CustomDomainNamefo rWebApp | | (Facoltativo) Sottodominio utilizzato dal portale web per fornire collegamenti per la parte web del sistema. |
| CustomDomainNameforVDI | | (Facoltativo) Sottodominio utilizzato dal portale web per fornire collegamenti per la VDI parte del sistema. |

| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| ACMCertificateARNforWebApp | | (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 distribuito risorse esterne automatizzate, queste sono state generate per te e le informazioni sono disponibili negli Output dello stack res-bi. Se devi generare un certificato per la tua applicazione web, consulta. Guida alla configurazione |
| CertificateSecretARNforVDI | | (Facoltativo) Questo ARN segreto memorizza il certificato pubblico per il certificato pubblico 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. |

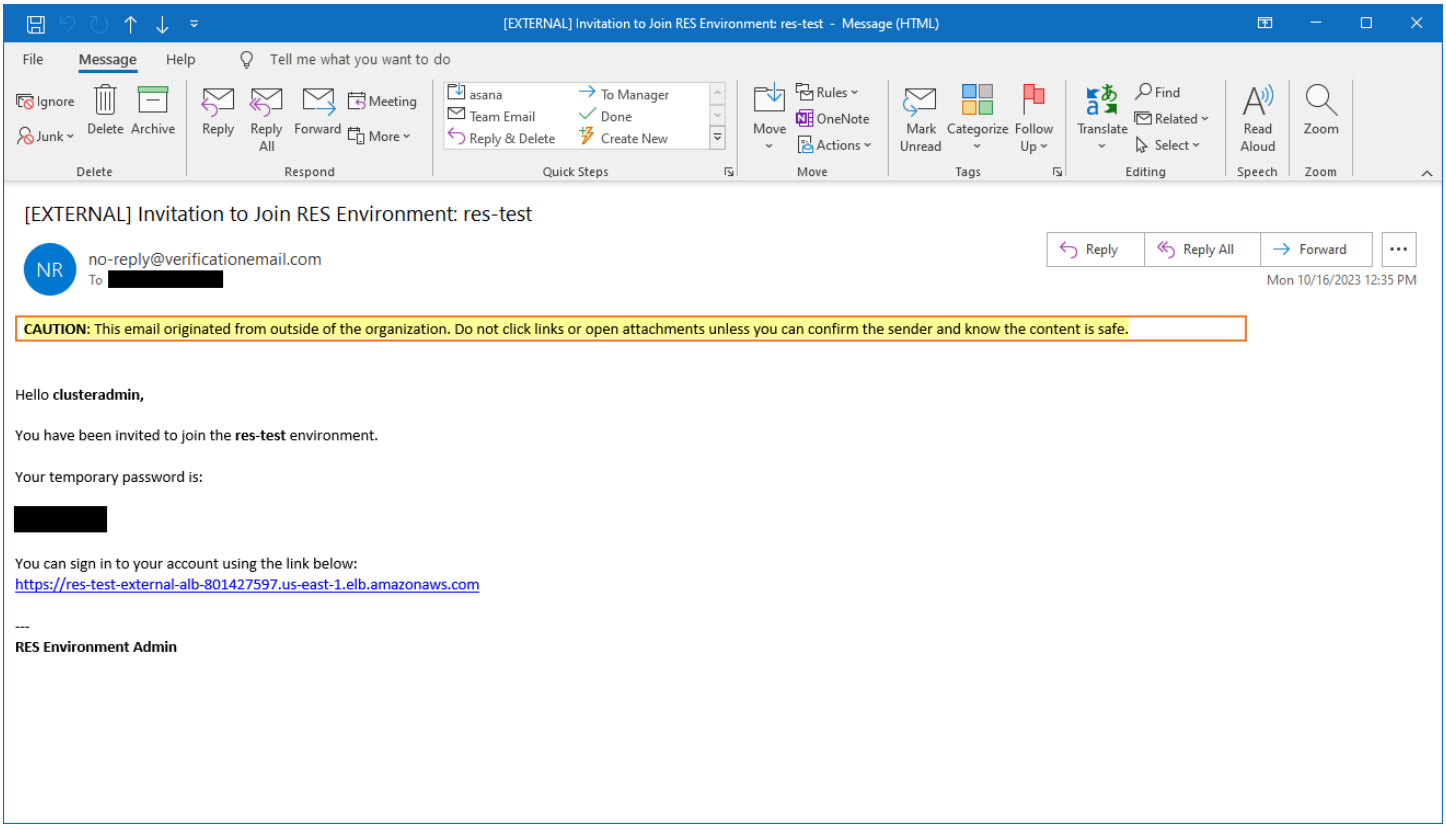
| Parametro | Predefinito | Descrizione |
| --- | --- | --- |
| PrivateKeySecretARNforVDI | | (Facoltativo) Questo ARN segreto memorizza la chiave privata per il certificato del tuo portale web. Se imposti un nome di dominio del portale per le tue risorse esterne automatizzate, puoi trovare questo valore 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 COMPLETE lo stato CREATE _ 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 il 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 SSO provider. Per informazioni sulla configurazione post-implementazione, consulta laGuida alla configurazione. Tieni presente che `clusteradmin` si tratta di un account break-glass: puoi utilizzarlo per creare progetti e assegnare l'appartenenza a utenti o gruppi a tali progetti; non può assegnare stack software o implementare un desktop per sé.

# Aggiorna il prodotto

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

RESutilizza 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 RES ambiente 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 la versione più recente 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 “Applica 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 aRES, non è richiesta una nuova installazione. È possibile aggiornare lo RES stack esistente aggiornando il relativo AWS CloudFormation modello. Controlla la

versione del tuo RES ambiente attuale AWS CloudFormation prima di distribuire l'aggiornamento. Il numero di versione è riportato 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 AWS prodotto da AWS Management Console o utilizzando il AWS Command Line Interface. È 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.

## Utilizzando il AWS Management Console

1. Accedere 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 a AWS Management Console e apri la EFS console Amazon 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 a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
4. Eliminare 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 a 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 Research and Engineering Studio. AWS

Argomenti



## Gestione di utenti e gruppi

Research and Engineering Studio può utilizzare qualsiasi SAML provider di identità conforme alla versione 2.0. Se l'implementazione è stata eseguita RES utilizzando risorse esterne o si prevede di utilizzare IAM Identity Center, vedere. Configurazione del single sign-on () SSO con Identity Center IAM Se disponi di un provider di identità personale conforme alla SAML versione 2.0, consulta. Configurazione del provider di identità per il Single Sign-on () SSO

Argomenti



### Configurazione del single sign-on () SSO con Identity Center IAM

Se non disponi già di un centro di identità collegato all'Active Directory gestita, inizia conPassaggio 1: configurare un centro di identità. Se hai già un centro di identità collegato all'Active Directory gestita, inizia conFase 2: Connect a un centro di identità.

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

## Passaggio 1: configurare un centro di identità

Attivazione di IAM Identity Center

1. Accedere alla console AWS Identity and Access Management.
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 Active Directory gestito.

Connessione di IAM Identity Center a un Active Directory gestito

Dopo aver abilitato IAM Identity Center, completa questi passaggi di configurazione consigliati:

1. Nel pannello di navigazione scegli Impostazioni.
2. In Origine dell'identità, scegli Azioni e scegli Cambia origine identità.
3. In Directory esistenti, seleziona la tua directory.
4. Scegli Next (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 Connessione di IAM Identity Center a un Active Directory gestito completate le modifiche apportate, viene visualizzato un banner di conferma 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. Scegli Next (Successivo).
6. Controlla le modifiche, quindi 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. Seleziona 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 IAM Identity Center

1. Aprire la console di IAM Identity Center.
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 SAML2.0.
6. Scegli Next (Successivo).
7. Inserisci il nome visualizzato e la descrizione che desideri utilizzare.
8. In Metadati di IAM Identity Center, copia il link per il file di SAMLmetadati di IAM Identity Center. Ne avrai bisogno per configurare IAM Identity Center con il portale. RES

9. In Proprietà dell'applicazione, inserisci l'avvio URL dell'applicazione. Ad esempio `<your-portal-domain>/sso`.
10. In Applicazione ACS URL, inserisci il reindirizzamento URL dal RES portale. Per trovare questo:
    a. In Gestione dell'ambiente, scegli Impostazioni generali.
    b. Seleziona la scheda Identity provider.
    c. In Single Sign-On, troverai il SAML reindirizzamento. URL
11. In Application SAML audience, accedi ad Amazon CognitoURN.

    Per creare l'urna:

    a. Dal RES portale, apri Impostazioni generali.
    b. Nella 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. Dopo aver effettuato l'accesso ad Amazon CognitoURN, scegli Invia.

Configurazione delle mappature degli attributi per l'applicazione

1. Dall'Identity Center, apri i dettagli dell'applicazione creata.
2. Scegli Azioni, quindi scegli Modifica mappature degli attributi.
3. In Oggetto, inserisci. **`${user:email}`**
4. In Formato, scegliete emailAddress.
5. Scegli Aggiungi nuova mappatura degli attributi.
6. Nella sezione Attributo utente dell'applicazione, inserisci 'email'.
7. In Associa questo valore di stringa o attributo utente in IAM Identity Center, inserisci. **`${user:email}`**
8. In Formato, inserisci «non specificato».
9. Scegli Save changes (Salva modifiche).

Aggiungere utenti all'applicazione in Identity Center IAM

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 di IAM Identity Center all'interno dell'RESambiente

1. Dall'ambiente Research and Engineering Studio, in Gestione dell'ambiente, apri Impostazioni generali.
2. Apri la scheda Identity provider.
3. In Single Sign-On, scegli Modifica (accanto a Stato).
4. Completa il modulo con le seguenti informazioni:
    a. Scegliete SAML.
    b. In Nome del fornitore, inserisci un nome intuitivo.
    c. Scegli Inserisci l'endpoint URL del documento di metadati.
    d. Inserisci quello che URL hai copiato durante. Configurazione dell'applicazione in IAM Identity Center
    e. In Attributo email del fornitore, inserisci '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 RES portale. Questi passaggi forniscono indicazioni per l'integrazione con il provider di identità SAML 2.0 scelto. Se intendi utilizzare IAM Identity Center, consultaConfigurazione del single sign-on () SSO con Identity Center IAM.

> **Note**
>
> L'indirizzo e-mail dell'utente deve corrispondere nell'IDPSAMLasserzione 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
- Problemi relativi al debug SAML dell'IdP

## Configura il tuo provider di identità

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

1. RESpresuppone 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 il tuo provider di identità (IdP). Questa configurazione richiede i seguenti parametri:
   - SAMLReindirizzamento URL: utilizzato dal URL tuo IdP per inviare SAML la risposta 2.0 al fornitore di servizi.

     > **Note**
     >
     > A seconda dell'IdP, il SAML reindirizzamento URL potrebbe avere un nome diverso:
     >
     > - Applicazione URL
     > - Assertion Consumer Service () ACS URL
     > - ACSPOSTVincolante URL

     Per ottenere il URL

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

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

  > **Note**
  >
  > A seconda dell'IdP, l'SAMLAudience URI potrebbe avere un nome diverso:
  >
  > - ClientID
  > - Destinatari delle applicazioni SAML
  > - ID dell'entità SP

  Fornisci l'input nel seguente formato.

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

  Per trovare il tuo SAML pubblico URI

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

3. L'SAMLasserzione pubblicata su RES deve avere i seguenti campi/affermazioni impostati sull'indirizzo e-mail dell'utente:
   - SAMLOggetto o NameID
   - SAMLe-mail
4. Il tuo IdP aggiunge campi/attestazioni all'SAMLasserzione, in base alla configurazione. RESrichiede 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` Replace (Sostituisci) *`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` Replace (Sostituisci) *`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` l'`saml2/idpresponse`endpoint del pool di utenti e `InResponseTo` l'ID della SAML richiesta 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 SAML applicazione ha un URL campo di logout, impostalo su:*`<domain-url>`*`/saml2/logout`.

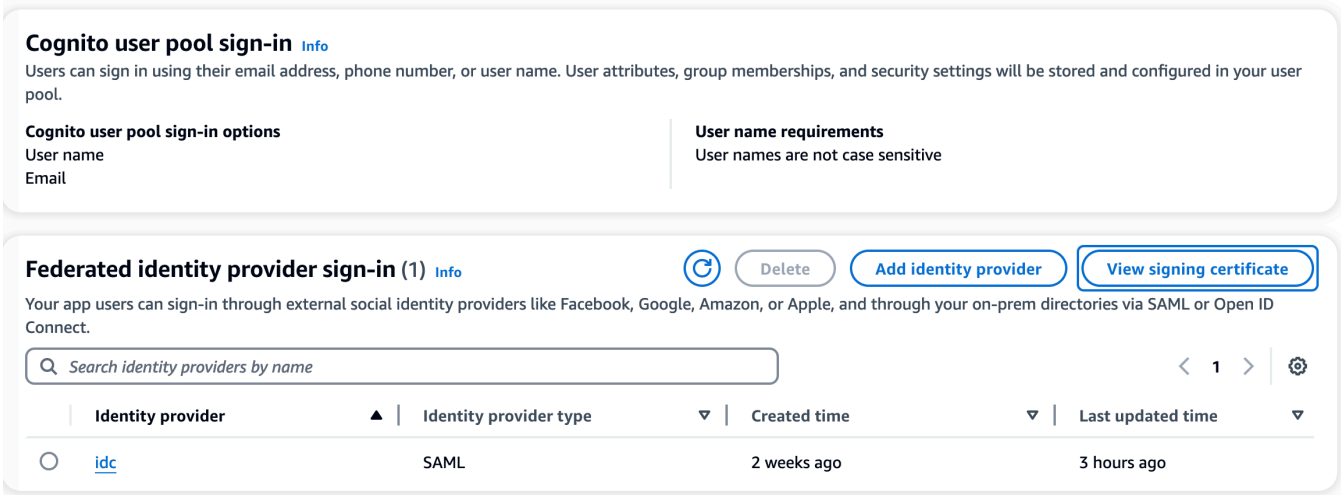
Per ottenere il dominio URL

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

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 essere`res-<environment name>-user-pool`.
3. Seleziona la scheda Esperienza di accesso.
4. Nella sezione di accesso al Federated Identity Provider, scegli Visualizza certificato di firma.




Puoi utilizzare questo certificato per configurare Active DirectoryIDP, aggiungerne uno `relying party trust` e abilitare il SAML supporto su questo relying party.

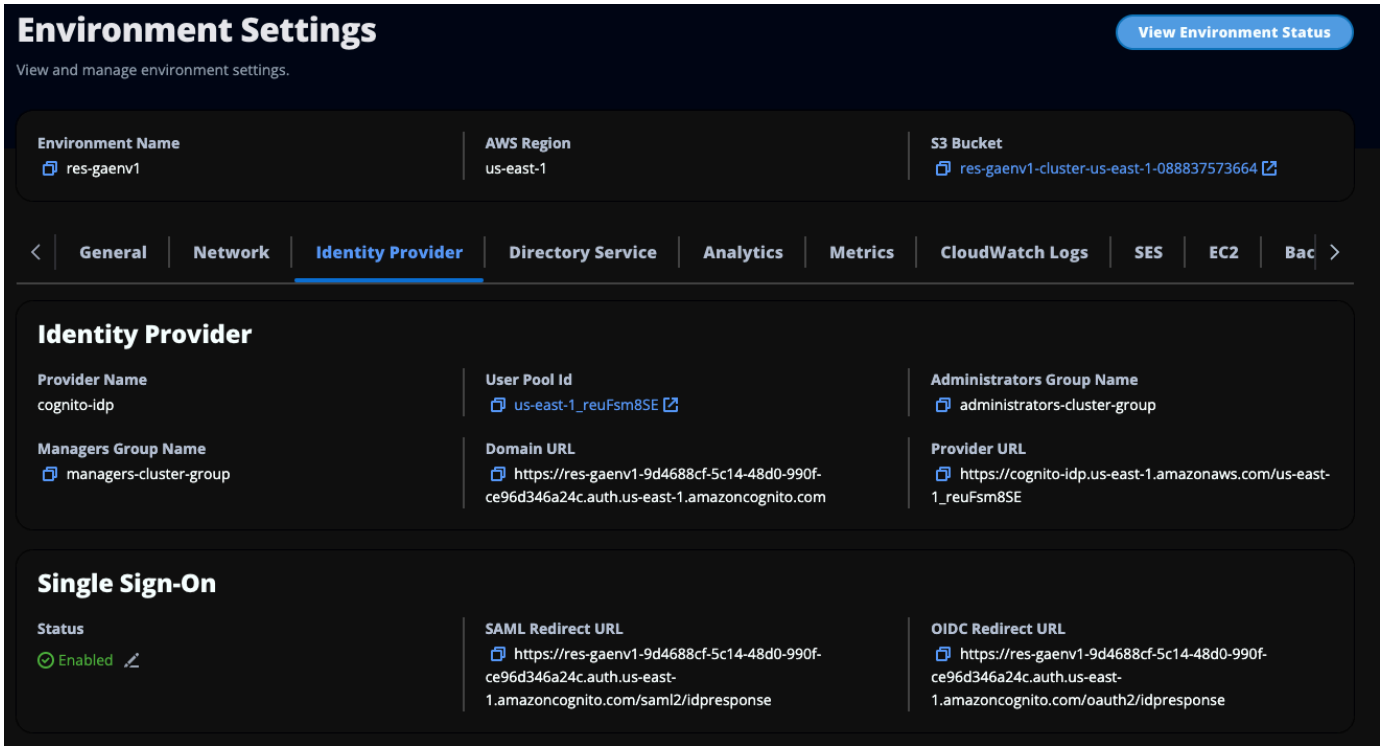
> **Note**
>
> Questo non si applica a Keycloak e. IDC

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

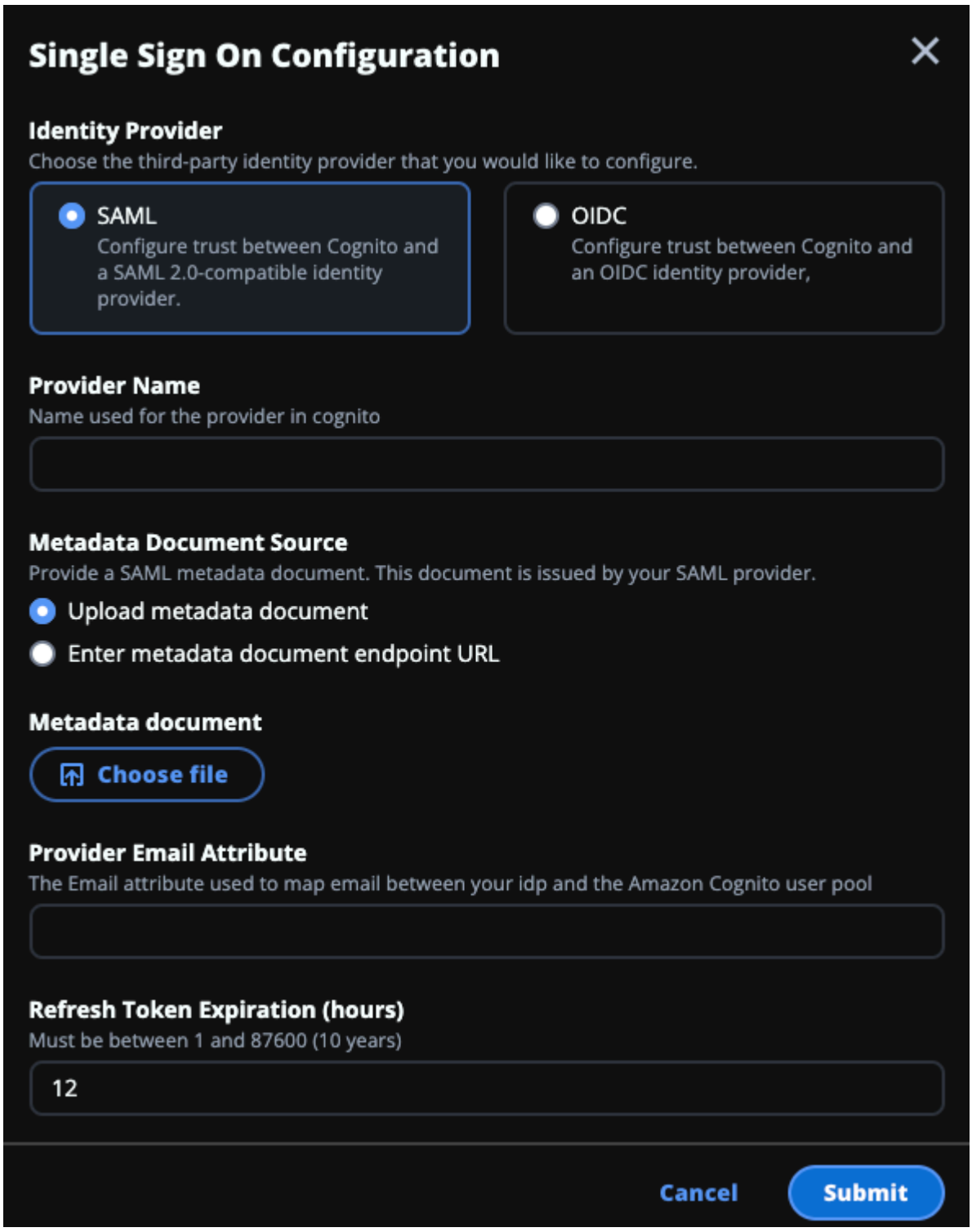
## Configura RES per utilizzare il tuo provider di identità

Per completare la configurazione Single Sign-On per RES

1. Accedi RES come amministratore o amministratore del cluster.
2. Passa 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. In Nome provider, inserisci un nome univoco per il tuo provider di identità.

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

c. In Origine del documento di metadati, scegli l'opzione appropriata e carica il XML documento di metadati o forniscilo 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.

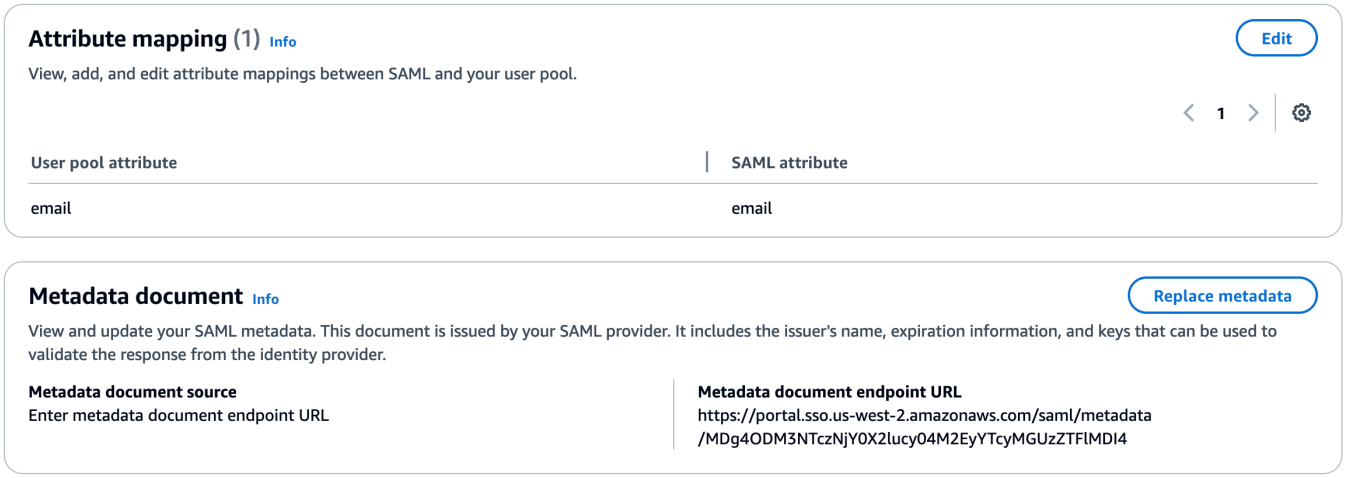
## Configurazione del provider di identità in un ambiente non di produzione

Se hai utilizzato le risorse esterne fornite per creare un RES ambiente 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 RES SSO di abilitazione richiede tre parametri di configurazione:

1. Nome del provider: non può essere modificato
2. Documento di metadati o URL — 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. Seleziona 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.

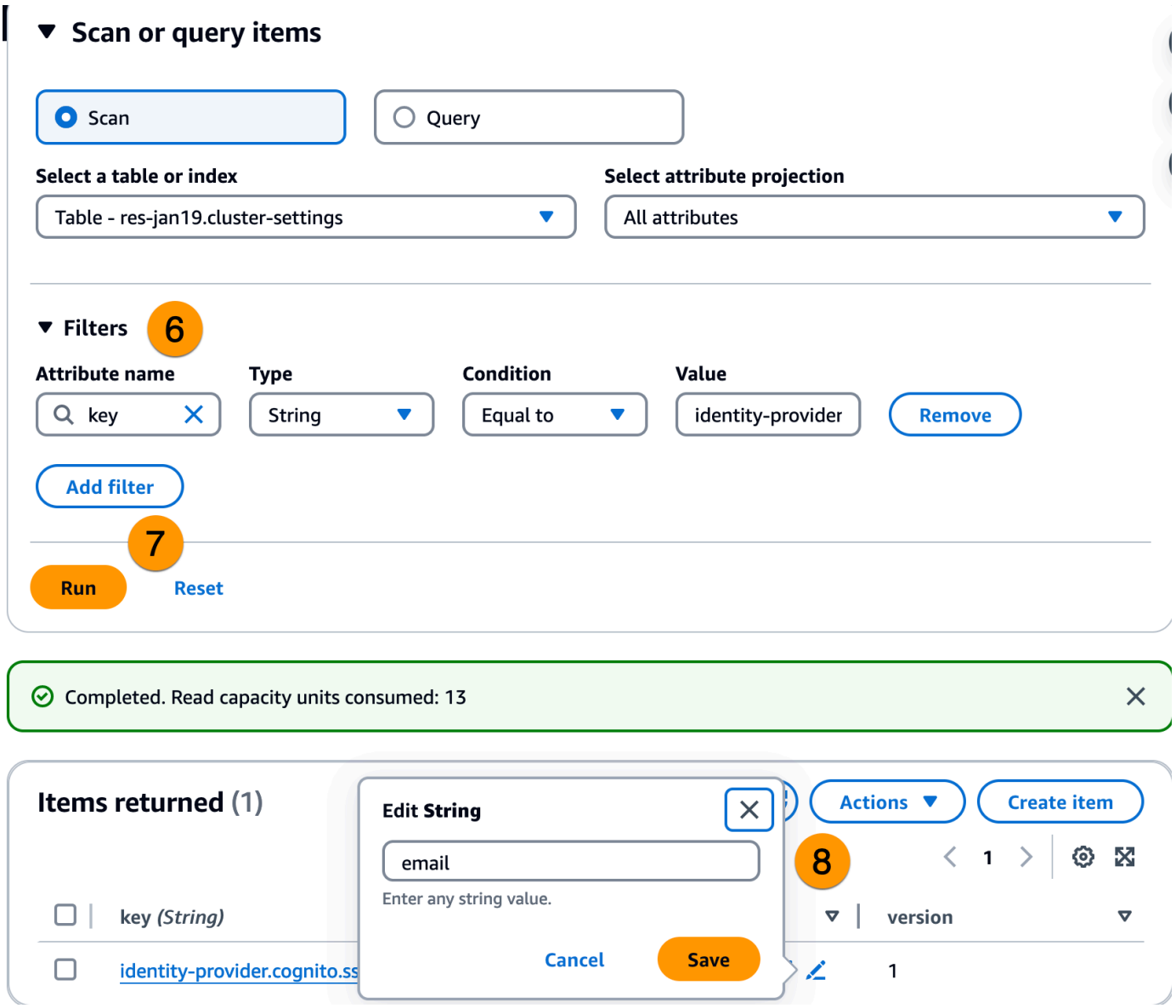
   b. Trova e seleziona la `<environment name>.cluster-settings` tabella e dal menu Azioni seleziona Esplora elementi.

   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.




## Problemi relativi al debug SAML dell'IdP

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

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

Amazon CloudWatch Logs: puoi controllare i tuoi RES log 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'SAMLintegrazione con Amazon Cognito, consulta SAML Aggiungere provider di identità 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, seleziona Reimposta la password utente.
3. Seleziona l'utente e inserisci una nuova password.
4. Scegli Reimposta password.

## Creazione di sottodomini

Se utilizzi un dominio personalizzato, dovrai configurare i sottodomini per supportare il Web e VDI parti del portale.

> **Note**
>
> Se esegui la distribuzione nella regione AWS GovCloud (Stati Uniti occidentali), configura l'applicazione Web e i VDI sottodomini nell'account di partizione commerciale che ospita la zona ospitata pubblica del dominio.

1. Apri la console Route 53.
2. Trova il dominio che hai creato e scegli Crea record.
3. Inserisci «web» come nome del record.
4. Seleziona CNAMEcome tipo di record.
5. Per Value, inserisci il link che hai ricevuto nell'e-mail iniziale.
6. Scegli Crea record.
7. Per creare un record per ilVDC, recupera l'NLBindirizzo.

    a. Apri la AWS CloudFormation console.

b. Scegli `<environment-name>-vdc`.

c. Scegli Risorse e apri`<environmentname>-vdc-external-nlb`.

d. Copia il DNS nome daNLB.

8. Apri la console Route 53.
9. Trova il tuo dominio e scegli Crea record.
10. In Nome del record, inserisci`vdc`.
11. In Tipo di record, selezionate CNAME.
12. PerNLB, inserisci ilDNS.
13. Scegli Crea record.

## Crea un ACM certificato

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 TLS certificatoSSL/pubblico fornito da te o richiesto da (). AWS Certificate Manager ACM Se lo utilizziACM, riceverai un nome di AWS risorsa che dovrai fornire come parametro per crittografare il TLS canaleSSL/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. 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 DNSconvalida.
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:
   - Implementazione 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 CNAME chiave e il valore. 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 certificato ARN 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/ <installation-stack-name>-cluster-endpoints` | Non scadono mai |
| `/aws/lambda/ <installation-stack-name>-cluster-manager-scheduled-ad-sync` | Non scadono mai |
| `/aws/lambda/ <installation-stack-name>-cluster-settings` | Non scadono mai |

| CloudWatch Gruppi di log | Retention |
| --- | --- |
| /aws/lambda/ *<installation-stack-name>*-oauth-credentials | 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/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope | Non scadono mai |
| /*<installation-stack-name>* /cluster-manager | 3 mesi |
| /*<installation-stack-name>* /vdc/controller | 3 mesi |
| /*<installation-stack-name>* /vdc/dcv-broker | 3 mesi |
| /*<installation-stack-name>* /vdc/dcv-connection-gateway | 3 mesi |

Se desideri modificare la conservazione predefinita per un gruppo di log, puoi andare alla CloudWatch console 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 RES allegando limiti di autorizzazione personalizzati. Un limite di autorizzazione personalizzato può essere definito come parte dell'RES AWS CloudFormation installazione fornendo i limiti di autorizzazione come parte del parametro. ARN IAMPermissionBoundary Nessun limite di autorizzazione viene impostato su alcun RES ruolo se questo parametro viene lasciato vuoto. Di seguito è riportato l'elenco delle azioni necessarie per il funzionamento RES dei ruoli. 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:*"
        ]
    }
]
```

# Configura RES -ready AMIs

Con RES -ready Amazon Machine Images (AMIs), puoi preinstallare RES le dipendenze per le istanze di desktop virtuali (VDIs) sulle tue istanze personalizzate. AMIs L'uso di RES -ready AMIs migliora i tempi di avvio delle VDI istanze che utilizzano le immagini predefinite. Utilizzando EC2 Image Builder, è possibile creare e registrare nuovi AMIs 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 IAM il ruolo per accedere all'ambiente RES
- Crea componente EC2 Image Builder
- Prepara la tua ricetta per EC2 Image Builder
- Configurazione EC2 dell'infrastruttura Image Builder
- Configurazione della pipeline di immagini di Image Builder
- Esegui la pipeline di immagini di Image Builder
- Registra un nuovo stack software in RES

## Prepara IAM il ruolo per accedere all'ambiente RES

Per accedere al servizio di RES ambiente da EC2 Image Builder, è necessario creare o modificare un IAM ruolo chiamato RES -. EC2InstanceProfileForImageBuilder Per informazioni sulla configurazione di un IAM ruolo da utilizzare in Image Builder, AWS Identity and Access Management vedere IAM () nella Guida per l'utente di Image Builder.

Il tuo ruolo richiede:

- Le relazioni di fiducia includono il EC2 servizio Amazon.
- A mazonSSMManaged InstanceCore e EC2InstanceProfileForImageBuilder politiche.

- RESPolicy personalizzata con accesso limitato a DynamoDB e Amazon S3 all'ambiente distribuito. RES

  (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"
        }
    ]
}
```

RESpolitica:

```
{
    "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.*",
                        "vdc.host_modules.*"
                    ]
                }
            }
        },
```

```
        {
            "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/*",
                "arn:aws:s3:::research-engineering-studio-{AWS-Region}/host_modules/*"
            ]
        }
    ]
}
```

## Crea 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 YAML file 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

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 da aggiungere per personalizzare l'immagine e verificare che tutto funzioni come previsto. È necessario creare o modificare una ricetta per costruire l'obiettivo AMI con le dipendenze RES software necessarie. Per ulteriori informazioni sulle ricette, consulta Gestire le ricette.

RESsupporta i seguenti sistemi operativi di immagini:

- Amazon Linux 2 (x86 eARM64)
- Ubuntu 22.04.3 (x86)
- RHEL8 (x86) e 9 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Aprire la console EC2 Image Builder all'indirizzo. https://console.aws.amazon.com/imagebuilder
2. In Risorse salvate, scegli Ricette con immagini.
3. Scegli Crea ricetta di immagine.

4. Inserisci un nome univoco e un numero di versione.
5. Seleziona un'immagine di base supportata daRES.
6. In Configurazione dell'istanza, installa un SSM agente se non è preinstallato. Inserisci le informazioni in Dati utente e qualsiasi altro dato utente necessario.

   > **Note**
   >
   > Per informazioni su come installare un SSM agente, consulta:
   >
   > - Installazione manuale SSM dell'agente su EC2 istanze per Linux.
   > - Installazione e disinstallazione manuale SSM dell'agente sulle EC2 istanze 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. RESgli script di installazione utilizzano il AWS CLI per fornire l'VDIaccesso 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, RESEnvNameRESEnvRegion, e. RESEnvReleaseVersion

   > **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 AMI possa essere avviato. 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 si dispone di una ricetta EC2 Image Builder esistente, è possibile 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. RESGli script di installazione utilizzano il AWS CLI per fornire l'VDIaccesso 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, RESEnvNameRESEnvRegion, e. RESEnvReleaseVersion

   > **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 EC2 dell'infrastruttura Image Builder

Puoi utilizzare le configurazioni dell'infrastruttura per specificare l'EC2infrastruttura Amazon utilizzata da Image Builder per creare e testare la tua immagine Image Builder. Da utilizzare conRES, puoi scegliere di creare una nuova configurazione dell'infrastruttura o utilizzarne una esistente.

- Per creare una nuova configurazione dell'infrastruttura, vedi 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 IAMruolo, inserisci il ruolo in cui hai configurato in Prepara IAM il ruolo per accedere all'ambiente RES precedenza.
2. Ad esempio, scegli un tipo con almeno 4 GB di memoria e che supporti l'AMIarchitettura di base scelta. Vedi i tipi di EC2 istanze Amazon.
3. Per VPCsottoreti e gruppi di sicurezza, devi 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 RES -readyAMIs, è possibile scegliere di creare una nuova pipeline o utilizzarne una esistente. Per ulteriori informazioni, consulta Creare e aggiornare pipeline di AMI immagini 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. Dal pannello di 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 inPrepara 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 di 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. Configurazione EC2 dell'infrastruttura 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 Regione AWS stesso ambiente. 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 per utilizzare la ricetta creata in. Prepara la tua ricetta per EC2 Image Builder

2. Scegli Save changes (Salva 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. 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 “Pile di software () AMIs” per registrare uno stack di software.
2. Per AMIID, inserisci l'AMIID dell'immagine di output integrata. Esegui la pipeline di immagini di Image Builder

# Guida per gli 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 dei segreti

Research and Engineering Studio mantiene i seguenti segreti utilizzando AWS Secrets Manager. REScrea 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 | RESgenerati | Amministratore inserito |
|---|---|---|---|
| `<envname> -sso-client-secret` | Single Sign-On OAuth2 Client Secret per l'ambiente | ✓ | |
| `<envname> -vdc-client-secret` | vdc ClientSecret | ✓ | |
| `<envname> -vdc-client-id` | vdc ClientId | ✓ | |
| `<envname> -vdc-gateway-certificate-private-key` | Chiave privata del certificato autofirmato per il dominio | ✓ | |

| Nome segreto | Descrizione | RESgenerati | Amministratore inserito |
|---|---|---|---|
| `<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> -external-certificate` | Certificato autofirmato per dominio | ✓ | |
| `<envname> -internal-private-key` | Chiave privata del certificato autofirmato per il dominio | ✓ | |
| `<envname> -internal-certificate` | Certificato autofirmato per dominio | ✓ | |

| Nome segreto | Descrizione | RESgenerati | Amministratore inserito |
|---|---|---|---|
| `<envname> -directoryservice-ServiceAccountUserDN` | L'attributo Distinguished Name (DN) dell' ServiceAccount utente. | ✓ | |

I seguenti ARN valori segreti sono contenuti nella `<envname>-cluster-settings` tabella 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` | |
| `cluster.secretsmanager.kms_key_id` | |

| Chiave | Origine |
| --- | --- |
| `cluster.load_balancers.external_alb.certificates.private_key_secret_arn` | stack |
| `cluster-manager.client_secret` | |

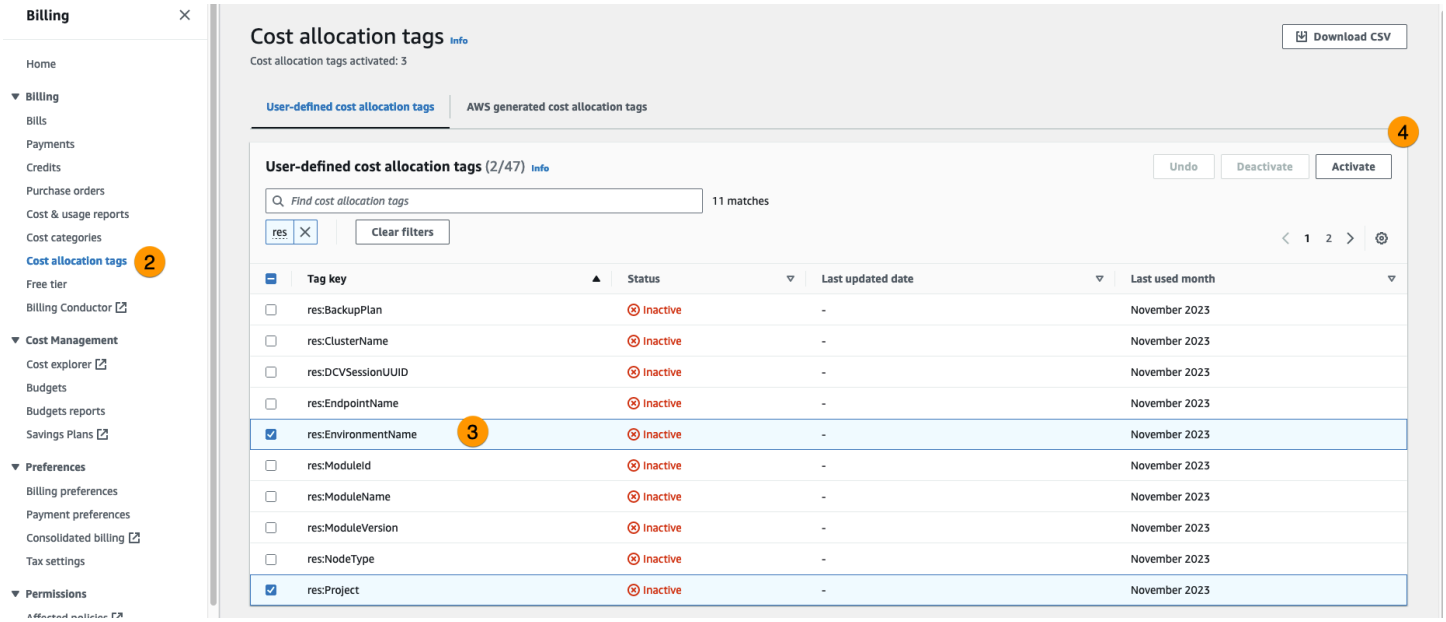
# Monitoraggio e controllo dei costi

> **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 “AWS servizi inclusi in questo prodotto”.

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

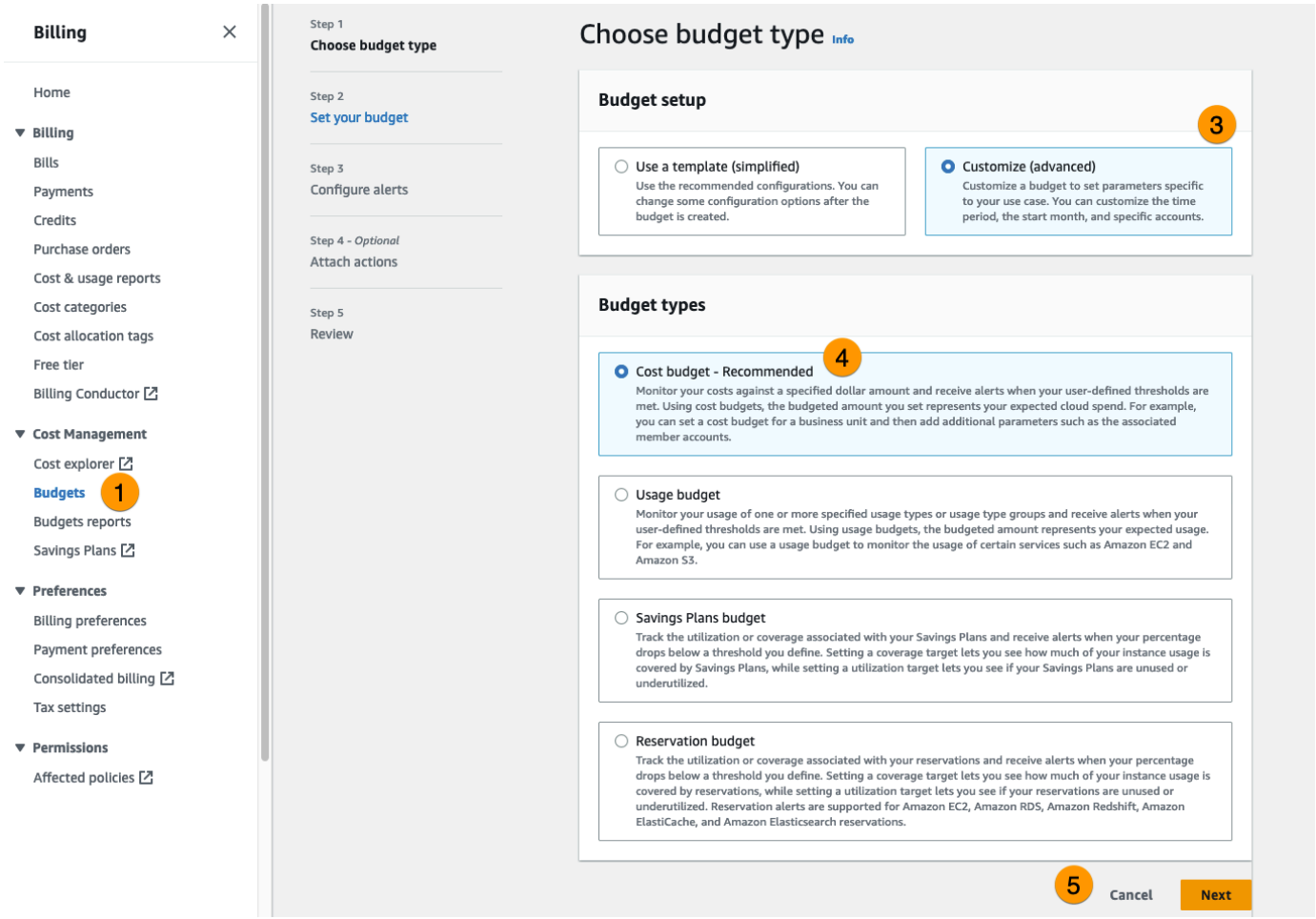
1. Accedi a AWS Management Console e apri la AWS Billing console all'indirizzo. https://console.aws.amazon.com/billing/
2. Scegli i tag di allocazione dei costi.
3. Cerca e seleziona i `res:EnvironmentName` tag `res:Project` and.
4. Seleziona Activate (Attiva).




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

Per creare un budget per RES le risorse:

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. Scegli Next (Successivo).

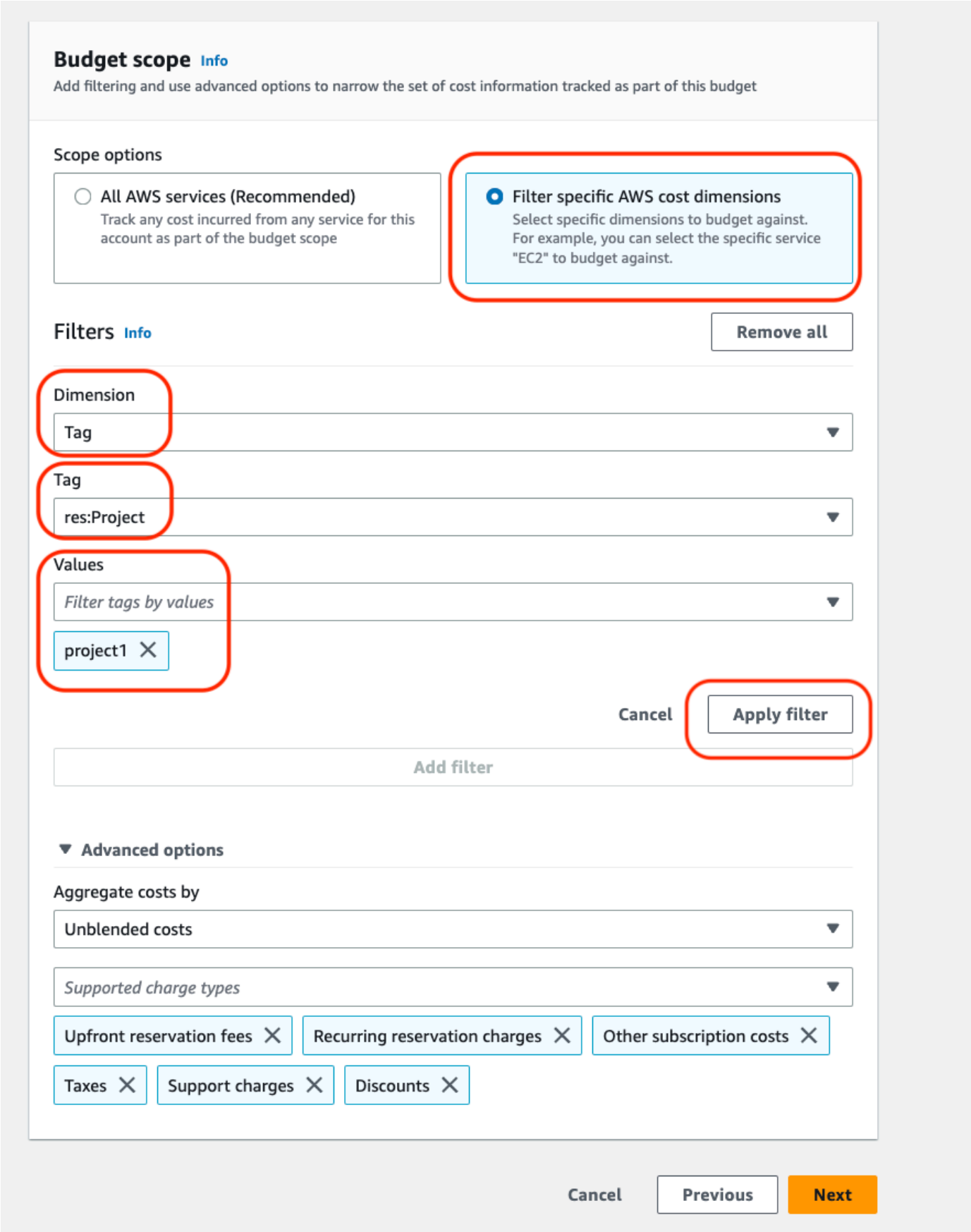



6. In Dettagli, inserisci un nome di budget significativo per il tuo budget per distinguerlo dagli altri budget del tuo account. Ad esempio *<EnvironmentName>-<ProjectName>-<BudgetName>*.
7. In Imposta l'importo del budget, inserisci l'importo previsto per il tuo progetto.
8. In Ambito del budget, scegli 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.

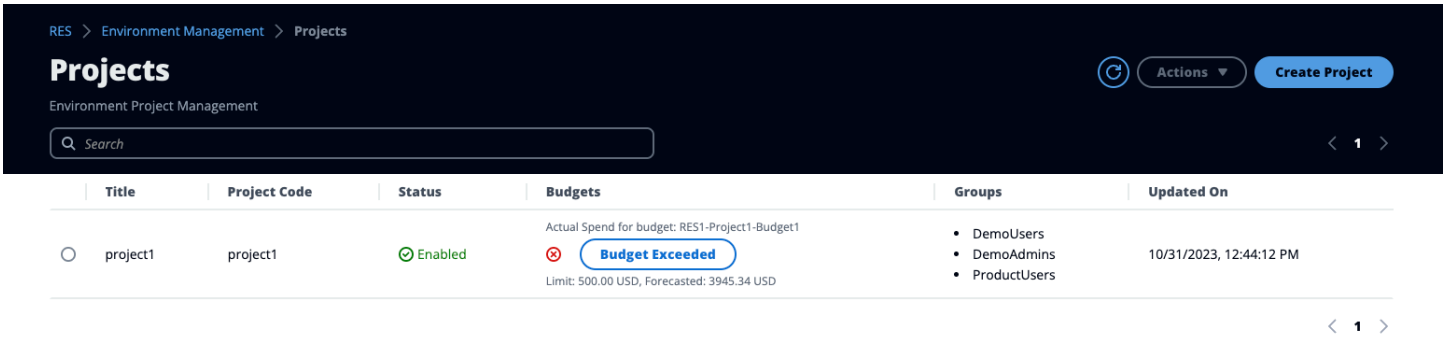
12. In Valori, seleziona il nome del progetto.
13. Scegli Applica filtro per allegare il filtro del progetto al budget.

14. Scegli Next (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. (Facoltativo) Aggiungi una soglia di avviso.
16. Scegli Next (Successivo).
17. (Facoltativo) Se è stato configurato un avviso, utilizza Allega azioni per configurare le azioni desiderate con l'avviso.
18. Scegli Next (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 entroRES. In alternativa, puoi modificare un progetto per disattivare un budget.

# Gestione della sessione

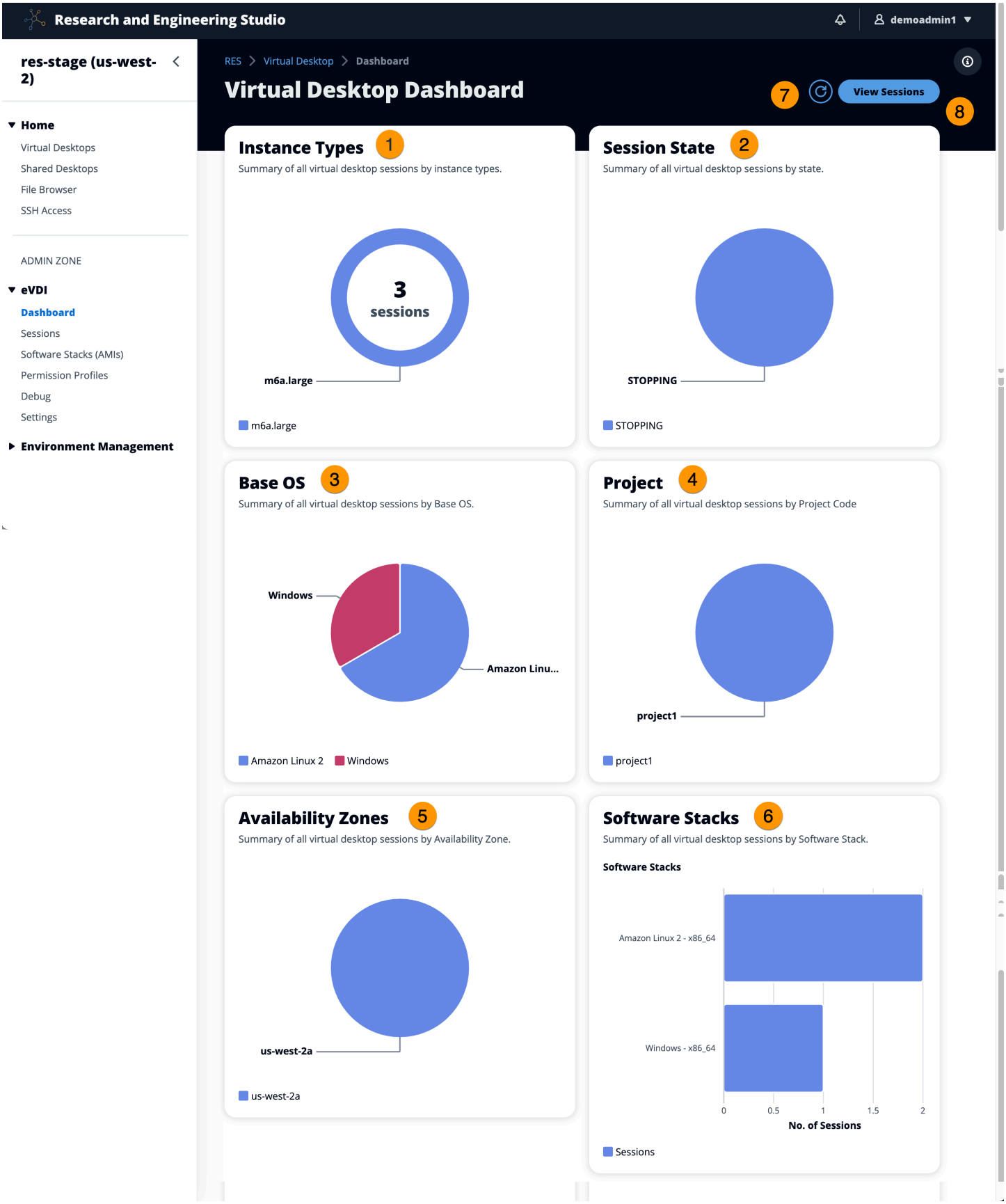
La gestione delle sessioni offre un ambiente flessibile e interattivo per lo sviluppo e il test delle sessioni. In qualità di utente amministrativo, puoi consentire agli utenti di creare e gestire sessioni interattive all'interno dei loro ambienti di progetto.

Argomenti

- Dashboard
- Sessioni

- Stack software () AMIs
- Debug
- Impostazioni del desktop

# 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:

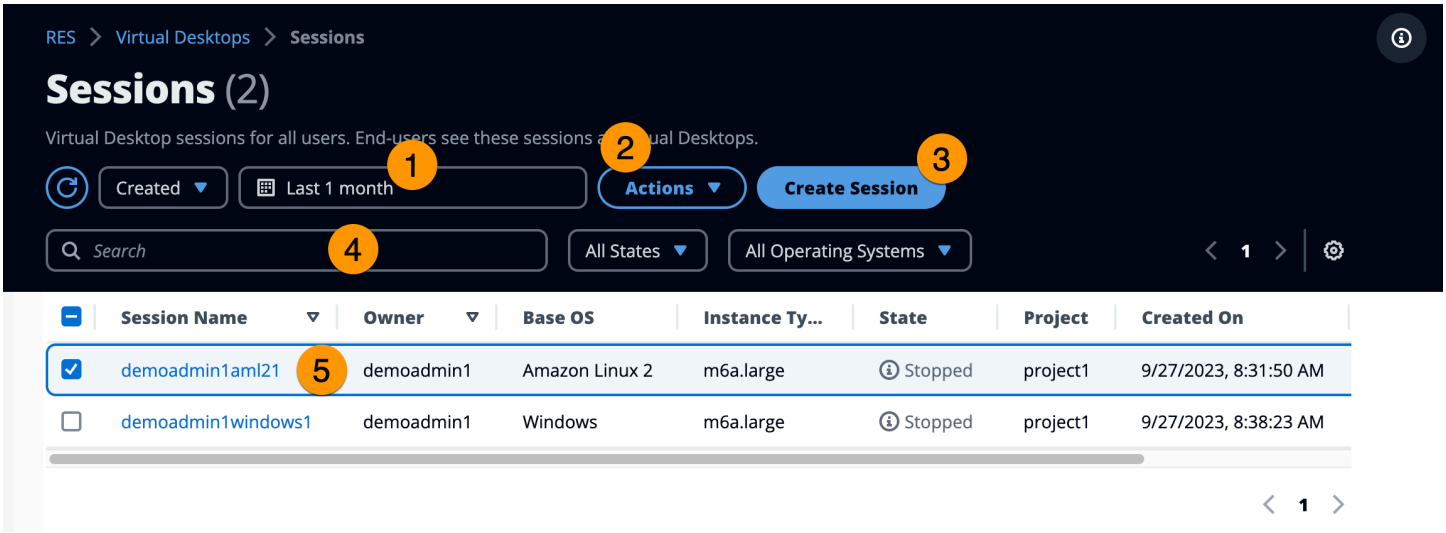
1. Tipi di istanza
2. Stati della sessione
3. Sistema operativo di base
4. Progetti
5. Zone di disponibilità
6. Pile di software

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. Seleziona il nome della sessione per visualizzare ulteriori 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. (Facoltativo) Attiva Mostra opzioni avanzate per fornire dettagli aggiuntivi come l'ID di sottorete e il tipo di DCV sessione.
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.

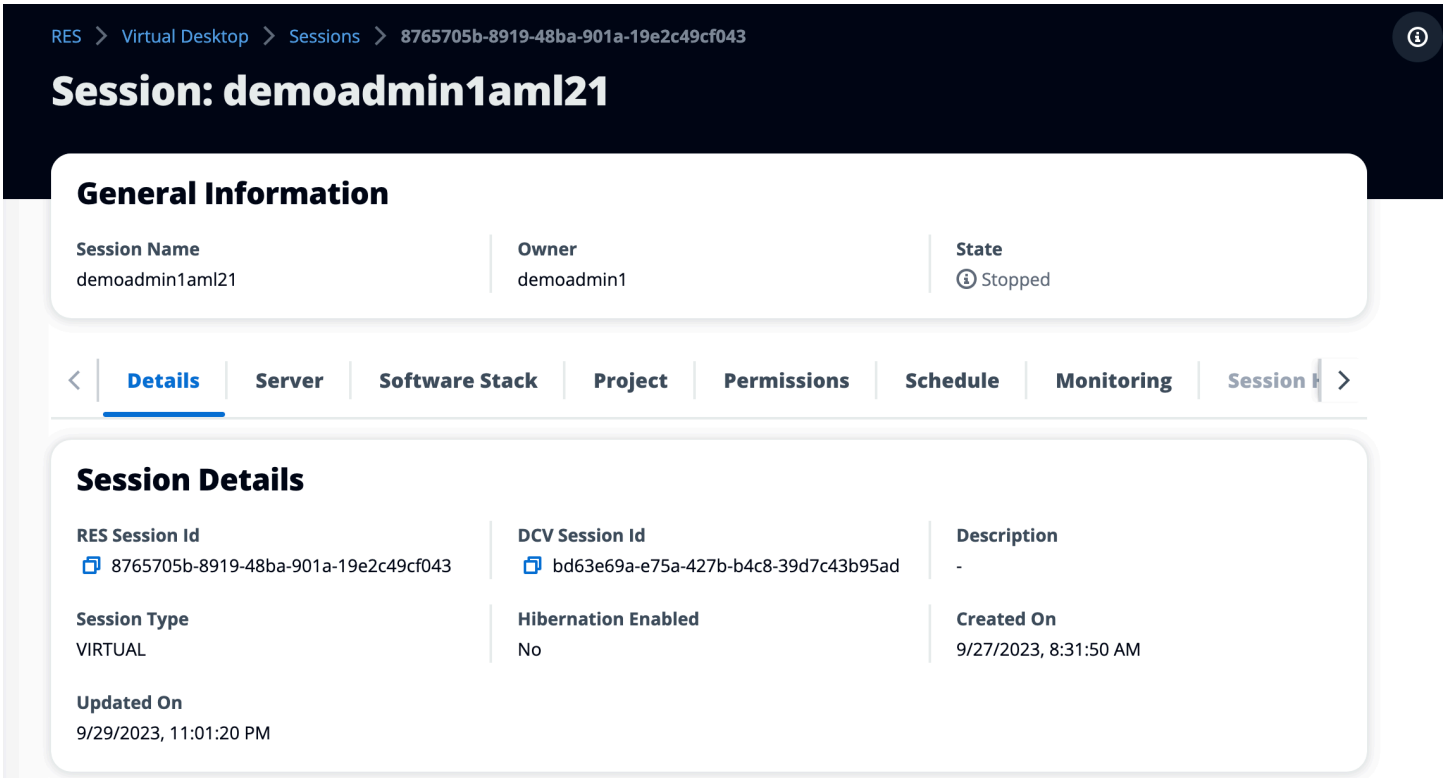
**Virtual Desktop Size**
Select a virtual desktop instance type

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

10

## Dettagli della sessione

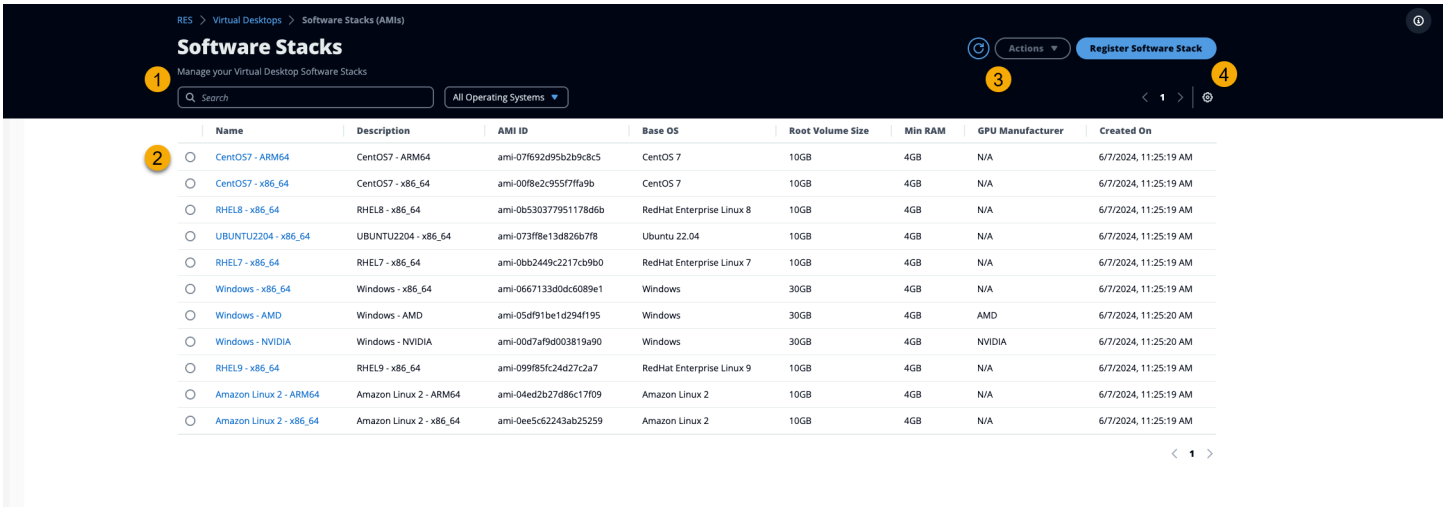
Dall'elenco Sessioni, seleziona il nome della sessione per visualizzare i dettagli della sessione.




# Stack software () AMIs

> **Note**
>
> Per eseguire lo stack SO7 software Cent fornito AWS GovCloud (US), è necessario abbonarsi a the AMI within Marketplace AWS utilizzando l'account standard collegato.

Dalla pagina Software Stacks, puoi configurare Amazon Machine Images (AMIs) o gestire quelle esistenti.




1. Per cercare uno stack software esistente, utilizza il menu a discesa del sistema operativo per filtrare per sistema operativo.
2. Seleziona 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

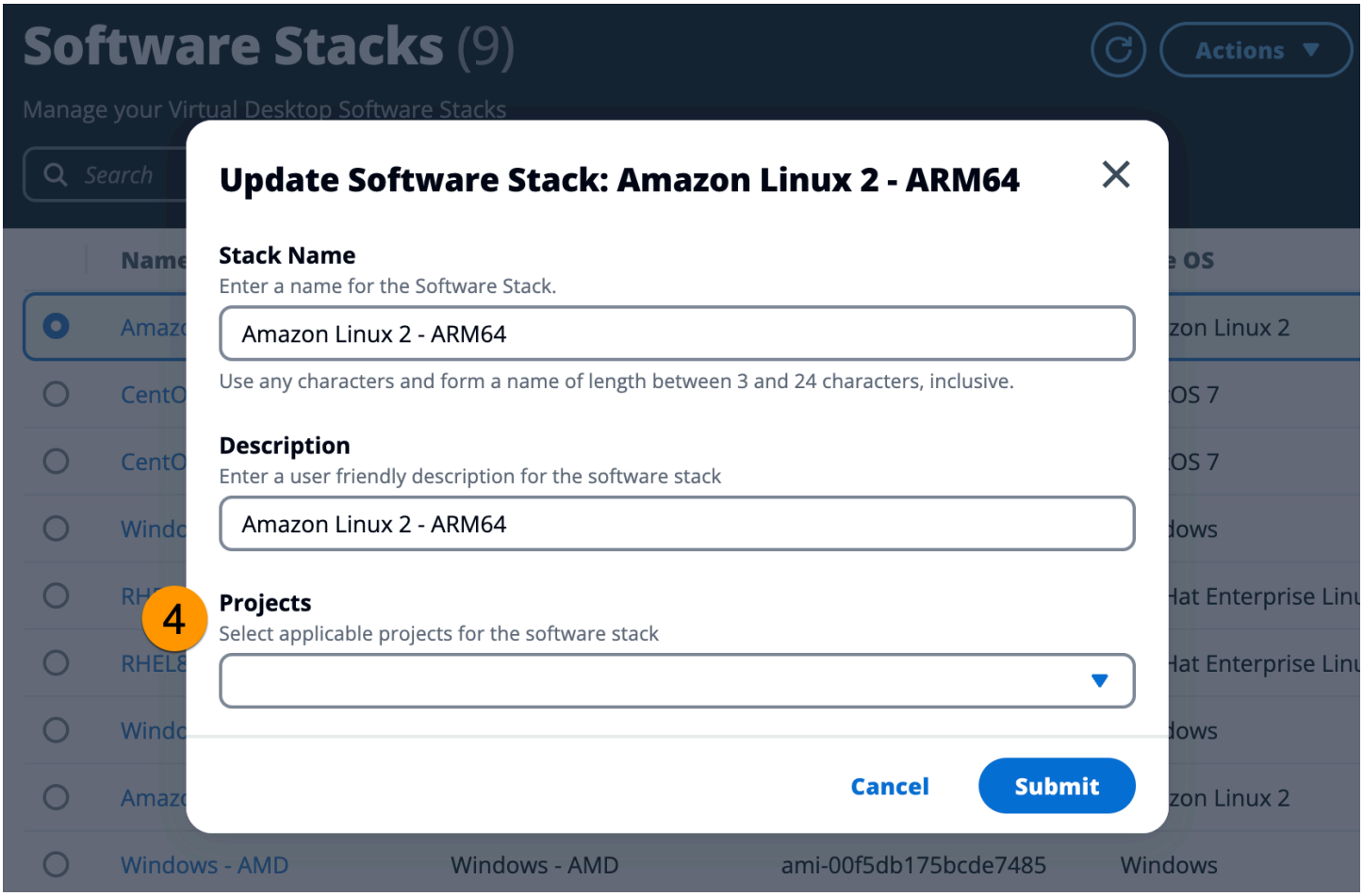
## Assegna uno stack software a un progetto

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.

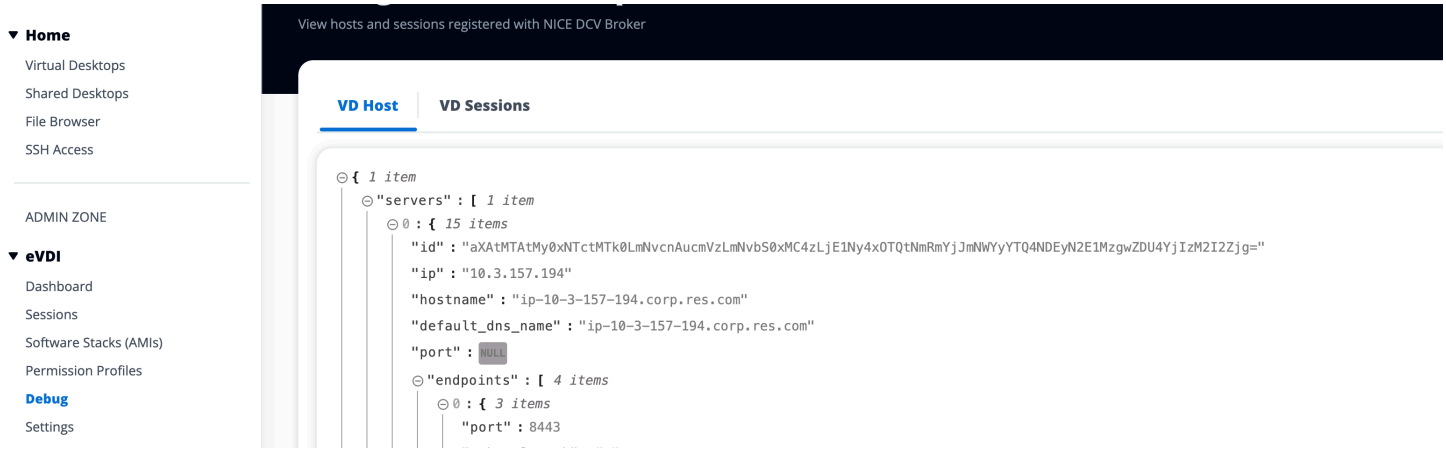



## Visualizza i dettagli dello stack software

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

# 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:

DCVtimeout di inattività della sessione

Il tempo dopo il quale la DCV sessione verrà disconnessa automaticamente. Ciò non modifica lo stato della sessione desktop, ma chiude solo la sessione dal DCV client o dal browser web.

Avviso di timeout di inattività

Il periodo dopo il quale verrà fornito un avviso di inattività al client.

CPUsoglia di utilizzo

L'CPUutilizzo da considerare inattivo.

Sessioni consentite per utente

Il numero di VDI sessioni che un singolo utente può avere in un determinato momento. Se un utente soddisfa o supera questo valore, ciò impedirà l'avvio di nuove sessioni dalla pagina I miei desktop virtuali. Questo valore non influisce sulla capacità di avviare sessioni tramite la pagina Sessioni.

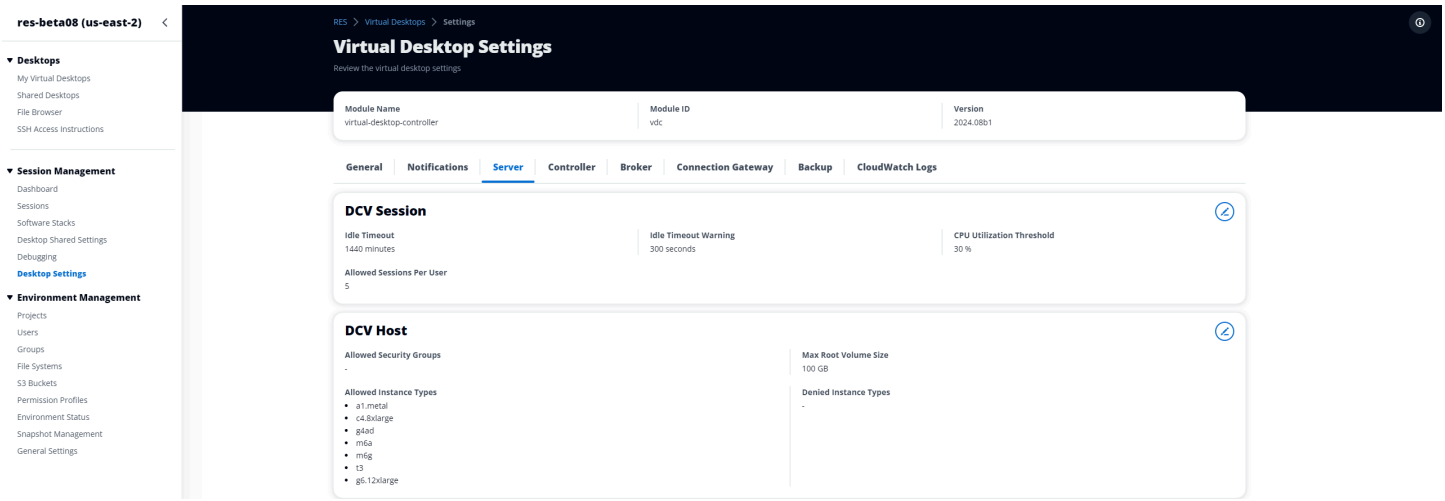
Dimensione massima del volume root

La dimensione predefinita del volume root nelle sessioni di desktop virtuale.

Tipi di istanze consentiti

L'elenco delle famiglie e delle dimensioni di istanze che possono essere lanciate per questo RES ambiente. Le combinazioni di famiglie di istanze e dimensioni delle istanze sono entrambe

accettate. Ad esempio, se specifichi 'm7a', tutte le dimensioni della famiglia m7a saranno disponibili per l'avvio come sessioni. VDI Se specifichi 'm7a.24xlarge', solo m7a.24xlarge sarà disponibile per l'avvio come sessione. VDI Questo elenco riguarda tutti i progetti nell'ambiente.




# Gestione dell'ambiente

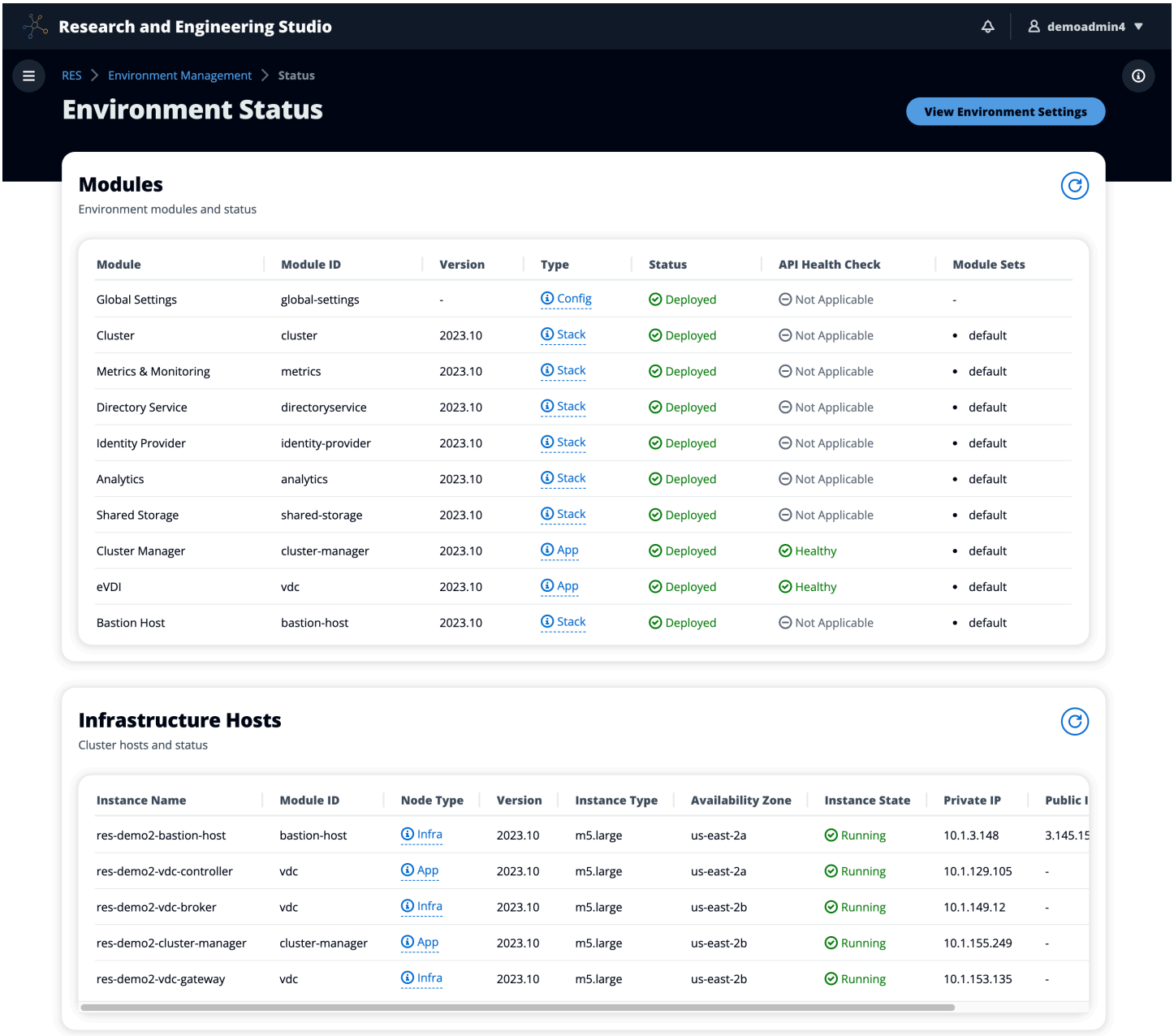
Dalla sezione Gestione dell'ambiente diRES, gli utenti amministrativi possono creare e gestire ambienti isolati per i propri progetti di ricerca e ingegneria. Questi ambienti possono includere risorse di elaborazione, storage e altri componenti necessari, il tutto all'interno di un ambiente sicuro. Gli 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

- Stato dell'ambiente
- Impostazioni di ambiente
- Utenti
- Gruppi
- Progetti
- Policy di autorizzazione
- File system
- Gestione delle istantanee
- Bucket Amazon S3

# 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.




# Impostazioni di ambiente

La pagina delle impostazioni ambientali mostra i dettagli della 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'VPCID, l'elenco IDs dei prefissi per l'accesso.

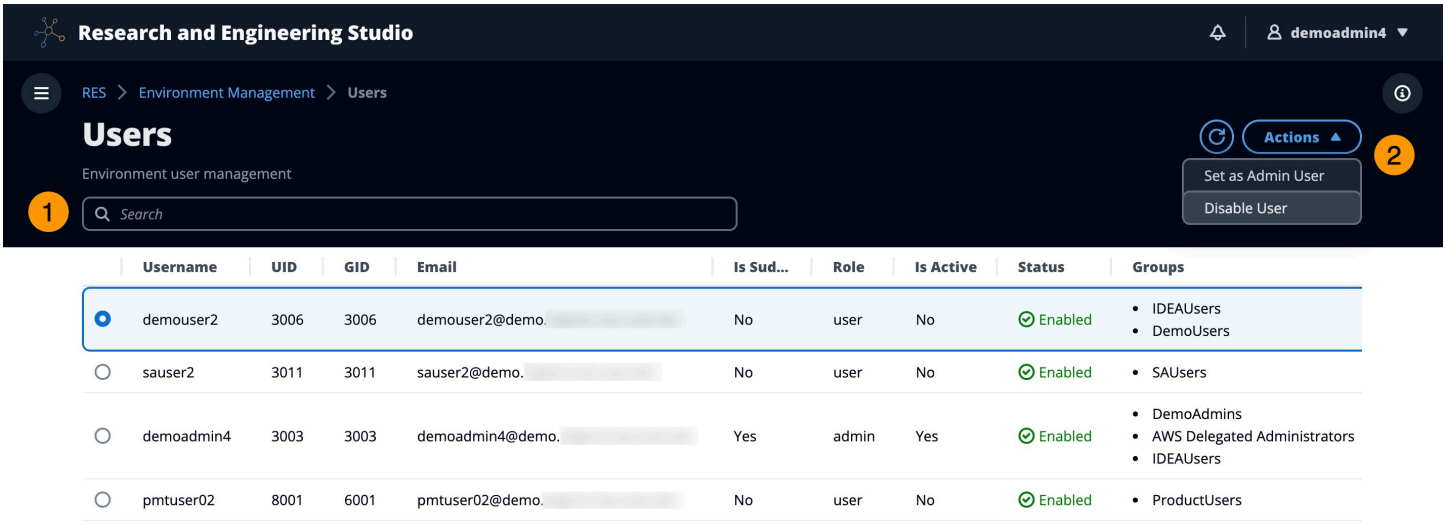
- Directory Service

  Visualizza le impostazioni di Active Directory e il gestore dei segreti degli account di servizio ARN per nome utente e password.

## 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.

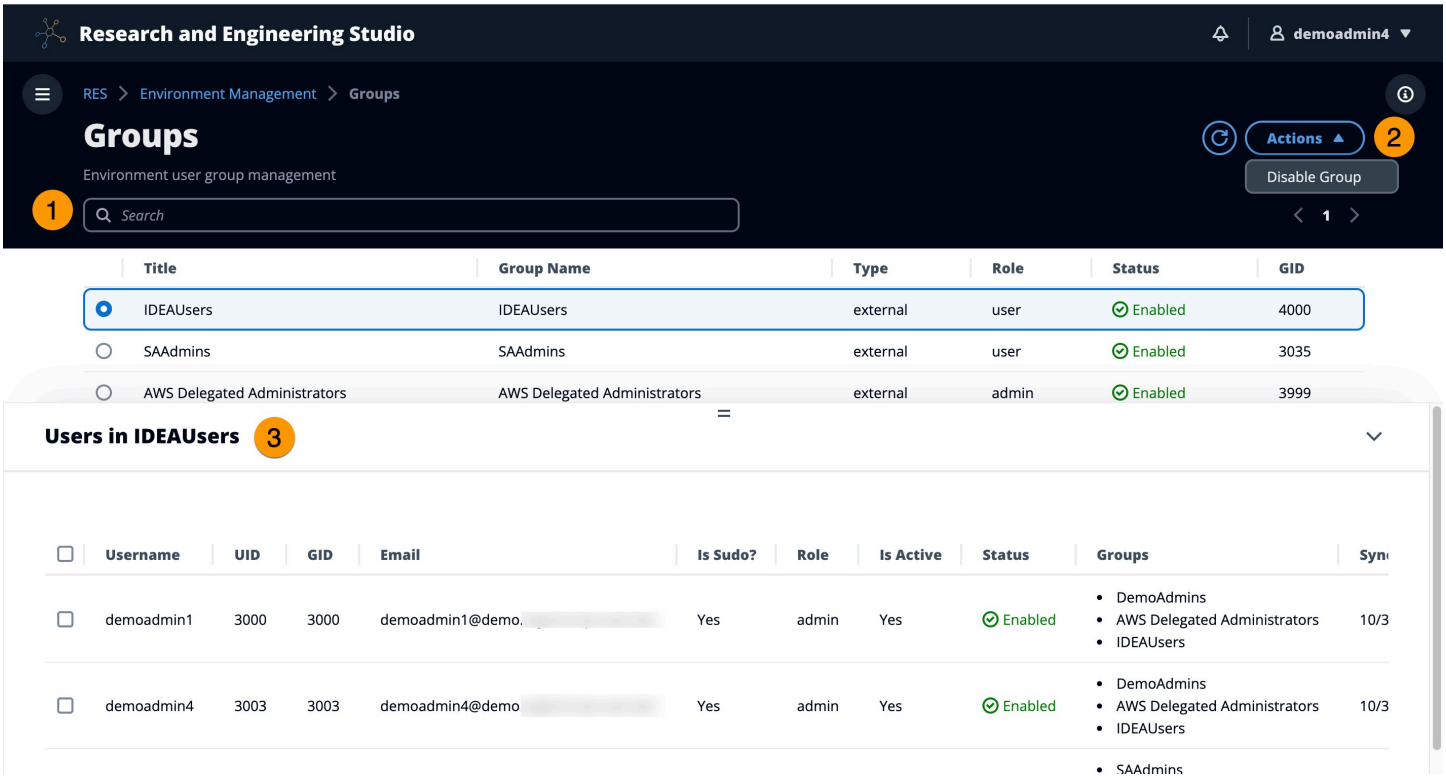



Dalla pagina Utenti, puoi:

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.

## Progetti

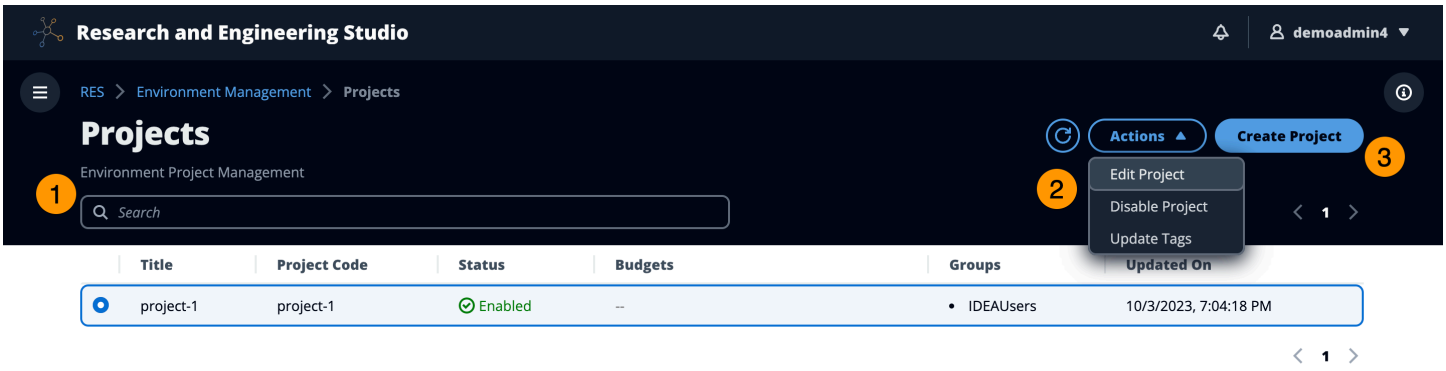
I progetti costituiscono un limite per desktop virtuali, team e budget. Quando crei un progetto, ne definisci le impostazioni, come il nome, la descrizione e la configurazione dell'ambiente. I progetti includono in genere uno o più ambienti, che possono essere personalizzati per soddisfare i requisiti 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
- Crea un progetto

- Modifica un progetto
- Aggiungere o rimuovere tag da un progetto
- Visualizza i file system associati a un progetto
- Aggiungi un modello di lancio

## 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.

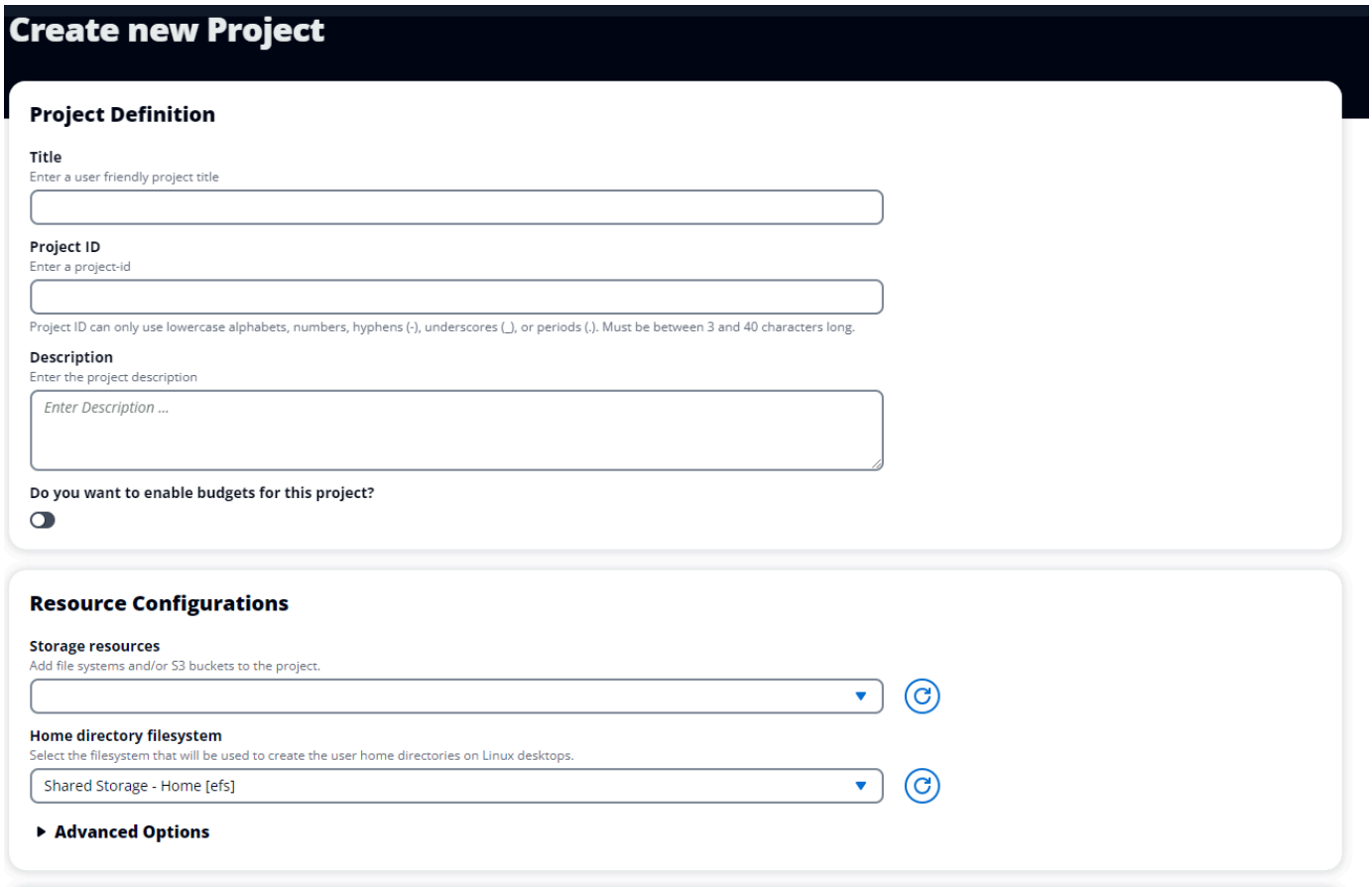
   L'ID del progetto è un tag di risorsa che può essere utilizzato per tenere traccia dell'allocazione dei costi in AWS Cost Explorer Service. Per ulteriori informazioni, vedere Attivazione dei tag di allocazione dei costi definiti dall'utente.

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

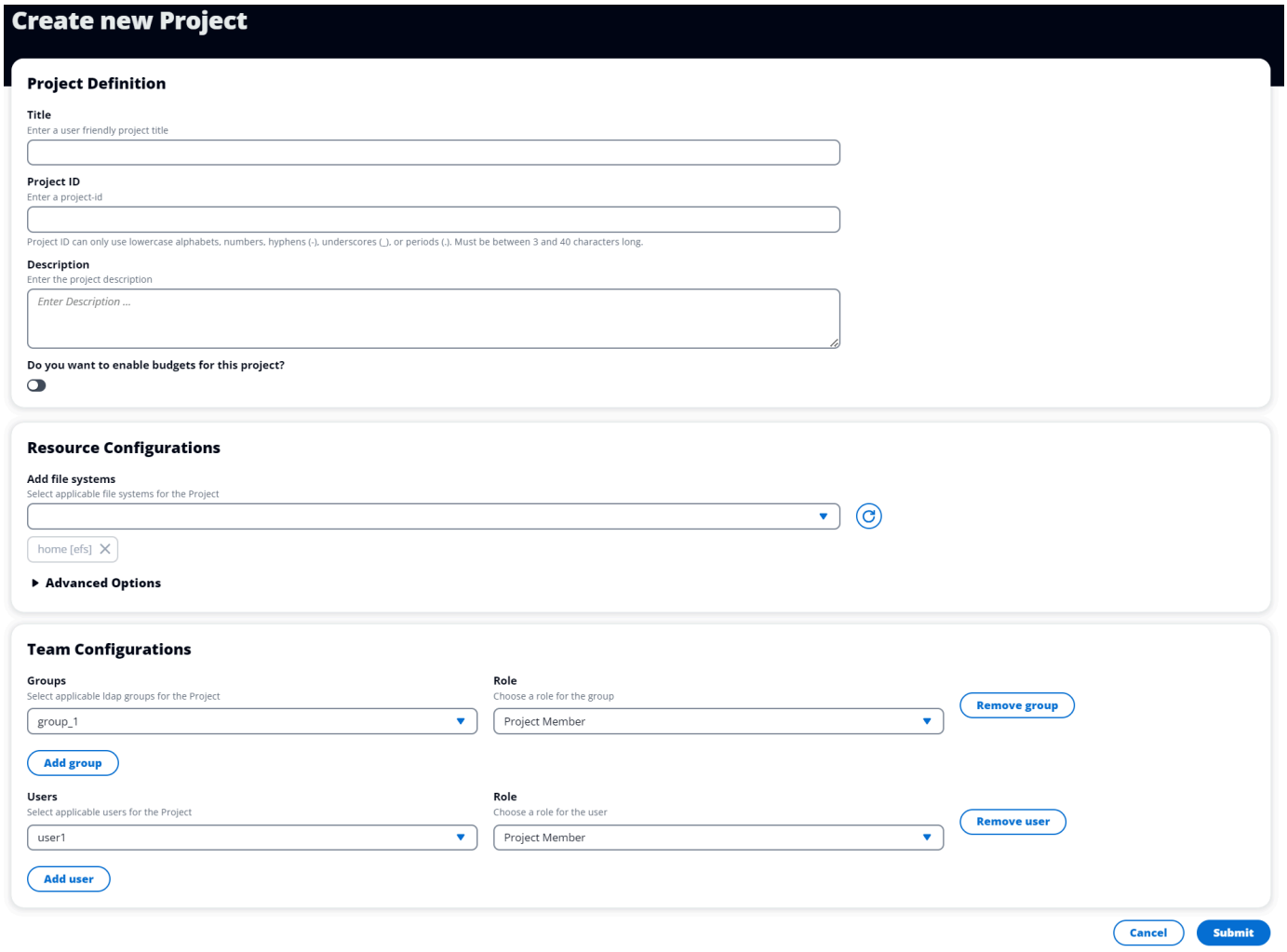
Per informazioni sulle opzioni avanzate, vedereAggiungi un modello di lancio.

3. (Facoltativo) Attiva i budget per il progetto. Per ulteriori informazioni sui budget, consulta. Monitoraggio e controllo dei costi
4. Il filesystem della directory home può utilizzare lo Shared Home Filesystem (impostazione predefinita), FSx per LustreEFS, o lo storage di volumi. FSx NetApp ONTAP EBS

   È importante notare che il file system home condiviso, FSx per LustreEFS, può essere condiviso tra più progetti e. FSx NetApp ONTAP VDIs Tuttavia, l'opzione di archiviazione VDI in EBS volume richiederà che ogni componente del progetto abbia la propria home directory che non sia condivisa tra altri progetti. VDIs

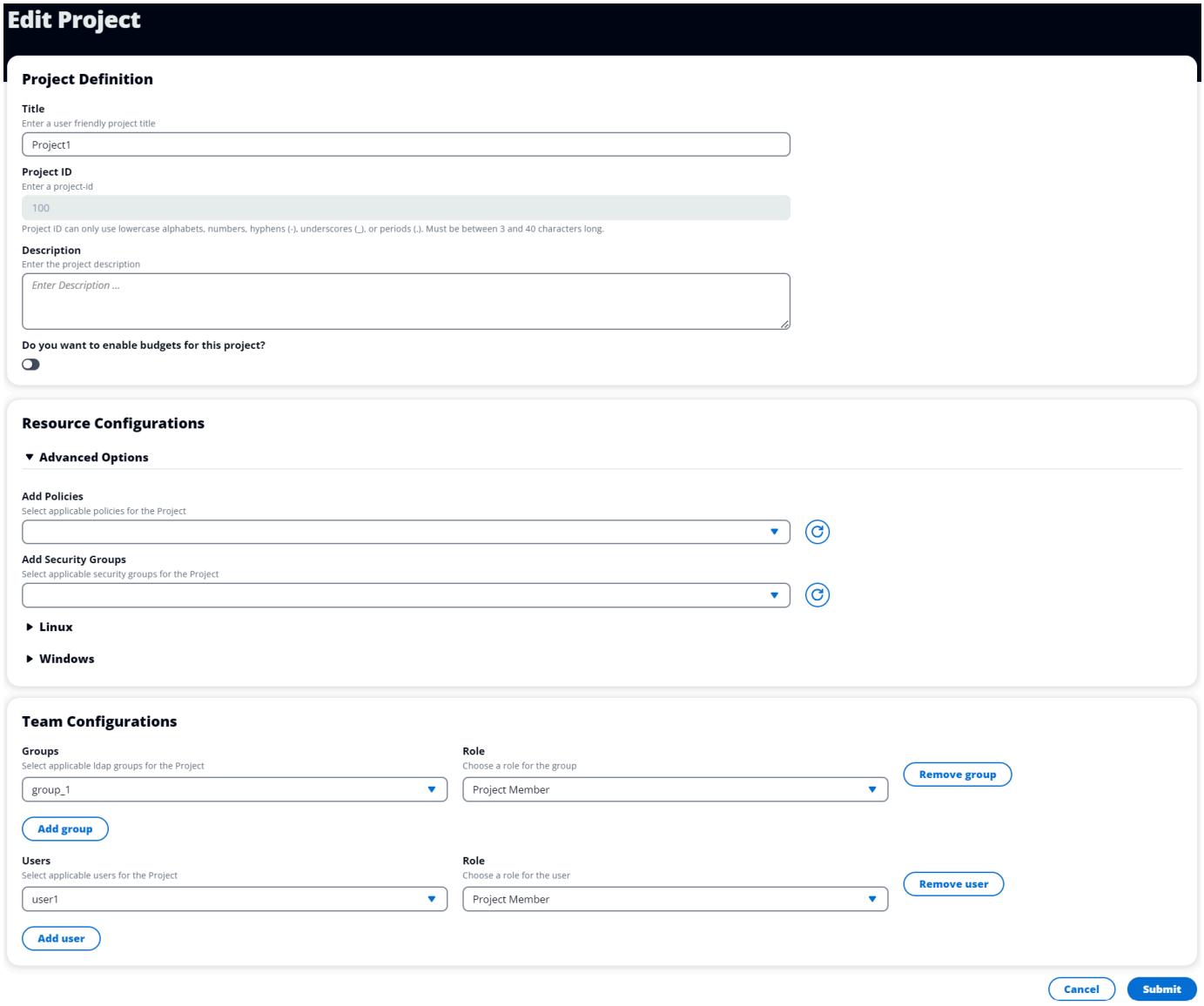


5. Assegna agli utenti e/o ai gruppi il ruolo appropriato («Membro del progetto» o «Proprietario del progetto»). Scopri profili di autorizzazioni predefiniti le azioni che ogni ruolo può intraprendere.
6. Scegli Invia.




## 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.



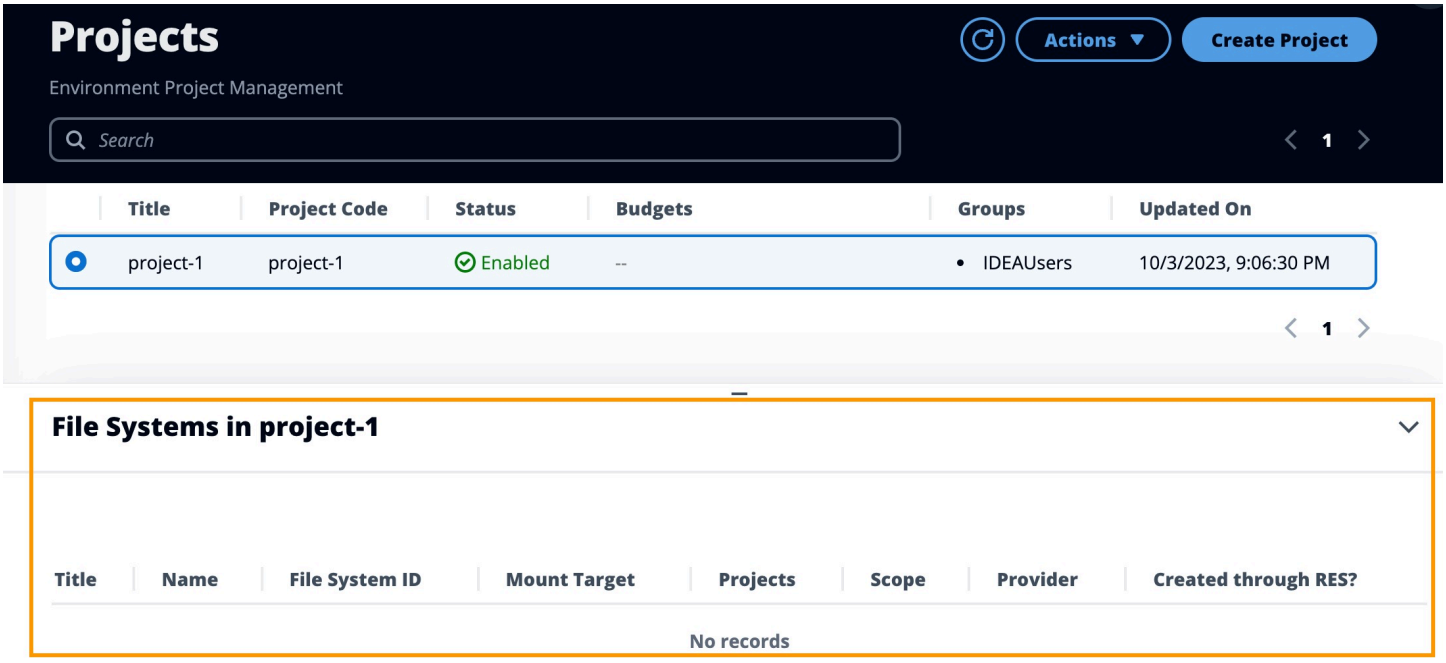

## Aggiungere o rimuovere tag da un progetto

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, IAM politiche e script di avvio per tutte le VDI istanze all'interno del progetto.

### Aggiungi politiche

Puoi aggiungere una IAM policy per controllare VDI l'accesso 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 IAM ruoli, 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 VDI istanze 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

Puoi aggiungere script di avvio che verranno avviati in tutte le VDI sessioni del progetto. RESsupporta l'avvio di script per Linux e Windows. Per l'avvio dello script, puoi scegliere tra:

Esegui script all'avvio VDI

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

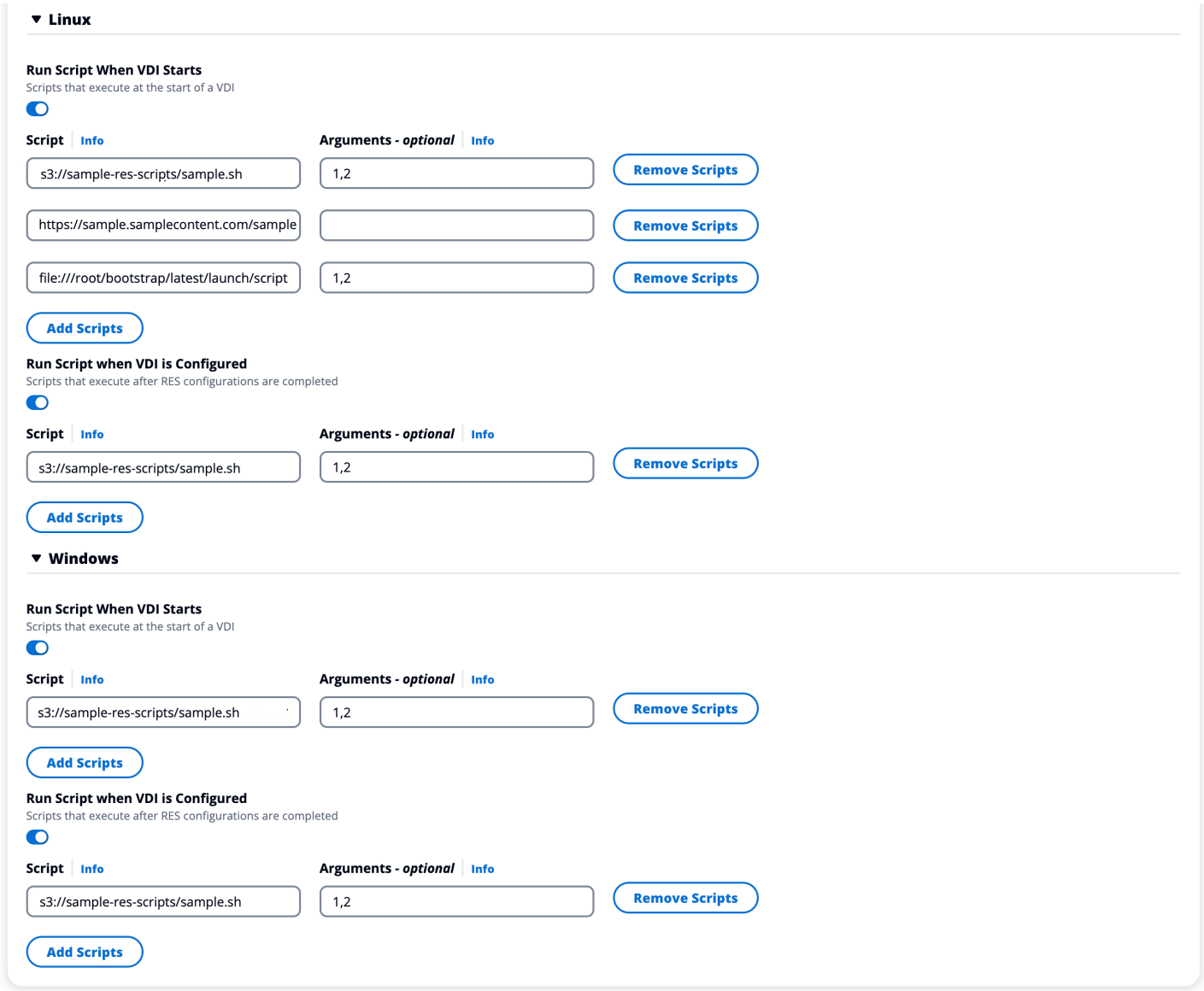
Esegui lo script quando è VDI configurato

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

Gli script supportano le seguenti opzioni:

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

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




Esempio di configurazione di progetto

# Policy di autorizzazione

Research and Engineering Studio (RES) consente a un utente amministrativo di creare profili di autorizzazione personalizzati che concedono agli utenti selezionati autorizzazioni aggiuntive per gestire il progetto di cui fanno parte. Ogni progetto è dotato di due profili di autorizzazione predefiniti: «Membro del progetto» e «Proprietario del progetto» che possono essere personalizzati dopo la distribuzione.

Attualmente, gli amministratori possono concedere due raccolte di autorizzazioni utilizzando un profilo di autorizzazione:

1. Autorizzazioni di gestione del progetto che consistono in «Aggiorna l'appartenenza al progetto», che consente a un utente designato di aggiungere o rimuovere altri utenti e gruppi da un progetto, e «Aggiorna lo stato del progetto», che consente a un utente designato di abilitare o disabilitare un progetto.
2. VDIautorizzazioni di gestione delle sessioni che consistono in «Crea sessione» che consente a un utente designato di creare una VDI sessione all'interno del proprio progetto e «Crea/Termina la sessione di un altro utente» che consente a un utente designato di creare o terminare le sessioni di altri utenti all'interno di un progetto.

In questo modo, gli amministratori possono delegare le autorizzazioni basate sul progetto ai non amministratori del proprio ambiente.

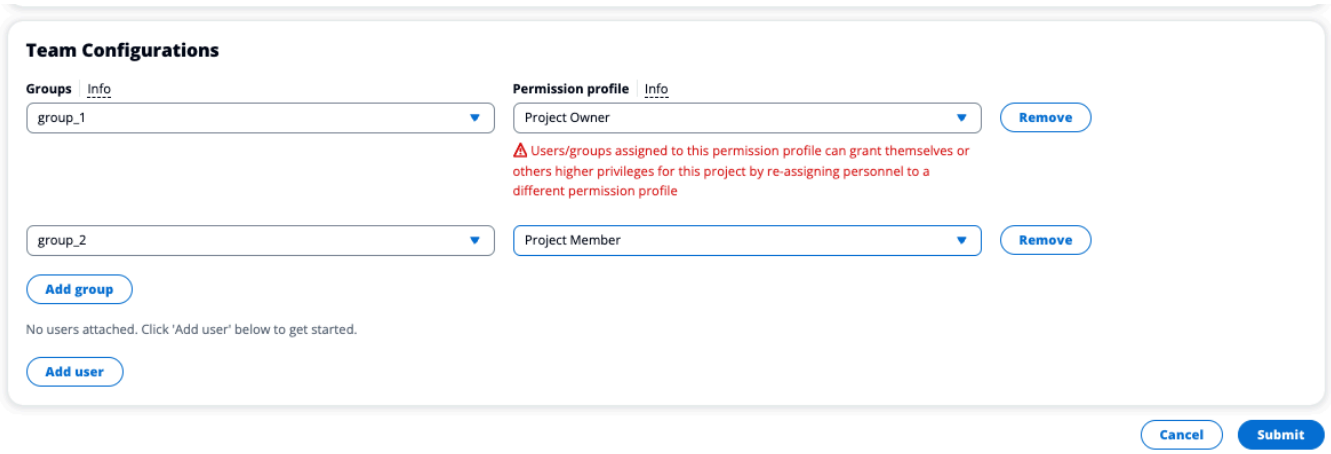
Argomenti



## Autorizzazioni per la gestione del progetto

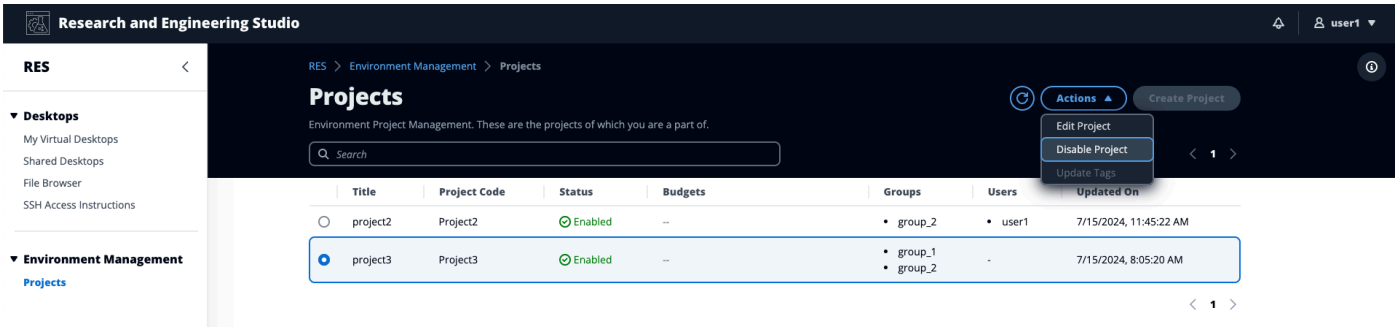
Aggiorna l'appartenenza al progetto

> Questa autorizzazione consente agli utenti non amministratori a cui è stata concessa di aggiungere e rimuovere utenti o gruppi da un progetto. Consente inoltre loro di impostare il profilo di autorizzazione e decidere il livello di accesso per tutti gli altri utenti e gruppi per quel progetto.




### Aggiorna lo stato del progetto

Questa autorizzazione consente agli utenti non amministratori a cui è stata concessa di abilitare o disabilitare un progetto utilizzando il pulsante Azioni nella pagina Progetti.

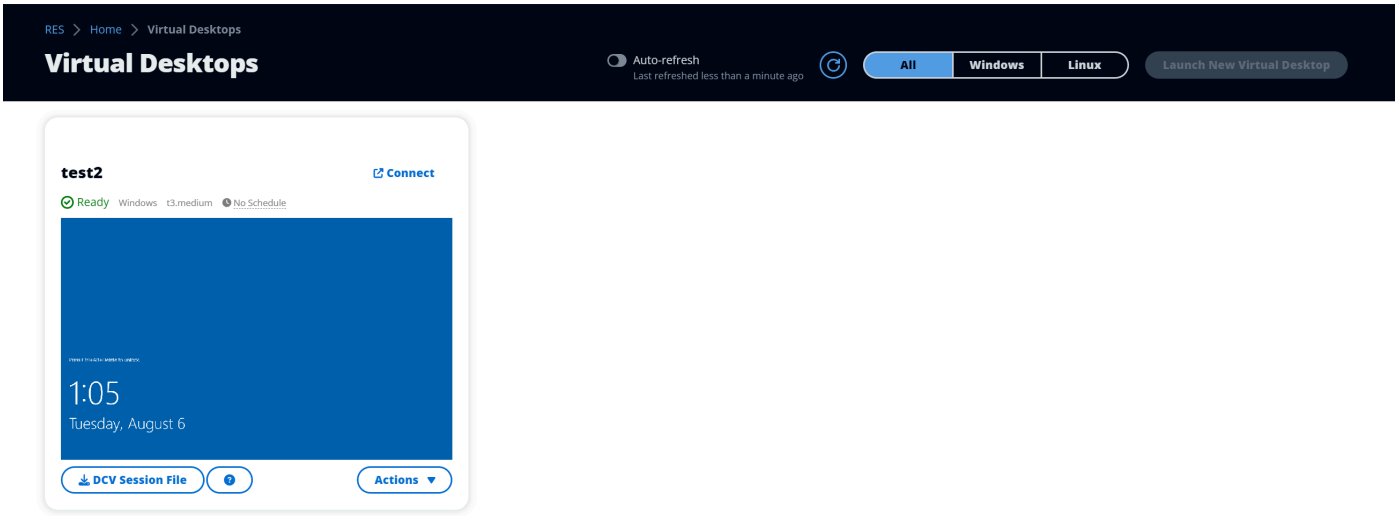



## VDIautorizzazioni per la gestione delle sessioni

### Creare una sessione

Controlla se un utente è autorizzato o meno ad avviare la propria VDI sessione dalla pagina I miei desktop virtuali. Disabilita questa opzione per negare agli utenti non amministratori la possibilità di avviare le proprie sessioni. VDI Gli utenti possono sempre interrompere e terminare le proprie sessioni. VDI

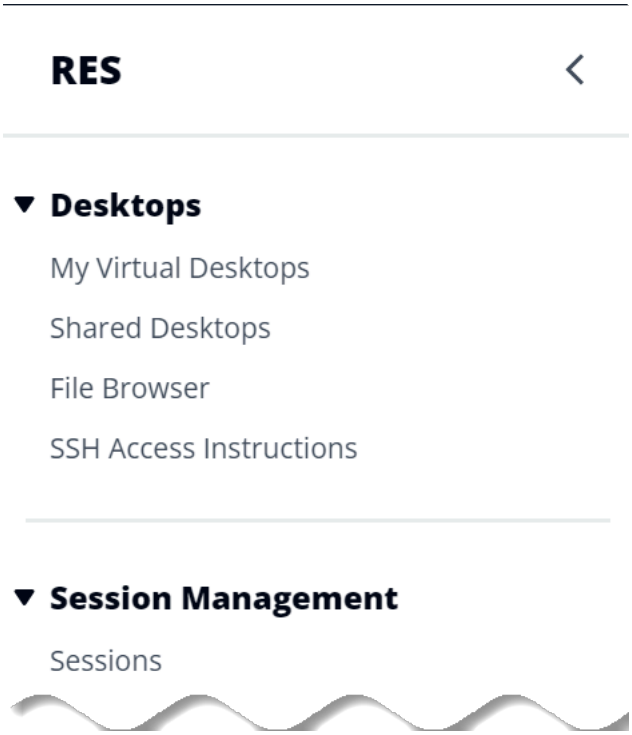
Se un utente non amministratore non dispone delle autorizzazioni per creare una sessione, il pulsante Avvia nuovo desktop virtuale verrà disabilitato per lui come mostrato di seguito:



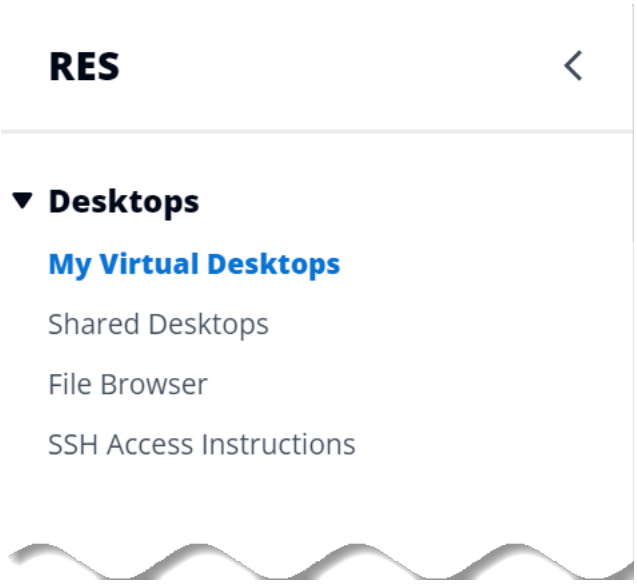

Crea o termina le sessioni di altri

Consente agli utenti non amministratori di accedere alla pagina Sessioni dal riquadro di navigazione a sinistra. Questi utenti saranno in grado di avviare VDI sessioni per altri utenti nei progetti per i quali è stata concessa questa autorizzazione.

Se un utente non amministratore è autorizzato ad avviare sessioni per altri utenti, nel riquadro di navigazione a sinistra verrà visualizzato il collegamento Sessioni in Gestione delle sessioni, come illustrato di seguito:



Se un utente non amministratore non dispone dell'autorizzazione per creare sessioni per altri utenti, il riquadro di navigazione a sinistra non mostrerà Gestione delle sessioni come illustrato di seguito:

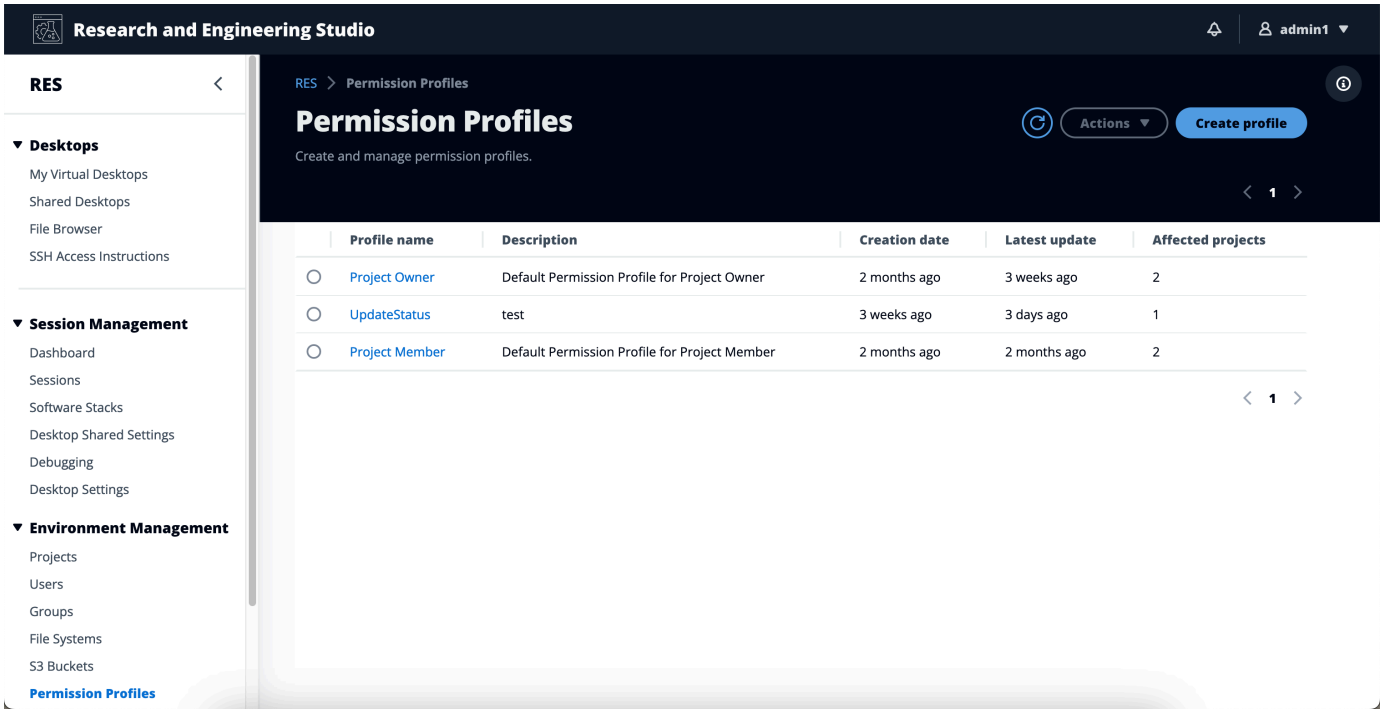



## Gestione dei profili di autorizzazione

In qualità di RES amministratore, puoi eseguire le seguenti azioni per gestire i profili di autorizzazione.

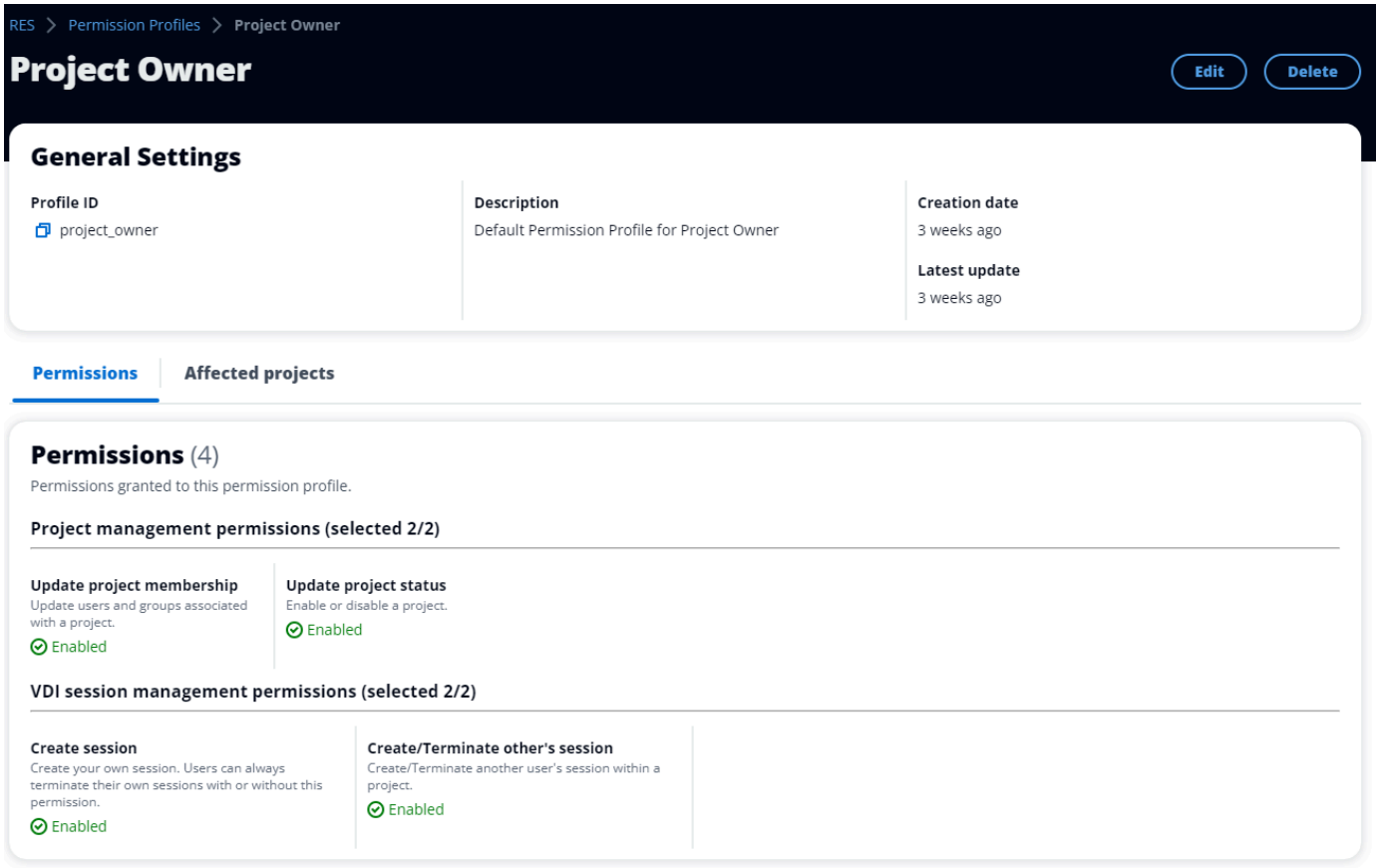
Elenca i profili di autorizzazione

- Dalla pagina della console di Research and Engineering Studio, scegli Profili di autorizzazione nel riquadro di navigazione a sinistra. Da questa pagina è possibile creare, aggiornare, elencare, visualizzare ed eliminare i profili di autorizzazione.

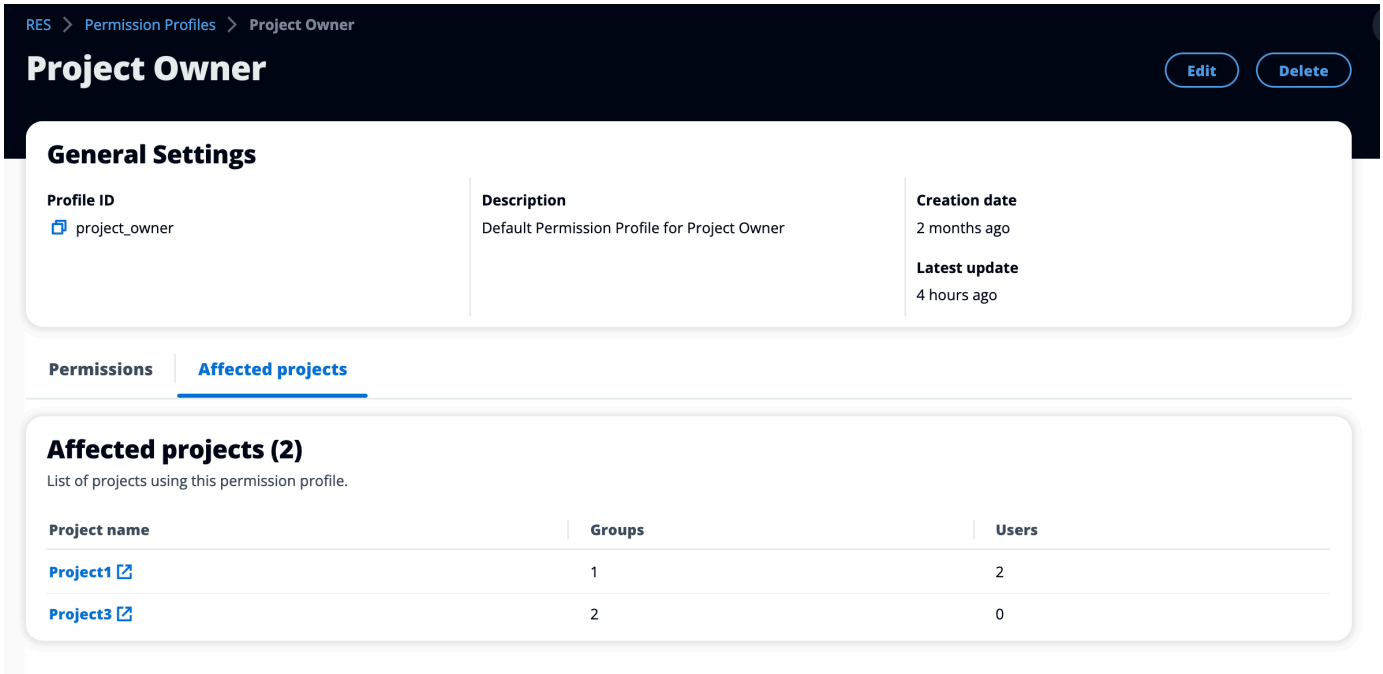



Visualizza i profili di autorizzazione

1. Nella pagina principale dei profili di autorizzazione, seleziona il nome del profilo di autorizzazione che desideri visualizzare. Da questa pagina è possibile modificare o eliminare il profilo di autorizzazione selezionato.

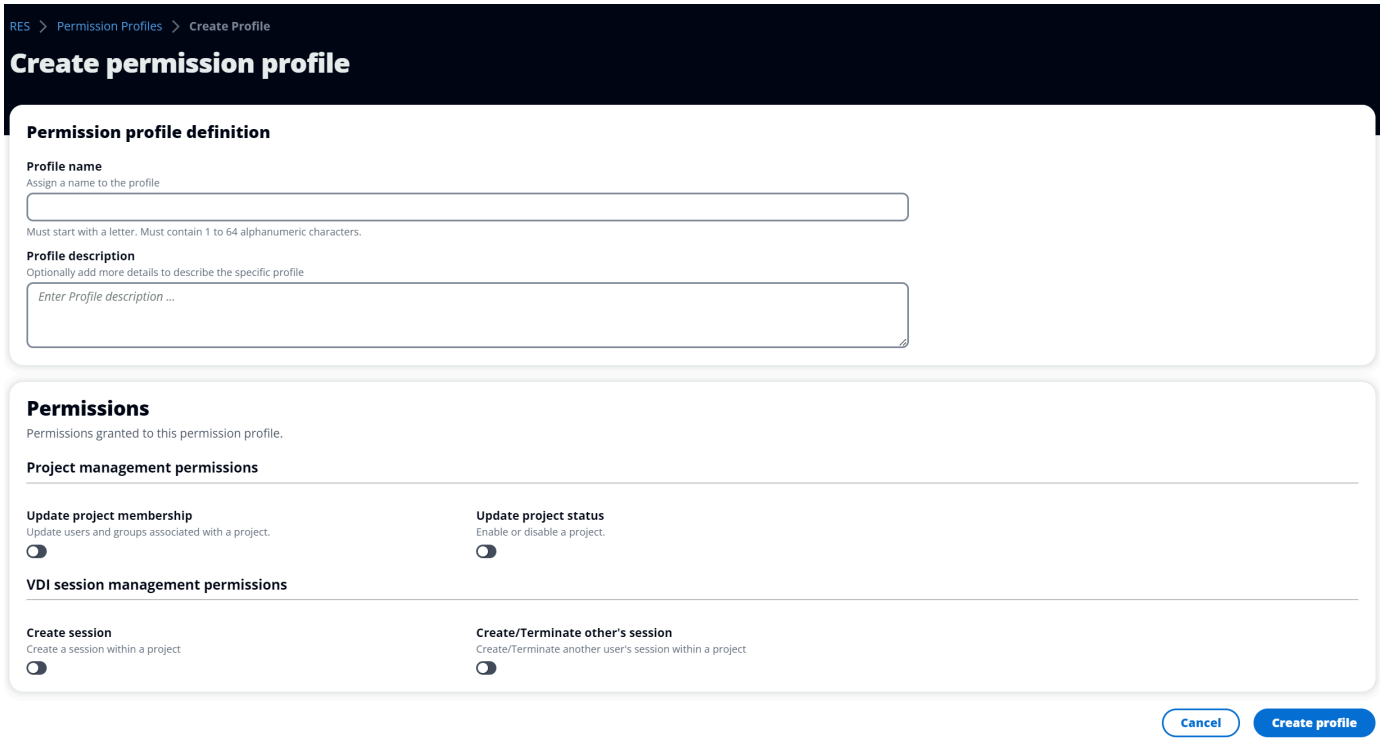



2. Seleziona la scheda Progetti interessati per visualizzare i progetti che attualmente utilizzano il profilo di autorizzazione.



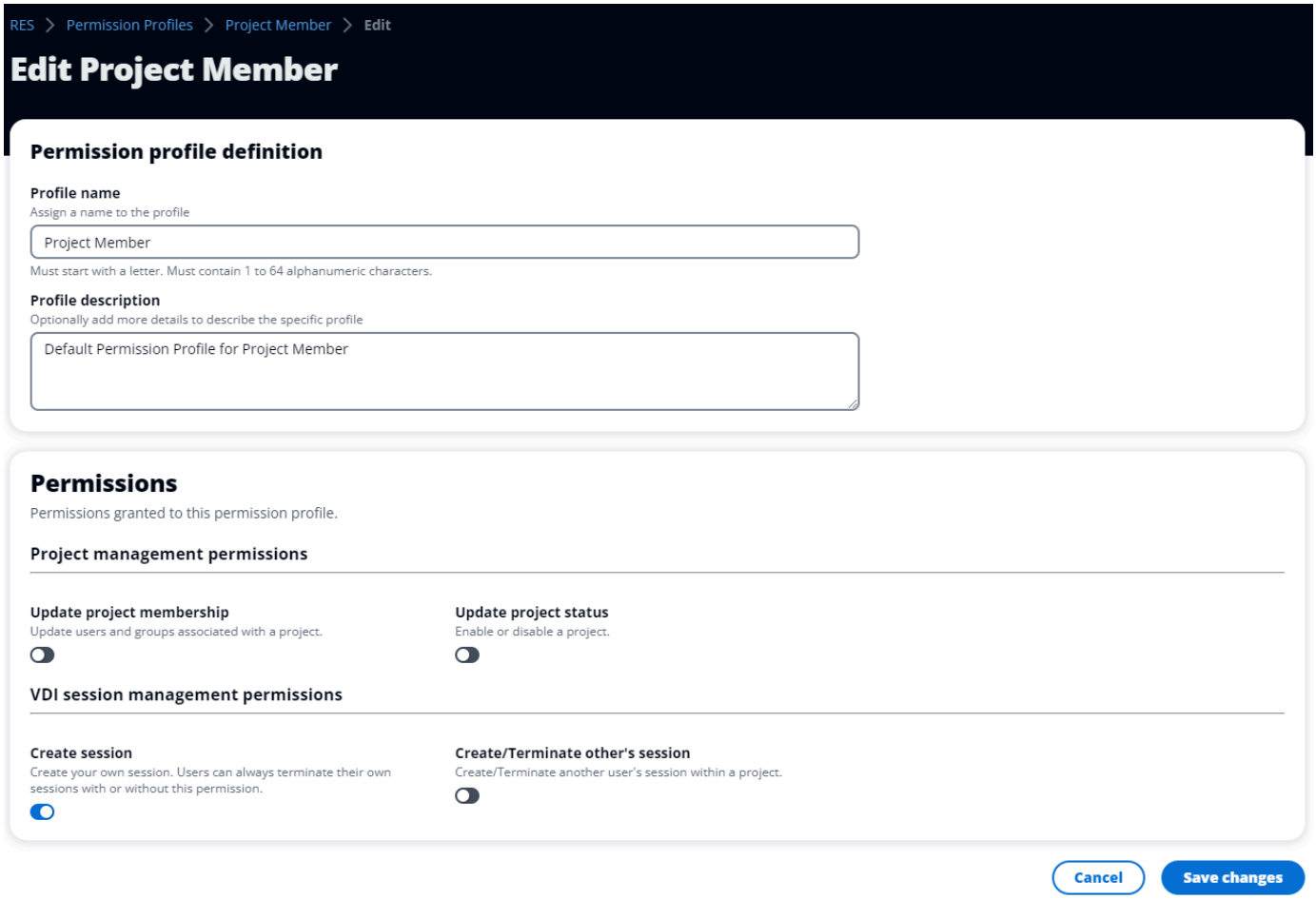
## Creare profili di autorizzazione

1. Nella pagina principale dei profili di autorizzazione, scegli Crea profilo per creare un profilo di autorizzazione.
2. Inserisci il nome e la descrizione del profilo di autorizzazione, quindi seleziona le autorizzazioni da concedere agli utenti o ai gruppi da assegnare a questo profilo.



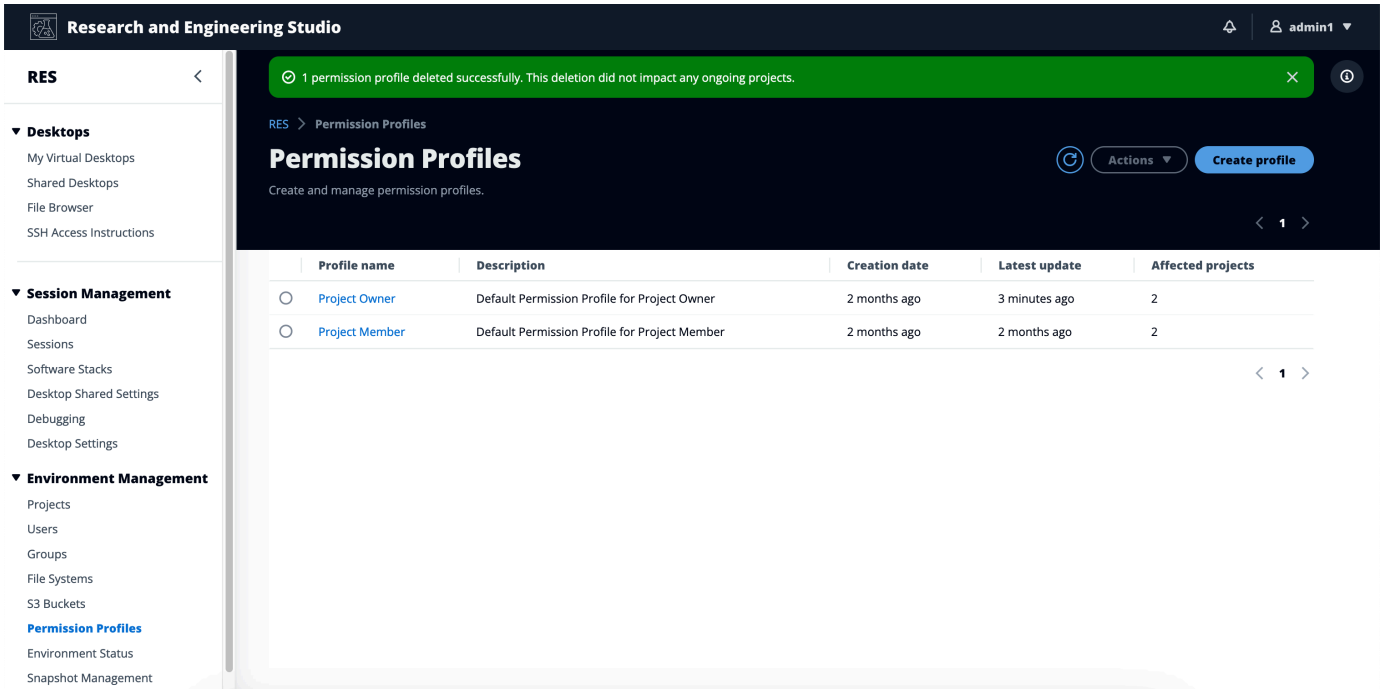

## Modificare i profili di autorizzazione

- Nella pagina principale dei profili di autorizzazione, seleziona un profilo facendo clic sul cerchio accanto ad esso, scegli Azioni, quindi scegli Modifica profilo per aggiornare il profilo di autorizzazione.




## Eliminare i profili di autorizzazione

- Nella pagina principale dei profili di autorizzazione, seleziona un profilo facendo clic sul cerchio accanto ad esso, scegli Azioni, quindi scegli Elimina profilo. Non è possibile eliminare un profilo di autorizzazione utilizzato da qualsiasi progetto esistente.




## profili di autorizzazioni predefiniti

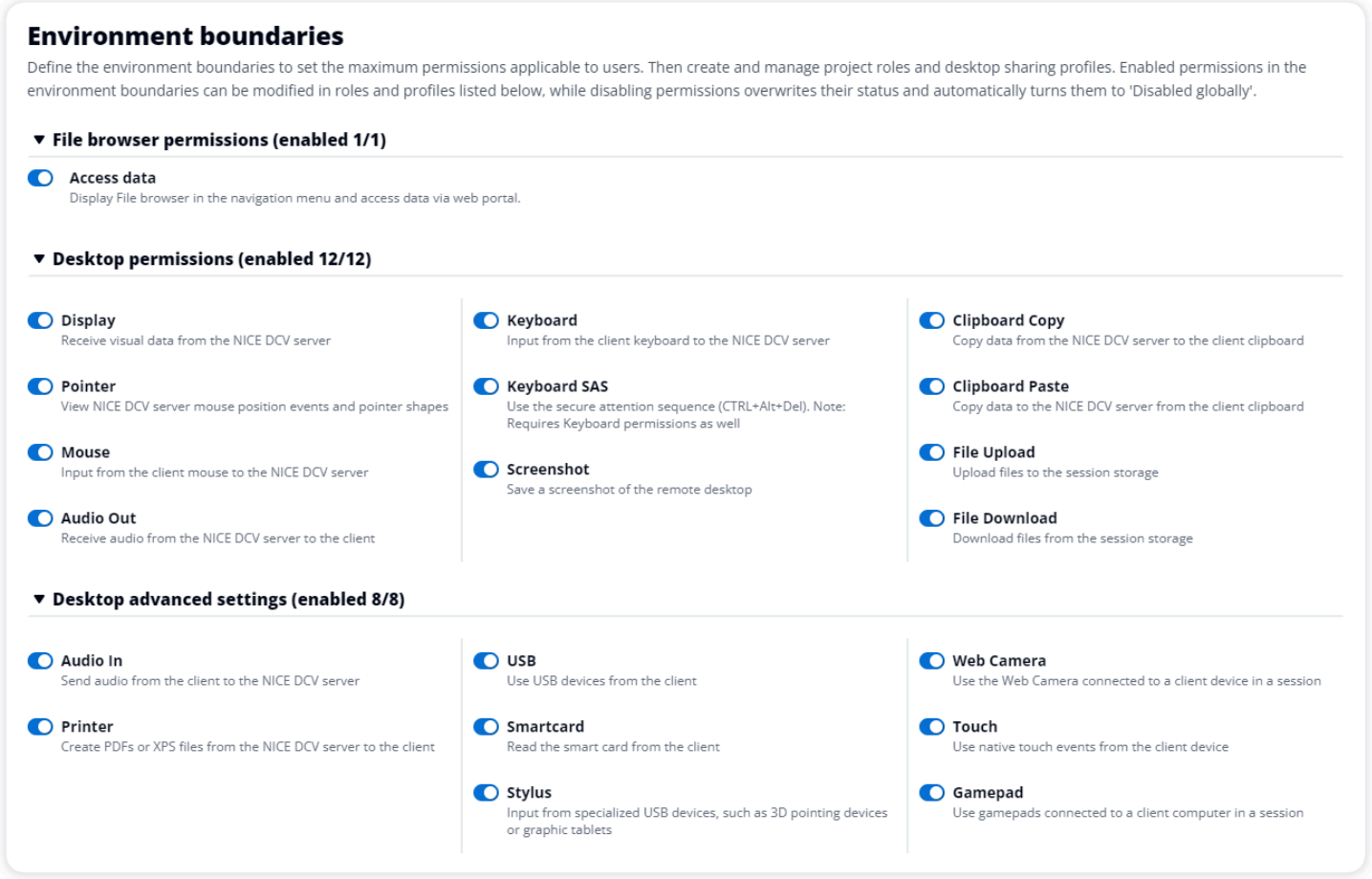
Ogni RES progetto è dotato di due profili di autorizzazione predefiniti che gli amministratori globali possono configurare. (Inoltre, gli amministratori globali possono creare e modificare nuovi profili di autorizzazione per un progetto.) La tabella seguente mostra le autorizzazioni consentite per i profili di autorizzazione predefiniti: «Membro del progetto» e «Proprietario del progetto». I profili di autorizzazione e le autorizzazioni che concedono a determinati utenti di un progetto si applicano solo al progetto a cui appartengono; gli amministratori globali sono utenti privilegiati che dispongono di tutte le autorizzazioni seguenti per tutti i progetti.

| Autorizzazioni | Descrizione | Membro del progetto | Proprietario del progetto | |
|---|---|---|---|---|
| Crea sessione | Crea la tua sessione. Gli utenti possono sempre interrompere e terminare le proprie sessioni con o senza | X | X | |

| Autorizzazioni | Descrizione | Membro del progetto | Proprietario del progetto | |
|---|---|---|---|---|
| | questa autorizza zione. | | | |
| Creare/terminare le sessioni altrui | Creare o terminare la sessione di un altro utente all'interno di un progetto. | | X | |
| Aggiorna l'appartenenza al progetto | Aggiorna utenti e gruppi associati a un progetto. | | X | |
| Aggiorna lo stato del progetto | Abilita o disabilit a un progetto. | | X | |

## Limiti dell'ambiente

I limiti dell'ambiente consentono agli amministratori di configurare le autorizzazioni che avranno effetto a livello globale per tutti gli utenti. Ciò include autorizzazioni come l'accesso al file browser e le autorizzazioni desktop.




Configurazione dell'accesso al file browser

Gli amministratori possono attivare o disattivare i dati di Access nelle autorizzazioni del browser di file. Se i dati di Access sono disattivati, gli utenti non vedranno la navigazione di File Browser nel loro portale web e non potranno caricare o scaricare i dati allegati al loro file system globale. Quando i dati di Access sono abilitati, gli utenti hanno accesso alla navigazione in File Browser nel proprio portale Web, che consente loro di caricare o scaricare dati allegati al proprio file system globale.

Quando la funzionalità dei dati di Access è attivata e successivamente disattivata, gli utenti che hanno già effettuato l'accesso al portale Web non saranno in grado di caricare o scaricare file, anche se si trovano nella pagina corrispondente. Inoltre, il menu di navigazione scompare quando aggiornano la pagina.

Configurazione delle autorizzazioni del desktop

Gli amministratori possono attivare o disattivare le autorizzazioni del desktop per gestire a livello globale le funzionalità di tutti i proprietari. VDI Tutte queste autorizzazioni, o un sottoinsieme, possono essere utilizzate per creare profili di condivisione del desktop che determinano quali azioni

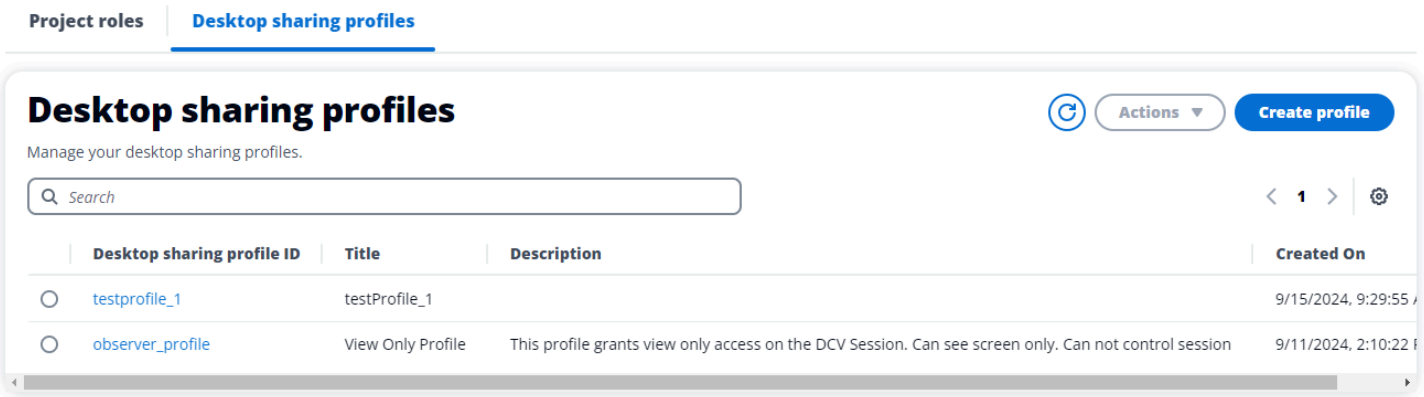
possono essere eseguite dagli utenti con cui viene condiviso un desktop. Se un'autorizzazione desktop è disabilitata, verranno disattivate automaticamente le autorizzazioni corrispondenti nei profili di condivisione del desktop. Queste autorizzazioni saranno etichettate come «Disattivate a livello globale». Anche se l'amministratore abilita nuovamente questa autorizzazione desktop, l'autorizzazione nel profilo di condivisione desktop rimarrà disabilitata finché l'amministratore non la abilita manualmente.

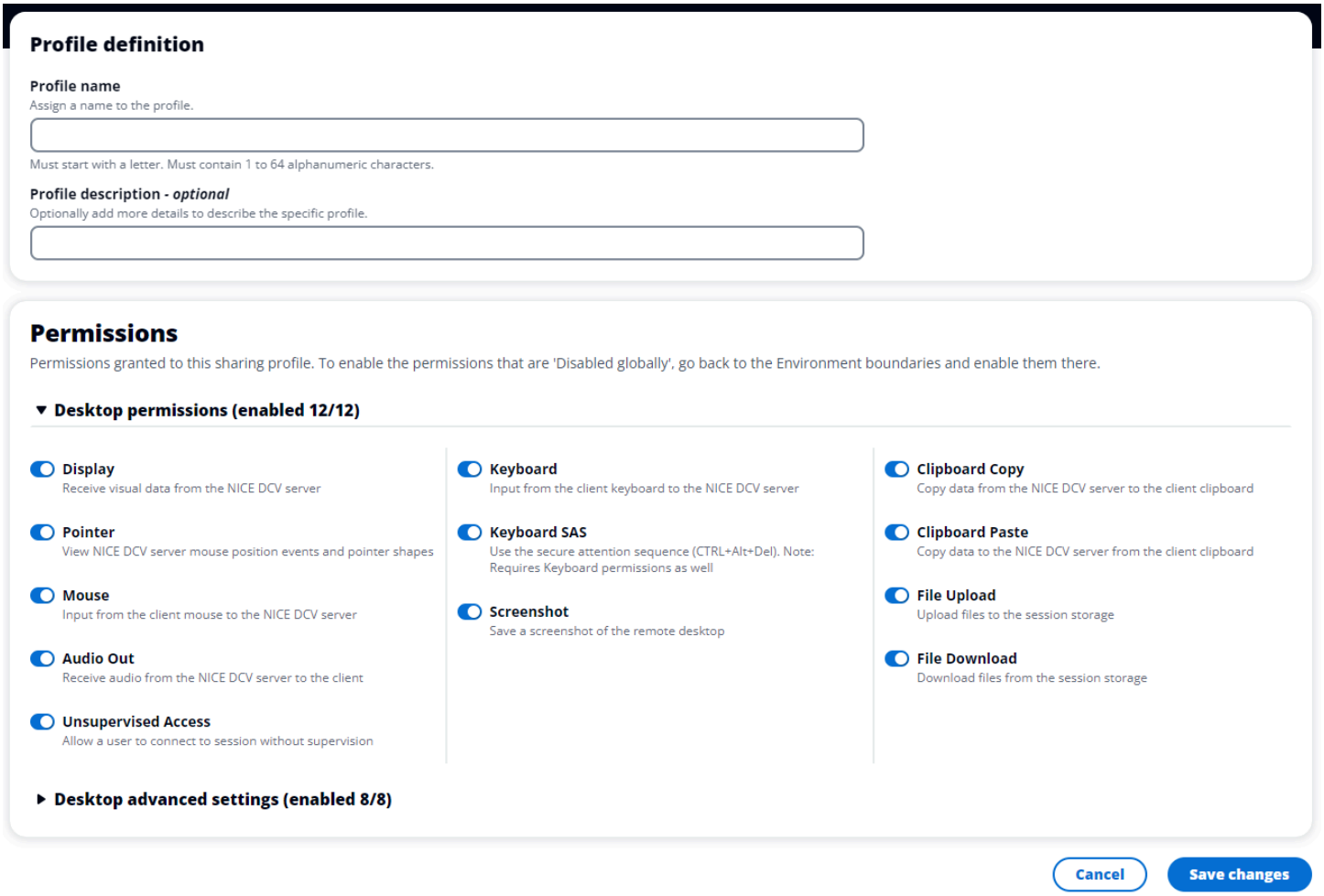
## Profili di condivisione del desktop

Gli amministratori possono creare nuovi profili e personalizzarli. Questi profili sono accessibili a tutti gli utenti e vengono utilizzati quando si condivide una sessione con altri. Le autorizzazioni massime concesse all'interno di questi profili non possono superare le autorizzazioni desktop consentite a livello globale.

### Crea profilo

Gli amministratori possono scegliere Crea profilo per creare un nuovo profilo. Quindi possono inserire un nome di profilo, una descrizione del profilo, impostare le autorizzazioni desiderate e salvare le modifiche.



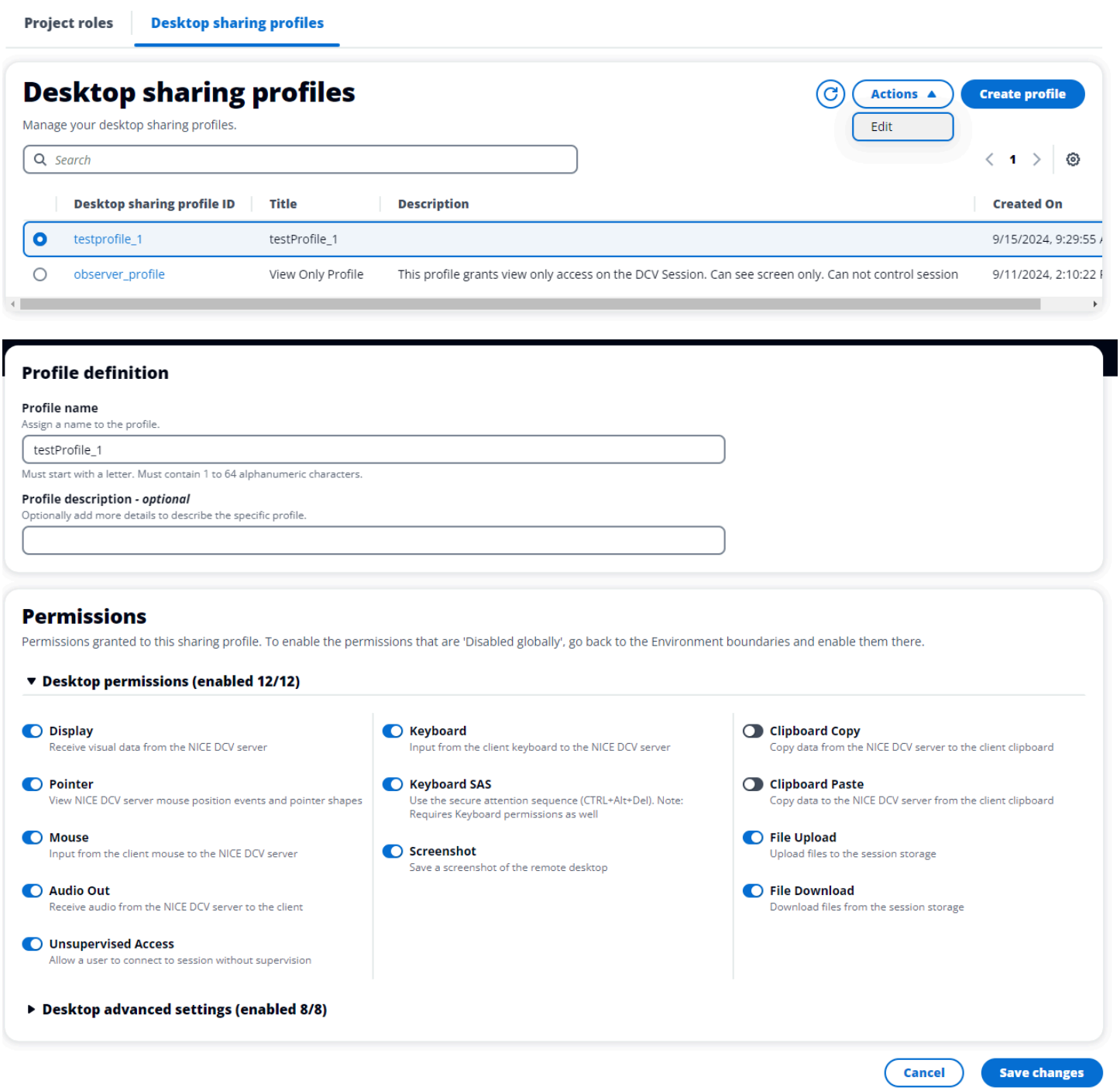



Modifica profilo

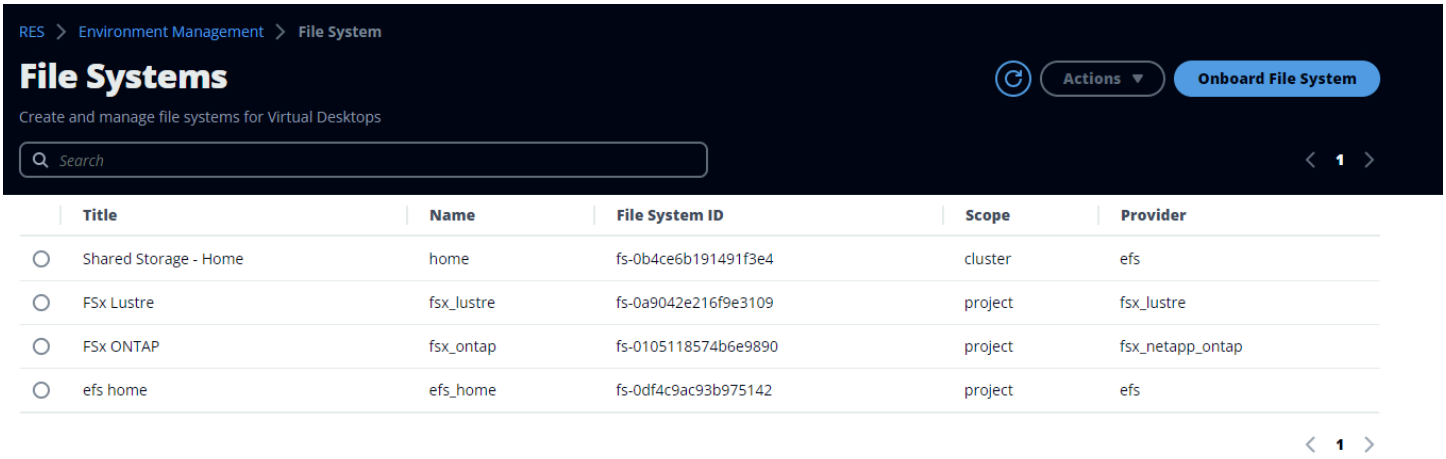
Per modificare un profilo:

1. Seleziona il profilo desiderato.
2. Scegli Azioni, quindi seleziona Modifica per modificare il profilo.
3. Modifica le autorizzazioni in base alle esigenze.
4. Scegli Save changes (Salva modifiche).

Qualsiasi modifica apportata al profilo verrà immediatamente applicata alle sessioni aperte correnti.


Project roles
Desktop sharing profiles
Desktop sharing profiles
Manage your desktop sharing profiles.
Actions
Create profile
Edit
Search
1
Desktop sharing profile ID
Title
Description
Created On
testprofile_1
testProfile_1
9/15/2024, 9:29:55
observer_profile
View Only Profile
This profile grants view only access on the DCV Session. Can see screen only. Can not control session
9/11/2024, 2:10:22
Profile definition
Profile name
Assign a name to the profile.
testProfile_1
Must start with a letter. Must contain 1 to 64 alphanumeric characters.
Profile description - optional
Optionally add more details to describe the specific profile.
Permissions
Permissions granted to this sharing profile. To enable the permissions that are 'Disabled globally', go back to the Environment boundaries and enable them there.
Desktop permissions (enabled 12/12)
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
Audio Out
Receive audio from the NICE DCV server to the client
Unsupervised Access
Allow a user to connect to session without supervision
Keyboard
Input from the client keyboard to the NICE DCV server
Keyboard SAS
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
Screenshot
Save a screenshot of the remote desktop
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
Desktop advanced settings (enabled 8/8)
Cancel
Save changes

# File system




Dalla pagina File system, è possibile:

1. Cercare 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.

Argomenti

- Creare un file system
- Incorpora un 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 una sottorete IDs da. VPC Puoi trovarli IDs 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

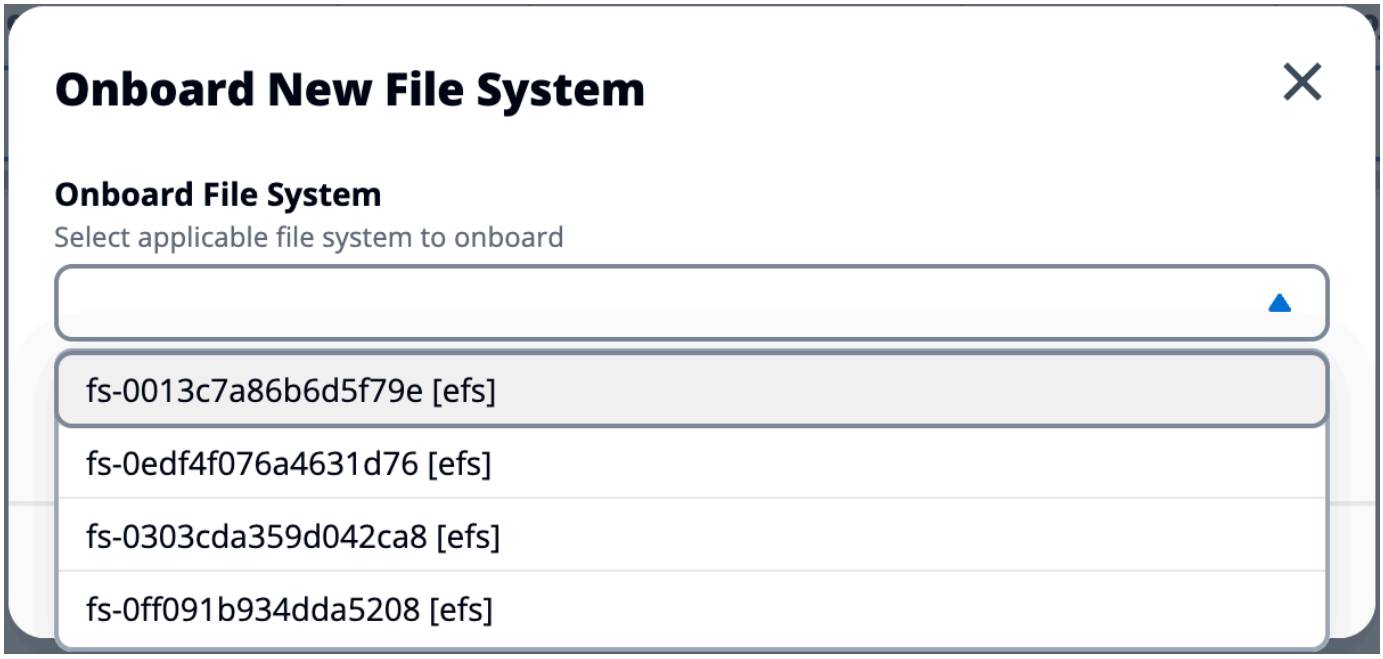
Subnet ID 1 and Subnet ID 2 should be in two different AZs

**Mount Directory**

Enter directory to mount the file system

## Incorpora un file system

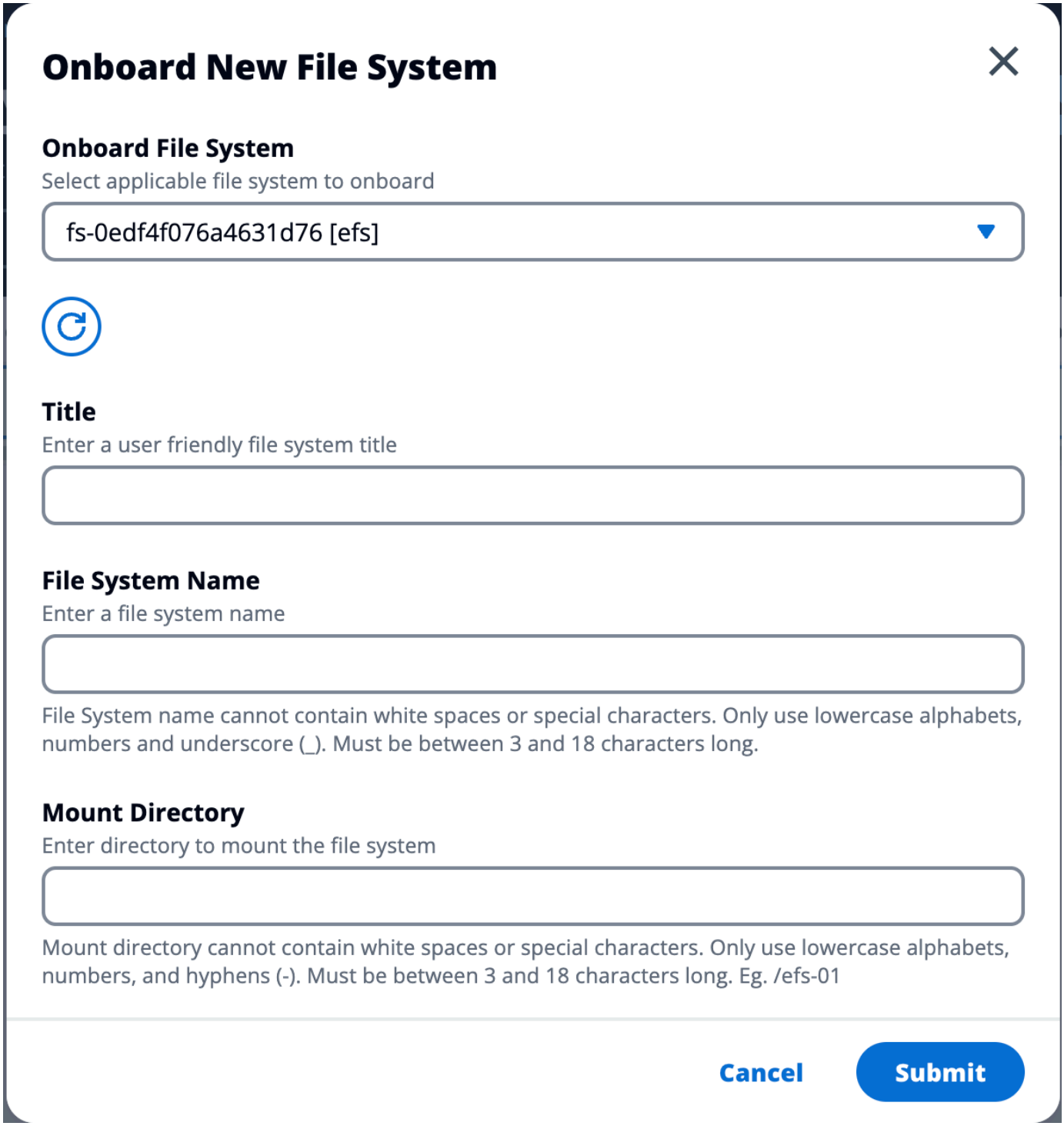
1. Scegli Onboard File System.
2. Seleziona un file system dal menu a discesa. Il modale si espanderà con ulteriori inserimenti di dettagli.




3. Inserisci i dettagli del file system.

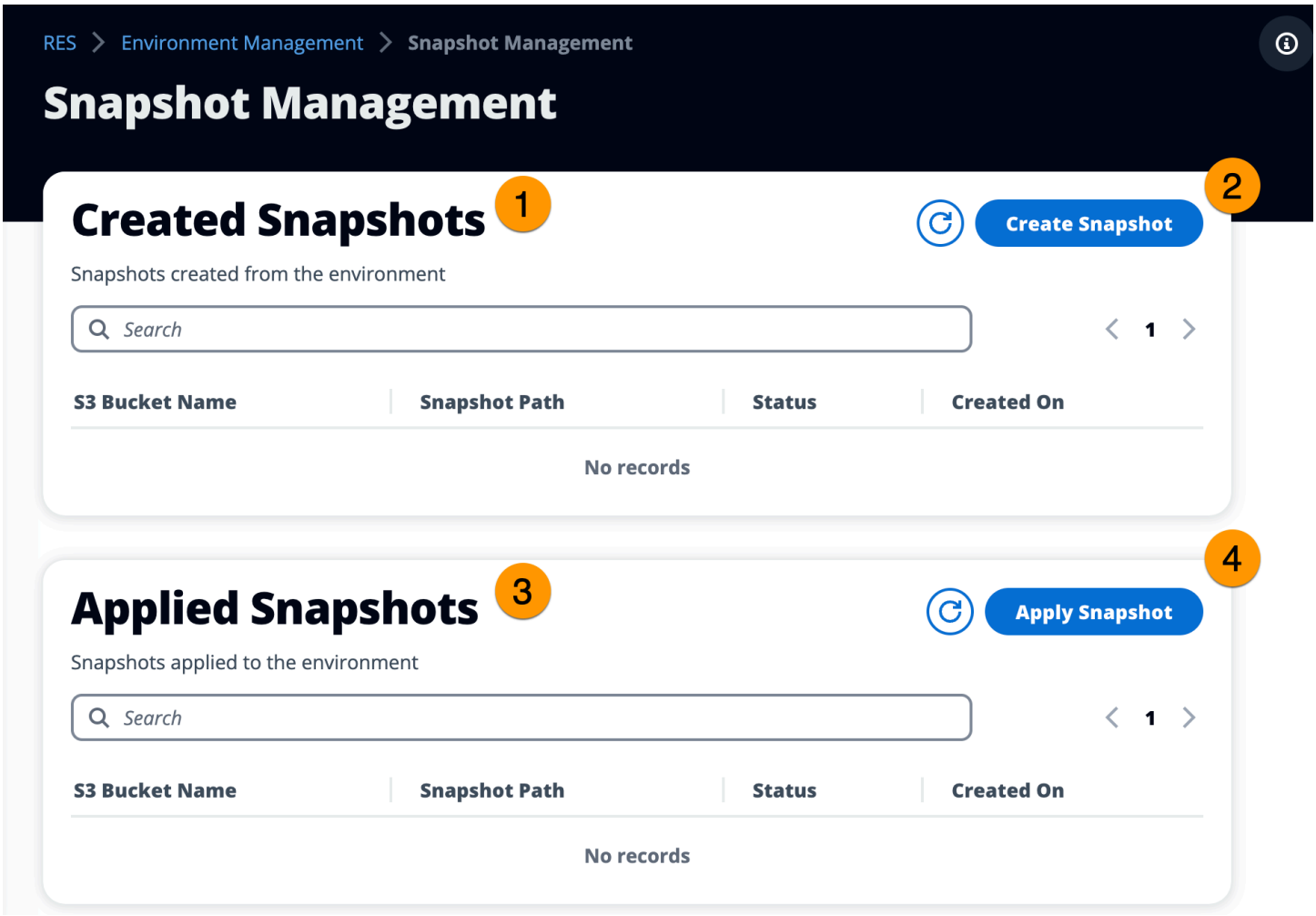
> **Note**
>
> Per impostazione predefinita, gli amministratori e i proprietari del progetto hanno la possibilità di scegliere un file system home quando creano un nuovo progetto, che non può essere modificato in seguito.
> I file system destinati a essere utilizzati come home directory nei progetti devono essere inseriti impostando il relativo percorso Mount Directory su. `/home` Questo popolerà il filesystem integrato nelle opzioni a discesa del filesystem della home directory. Questa funzionalità aiuta a mantenere i dati isolati tra i progetti poiché solo gli utenti associati al progetto avranno accesso al filesystem tramite i propri. VDIs VDIsmonterà il filesystem nel punto di montaggio selezionato durante l'onboarding di un filesystem.

4. Scegli Invia.


Onboard New File System
Onboard File System
Select applicable file system to onboard
fs-0edf4f076a4631d76 [efs]
Title
Enter a user friendly file system title
File System Name
Enter a file system name
File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.
Mount Directory
Enter directory to mount the file system
Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01
Cancel
Submit

# 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.

Argomenti

- Creazione di una snapshot
- 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:

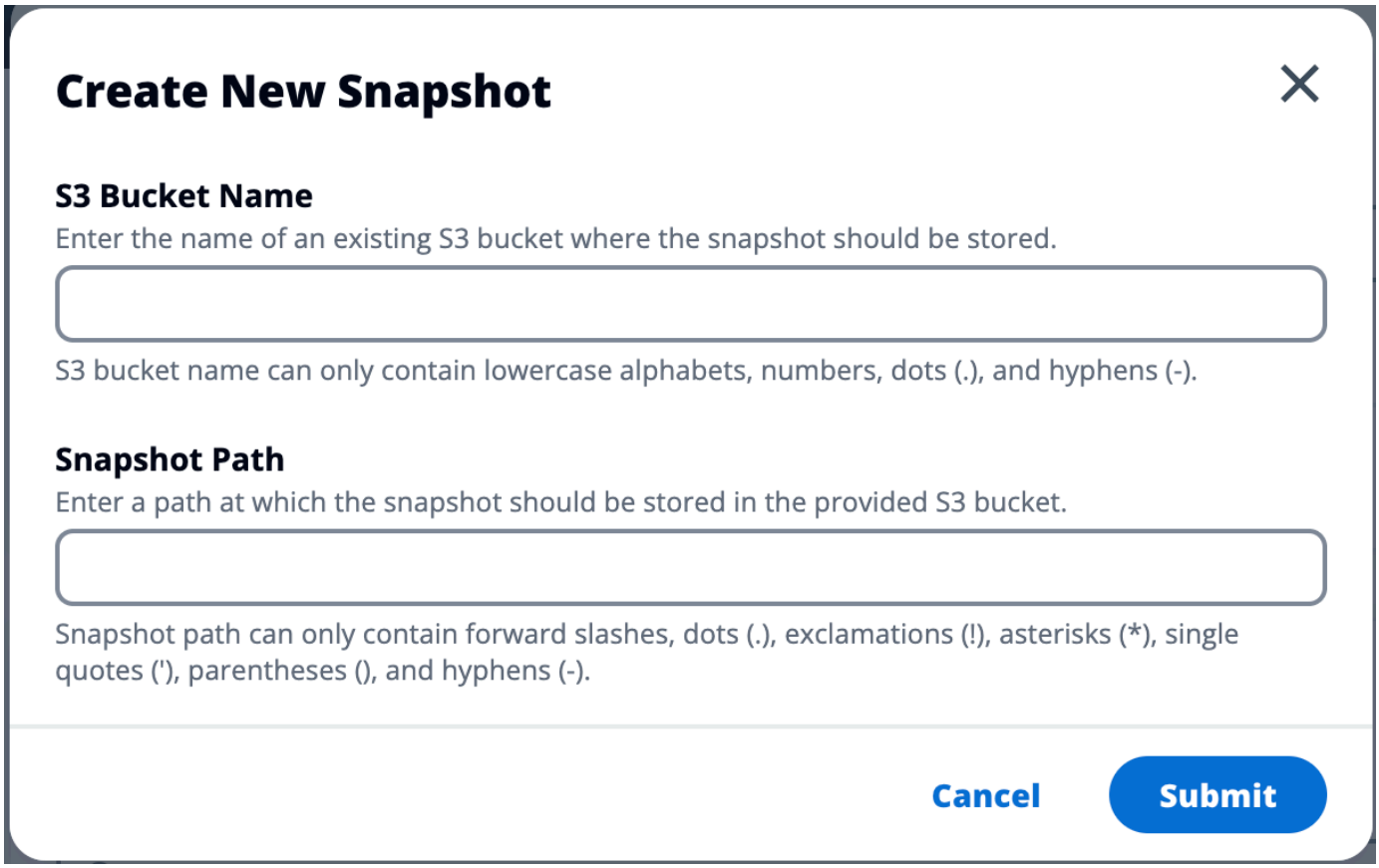
1. Seleziona il bucket che hai creato dall'elenco dei bucket.
2. Seleziona la scheda Autorizzazioni.
3. In Bucket Policy (Policy del bucket) scegliere Edit (Modifica).
4. Aggiungi la seguente dichiarazione alla policy del bucket. Sostituire questi valori con i propri valori:
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - BUCKETS3_ _ NAME

> **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 cambierà da IN_ a. PROGRESS 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. Seleziona il bucket che hai creato dall'elenco dei bucket.
2. Seleziona 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:

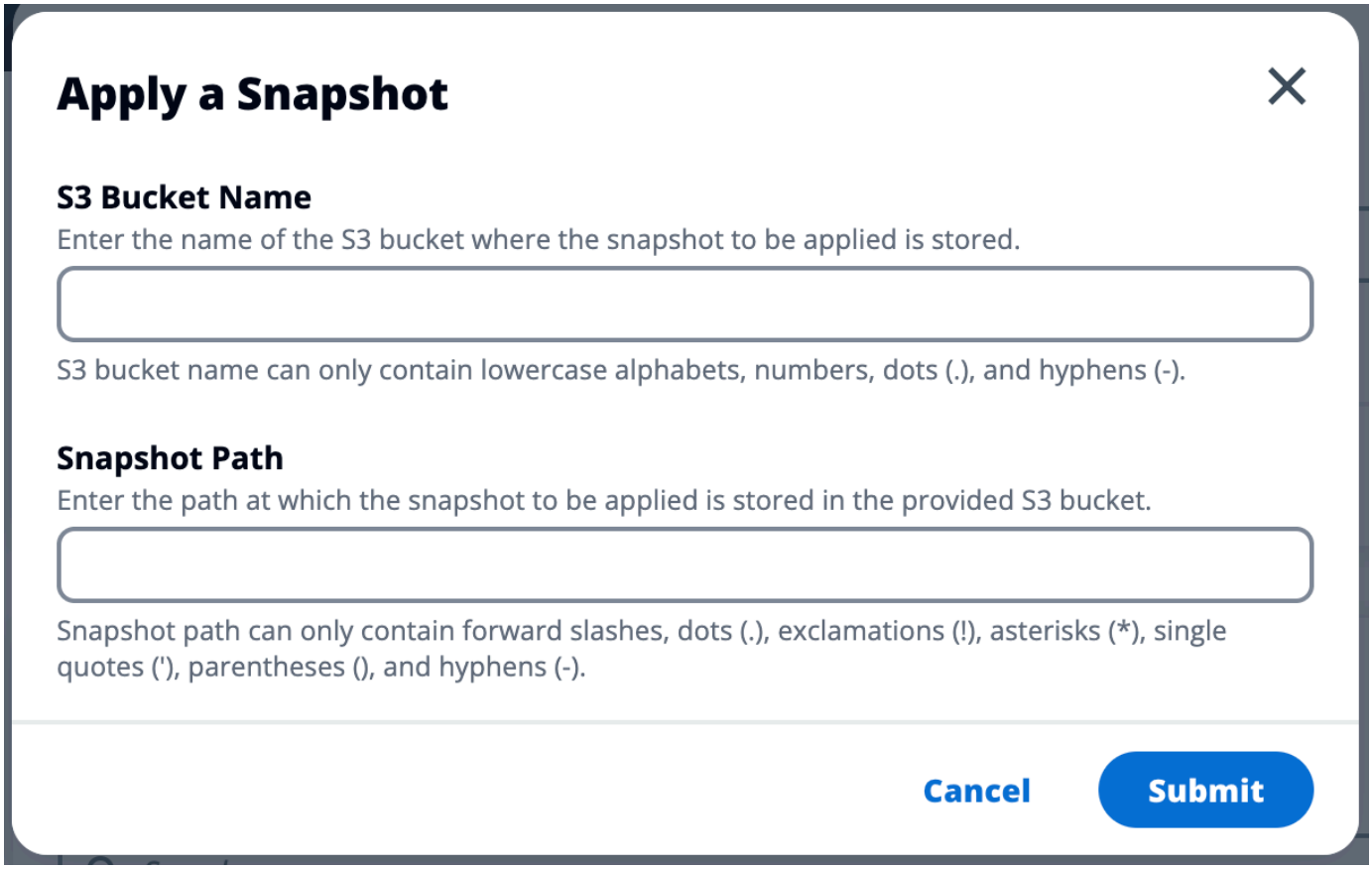
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - BUCKETS3_ _ NAME

```
{
    "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 un'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.

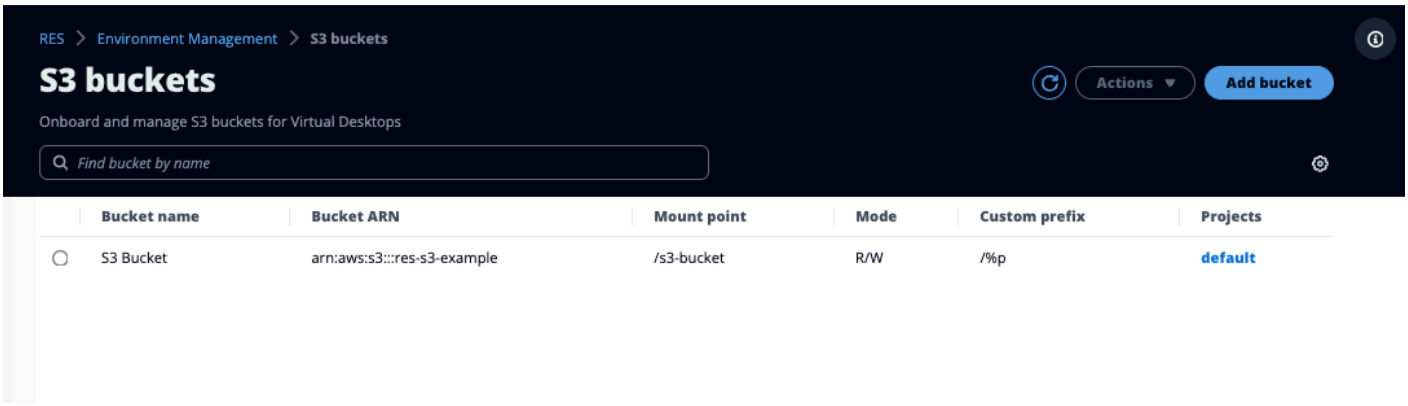
## Bucket Amazon S3

Research and Engineering Studio (RES) supporta il montaggio di bucket Amazon S3 su istanze Linux Virtual Desktop Infrastructure ()VDI. RESGli amministratori possono integrare i bucket S3RES, collegarli ai progetti, modificarne la configurazione e rimuovere i bucket nella scheda S3 bucket in Environment Management.

La dashboard dei bucket S3 fornisce un elenco di bucket S3 integrati disponibili. Dalla dashboard dei bucket S3, puoi:

1. Usa Aggiungi bucket per effettuare l'onboard di un bucket S3. RES
2. Seleziona un bucket S3 e usa il menu Azioni per:
   - Modificare un bucket
   - Rimuovi un secchio

3. Usa il campo di ricerca per cercare in base al nome del bucket e trovare i bucket S3 integrati.




Le seguenti sezioni descrivono come gestire i bucket Amazon S3 nei tuoi progetti. RES

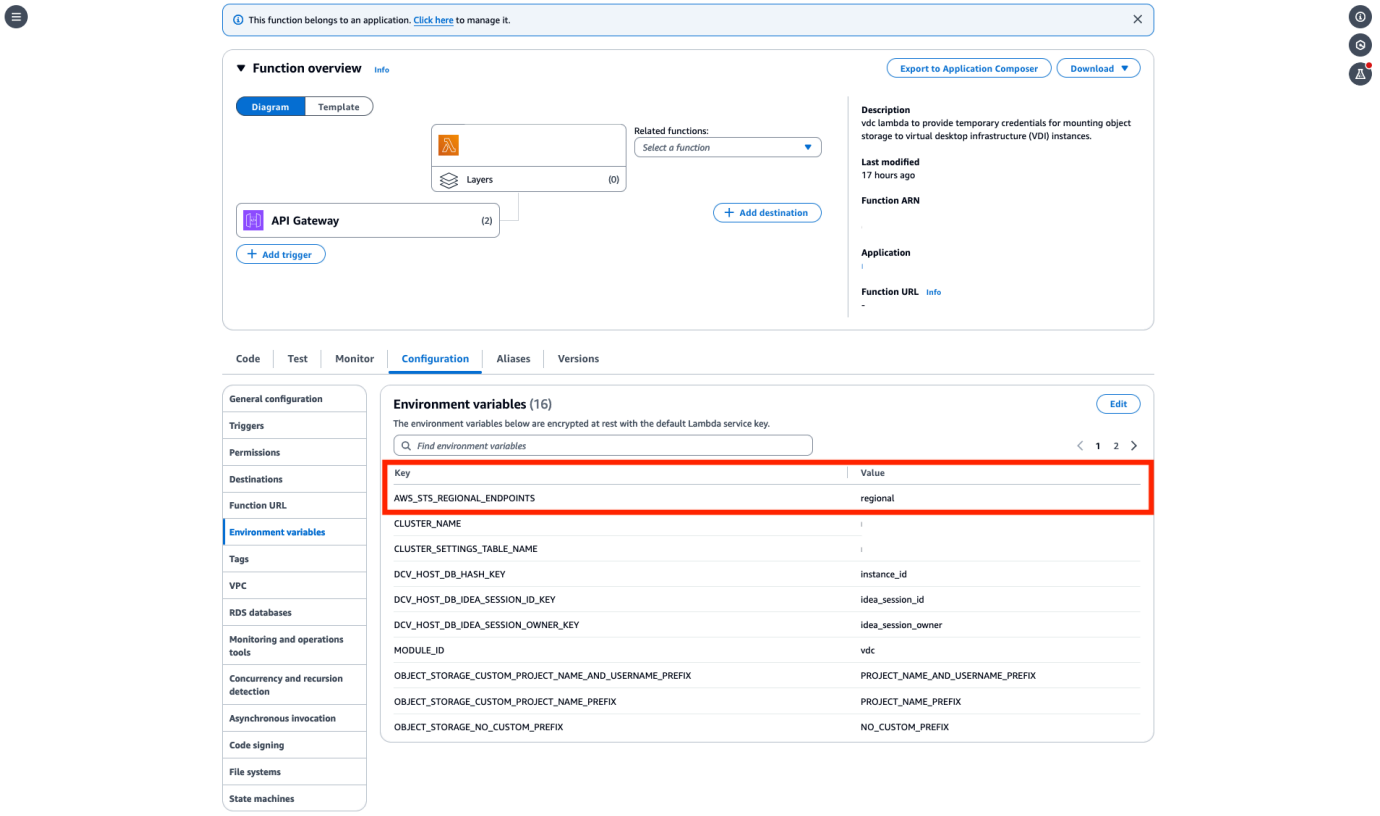
Argomenti



## Prerequisiti del bucket Amazon S3 per distribuzioni isolate VPC

Se stai implementando Research and Engineering Studio in un ambiente isolatoVPC, segui questi passaggi per aggiornare i parametri di configurazione lambda dopo la distribuzione nel tuo account. RES AWS

1. Accedi alla console Lambda dell' AWS account in cui è distribuito Research and Engineering Studio.
2. Trova e vai alla funzione Lambda denominata. `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`
3. Seleziona la scheda Configurazione della funzione.




4. Sul lato sinistro, scegli Variabili d'ambiente per visualizzare quella sezione.
5. Scegliete Modifica e aggiungete la seguente nuova variabile di ambiente alla funzione:
   - Chiave: `AWS_STS_REGIONAL_ENDPOINTS`
   - Valore: `regional`
6. Seleziona Salva.

## Aggiungi un bucket Amazon S3

Per aggiungere un bucket S3 al tuo ambiente: RES

1. Scegliere Add bucket (Aggiungi bucket).
2. Inserisci i dettagli del bucket come il nome del bucket e il punto di montaggioARN.

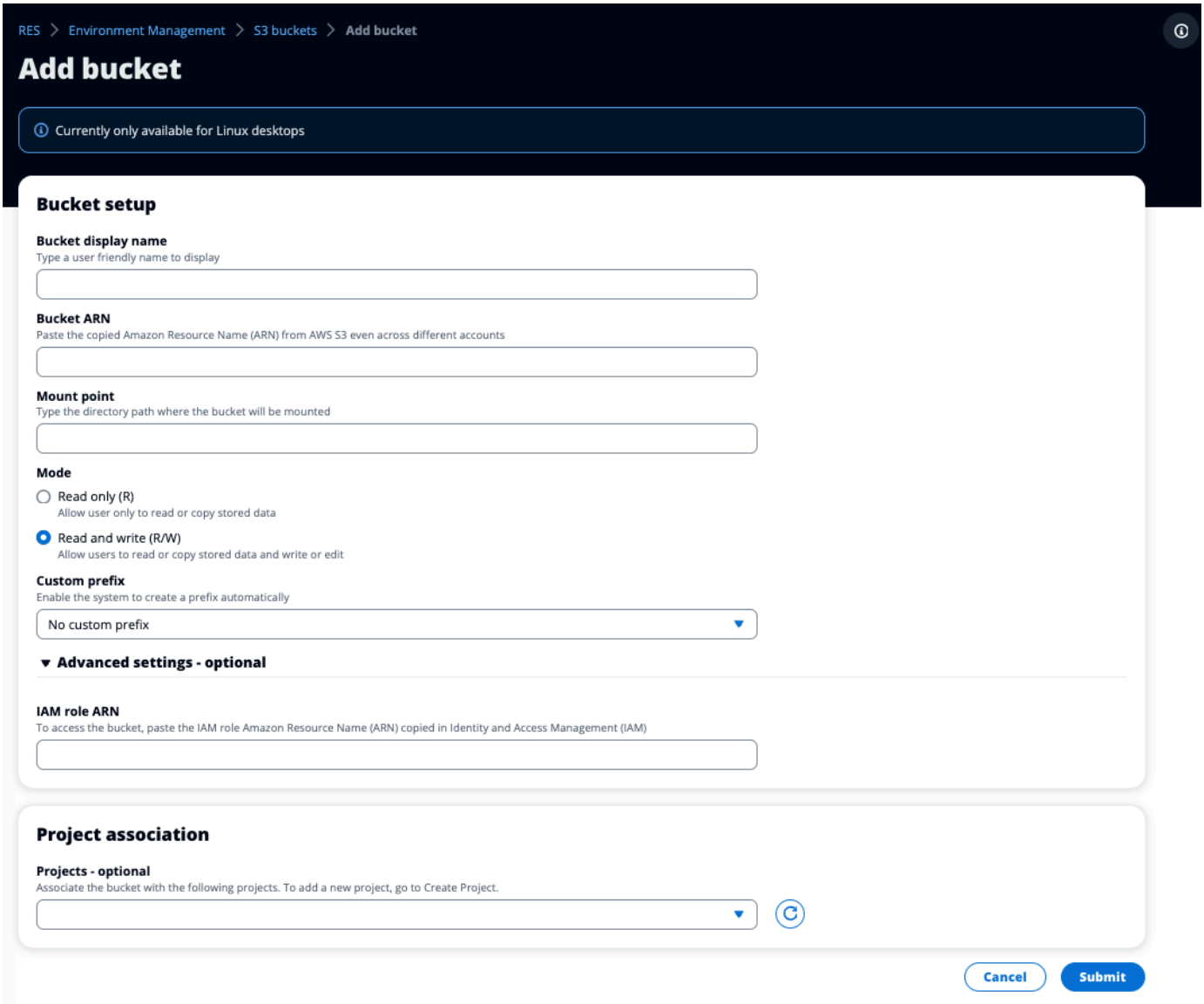
> **Important**
>
> - Il bucketARN, il punto di montaggio e la modalità forniti non possono essere modificati dopo la creazione.

- Il bucket ARN può contenere un prefisso che isolerà il bucket S3 integrato in base a quel prefisso.

3. Seleziona una modalità in cui inserire il tuo bucket.

> **Important**
>
> - Isolamento dei datiPer ulteriori informazioni relative all'isolamento dei dati con modalità specifiche, consulta.

4. In Opzioni avanzate, puoi fornire un IAM ruolo ARN per montare i bucket per l'accesso da più account. Segui i passaggi indicati Accesso a diversi bucket di account per creare il IAM ruolo richiesto per l'accesso da più account.
5. (Facoltativo) Associa il bucket ai progetti, che possono essere modificati in seguito. Tuttavia, un bucket S3 non può essere montato nelle sessioni esistenti di un progetto. VDI Solo le sessioni avviate dopo che il progetto è stato associato al bucket monteranno il bucket.
6. Scegli Invia.




## Modifica un bucket Amazon S3

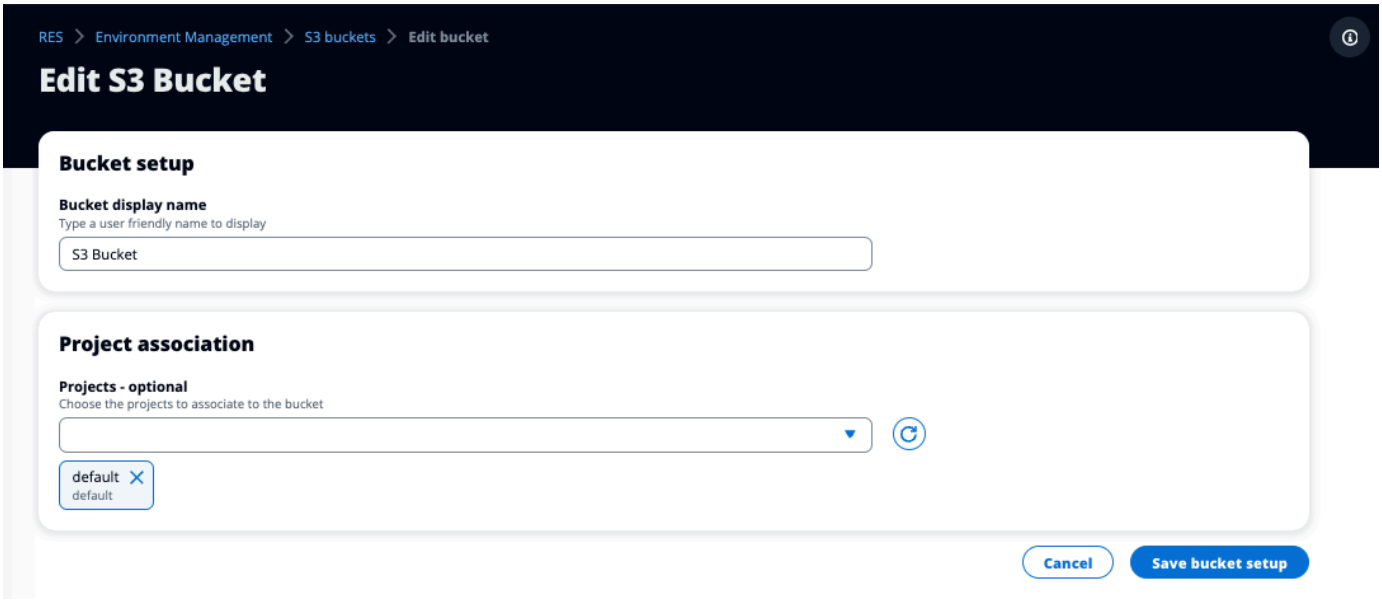
1. Seleziona un bucket S3 nell'elenco dei bucket S3.
2. Dal menu Azioni, seleziona Modifica.
3. Inserisci i tuoi aggiornamenti.

> **Important**
>
> - L'associazione di un progetto a un bucket S3 non comporterà il montaggio del bucket sulle istanze dell'infrastruttura desktop virtuale () esistenti di quel progetto. VDI Il

bucket verrà montato sulle VDI sessioni avviate in un progetto solo dopo che il bucket sarà stato associato a quel progetto.

- La dissociazione di un progetto da un bucket S3 non influirà sui dati contenuti nel bucket S3, ma comporterà la perdita dell'accesso a tali dati da parte degli utenti desktop.

4. Scegli Save bucket setup.




## Rimuovere un bucket Amazon S3

1. Seleziona un bucket S3 nell'elenco dei bucket S3.
2. Dal menu Azioni, seleziona Rimuovi.

> **Important**
>
> - È innanzitutto necessario rimuovere tutte le associazioni di progetto dal bucket.
> - L'operazione di rimozione non ha alcun impatto sui dati nel bucket S3. Rimuove solo l'associazione del bucket S3 con. RES
> - La rimozione di un bucket farà sì che VDI le sessioni esistenti perdano l'accesso al contenuto di quel bucket alla scadenza delle credenziali di quella sessione (~1 ora).

## Isolamento dei dati

Quando aggiungi un bucket S3 aRES, hai la possibilità di isolare i dati all'interno del bucket per progetti e utenti specifici. Nella pagina Aggiungi bucket, puoi selezionare una modalità di sola lettura (R) o lettura e scrittura (R/W).

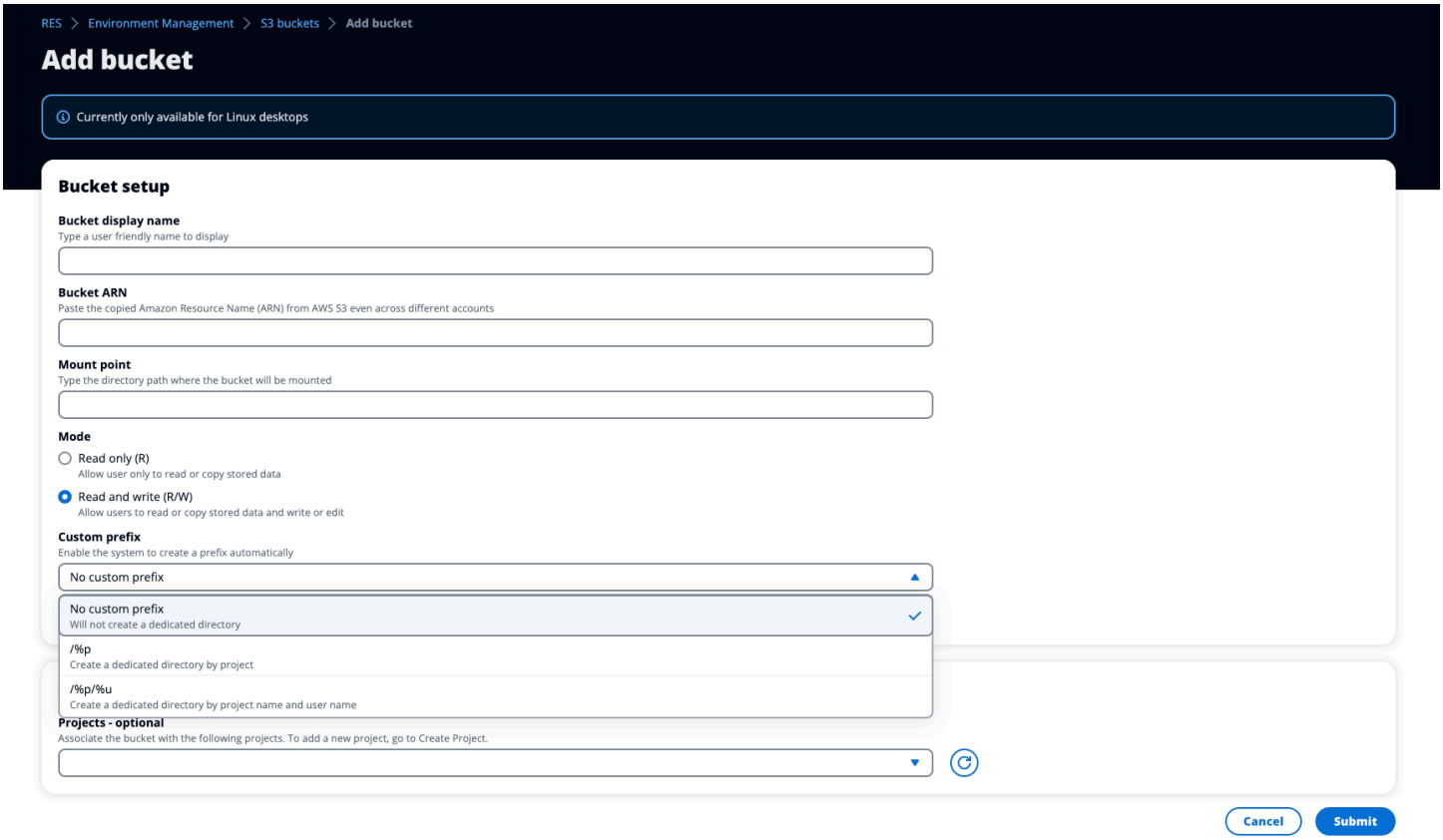
### Sola lettura

Se `Read Only (R)` selezionato, l'isolamento dei dati viene applicato in base al prefisso del bucket (ARNAmazon Resource Name). Ad esempio, se un amministratore aggiunge un bucket all'RESutilizzo di e lo associa al Progetto A ARN `arn:aws:s3:::`*`bucket-name/example-data/`* e al Progetto B, gli utenti che eseguono l'avvio VDIs dall'interno del Progetto A e del Progetto B possono leggere solo i dati che si trovano sotto il percorso. *`bucket-name /example-data`* Non avranno accesso ai dati al di fuori di quel percorso. Se non viene aggiunto alcun prefisso al bucketARN, l'intero bucket verrà reso disponibile per qualsiasi progetto ad esso associato.

### Leggi e scrivi

Se `Read and Write (R/W)` è selezionata, l'isolamento dei dati viene comunque applicato in base al prefisso del bucketARN, come descritto sopra. Questa modalità dispone di opzioni aggiuntive per consentire agli amministratori di fornire un prefisso basato su variabili per il bucket S3. Quando `Read and Write (R/W)` è selezionata, diventa disponibile una sezione Prefisso personalizzato che offre un menu a discesa con le seguenti opzioni:

- Nessun prefisso personalizzato
- /%p
- /%p/%u




Nessun isolamento personalizzato dei dati

Quando `No custom prefix` è selezionato per Prefisso personalizzato, il bucket viene aggiunto senza alcun isolamento dei dati personalizzato. Ciò consente a tutti i progetti associati al bucket di avere accesso in lettura e scrittura. Ad esempio, se un amministratore aggiunge un bucket all'RESutilizzo di ARN `arn:aws:s3:::bucket-name` with `No custom prefix` selected e lo associa al Progetto A e al Progetto B, gli utenti che eseguono l'avvio VDIs dall'interno del Progetto A e del Progetto B avranno accesso illimitato in lettura e scrittura al bucket.

Isolamento dei dati a livello di progetto

Quando `/%p` è selezionato per Prefisso personalizzato, i dati nel bucket vengono isolati per ogni progetto specifico ad esso associato. La `%p` variabile rappresenta il codice del progetto. Ad esempio, se un amministratore aggiunge un bucket all'RESutilizzo di ARN `arn:aws:s3:::bucket-name` with `/%p` selected e un Mount Point di `/bucket`, e associa questo bucket al Progetto A e al Progetto B, l'utente A nel Progetto A può scrivere un file su `/bucket`. L'utente B del Progetto A può anche vedere il file in cui l'utente A ha scritto `/bucket`. Tuttavia, se l'utente B avvia a VDI nel Progetto B e cerca `/bucket`, non vedranno il file scritto

dall'utente A, poiché i dati sono isolati dal progetto. Il file scritto dall'utente A si trova nel bucket S3 sotto il prefisso, `/ProjectA` mentre l'utente B può accedervi solo `/ProjectB` quando lo utilizza dal Progetto B. VDIs

Isolamento dei dati a livello di progetto e utente

Quando `/%p/%u` è selezionato per Prefisso personalizzato, i dati nel bucket vengono isolati per ogni progetto specifico e utente associato a quel progetto. La `%p` variabile rappresenta il codice del progetto e `%u` rappresenta il nome utente. Ad esempio, un amministratore aggiunge un bucket all'RESutilizzo di ARN `arn:aws:s3:::bucket-name` with `/%p/%u` selected e un Mount Point di `/bucket`. Questo bucket è associato al Progetto A e al Progetto B. L'utente A del Progetto A può scrivere un file in `/bucket`. A differenza dello scenario precedente con il solo `%p` isolamento, l'utente B in questo caso non vedrà il file che l'utente A ha scritto nel Progetto A in `/bucket`, poiché i dati sono isolati sia dal progetto che dall'utente. Il file scritto dall'utente A si trova nel bucket S3 sotto il prefisso, `/ProjectA/UserA` mentre l'utente B può accedervi solo `/ProjectA/UserB` quando lo utilizza nel Progetto A. VDIs

## Accesso a diversi bucket di account

RESha la capacità di montare bucket da altri AWS account, a condizione che questi bucket abbiano le autorizzazioni giuste. Nello scenario seguente, un RES ambiente nell'Account A desidera montare un bucket S3 nell'Account B.

Fase 1: Creare un IAM ruolo nell'account RES distribuito in (denominato Account A):

1. Accedi alla console di AWS gestione dell'RESaccount che deve accedere al bucket S3 (account A).
2. Apri la console: IAM
   a. Vai alla IAM dashboard.
   b. Nel riquadro di navigazione, seleziona Policy.
3. Crea una politica:
   a. Scegli Create Policy (Crea policy).
   b. Seleziona la scheda JSON.
   c. Incolla la seguente JSON policy (`<BUCKET-NAME>`sostituiscila con il nome del bucket S3 che si trova nell'Account B):

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

d. Scegli Next (Successivo).

4. Rivedi e crea la politica:

   a. Fornisci un nome per la politica (ad esempio, «AccessPolicyS3").

   b. Aggiungi una descrizione opzionale per spiegare lo scopo della politica.

   c. Rivedi la politica e scegli Crea politica.

5. Apri la IAM console:

   a. Vai alla IAM dashboard.

   b. Nel riquadro di navigazione, seleziona Ruoli.

6. Crea un ruolo:

   a. Scegliere Crea ruolo.

   b. Scegli la politica di fiducia personalizzata come tipo di entità affidabile.

   c. Incolla la seguente JSON politica (sostituiscila *<ACCOUNT_ID>* con l'ID account effettivo dell'account A, *<ENVIRONMENT_NAME>* con il nome dell'ambiente della RES distribuzione e *<REGION>* con la AWS regione in cui RES viene distribuita):

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

d. Scegli Next (Successivo).

7. Allega politiche di autorizzazione:

   a. Cerca e seleziona la politica che hai creato in precedenza.

   b. Scegli Next (Successivo).

8. Etichetta, rivedi e crea il ruolo:

   a. Inserisci il nome di un ruolo (ad esempio, «AccessRoleS3").

   b. Nel passaggio 3, scegli Aggiungi tag, quindi inserisci la chiave e il valore seguenti:

      - Chiave: `res:Resource`
      - Valore: `s3-bucket-iam-role`

   c. Rivedi il ruolo e scegli Crea ruolo.

9. Usa il IAM ruolo inRES:

   a. Copia il IAM ruolo ARN che hai creato.

   b. Accedi alla RES console.

   c. Nel riquadro di navigazione a sinistra, scegli S3 Bucket.

   d. Scegli Aggiungi un bucket e compila il modulo con il bucket S3 per più account. ARN

   e. Scegli le impostazioni avanzate (menu a discesa opzionale).

   f. Inserisci il ruolo ARN nel ARN campo del IAM ruolo.

   g. Scegli Aggiungi secchio.

Passaggio 2: modifica la politica del bucket nell'account B

1. Accedi alla console di AWS gestione per l'account B.
2. Apri la console S3:
   a. Vai alla dashboard di S3.
   b. Seleziona il bucket a cui vuoi concedere l'accesso.
3. Modifica la politica del bucket:
   a. Seleziona la scheda Autorizzazioni e scegli la politica Bucket.
   b. Aggiungi la seguente politica per concedere al IAM ruolo dell'Account A l'accesso al bucket (sostituisci) *<AccountA_ID>* con l'ID effettivo dell'account A e *<BUCKET-NAME>* con il nome del bucket S3):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountA_ID:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

   c. Seleziona Salva.

## Prevenzione dell'esfiltrazione dei dati in ambienti privati VPC

Per impedire agli utenti di esfiltrare i dati dai bucket S3 sicuri verso i propri bucket S3 del proprio account, puoi collegare un endpoint per proteggere i dati privati. VPC VPC I passaggi seguenti mostrano come creare un VPC endpoint per il servizio S3 che supporti l'accesso ai bucket S3 all'interno del tuo account, oltre a qualsiasi account aggiuntivo con bucket tra account.

1. Apri la VPC console Amazon:
   a. Accedi alla console AWS di gestione.
   b. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Crea un VPC endpoint per S3:
   a. Nel riquadro di navigazione a sinistra, scegli Endpoints (Endpoint).
   b. Scegliere Create Endpoint (Crea endpoint).
   c. In Categoria servizio, assicurati che Servizi AWS sia selezionato.
   d. Nel campo Service Name, inserisci `com.amazonaws.<region>.s3` (sostituisci *<region>* con la tua AWS regione) o cerca «S3".
   e. Seleziona il servizio S3 dall'elenco.
3. Configura le impostazioni degli endpoint:
   a. Per VPC, seleziona il VPC punto in cui desideri creare l'endpoint.
   b. Per le sottoreti, seleziona entrambe le sottoreti private utilizzate per le sottoreti durante la distribuzione. VDI
   c. Per Abilita DNS nome, assicurati che l'opzione sia selezionata. Ciò consente di risolvere il DNS nome host privato nelle interfacce di rete dell'endpoint.
4. Configura la politica per limitare l'accesso:
   a. In Policy, scegli Personalizzato.
   b. Nell'editor delle politiche, inserisci una politica che limiti l'accesso alle risorse all'interno del tuo account o di un account specifico. Ecco un esempio di politica (sostituisci *mybucket* con il nome del tuo bucket S3 e *111122223333* e *444455556666* con l' AWS account appropriato a IDs cui desideri avere accesso):

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

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

5. Crea l'endpoint:
   a. Verificare le impostazioni.
   b. Seleziona Crea endpoint.
6. Verifica l'endpoint:
   a. Una volta creato l'endpoint, vai alla sezione Endpoints nella console. VPC
   b. Seleziona l'endpoint appena creato.
   c. Verifica che lo stato sia disponibile.

Seguendo questi passaggi, crei un VPC endpoint che consente l'accesso a S3 limitato alle risorse all'interno del tuo account o a un ID account specificato.

## Risoluzione dei problemi

Come verificare se un bucket non riesce a montarsi su un VDI

Se un bucket non riesce a montarsi su unVDI, ci sono alcune posizioni in cui è possibile verificare la presenza di errori. Segui i passaggi seguenti.

1. Controlla i VDI registri:

a. Accedere alla console AWS di gestione.
b. Apri la EC2 console e vai a Istanze.
c. Seleziona l'VDIistanza che hai avviato.
d. Connect a VDI tramite Session Manager.
e. Esegui i comandi seguenti:

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

Qui troverai i log di bootstrap. I dettagli di ogni errore si troveranno nel `configure.log.{time}` file.

Inoltre, controlla il `/etc/message` registro per maggiori dettagli.

2. Controlla i log CloudWatch Lambda di Custom Credential Broker:

a. Accedere alla console di gestione AWS .
b. Apri la CloudWatch console e vai a Gruppi di log.
c. Cerca il gruppo di log`/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.
d. Esamina il primo gruppo di log disponibile e individua eventuali errori all'interno dei log. Questi registri conterranno dettagli sui potenziali problemi relativi alla fornitura di credenziali personalizzate temporanee per il montaggio dei bucket S3.

3. Controlla i log di Custom Credential Broker Gateway: API CloudWatch

a. Accedere alla console di AWS gestione.
b. Apri la CloudWatch console e vai a Gruppi di log.
c. Cerca il gruppo di log`<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`.
d. Esamina il primo gruppo di log disponibile e individua eventuali errori all'interno dei log. Questi log conterranno dettagli riguardanti eventuali richieste e risposte al API Gateway per le credenziali personalizzate necessarie per montare i bucket S3.

Come modificare la configurazione dei ruoli di un bucket dopo l'onboarding IAM

1. Accedi alla console AWS DynamoDB.

2. Seleziona la tabella:

   a. Nel riquadro di navigazione a sinistra, selezionare Tables (Tabelle).

   b. Trova e seleziona`<stack-name>.cluster-settings`.

3. Scansiona la tabella:

   a. Scegli Explore table items (Esplora elementi della tabella).

   b. Assicurati che Scan sia selezionato.

4. Aggiungi un filtro:

   a. Scegli Filtri per aprire la sezione di immissione del filtro.

   b. Imposta il filtro in modo che corrisponda alla tua chiave-

      - Attributo: inserisci la chiave.
      - Condizione: Seleziona Inizia con.
      - Valore: inserire `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` la sostituzione `<filesystem_id>` con il valore del filesystem che deve essere modificato.

5. Esegui la scansione:

   Scegli Esegui per eseguire la scansione con il filtro.

6. Controlla il valore:

   Se la voce esiste, assicurati che il valore sia impostato correttamente con il IAM ruolo giustoARN.

   Se la voce non esiste:

   a. Scegli Crea elemento.

   b. Inserisci i dettagli dell'articolo:

      - Per l'attributo chiave, inserisci`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
      - Aggiungi il IAM ruolo correttoARN.

   c. Scegli Salva per aggiungere l'articolo.

7. Riavvia le VDI istanze:

Riavvia l'istanza per assicurarti VDIs che quelle interessate dal IAM ruolo errato ARN vengano montate nuovamente.

## Abilitazione CloudTrail

Per abilitare CloudTrail il tuo account utilizzando la CloudTrail console, segui le istruzioni fornite nella sezione Creazione di un percorso con la CloudTrail console nella Guida per l'AWS CloudTrail utente. CloudTrail registrerà l'accesso ai bucket S3 registrando il IAM ruolo che vi ha effettuato l'accesso. Questo può essere ricollegato a un ID di istanza, che è collegato a un progetto o a un utente.

# Usa il prodotto

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

Argomenti



## SSHaccesso

Da utilizzare SSH per accedere al bastion host:

1. Dal RES menu, scegli SSHaccesso.
2. Segui le istruzioni sullo schermo per utilizzare uno dei due SSH o Pu TTY per accedere.

## Desktop virtuali

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

Sistemi operativi supportati

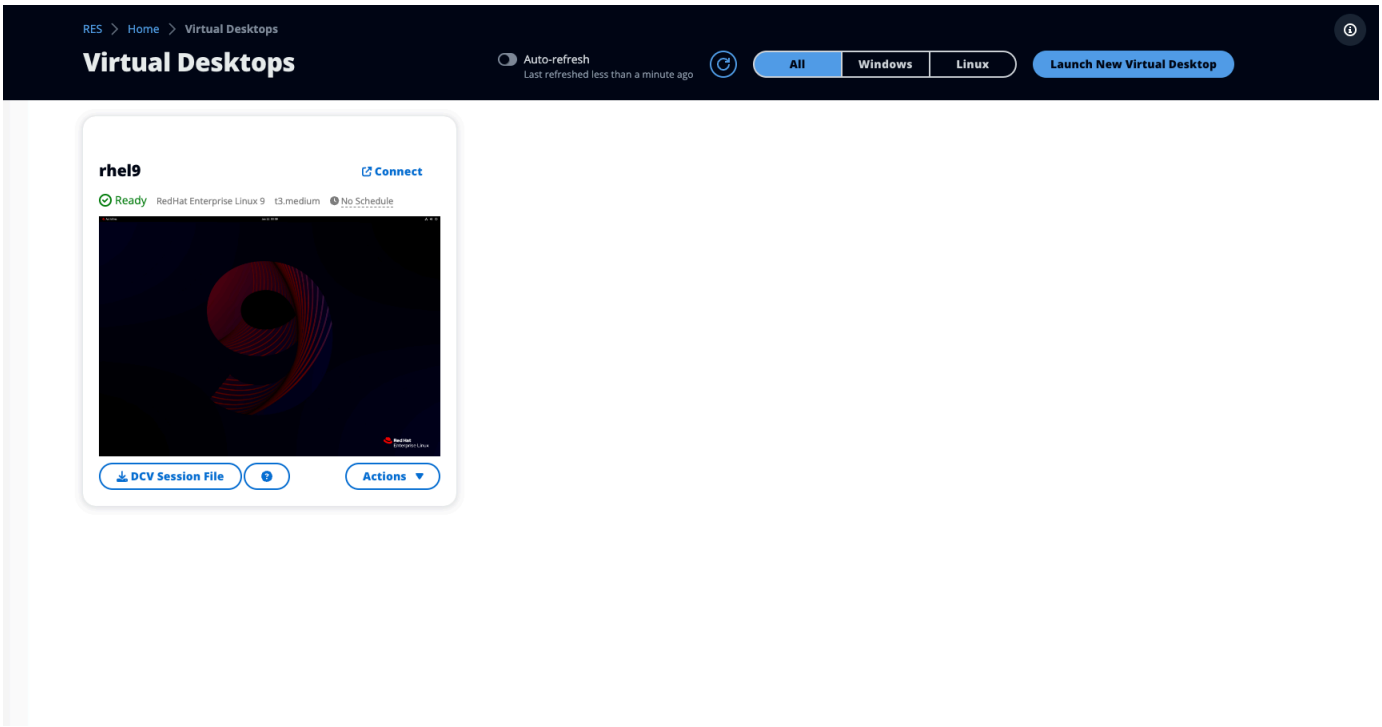
RESattualmente supporta l'avvio di desktop virtuali utilizzando i seguenti sistemi operativi:

- Amazon Linux 2 (x86 eARM64)
- Ubuntu 22.04.03 (x86)
- RHEL8 (x86) e 9 (x86)
- Windows 2019, 2022 (x86)

Argomenti

## 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. RESrileva le GPU istanze e installa i driver pertinenti.

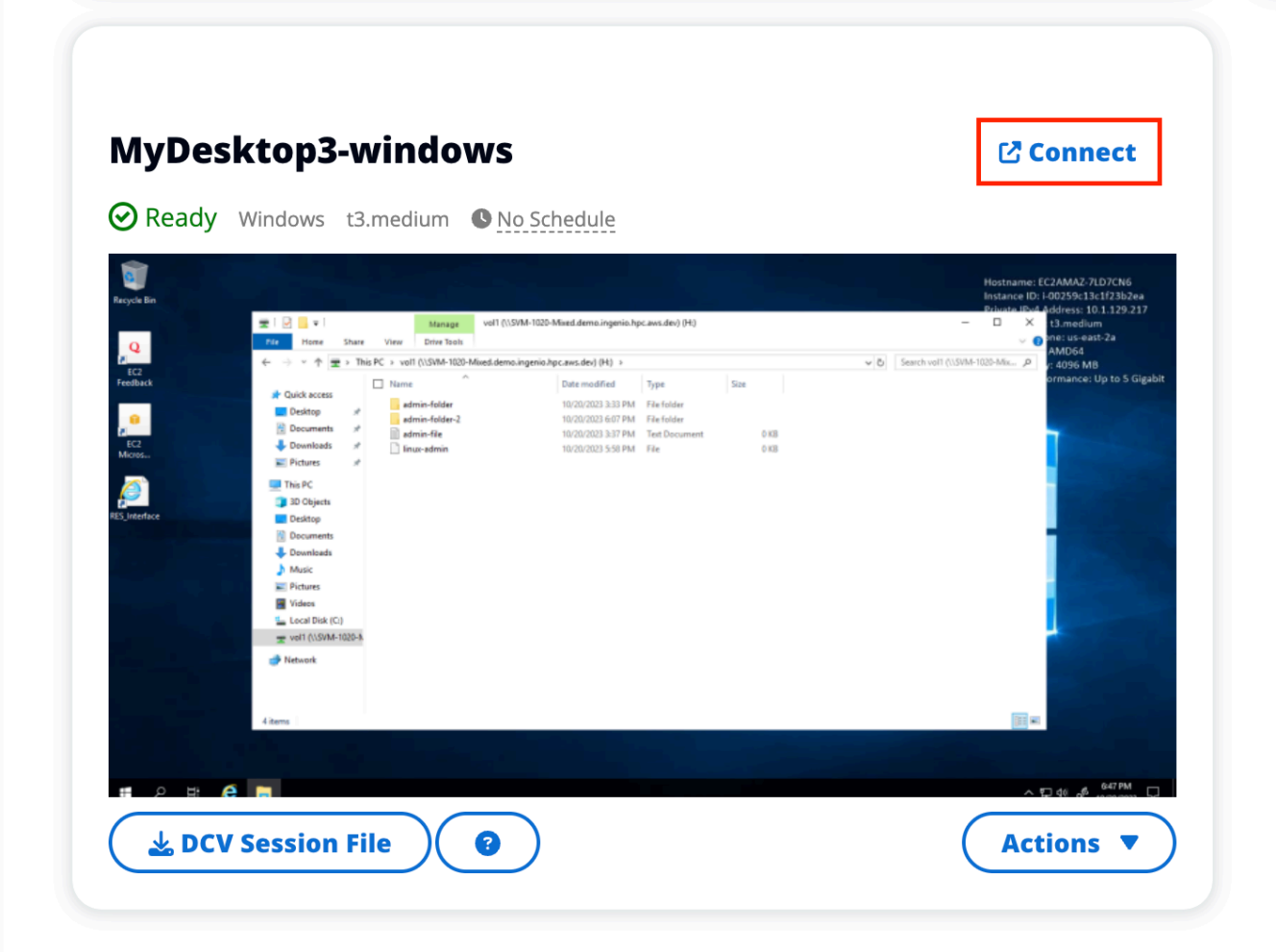
# Accedi al tuo desktop

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

Web connection

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

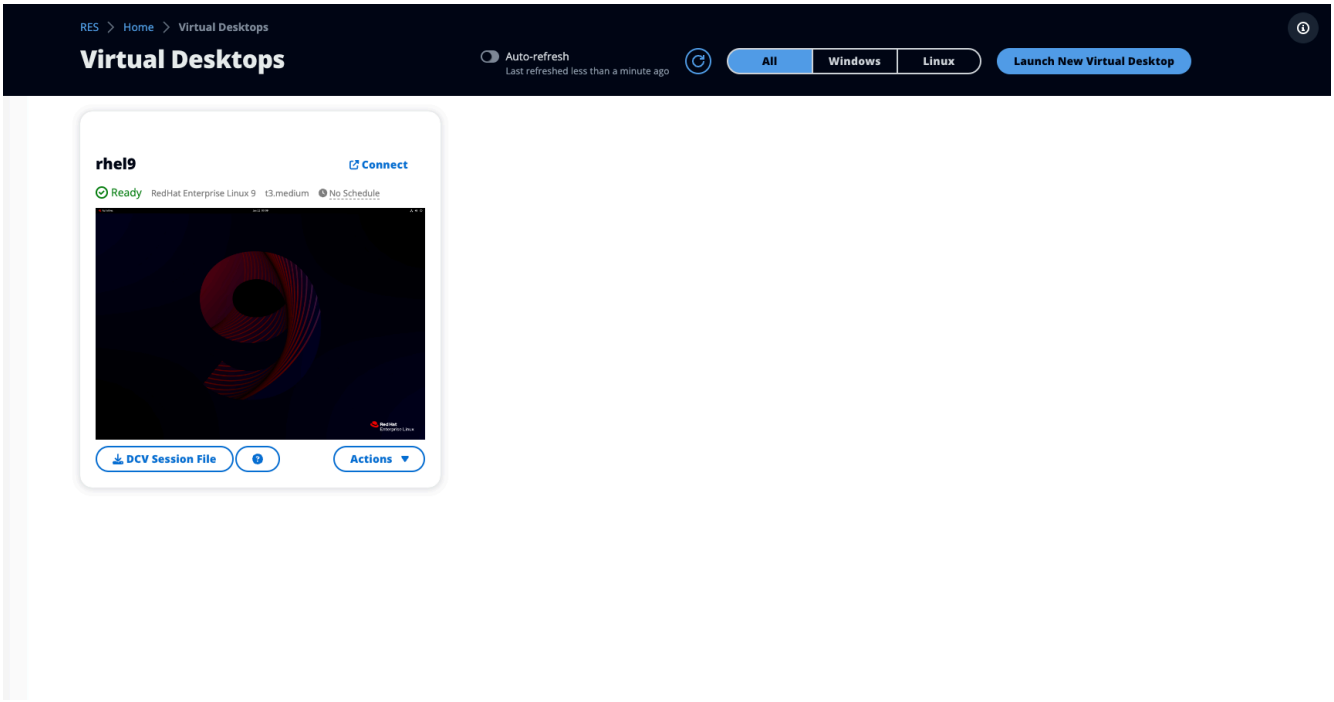
- Scegli Connect o scegli la miniatura per accedere al desktop direttamente tramite il browser.



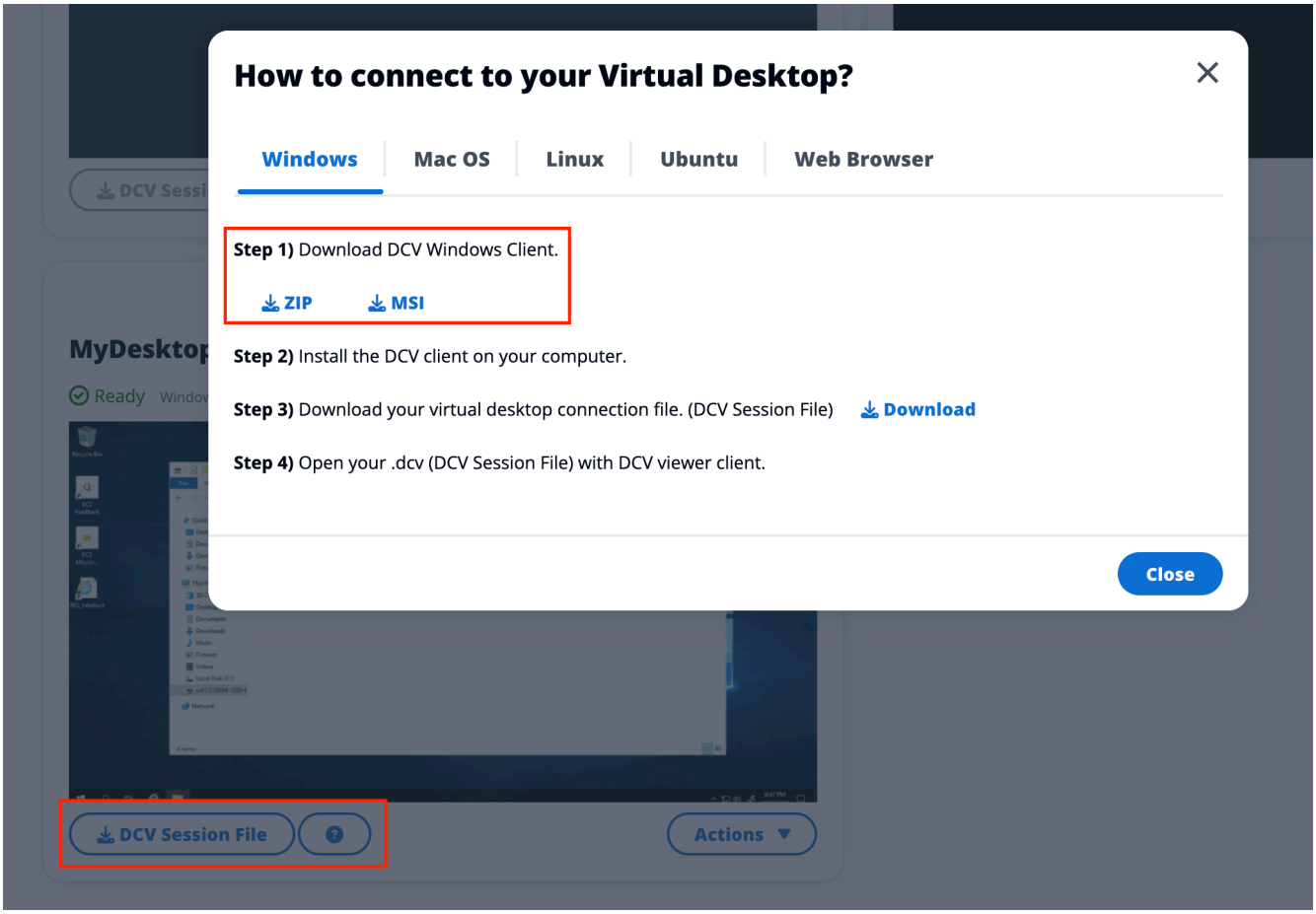

DCV connection

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

1. Scegli File di DCV sessione per scaricare il `.dcv` file. Avrai bisogno di un DCV client installato sul tuo sistema.



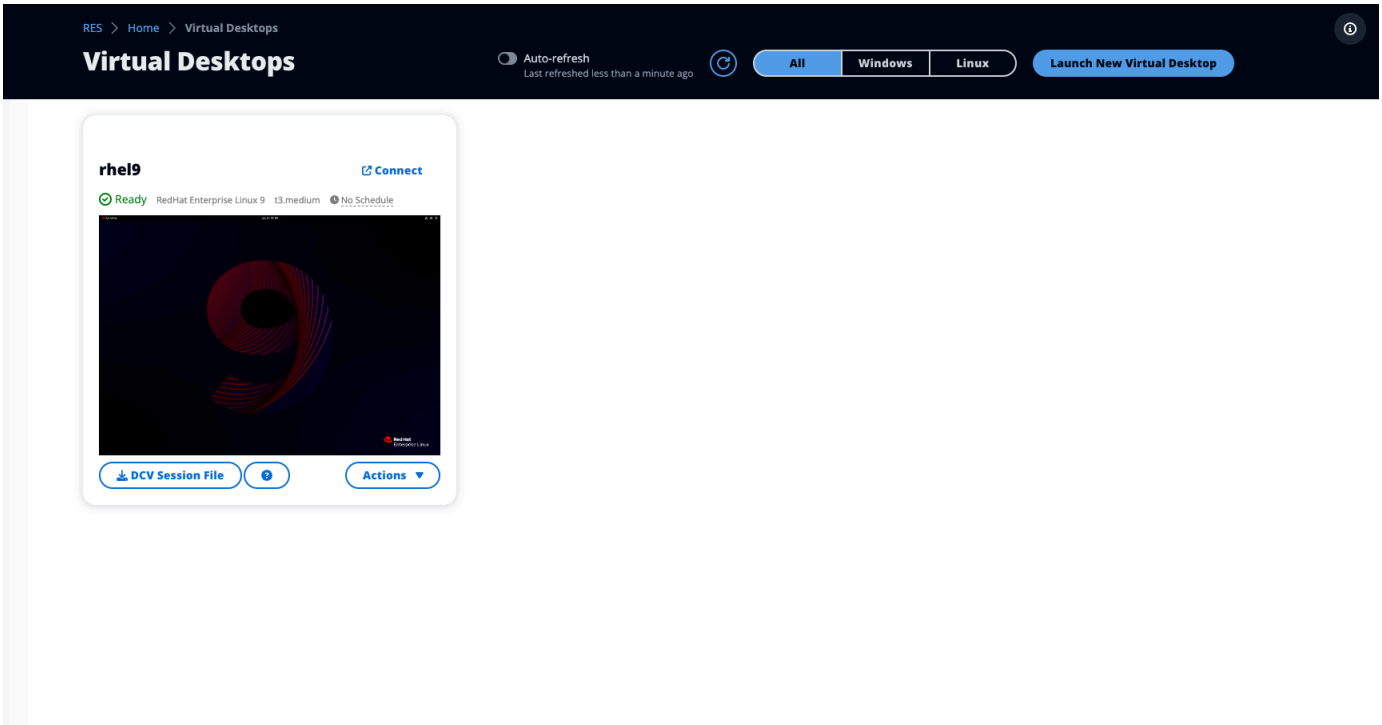

2. Per le istruzioni di installazione, scegli l'opzione? icona.



# Controlla lo stato del tuo 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 prima di terminareRES.

   - Ibernazione

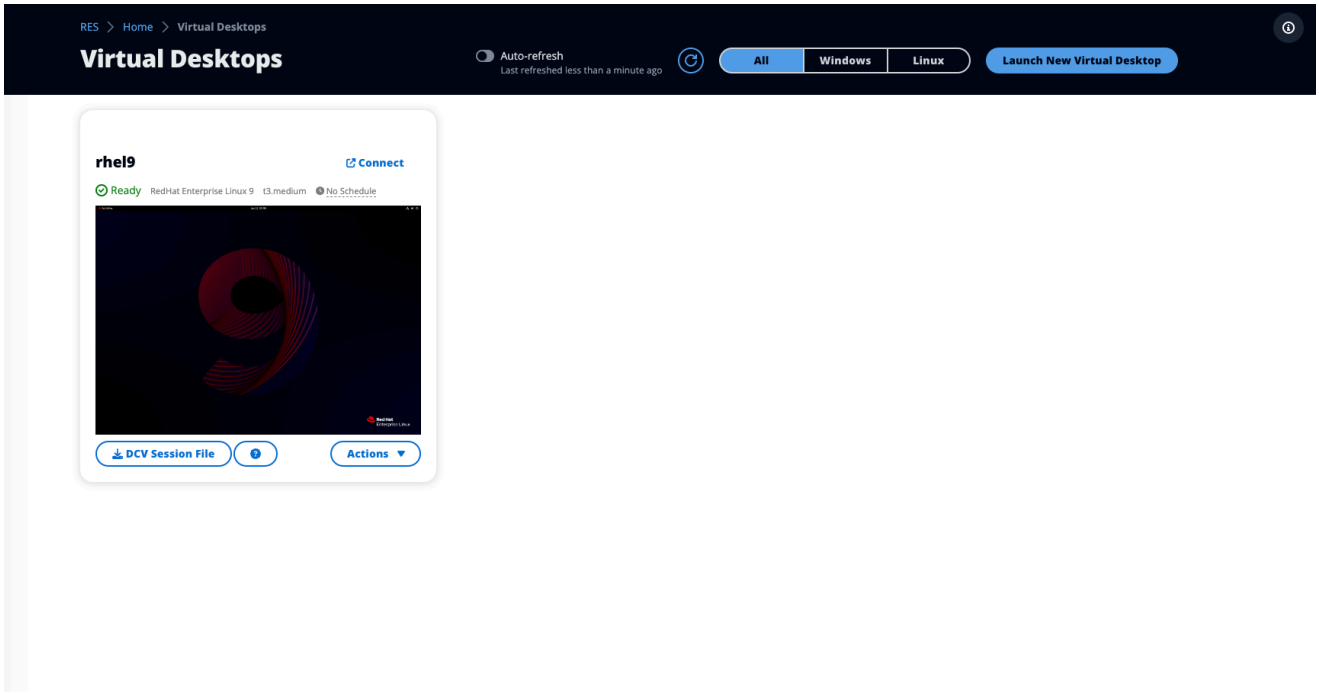
Lo stato del desktop verrà salvato in memoria. Al riavvio del desktop, le applicazioni riprenderanno ma eventuali connessioni remote potrebbero andare perse. Non tutte le istanze supportano l'ibernazione e l'opzione è disponibile solo se è stata abilitata durante la creazione dell'istanza. Per verificare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

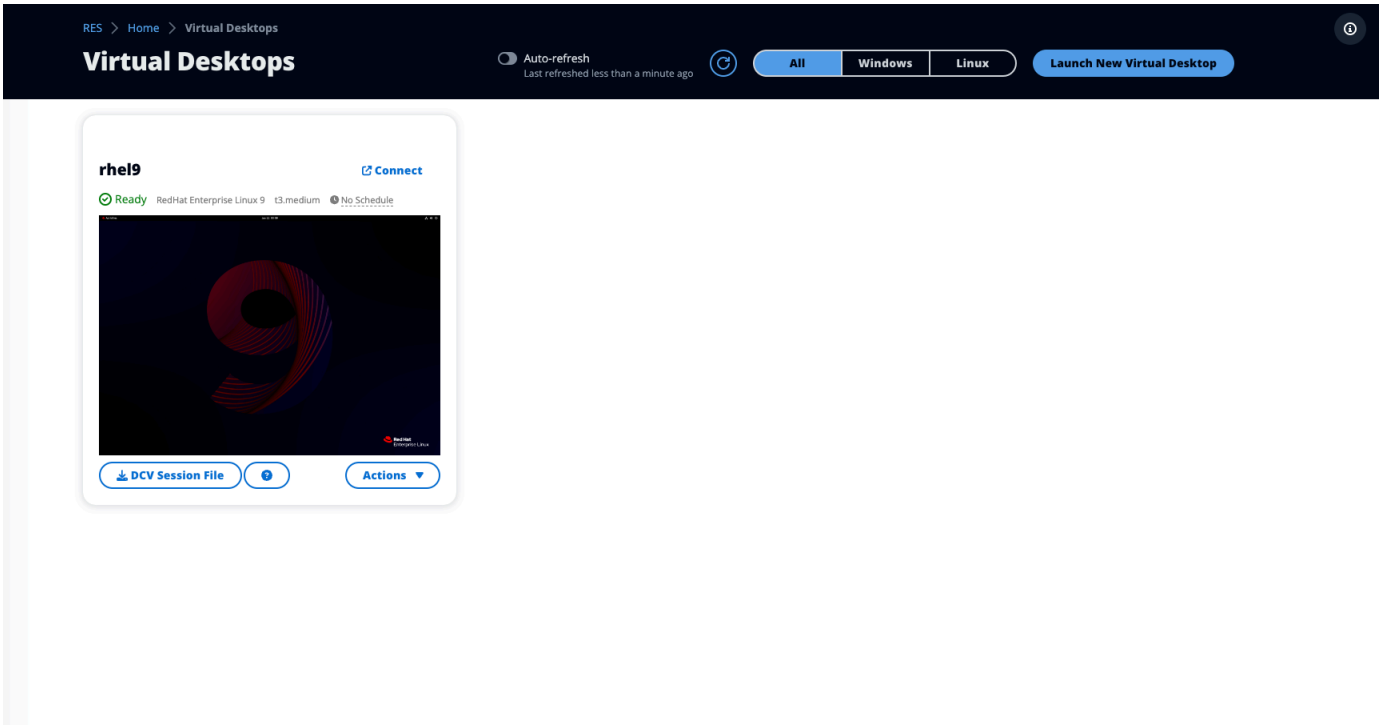
> **Note**
>
> Non è possibile aggiornare le dimensioni del desktop per le sessioni ibernate.

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.

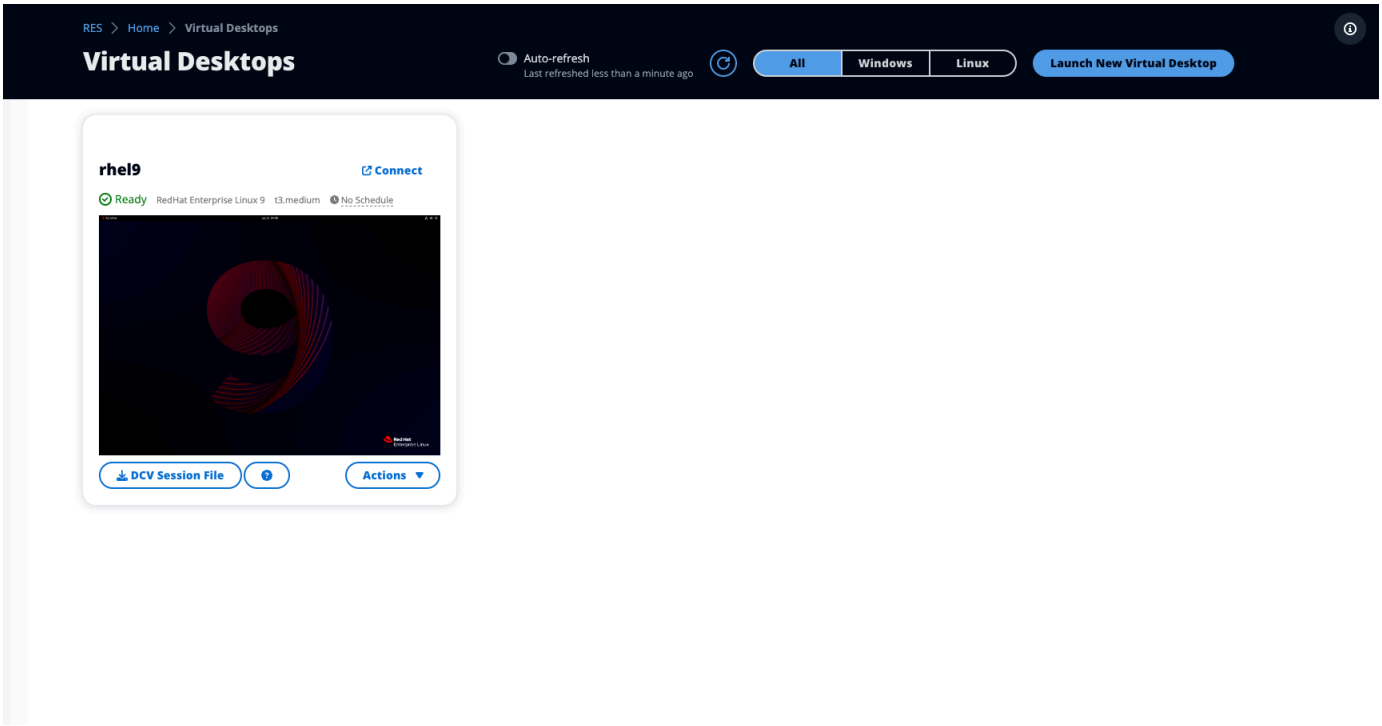



2. Scegli Mostra informazioni.

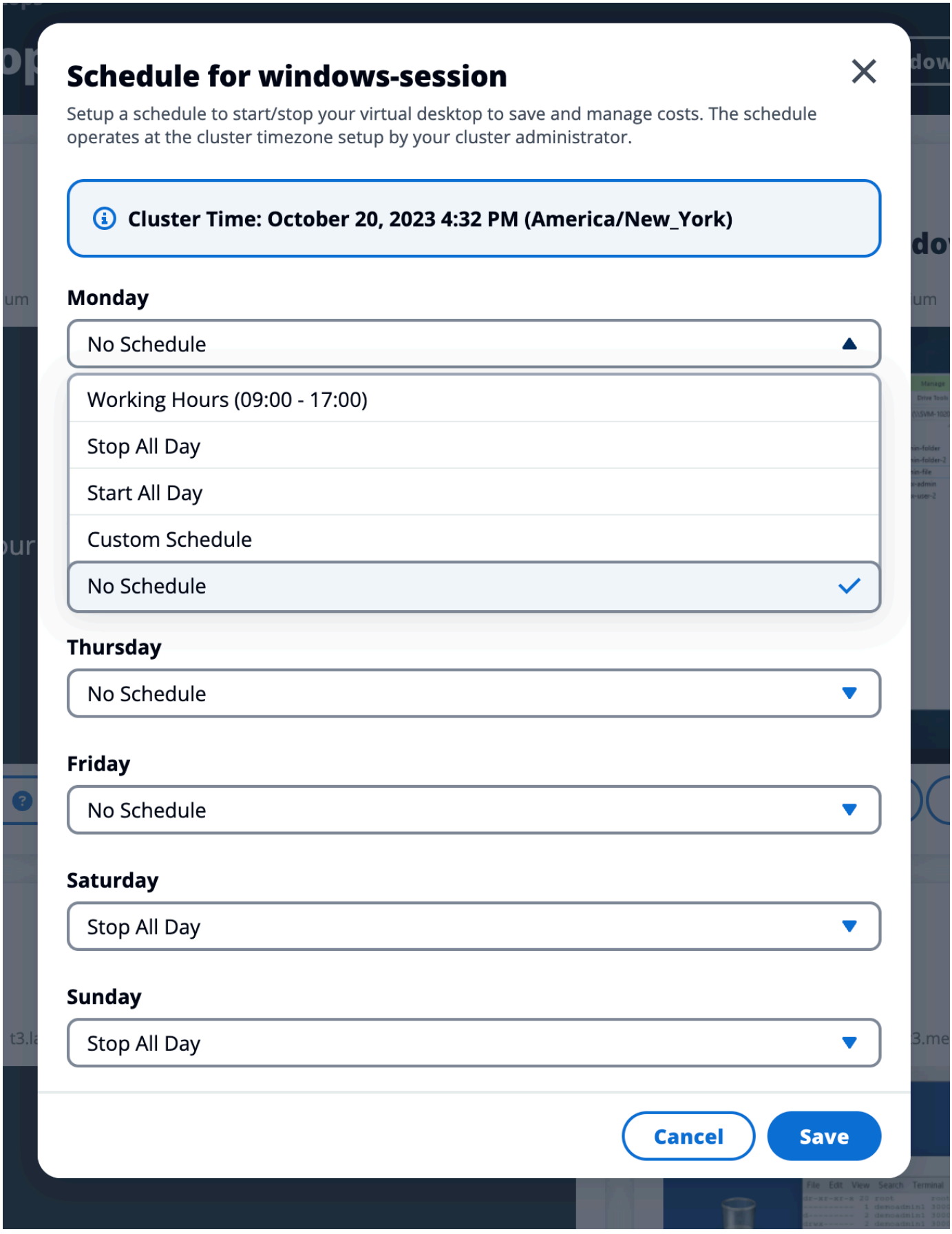
## Pianifica i desktop virtuali

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'CPUutilizzo inferiore al 15% per almeno 15 minuti. È possibile configurare una pianificazione per avviare e arrestare automaticamente il desktop.

1. Scegli Azioni.



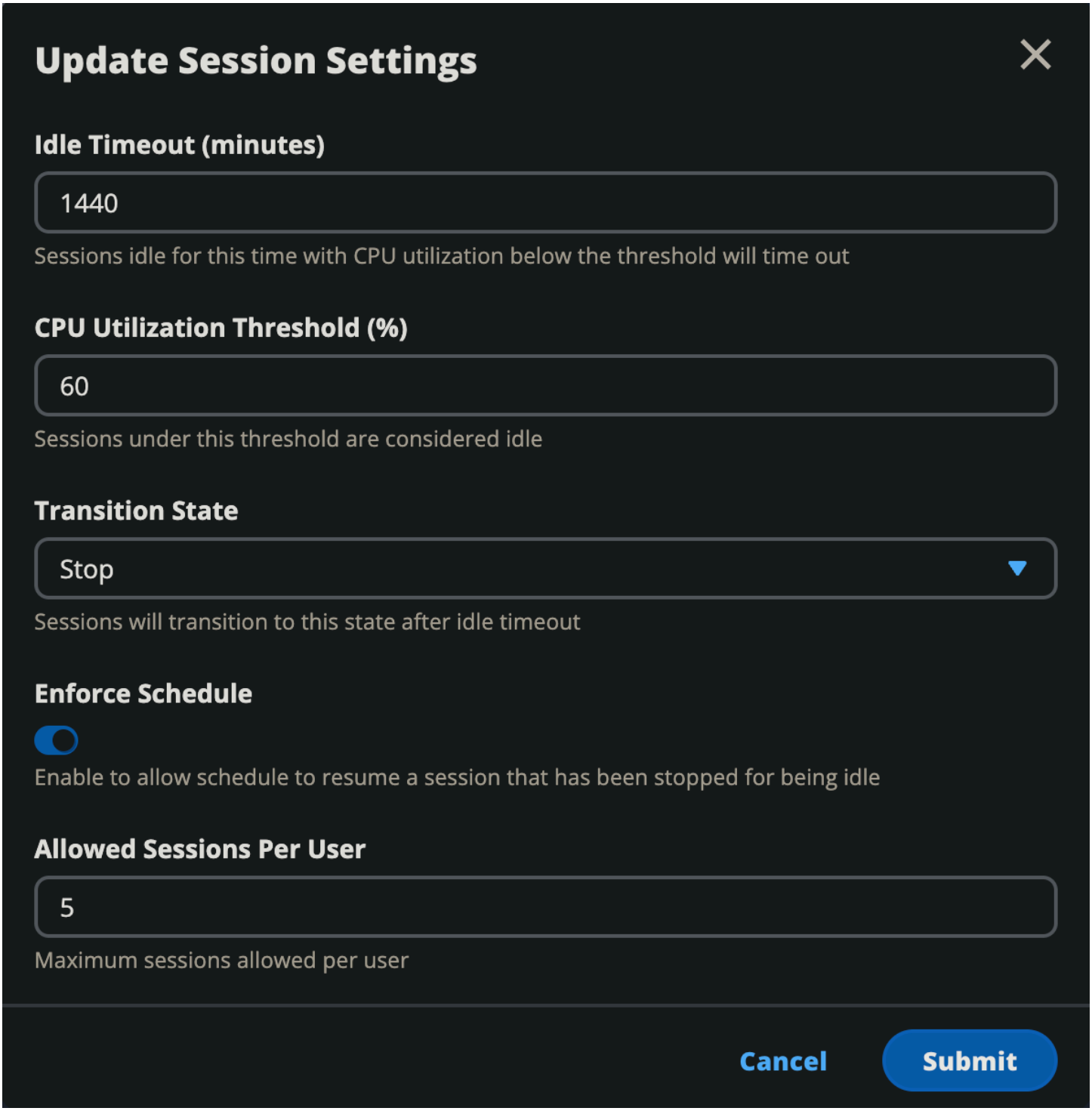

2. Seleziona Schedule (Pianifica).
3. Imposta il tuo programma per ogni giorno.
4. Seleziona Salva.


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

# Interruzione automatica dell'interfaccia desktop virtuale

Gli amministratori possono configurare le impostazioni per consentire l'interruzione o la cessazione dell'VDIsinattività. Sono disponibili 4 impostazioni configurabili:

1. Timeout di inattività: le sessioni inattive per questo periodo con un CPU utilizzo inferiore alla soglia verranno scadute.
2. CPUSoglia di utilizzo: le sessioni senza interazione e al di sotto di questa soglia sono considerate inattive. Se questo valore è impostato su 0, le sessioni non verranno mai considerate inattive.
3. Stato di transizione: dopo il timeout di inattività, le sessioni passeranno a questo stato (interrotte o terminate).
4. Applica pianificazione: se selezionata, una sessione che è stata interrotta perché inattiva può essere ripresa secondo la pianificazione giornaliera.

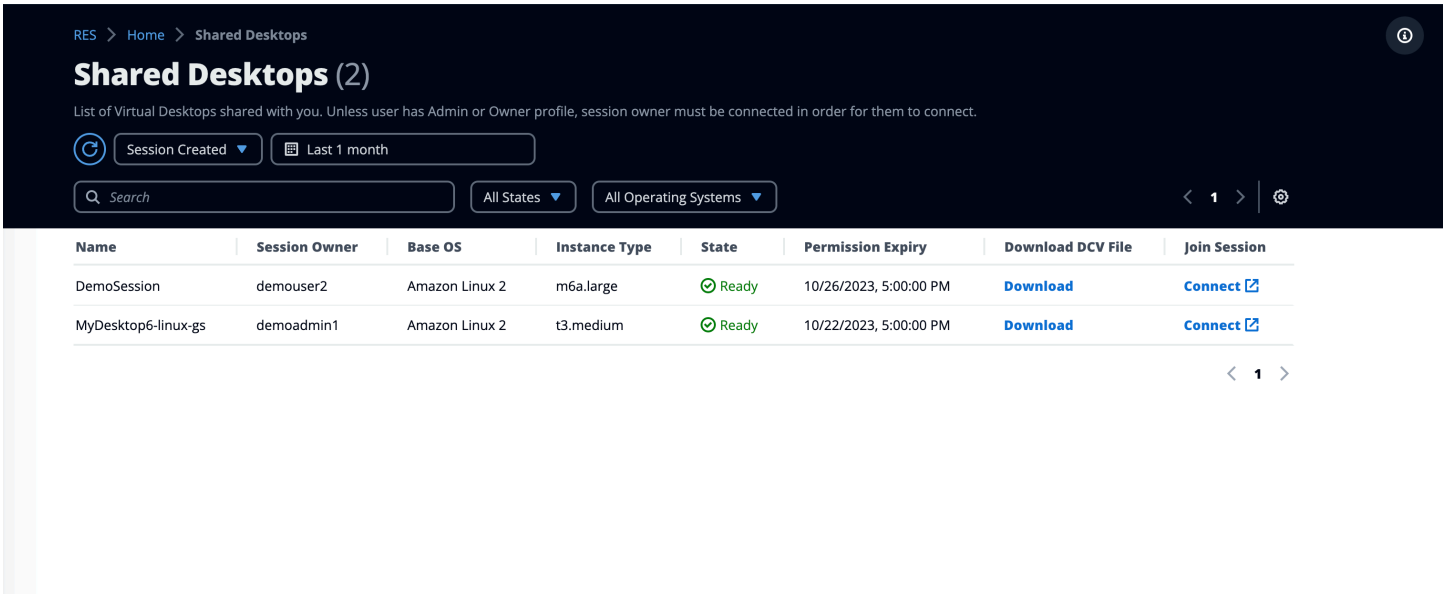



Queste impostazioni sono presenti nella pagina Impostazioni del desktop nella scheda Server. Dopo aver aggiornato le impostazioni in base alle tue esigenze, fai clic su Invia per salvare le impostazioni. Le nuove sessioni utilizzeranno le impostazioni aggiornate, ma tieni presente che le sessioni esistenti continueranno a utilizzare le impostazioni che avevano al momento dell'avvio.

Dopo il timeout, le sessioni termineranno o passeranno allo `STOPPED_IDLE` stato in base alla loro configurazione. Gli utenti avranno la possibilità di avviare `STOPPED_IDLE` le sessioni dall'interfaccia utente.

# 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.



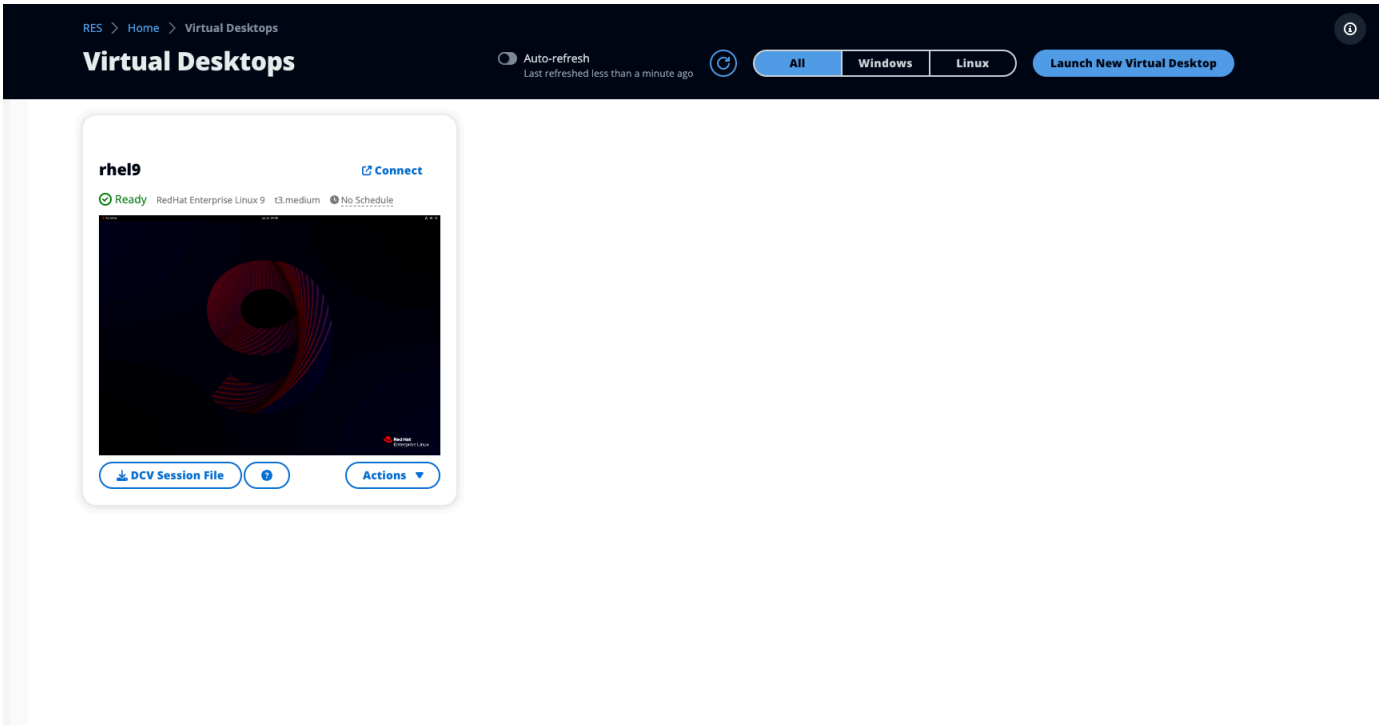

Durante la condivisione di una sessione, puoi configurare le autorizzazioni per i tuoi collaboratori. Ad esempio, puoi concedere l'accesso in sola lettura a un collega del team con cui collabori.

Argomenti

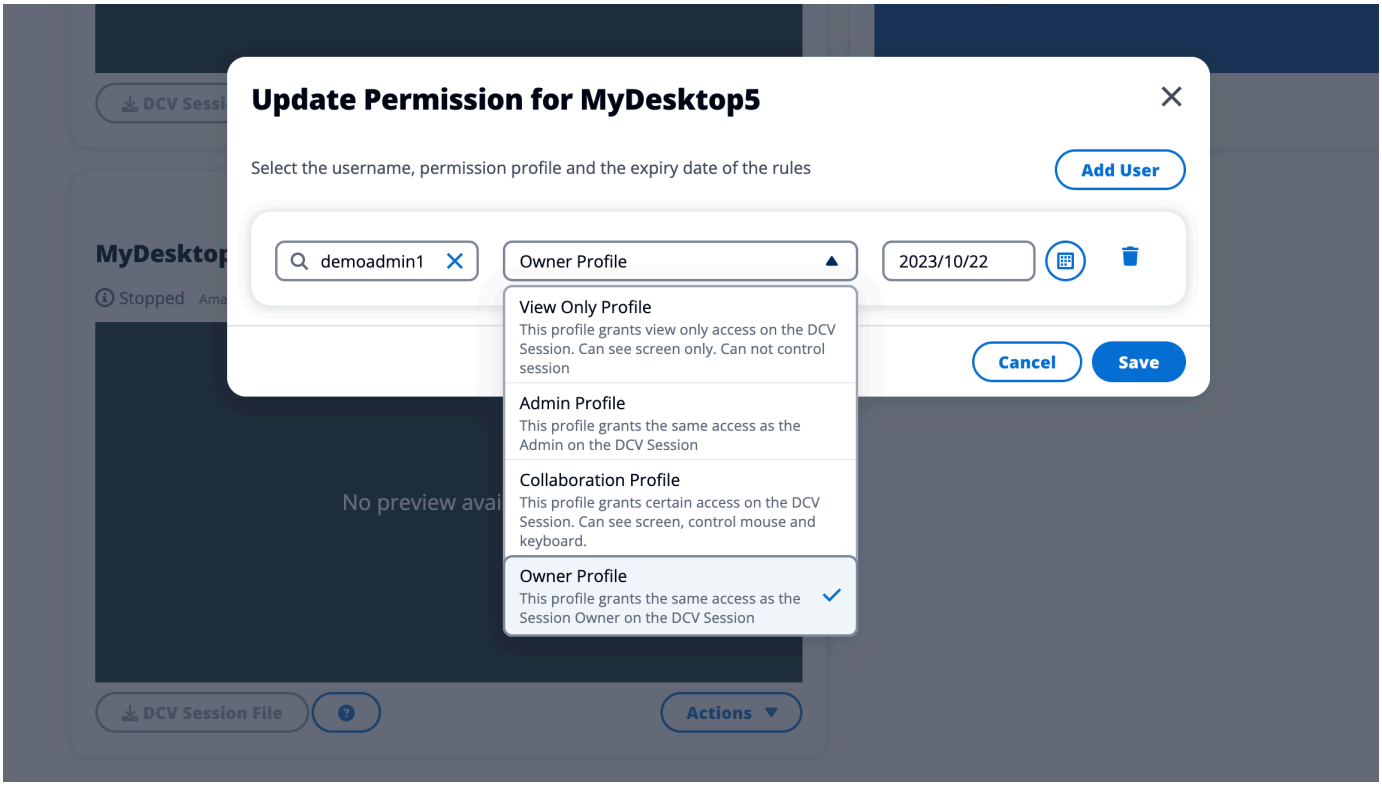
- Condividi un desktop
- Accedere a un desktop condiviso

## Condividi un desktop

1. Dalla sessione desktop, scegli Azioni.




2. Seleziona Autorizzazioni di sessione.
3. Seleziona l'utente e il livello di autorizzazione. Puoi anche impostare un orario di scadenza.
4. Seleziona Salva.



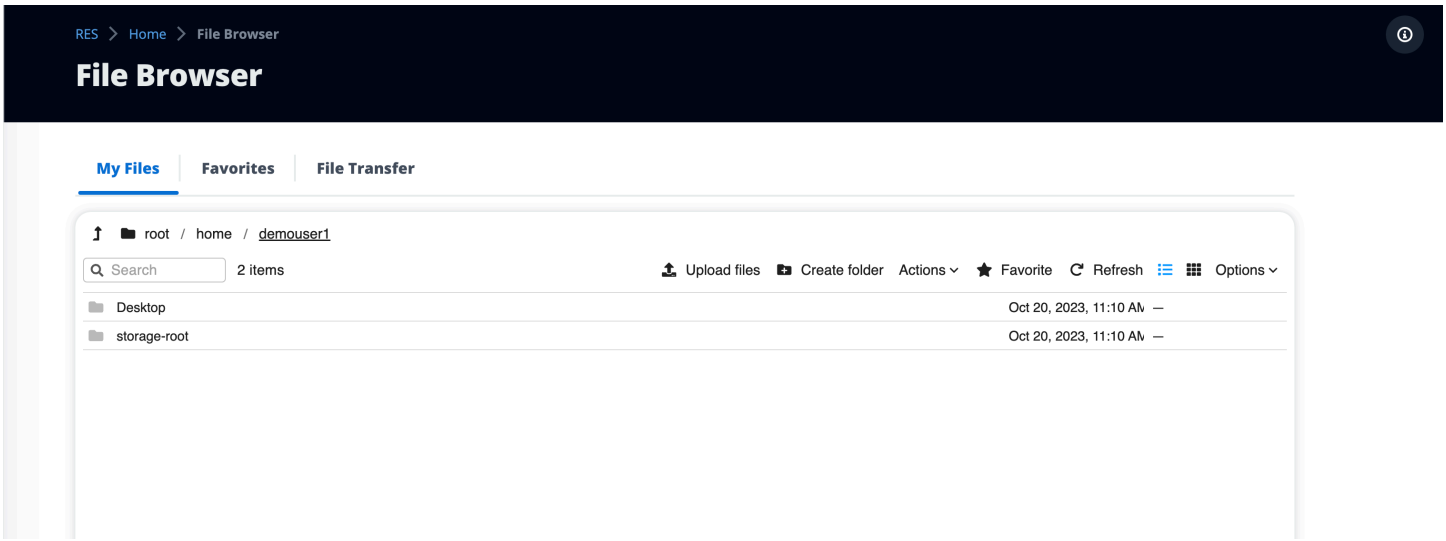
Per ulteriori informazioni sulle autorizzazioni, vedere. the section called “Policy di autorizzazione”

## 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 indicazioni riportate inAccedi 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 (AmazonEFS) è disponibile per tutti i nodi Linux. Per i nodi Linux e Windows, FSx for ONTAP è disponibile. L'aggiornamento dei file sul desktop virtuale equivale all'aggiornamento di un file tramite il terminale o il browser di file basato sul Web.

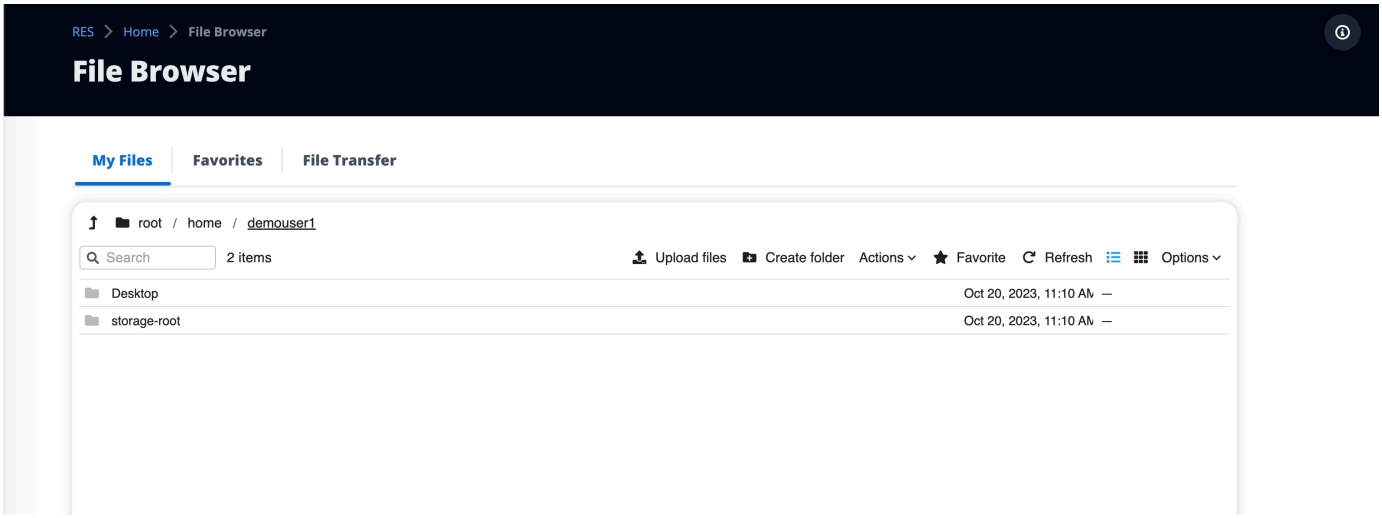



Argomenti

- Carica file
- Elimina uno o più file
- Gestisci i preferiti
- Modifica i file
- Trasferimento dei file

# Carica file

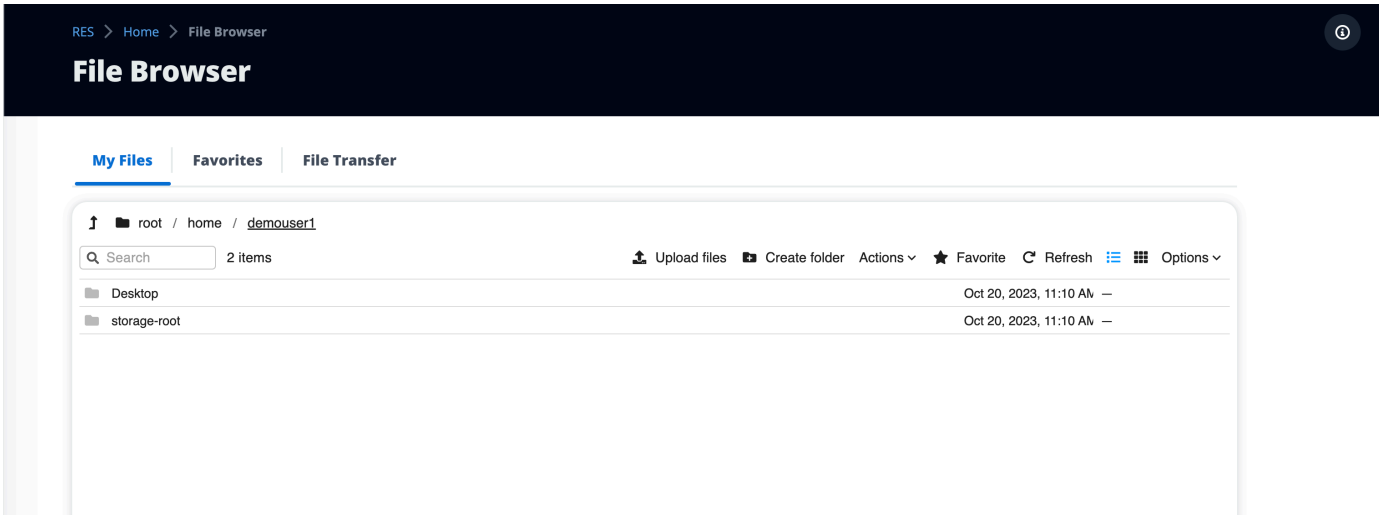
1. Scegli Carica file.




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

# Elimina uno o più file

1. Seleziona i file che desideri eliminare.



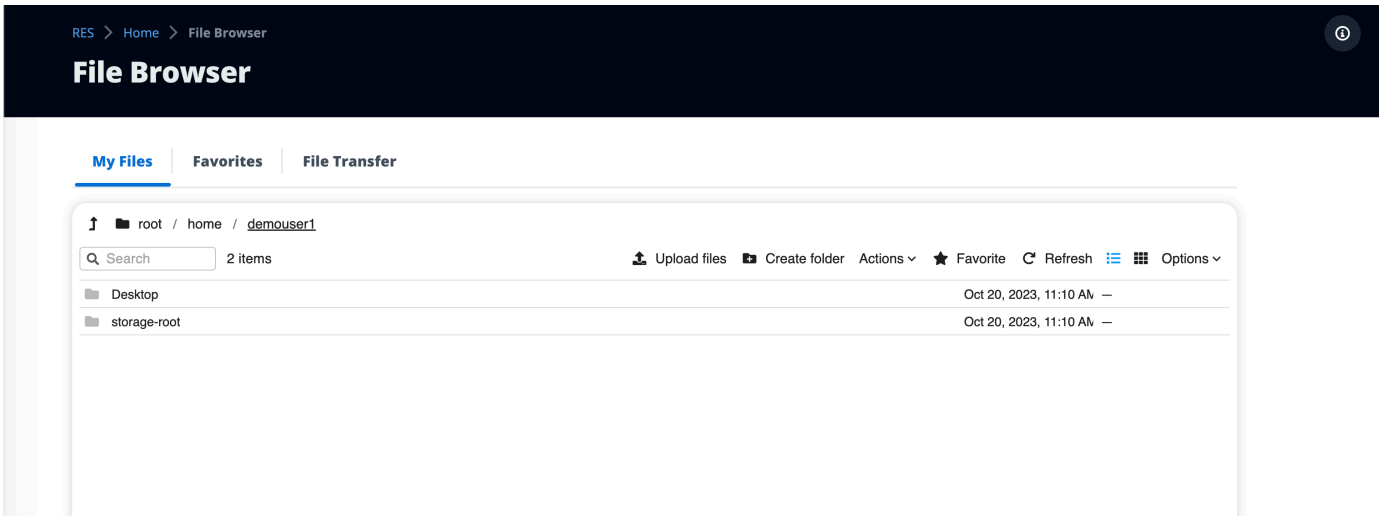

2. Scegli Azioni.
3. Seleziona Elimina file.

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

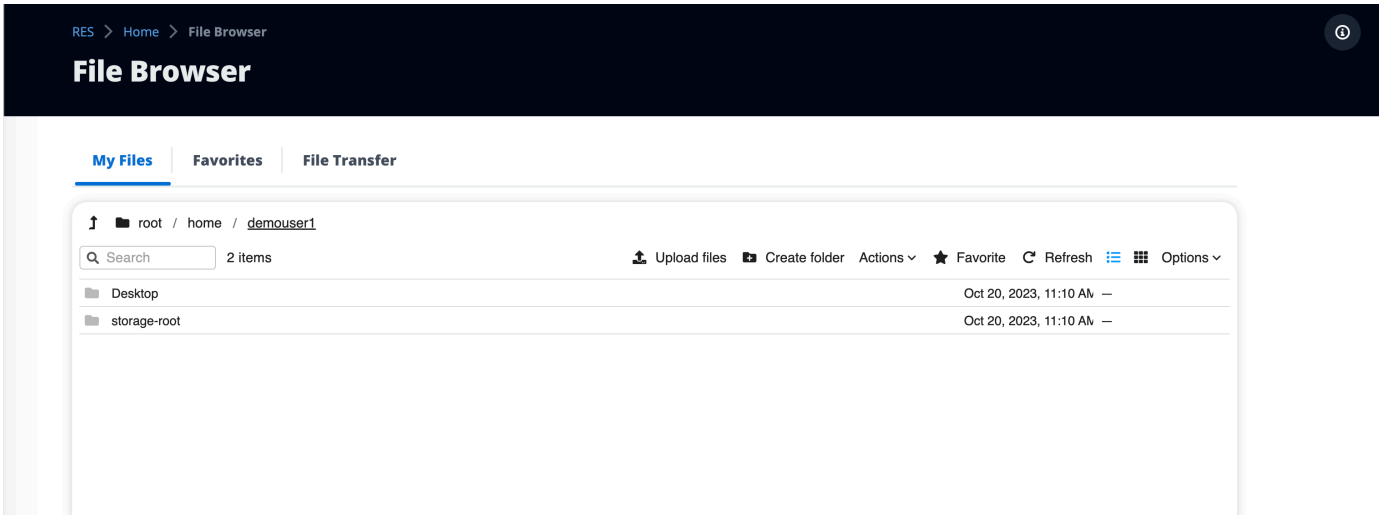
In alternativa, puoi fare clic con il pulsante destro del mouse su qualsiasi file o cartella e selezionare Preferito.

> **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. Seleziona il file che desideri aggiornare. Si aprirà un modale con il contenuto del file.

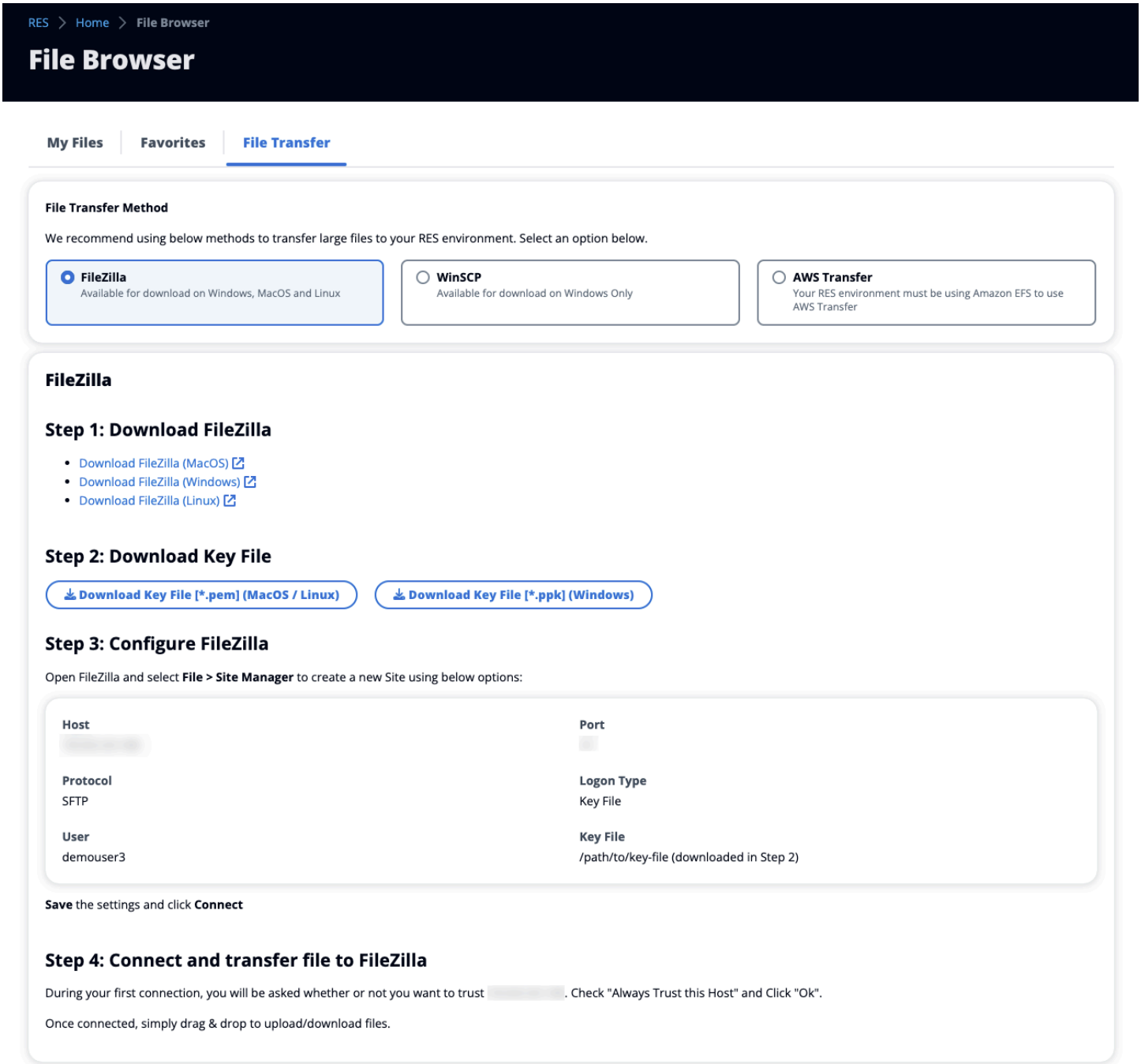



2. Effettua gli aggiornamenti e scegli Salva.

## 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)
- Windows SCP (Windows)
- AWS Transfer for FTP (AmazonEFS)


RES > Home > File Browser
File Browser
My Files
Favorites
File Transfer
File Transfer Method
We recommend using below methods to transfer large files to your RES environment. Select an option below.
FileZilla
Available for download on Windows, MacOS and Linux
WinSCP
Available for download on Windows Only
AWS Transfer
Your RES environment must be using Amazon EFS to use AWS Transfer
FileZilla
Step 1: Download FileZilla
Download FileZilla (MacOS)
Download FileZilla (Windows)
Download FileZilla (Linux)
Step 2: Download Key File
Download Key File [*.pem] (MacOS / Linux)
Download Key File [*.ppk] (Windows)
Step 3: Configure FileZilla
Open FileZilla and select File > Site Manager to create a new Site using below options:
Host
Port
Protocol
SFTP
Logon Type
Key File
User
demouser3
Key File
/path/to/key-file (downloaded in Step 2)
Save the settings and click Connect
Step 4: Connect and transfer file to FileZilla
During your first connection, you will be asked whether or not you want to trust . Check "Always Trust this Host" and Click "Ok".
Once connected, simply drag & drop to upload/download files.

# Risoluzione dei problemi

Questa sezione contiene informazioni su come monitorare il sistema e risolvere problemi specifici che possono verificarsi.

Argomenti



Contenuti dettagliati:

- (2024.08) I desktop virtuali non riescono a montare il bucket Amazon S3 di lettura/scrittura con bucket root e prefisso personalizzato ARN
- (2024.06) L'applicazione dell'istantanea non riesce quando il nome del gruppo AD contiene spazi
- (2024.04-2024.04.02) Limite di autorizzazione fornito non associato al ruolo delle istanze IAM VDI
- (2024.04.02 e versioni precedenti) NVIDIA Le istanze di Windows in ap-southeast-2 (Sydney) non vengono avviate
- (2024.04 e 2024.04.01) errore di eliminazione in RES GovCloud
- (2024.04 - 2024.04.02) Il desktop virtuale Linux potrebbe rimanere bloccato nello stato "" al riavvio RESUMING
- (2024.04.02 e versioni precedenti) Non riesce a sincronizzare gli utenti AD il cui SAMAccountName attributo include lettere maiuscole o caratteri speciali
- (2024.04.02 e versioni precedenti) La chiave privata per accedere all'host bastion non è valida
- (2024.06 e versioni precedenti) I membri del gruppo non sono stati sincronizzati durante la sincronizzazione AD RES
- (2024.06 e versioni precedenti) CVE -2024-6387, RegreSSHion, vulnerabilità di sicurezza in e Ubuntu RHEL9 VDIs

## Debug e monitoraggio generali

Questa sezione contiene informazioni sulla posizione in cui è possibile trovare le informazioni all'interno. RES

- Utili fonti di informazioni sui registri e sugli eventi
  - File di log sull'ambiente (EC2istanze Amazon)
  - CloudFormation pile
  - Guasti di sistema dovuti a un problema e riportati dall'attività del gruppo Amazon EC2 Auto Scaling
- Aspetto tipico EC2 della console Amazon
  - Host dell'infrastruttura
  - Host dell'infrastruttura e desktop virtuali
  - Host in uno stato terminato

  - Utili comandi di riferimento relativi ad Active Directory (AD)
- DCVDebug di Windows
- Trova informazioni sulla DCV versione di Amazon

## Utili fonti di informazioni sui registri e sugli eventi

Esistono varie fonti di informazioni conservate a cui è possibile fare riferimento per la risoluzione dei problemi e il monitoraggio.

### File di log sull'ambiente (EC2istanze Amazon)

I file di registro esistono nelle EC2 istanze Amazon utilizzate daRES. Il SSM Session Manager può essere utilizzato per aprire una sessione sull'istanza per l'esame di questi file.

Nelle istanze dell'infrastruttura come cluster-manager e vdc-controller, l'applicazione e altri registri sono disponibili nelle seguenti posizioni.

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

Su un desktop virtuale Linux, quanto segue contiene utili file di registro

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

Nelle istanze di desktop virtuale Windows, i log sono disponibili all'indirizzo

- PS C:\ ProgramData\nice\ dcv\ log

- PS C:\ ProgramData\nice\\ log DCVSessionManagerAgent

Su Windows, la registrazione di alcune applicazioni è disponibile all'indirizzo:

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

In Windows, i file dei NICE DCV certificati sono disponibili in:

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

Gruppi Amazon CloudWatch Log

Amazon EC2 e le risorse di AWS Lambda calcolo registrano le informazioni su Amazon CloudWatch Log Groups. Le voci di registro al loro interno possono fornire informazioni utili per la risoluzione di potenziali problemi o per informazioni generali.

Questi gruppi sono denominati come segue:

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

Quando si esaminano i gruppi di log, può essere utile filtrare utilizzando stringhe maiuscole e minuscole come le seguenti. Questo produrrà solo i messaggi contenenti le stringhe annotate.

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

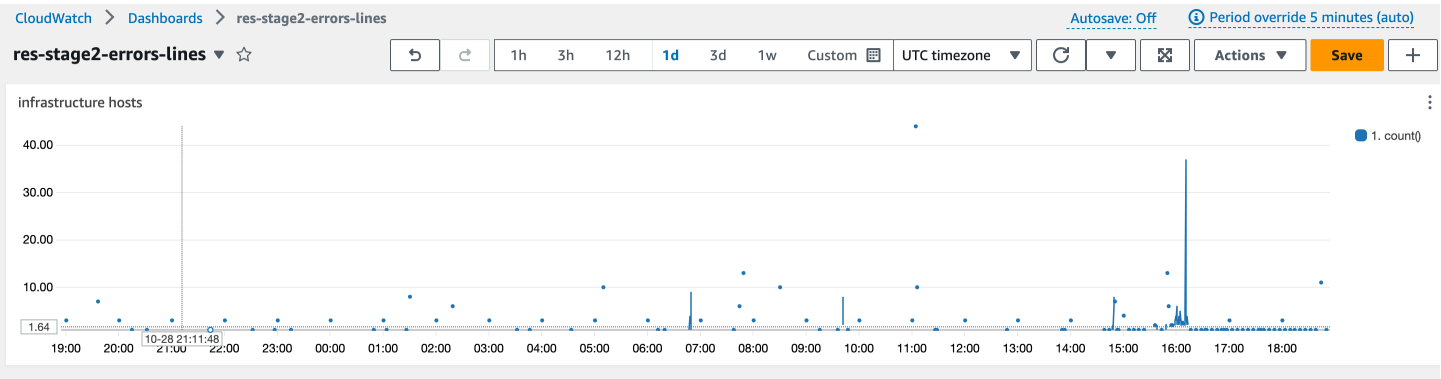
Un altro metodo di monitoraggio dei problemi consiste nel creare CloudWatch dashboard Amazon che contengano widget che visualizzano i dati di interesse.

Un esempio consiste nel creare un widget che conti l'occorrenza dell'errore delle stringhe ERROR e le rappresenti graficamente come linee. Questo metodo semplifica l'individuazione di potenziali problemi o tendenze che indicano che si è verificata una modifica del modello.

Di seguito è riportato un esempio di ciò per gli host dell'infrastruttura. Per utilizzarlo, concatenate le righe di query e sostituite `<region>` gli attributi `<envname>` and con i valori appropriati.

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

Un esempio di Dashboard potrebbe apparire come segue:




## CloudFormation pile

Gli CloudFormation stack creati durante la creazione dell'ambiente contengono risorse, eventi e informazioni di output associati alla configurazione dell'ambiente.

Per ciascuno degli stack, è possibile fare riferimento alla scheda Eventi, risorse e uscite per informazioni sugli stack.

RESpile:

- <envname>-bootstrap
- <envname>-ammasso
- <envname>-metriche
- <envname>- servizio di elenchi
- <envname>-fornitore di identità
- <envname>- archiviazione condivisa
- <envname>-gestore di cluster
- <envname>-vdc
- <envname>-bastione-host

Demo Environment Stack (se stai implementando un ambiente demo e non disponi di queste risorse esterne, puoi utilizzare le ricette AWS High Performance Compute per generare risorse per un ambiente demo).

- <envname>
- <envname>-Rete

- <envname>- DirectoryService
- <envname>-Archiviazione
- <envname>- WindowsManagementHost

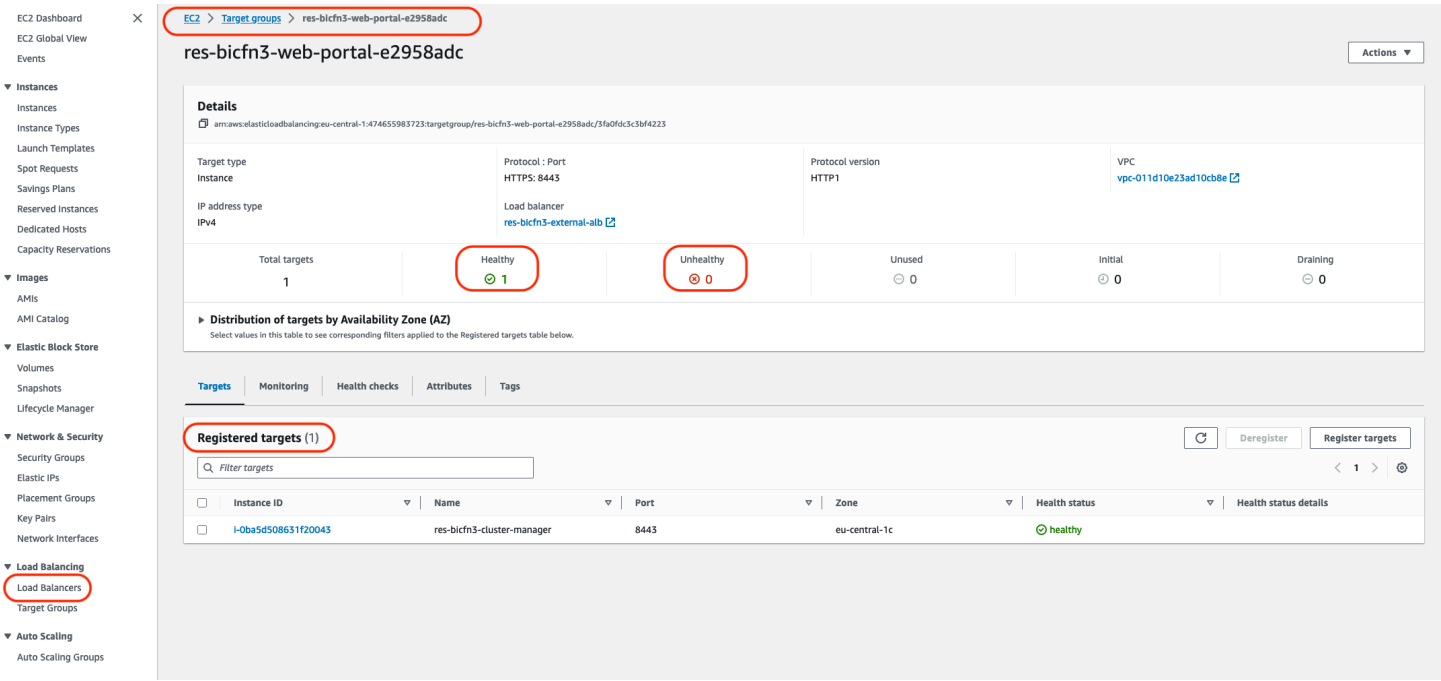
## Guasti di sistema dovuti a un problema e riportati dall'attività del gruppo Amazon EC2 Auto Scaling

Se RES UIs indicano errori del server, la causa potrebbe essere un'applicazione software o un altro problema.

Ciascuno dei gruppi di autoscaling delle EC2 istanze Amazon (ASGs) dell'infrastruttura contiene una scheda Attività che può essere utile per rilevare l'attività di scalabilità delle istanze. Se le pagine dell'interfaccia utente rilevano errori o non sono accessibili, controlla la presenza di più istanze terminate nella EC2 console Amazon e controlla la scheda Auto Scaling Group Activity per le ASG relative istanze per determinare se le istanze EC2 Amazon sono in ciclo.

In tal caso, utilizza il gruppo di CloudWatch log Amazon correlato per l'istanza per determinare se vengono registrati errori che potrebbero indicare la causa del problema. Potrebbe anche essere possibile utilizzare la console di SSM sessione per aprire una sessione su un'istanza in esecuzione di quel tipo ed esaminare i file di registro sull'istanza per determinare la causa prima che l'istanza venga contrassegnata come non integra e terminata dal. ASG

Se si verifica questo problema, la ASG console potrebbe mostrare attività simili alle seguenti.

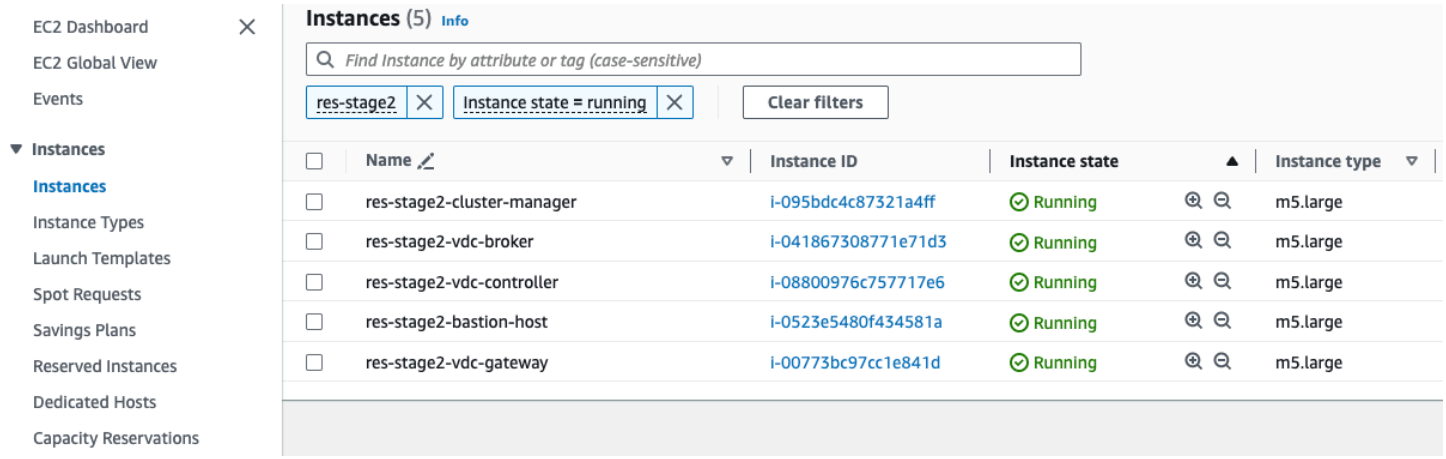


# Aspetto tipico EC2 della console Amazon

Questa sezione contiene schermate del sistema operativo in vari stati.

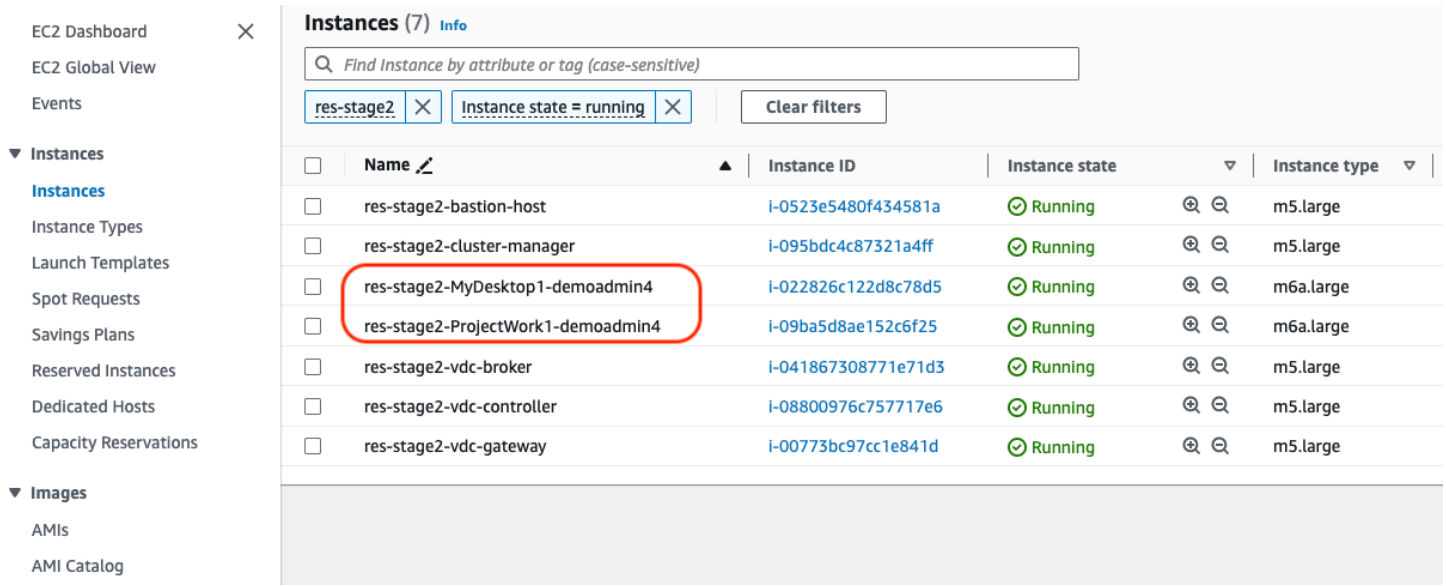
## Host dell'infrastruttura

La EC2 console Amazon, quando nessun desktop è in esecuzione, in genere ha un aspetto simile alla seguente. Le istanze mostrate sono l'RESinfrastruttura EC2 host di Amazon. Il prefisso nel nome di un'istanza è il nome dell'RESambiente.




## Host dell'infrastruttura e desktop virtuali

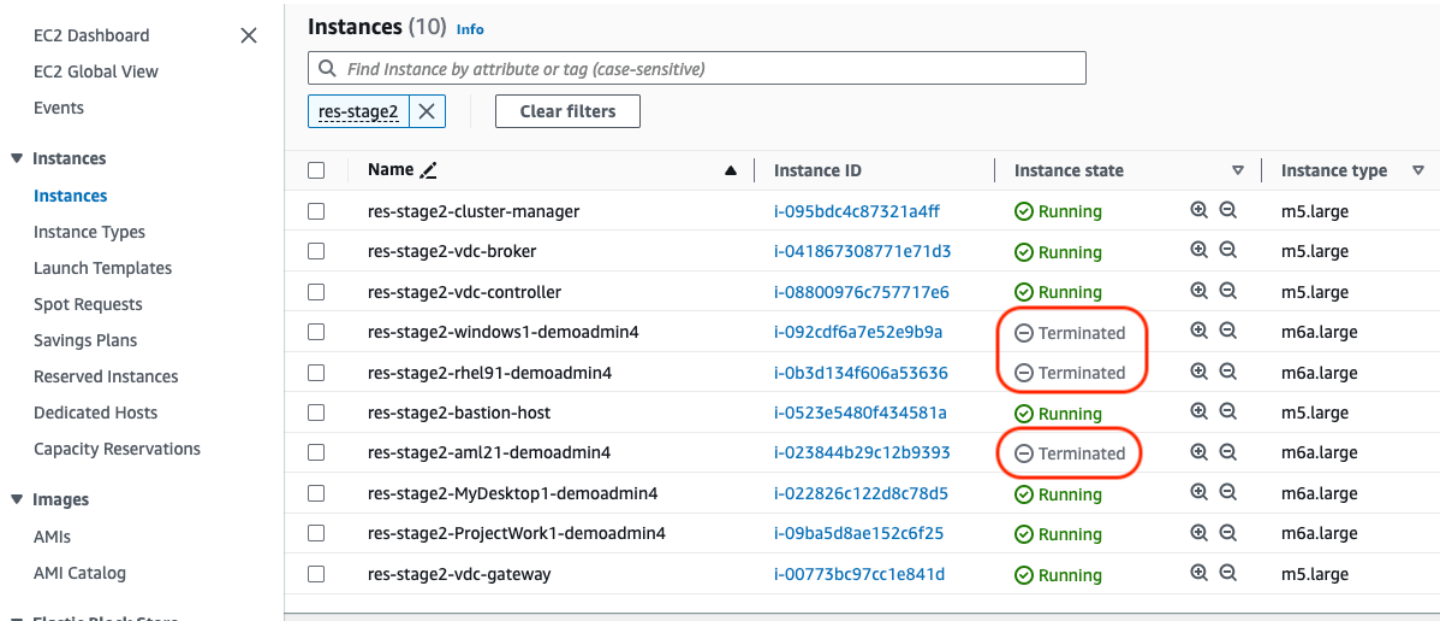
Nella EC2 console Amazon, quando i desktop virtuali sono in esecuzione, appaiono simili ai seguenti. In questo caso, i desktop virtuali sono indicati in rosso. Il suffisso del nome dell'istanza è l'utente che ha creato il desktop. Il nome al centro è il nome della sessione impostato al momento dell'avvio e può essere il "MyDesktop" predefinito o il nome impostato dall'utente.



## Host in uno stato terminato

Quando la EC2 console Amazon mostra istanze terminate, in genere si tratta di host desktop che sono stati terminati. Se la console include host di infrastruttura in uno stato terminato, in particolare se ce ne sono più dello stesso tipo, ciò potrebbe indicare che è in corso un problema di sistema.

L'immagine seguente mostra le istanze desktop che sono state terminate.




## Utili comandi di riferimento relativi ad Active Directory (AD)

Di seguito sono riportati alcuni esempi di comandi relativi a ldap che è possibile immettere negli host dell'infrastruttura per visualizzare le informazioni relative alla configurazione di AD. Il dominio e gli altri parametri utilizzati devono riflettere quelli immessi al momento della creazione dell'ambiente.

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

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

# DCVDebug di Windows

Su un desktop Windows, è possibile elencare la sessione associata utilizzando quanto segue:

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

## Trova informazioni sulla DCV versione di Amazon

Amazon DCV viene utilizzato per sessioni di desktop virtuali. AWS Amazon DCV. I seguenti esempi mostrano come determinare la versione del DCV software installato.

Linux

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

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

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

Windows

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

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

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

# Problema RunBooks

La sezione seguente contiene i problemi che possono verificarsi, come rilevarli e suggerimenti su come risolverli.

- Problemi di installazione
  - Desidero configurare domini personalizzati dopo l'installazione RES

- Errore di accesso all'ambiente demo durante la gestione della richiesta di autenticazione al provider di identità

## Problemi di installazione

Argomenti

- Desidero configurare domini personalizzati dopo l'installazione RES
- AWS CloudFormation lo stack non riesce a creare il messaggio «messaggio non riuscito ricevuto»WaitCondition . Errore: Stati. TaskFailed»
- Notifica e-mail non ricevuta dopo che gli AWS CloudFormation stack sono stati creati correttamente
- Istanze in ciclo o vdc-controller in stato di errore
- Impossibile eliminare CloudFormation lo stack di ambiente a causa di un errore dell'oggetto dipendente
- Errore rilevato per il parametro di CIDR blocco durante la creazione dell'ambiente
- CloudFormation errore di creazione dello stack durante la creazione dell'ambiente
- La creazione dello stack di risorse esterne (demo) non riesce con _ AdDomainAdminNode CREATE FAILED

.....

### Desidero configurare domini personalizzati dopo l'installazione RES

> **Note**
>
> Prerequisiti: è necessario archiviare il certificato e PrivateKey il contenuto in un segreto di Secrets Manager prima di eseguire questi passaggi.

Aggiungere certificati al client Web

1. Aggiorna il certificato allegato al listener del load balancer external-alb:

   a. Passa al sistema di bilanciamento del carico RES esterno nella AWS console sotto > Load Balancing > Load Balancers. EC2

b. Cerca il load balancer che segue la convenzione di denominazione. *<env-name>*-external-alb

c. Controlla gli ascoltatori collegati al sistema di bilanciamento del carico.

d. Aggiorna il listener a cui è allegato un TLS certificato DefaultSSL/con i dettagli del nuovo certificato.

e. Salvare le modifiche.

2. Nella tabella delle impostazioni del cluster:

a. Trova la tabella delle impostazioni del cluster in DynamoDB -> Tabelle ->. *<env-name>*.cluster-settings

b. Vai a Esplora gli elementi e filtra per attributo: nome «chiave», tipo «stringa», condizione «contiene» e valore «external_alb».

c. Impostato su True. cluster.load_balancers.external_alb.certificates.provided

d. Aggiorna il valore dicluster.load_balancers.external_alb.certificates.custom_dns_name. Questo è il nome di dominio personalizzato per l'interfaccia utente web.

e. Aggiorna il valore dicluster.load_balancers.external_alb.certificates.acm_certificate_arn. Questo è l'Amazon Resource Name (ARN) per il certificato corrispondente memorizzato in Amazon Certificate Manager (ACM).

3. Aggiorna il record di sottodominio Route53 corrispondente che hai creato per il tuo client web in modo che punti al DNS nome del bilanciatore di carico alb esterno. <env-name>-external-alb

4. Se SSO è già configurato nell'ambiente, riconfiguralo SSO con gli stessi input utilizzati inizialmente dal pulsante Impostazioni generali > Identity Provider > Single Sign On > Status > Modifica nel portale web. RES

Aggiungi certificati al VDIs

1. Concedi all'RESapplicazione il permesso di eseguire un' GetSecret operazione sul segreto aggiungendo i seguenti tag ai segreti:

- res:EnvironmentName : *<env-name>*
- res:ModuleName : virtual-desktop-controller

2. Nella tabella delle impostazioni del cluster:

   a. Trova la tabella delle impostazioni del cluster in DynamoDB -> Tabelle ->. `<env-name>.cluster-settings`

   b. Vai a Esplora gli elementi e filtra per attributo: nome «chiave», tipo «stringa», condizione «contiene» e valore «dcv_connection_gateway».

   c. Impostato su True. `vdc.dcv_connection_gateway.certificate.provided`

   d. Aggiorna il valore divdc.`dcv_connection_gateway.certificate.custom_dns_name`. Questo è il nome di dominio personalizzato per VDI l'accesso.

   e. Aggiorna il valore divdc.`dcv_connection_gateway.certificate.certificate_secret_arn`. Questo è ARN il segreto che contiene il contenuto del certificato.

   f. Aggiorna il valore divdc.`dcv_connection_gateway.certificate.private_key_secret_arn`. Questo è ARN il segreto che contiene il contenuto della chiave privata.

3. Aggiorna il modello di avvio utilizzato per l'istanza del gateway:

   a. Apri il gruppo Auto Scaling nella AWS Console sotto EC2> Auto Scaling > Auto Scaling Groups.

   b. Seleziona il gruppo di auto scaling del gateway che corrisponde all'RESambiente. Il nome segue la convenzione di denominazione. `<env-name>-vdc-gateway-asg`

   c. Trova e apri il Launch Template nella sezione dei dettagli.

   d. In Dettagli > Azioni > scegli Modifica modello (Crea nuova versione).

   e. Scorri verso il basso fino a Dettagli avanzati.

   f. Scorri fino in fondo, fino a Dati utente.

   g. Cerca le parole `CERTIFICATE_SECRET_ARN` e`PRIVATE_KEY_SECRET_ARN`. Aggiorna questi valori con quelli ARNs assegnati ai segreti che contengono il certificato (vedi passaggio 2.c) e la chiave privata (vedi passaggio 2.d).

   h. Assicurati che il gruppo Auto Scaling sia configurato per utilizzare la versione recentemente creata del modello di avvio (dalla pagina del gruppo Auto Scaling).

4. Aggiorna il record del sottodominio Route53 corrispondente che hai creato per i tuoi desktop virtuali in modo che punti al DNS nome del sistema di bilanciamento del carico nlb esterno:. `<env-name>-external-nlb`

5. Termina l'istanza dcv-gateway esistente e attendi che ne venga avviata una nuova*<env-name>*-vdc-gateway.

.....

## AWS CloudFormation lo stack non riesce a creare il messaggio «messaggio non riuscito ricevuto»WaitCondition . 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 gli AWS CloudFormation stack sono stati creati 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 possibile accedervi, elimina e ridistribuisci l'ambiente Research and Engineering Studio.
2. Controlla la EC2 console di Amazon per le prove delle istanze cicliche.

   Se ci sono EC2 istanze Amazon con il <envname> prefisso che sembrano terminate 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 risorse esterne, conferma che le sottoreti private e pubbliche e gli altri parametri selezionati siano stati creati dallo stack. VPC

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 le tue risorse esterne, verifica che la rete e Active Directory corrispondano alla configurazione prevista.

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

.....

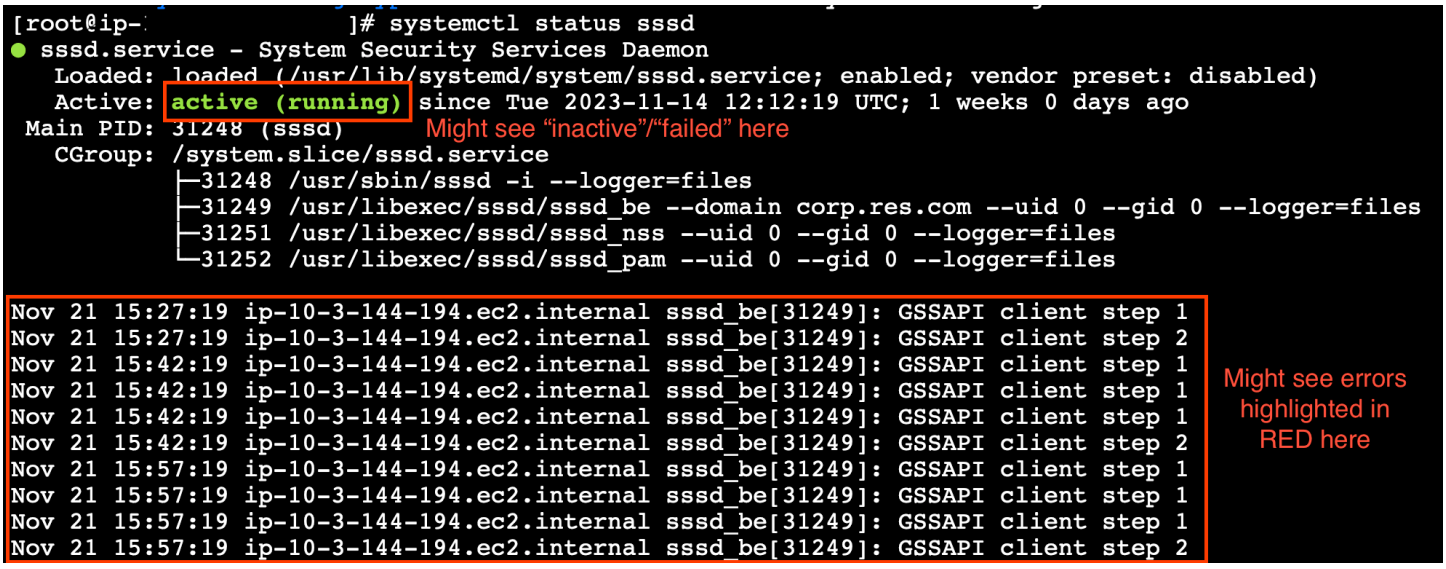
## Istanze in ciclo o vdc-controller in stato di errore

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

Per verificare il problema:

1. Dalla riga di comando, avviate una sessione con SSM l'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.



SSMregistro degli errori

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 avere 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 RES dello stack.
   - 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, eliminate il cluster-manager e il vdc-controller 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 RES directory e scegli Azioni.

iii. Seleziona 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, quindi scegli Testo normale.

iv. Scegli Modifica.

v. Imposta una nuova password per l' ServiceAccount utente e scegli Salva.

5. Se hai aggiornato il valore, 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'EC2istanza Amazon che è stata lanciata in una sottorete o in un gruppo di sicurezza RES creato utilizzando la Console. AWS

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

.....

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

Durante la creazione di un ambiente, viene visualizzato un errore per il parametro di CIDR blocco 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 _ AdDomainAdminNode CREATE FAILED

Se la creazione dello stack dell'ambiente demo fallisce con il seguente errore, potrebbe essere dovuto all'applicazione di EC2 patch da parte di Amazon in modo imprevisto 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 SSM documento relativo all'applicazione di patch coincide con l'avvio di un'istanza.
3. Nei file di registro per le EC2 istanze Amazon 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 almeno 15 minuti dopo l'RESavvio.

.....

## 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 SSO configurazione, consulta:

- the section called “Configurazione SSO con Identity Center IAM”
- the section called “Configurazione del provider di identità per SSO”

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

Argomenti

- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere al mio Research and Engineering Studio sulle AWS risorse
- 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 da 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)

.....

### Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'PassRole azione iam:, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo aRES.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente di nome marymajor tenta di utilizzare la console per eseguire un'azione in. RES Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le politiche di Mary devono essere aggiornate per consentirle di eseguire l'azione iam:PassRole . Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

.....

## Voglio consentire a persone esterne al mio AWS account di accedere al mio Research and Engineering Studio sulle AWS risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere come fornire l'accesso alle tue risorse su più AWS account di tua proprietà, consulta Fornire l'accesso a un IAM utente in un altro AWS account di tua proprietà nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta Fornire l'accesso agli AWS account di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo dei ruoli e delle politiche basate sulle risorse per l'accesso tra account diversi, consulta In che modo i IAM ruoli differiscono dalle politiche basate sulle risorse nella Guida per l'utente. IAM

.....

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

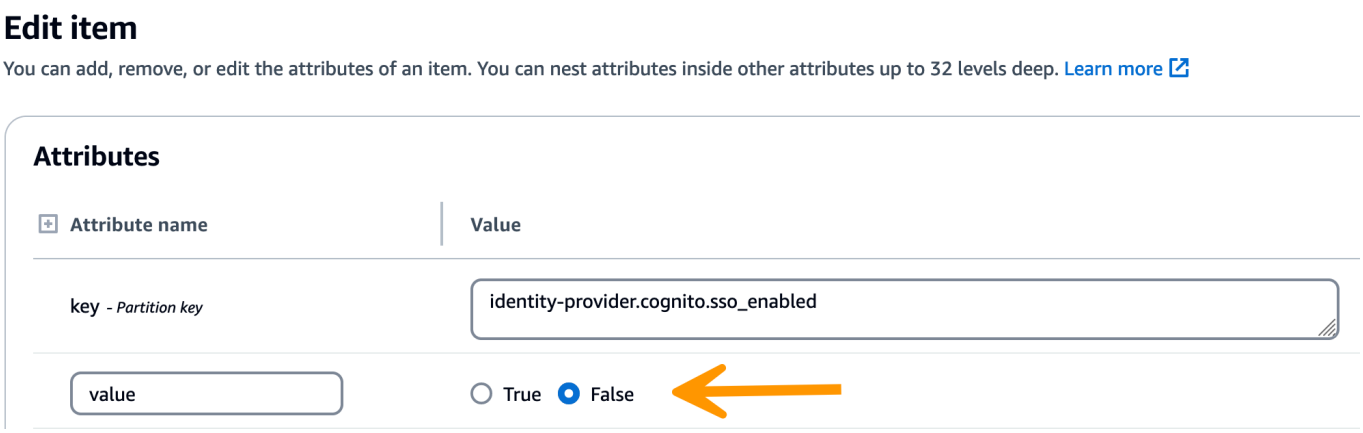
Questo problema si verifica quando l'SSOintegrazione non è configurata correttamente. Per determinare il problema, controlla i registri delle istanze del controller e verifica la presenza di errori nelle impostazioni di configurazione.

Per controllare i log:

1. Apri la CloudWatch console.
2. In Gruppi di log, 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
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. Seleziona Esegui.
6. Nella stringa restituita, verificate che i valori di SSO configurazione siano corretti. Se non sono corretti, modificate il valore della chiave sso_enabled su False.




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

.....

## Errore «Utente non trovato» durante il tentativo di accesso

Se un utente riceve l'errore «Utente non trovato» quando tenta di accedere all'RESinterfaccia e l'utente è presente in Active Directory:

- Se l'utente non è presente in RES e l'hai recentemente aggiunto ad AD
  - È possibile che l'utente non sia ancora sincronizzato con. RES RESsi 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 i passaggi indicati in. Utente aggiunto in Active Directory, ma mancante da RES
- Se l'utente è presente inRES:
  1. Assicurati che la mappatura degli attributi sia configurata correttamente. Per ulteriori informazioni, consulta Configurazione del provider di identità per il Single Sign-on () SSO.
  2. Assicurati che l'SAMLoggetto e l'SAMLe-mail corrispondano entrambi all'indirizzo e-mail dell'utente.

.....

## Utente aggiunto in Active Directory, ma mancante da RES

Se hai aggiunto un utente ad Active Directory ma non è presenteRES, è necessario attivare la sincronizzazione AD. La sincronizzazione AD viene eseguita ogni ora da una funzione Lambda che importa le voci AD RES nell'ambiente. A volte, 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 SQSconsole Amazon.
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 l'ID del gruppo di messaggi, inserisci: **`adsync.sync-from-ad`**
6. Per ID di deduplicazione dei messaggi, inserisci una stringa alfanumerica casuale. Questa immissione deve essere diversa da tutte le chiamate effettuate negli ultimi cinque minuti o 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 IDP di ricerca LDAP.

.....

## Storage

Argomenti

- Ho creato il file system tramite RES ma non si monta sugli host VDI
- Ho effettuato l'onboarding di un file system tramite RES ma non viene montato sugli host VDI
- Non sono in grado di leggere/scrivere dagli host VDI
- Ho creato Amazon FSx per NetApp ONTAP from RES ma non è entrato a far parte del mio dominio

.....

## Ho creato il file system tramite RES ma non si monta sugli host VDI

I file system devono essere nello stato «Disponibile» prima di poter essere montati dagli VDI host. Segui i passaggi seguenti per verificare che il file system sia nello stato richiesto.

Amazon EFS

1. Vai alla EFSconsole Amazon.
2. Verifica che lo stato del file system sia Disponibile.
3. Se lo stato del file system non è Disponibile, attendi prima di avviare VDI gli host.

Amazon FSx ONTAP

1. Vai alla FSxconsole Amazon.
2. Verifica che lo stato sia disponibile.
3. Se lo stato non è disponibile, attendi prima di avviare VDI gli host.

.....

## Ho effettuato l'onboarding di un file system tramite RES ma non viene montato sugli host VDI

I file system su cui è stato effettuato l'onboard RES devono avere le regole di gruppo di sicurezza richieste configurate per consentire agli VDI host di montare i file system. Poiché questi file system vengono creati esternamenteRES, RES non gestisce le regole dei gruppi di sicurezza associati.

Il gruppo di sicurezza associato ai file system integrati dovrebbe consentire il seguente traffico in entrata:

- NFStraffico (porta: 2049) proveniente dagli host linux VDC
- SMBtraffico (porta: 445) proveniente dagli host Windows VDC

.....

## Non sono in grado di leggere/scrivere dagli host VDI

ONTAPsupporti UNIX NTFS e stile MIXED di sicurezza per i volumi. Gli stili di sicurezza determinano il tipo di autorizzazioni ONTAP utilizzate per controllare l'accesso ai dati e il tipo di client che può modificare tali autorizzazioni.

Ad esempio, se un volume utilizza uno stile UNIX di sicurezza, SMB i client possono comunque accedere ai dati (a condizione che si autentichino e autorizzino correttamente) grazie alla natura multiprotocollo di. ONTAP Tuttavia, ONTAP utilizza UNIX autorizzazioni che solo UNIX i client possono modificare utilizzando strumenti nativi.

Esempi di casi d'uso per la gestione delle autorizzazioni

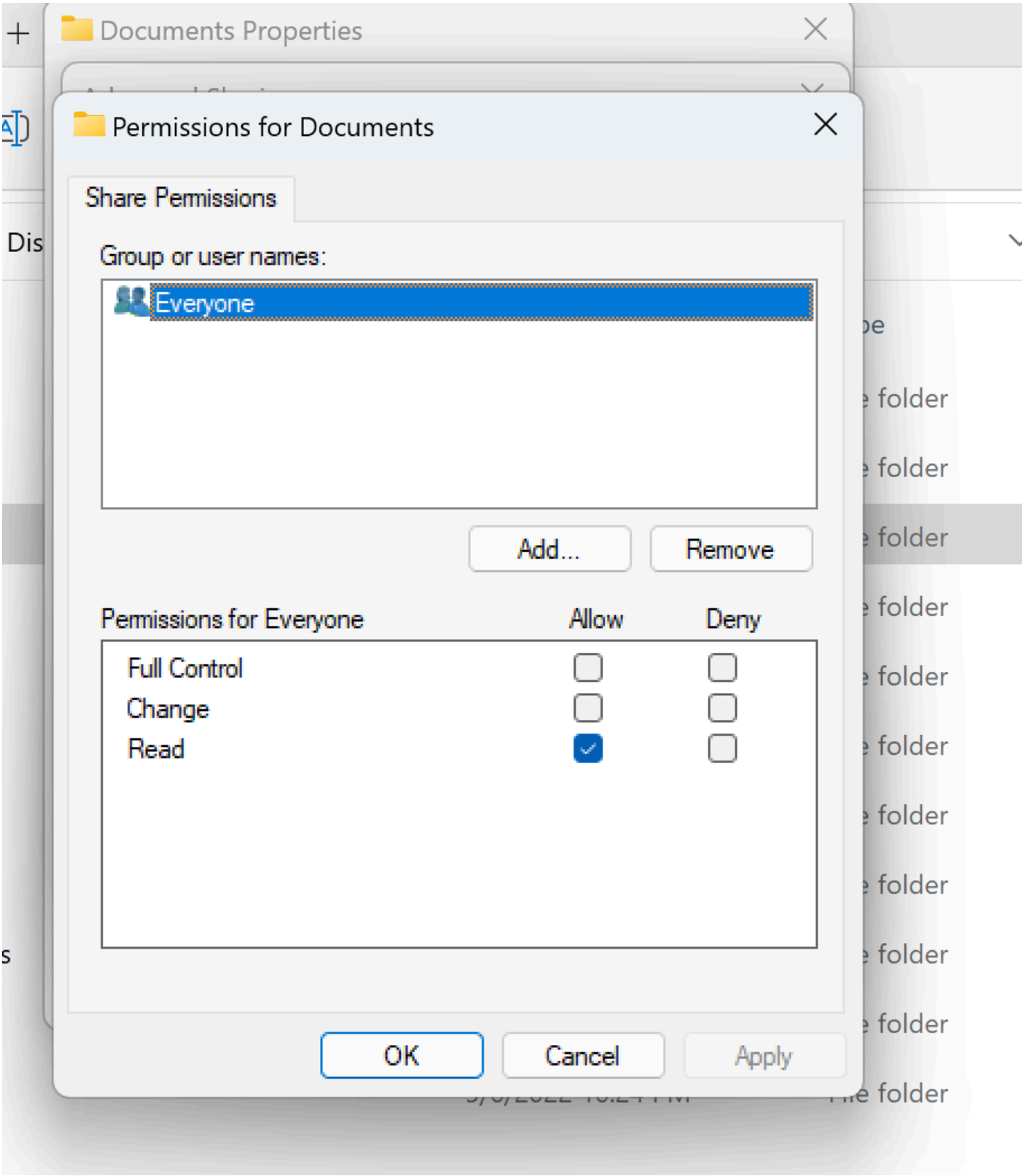
Utilizzo di UNIX style volume con carichi di lavoro Linux

Le autorizzazioni possono essere configurate dal sudoer per altri utenti. Ad esempio, quanto segue fornirebbe a tutti i membri le autorizzazioni `<group-ID>` complete di lettura/scrittura sulla directory: `/<project-name>`

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

Utilizzo di NTFS style volume con carichi di lavoro Linux e Windows

Le autorizzazioni di condivisione possono essere configurate utilizzando le proprietà di condivisione di una cartella particolare. Ad esempio, in base a un utente `user_01` e a una cartella`myfolder`, è possibile impostare le autorizzazioni di `Full ControlChange`, o `Read` su `Allow` o: `Deny`


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

Se il volume verrà utilizzato da client Linux e Windows, è necessario impostare una mappatura dei nomi in SVM cui assocerà qualsiasi nome utente Linux allo stesso nome utente con il formato del nome di dominio di rete BIOS dominio dominio\ nome utente. Questo è necessario per tradurre tra utenti Linux e Windows. Per riferimento, consulta Abilitazione dei carichi di lavoro multiprotocollo con Amazon FSx for. NetApp ONTAP

.....

## Ho creato Amazon FSx per NetApp ONTAP from RES ma non è entrato a far parte del mio dominio

Attualmente, quando crei Amazon FSx for NetApp ONTAP dalla RES console, il file system viene fornito ma non entra a far parte del dominio. Per aggiungere il ONTAP file system creato SVM al tuo dominio, consulta Registrazione SVMs a Microsoft Active Directory e segui i passaggi sulla FSxconsole Amazon. Assicurati che le autorizzazioni richieste siano delegate all'account Amazon FSx Service in AD. Una volta SVM aggiunto correttamente al dominio, vai su SVM Riepilogo > Endpoints > SMB DNS nome e copia il DNS nome perché ti servirà in seguito.

Dopo averlo aggiunto al dominio, modifica la chiave di SMB DNS configurazione nella tabella DynamoDB delle impostazioni del cluster:

1. Vai alla console Amazon DynamoDB.
2. Scegli Tabelle, quindi scegli. `<stack-name>-cluster-settings`
3. In Esplora gli elementi della tabella, espandi Filtri e inserisci il seguente filtro:
   - Nome dell'attributo: chiave
   - Condizione: uguale a
   - Valore - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. Seleziona l'articolo restituito, quindi Azioni, Modifica articolo.
5. Aggiorna il valore con il SMB DNS nome che hai copiato in precedenza.
6. Selezionare Save and close (Salva e chiudi).

Inoltre, assicurati che il gruppo di sicurezza associato al file system consenta il traffico come consigliato in File System Access Control with Amazon VPC. VDII nuovi host che utilizzano il file system saranno ora in grado di montare il dominio unito SVM e il file system.

In alternativa, è possibile effettuare l'onboarding di un file system esistente che fa già parte del dominio utilizzando la funzionalità RES Onboard File System: da Environment Management scegli File Systems, Onboard File System.

.....

# Snapshot

Argomenti



.....

## Lo stato di un'istantanea è Fallito

Nella pagina RES Snapshot, se uno snapshot ha lo stato Failed, la causa può essere determinata accedendo al gruppo di CloudWatch log di Amazon per il gestore del cluster per il momento in cui si è verificato l'errore.

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

.....

## Uno snapshot non viene applicato con i log che indicano che le tabelle non possono essere importate.

Se un'istantanea scattata da un ambiente precedente non viene applicata in un nuovo ambiente, esamina i CloudWatch log di Cluster-Manager per identificare il problema. Se il problema indica che le tabelle richieste dal cloud non possono essere importate, verifica che lo snapshot sia in uno stato valido.

1. Scaricate il file metadata.json e verificate che ExportStatus per le varie tabelle sia impostato lo stato. COMPLETED Assicurati che il campo sia impostato nelle varie tabelle. `ExportManifest` Se non trovi i campi precedenti impostati, l'istantanea è in uno stato non valido e non può essere utilizzata con la funzionalità di applicazione dell'istantanea.
2. Dopo aver avviato la creazione di un'istantanea, assicurati che lo stato dell'istantanea sia attivato. COMPLETED RES Il processo di creazione dell'istantanea richiede da 5 a 10 minuti. Ricarica o rivisita la pagina di gestione delle istantanee per assicurarti che l'istantanea sia stata creata correttamente. Ciò garantirà che l'istantanea creata sia in uno stato valido.

.....

# Infrastruttura

Argomenti

- Load Balancer si rivolge a gruppi target senza istanze integre

.....

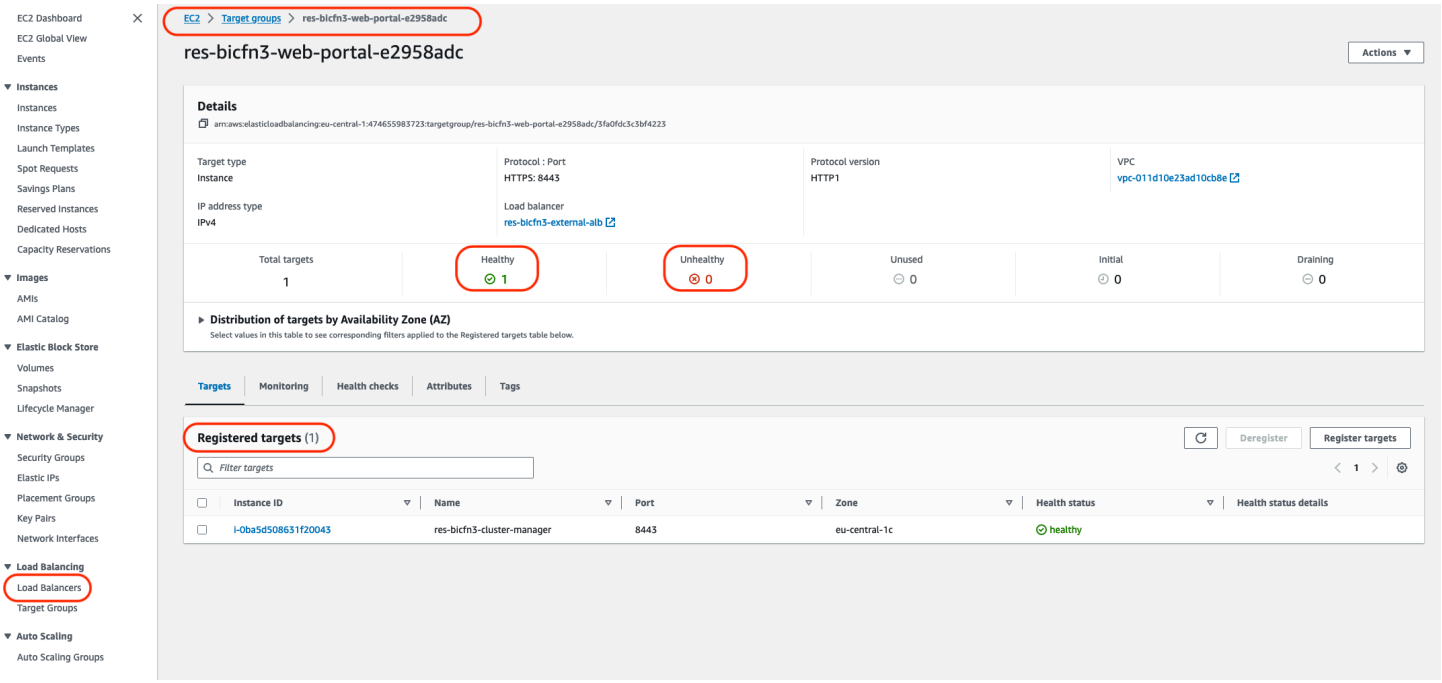
## Load Balancer si rivolge a gruppi target senza istanze integre

Se nell'interfaccia utente compaiono problemi come messaggi di errore del server o le sessioni desktop non riescono a connettersi, ciò potrebbe indicare un problema nell'infrastruttura delle EC2 istanze Amazon.

I metodi per determinare l'origine del problema consistono innanzitutto nel controllare la EC2 console Amazon per eventuali EC2 istanze Amazon che sembrano terminare ripetutamente e essere sostituite da nuove istanze. In tal caso, il controllo dei CloudWatch log di Amazon può determinarne la causa.

Un altro metodo è controllare i sistemi di bilanciamento del carico nel sistema. Un'indicazione che potrebbero esserci problemi di sistema è se alcuni sistemi di bilanciamento del carico presenti sulla EC2 console Amazon non mostrano alcuna istanza integra registrata.

Di seguito è riportato un esempio di aspetto normale:




Se la voce Healthy è 0, ciò indica che nessuna EC2 istanza Amazon è disponibile per elaborare le richieste.

Se la voce Unhealthy è diversa da 0, ciò indica che EC2 un'istanza Amazon potrebbe essere in ciclo. Ciò può essere dovuto al fatto che il software delle applicazioni installate non supera i controlli sanitari.

Se entrambe le voci Healthy e Unhealthy sono 0, ciò indica una potenziale configurazione errata della rete. Ad esempio, le sottoreti pubbliche e private potrebbero non avere corrispondenze. AZs Se si verifica questa condizione, è possibile che sulla console sia presente un testo aggiuntivo che indica l'esistenza dello stato della rete.

.....

# Avvio di desktop virtuali

Argomenti

- Un desktop virtuale che in precedenza funzionava non è più in grado di connettersi correttamente
- Sono in grado di avviare solo 5 desktop virtuali
- I tentativi di connessione su Desktop Windows falliscono e viene visualizzato il messaggio «La connessione è stata chiusa. Errore di trasporto»
- VDIsbloccato nello stato di Provisioning

- VDIsentra nello stato di errore dopo l'avvio

.....

## Un desktop virtuale che in precedenza funzionava non è più in grado di connettersi correttamente

Se una connessione desktop si chiude o non riesci più a connetterti ad essa, il problema potrebbe essere dovuto al guasto dell'EC2istanza Amazon sottostante o l'istanza Amazon EC2 potrebbe essere stata terminata o interrotta al di fuori dell'ambiente. RES Lo stato dell'interfaccia utente di amministrazione può continuare a mostrare uno stato pronto, ma i tentativi di connessione non riescono.

La EC2 console Amazon deve essere utilizzata per determinare se l'istanza è stata interrotta o interrotta. Se interrotta, prova a riavviarla. Se lo stato viene terminato, sarà necessario creare un altro desktop. Tutti i dati archiviati nella home directory dell'utente dovrebbero essere ancora disponibili all'avvio della nuova istanza.

Se l'istanza che aveva avuto esito negativo in precedenza è ancora presente nell'interfaccia utente di amministrazione, potrebbe essere necessario chiuderla utilizzando l'interfaccia utente di amministrazione.

.....

## Sono in grado di avviare solo 5 desktop virtuali

Il limite predefinito per il numero di desktop virtuali che un utente può avviare è 5. Questo può essere modificato da un amministratore utilizzando l'interfaccia utente di amministrazione come segue:

- Vai a Impostazioni del desktop.
- Seleziona la scheda Server.
- Nel pannello DCVSessione, fai clic sull'icona di modifica a destra.
- Modificate il valore in Sessioni consentite per utente con il nuovo valore desiderato.
- Scegli Invia.
- Aggiorna la pagina per confermare che la nuova impostazione è attiva.

.....

## I tentativi di connessione su Desktop Windows falliscono e viene visualizzato il messaggio «La connessione è stata chiusa. Errore di trasporto»

Se una connessione desktop Windows fallisce e viene visualizzato l'errore dell'interfaccia utente «La connessione è stata chiusa. «Errore di trasporto», la causa può essere dovuta a un problema nel software del DCV server relativo alla creazione di certificati nell'istanza di Windows.

Il gruppo di CloudWatch log di Amazon `<envname>/vdc/dcv-connection-gateway` può registrare l'errore del tentativo di connessione con messaggi simili ai seguenti:

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]

Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

In tal caso, una soluzione potrebbe essere quella di utilizzare il SSM Session Manager per aprire una connessione all'istanza di Windows e rimuovere i seguenti 2 file relativi al certificato:

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

I file devono essere ricreati automaticamente e un successivo tentativo di connessione potrebbe avere successo.

Se questo metodo risolve il problema e se i nuovi avvii dei desktop Windows generano lo stesso errore, utilizzate la funzione Create Software Stack per creare un nuovo stack software Windows dell'istanza fissa con i file di certificato rigenerati. Ciò può produrre uno stack di software Windows che può essere utilizzato per avvii e connessioni di successo.

.....

## VDIsbloccato nello stato di Provisioning

Se il lancio di un desktop rimane nello stato di provisioning nell'interfaccia utente di amministrazione, ciò può essere dovuto a diversi motivi.

Per determinare la causa, esamina i file di registro sull'istanza desktop e cerca gli errori che potrebbero causare il problema. Questo documento contiene un elenco di file di log e gruppi di CloudWatch log Amazon che contengono informazioni pertinenti nella sezione denominata Fonti utili di informazioni su log ed eventi.

Di seguito sono elencate le possibili cause di questo problema.

- L'AMIid utilizzato è stato registrato come stack software ma non è supportato da. RES

  Lo script di provisioning bootstrap non è stato completato perché Amazon Machine Image (AMI) non dispone della configurazione o degli strumenti previsti richiesti. I file di registro sull'istanza, ad esempio `/root/bootstrap/logs/` su un'istanza Linux, possono contenere informazioni utili in merito. AMIsGli id presi dal AWS Marketplace potrebbero non funzionare per le istanze RES desktop. Richiedono dei test per confermare se sono supportati.
- Gli script dei dati utente non vengono eseguiti quando l'istanza del desktop virtuale di Windows viene avviata da un'istanza personalizzataAMI.

  Per impostazione predefinita, gli script dei dati utente vengono eseguiti una sola volta all'avvio di un'EC2istanza Amazon. Se ne crei un'istanza AMI da un'istanza di desktop virtuale esistente, quindi registri uno stack software con AMI e provi ad avviare un altro desktop virtuale con questo stack software, gli script dei dati utente non verranno eseguiti sulla nuova istanza di desktop virtuale.

  Per risolvere il problema, apri una finestra di PowerShell comando come amministratore sull'istanza di desktop virtuale originale utilizzata per creare ed AMI esegui il comando seguente:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Quindi creane una nuova AMI dall'istanza. È possibile utilizzare il nuovo AMI per registrare gli stack software e avviare successivamente nuovi desktop virtuali. Tieni presente che puoi anche eseguire lo stesso comando sull'istanza che rimane nello stato di provisioning e riavviare l'istanza per correggere la sessione del desktop virtuale, ma riscontrerai nuovamente lo stesso problema all'avvio di un altro desktop virtuale da un desktop non configurato correttamente. AMI

.....

## VDIsentra nello stato di errore dopo l'avvio

Possibile problema 1: il filesystem home ha una directory per l'utente con permessi diversi. POSIX

Questo potrebbe essere il problema che stai affrontando se si verificano i seguenti scenari:

1. La RES versione distribuita è 2024.01 o successiva.
2. Durante la distribuzione dello RES stack l'attributo for `EnableLdapIDMapping` è stato impostato su. `True`
3. Il filesystem home specificato durante la distribuzione dello RES stack è stato utilizzato nella versione precedente alla RES 2024.01 o è stato utilizzato in un ambiente precedente con impostato su. `EnableLdapIDMapping` `False`

Fasi di risoluzione: eliminare le directory utente nel filesystem.

1. SSMall'host del gestore del cluster.
2. `cd /home`.
3. `ls`- dovrebbe elencare le directory con nomi di directory che corrispondono ai nomi utente`admin1`, come`admin2`.. e così via.
4. Eliminare le directory,. `sudo rm -r 'dir_name'` Non eliminate le directory ssm-user ed ec2-user.
5. Se gli utenti sono già sincronizzati con il nuovo env, elimina quelli dell'utente dalla tabella dell'utente (eccetto clusteradmin). DDB
6. Avvia la sincronizzazione AD: eseguila `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` nel gestore di cluster Amazon. EC2
7. Riavvia l'VDIistanza nello `Error` stato della pagina web. RES Verifica che le VDI transizioni entrino `Ready` nello stato in circa 20 minuti.

.....

# Componente del desktop virtuale

Argomenti



.....

## L'EC2istanza Amazon viene ripetutamente visualizzata come terminata nella console

Se un'istanza dell'infrastruttura viene ripetutamente visualizzata come terminata nella EC2 console Amazon, la causa potrebbe essere correlata alla sua configurazione e dipendere dal tipo di istanza dell'infrastruttura. Di seguito sono riportati i metodi per determinare la causa.

Se l'istanza vdc-controller mostra stati terminati ripetuti nella EC2 console Amazon, ciò può essere dovuto a un tag segreto errato. I segreti gestiti da RES hanno tag che vengono utilizzati come parte delle politiche di controllo degli IAM accessi allegate alle EC2 istanze dell'infrastruttura Amazon. Se il controller vdc è in esecuzione ciclica e nel gruppo di CloudWatch log viene visualizzato il seguente errore, è possibile che un segreto non sia stato etichettato correttamente. Nota che il segreto deve essere etichettato con quanto segue:

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

Il messaggio di CloudWatch log di Amazon relativo a questo errore apparirà simile al seguente:

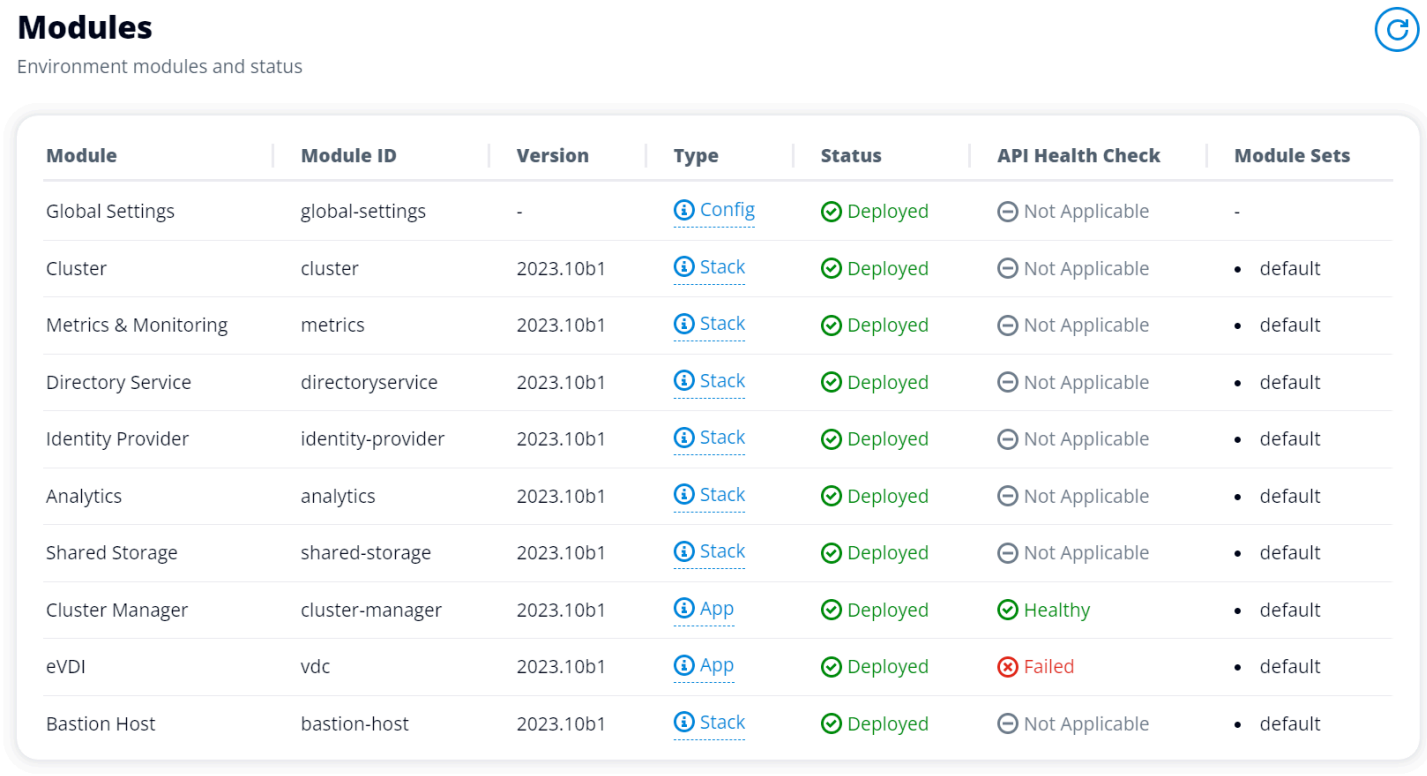
```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Controlla i tag sull'EC2istanza Amazon e verifica che corrispondano all'elenco precedente.

.....

## L'istanza vdc-controller è ciclica a causa della mancata adesione ad//e il modulo VDI mostra Failed Health Check API

Se il VDI modulo e non funziona durante il controllo di integrità, nella sezione Environment Status verrà visualizzato quanto segue.



**Modules**

Environment modules and status

| Module | Module ID | Version | Type | Status | API Health Check | Module Sets |
|---|---|---|---|---|---|---|
| Global Settings | global-settings | - | Config | Deployed | Not Applicable | - |
| Cluster | cluster | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Metrics & Monitoring | metrics | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Directory Service | directoryservice | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Identity Provider | identity-provider | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Analytics | analytics | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Shared Storage | shared-storage | 2023.10b1 | Stack | Deployed | Not Applicable | • default |
| Cluster Manager | cluster-manager | 2023.10b1 | App | Deployed | Healthy | • default |
| eVDI | vdc | 2023.10b1 | App | Deployed | Failed | • default |
| Bastion Host | bastion-host | 2023.10b1 | Stack | Deployed | Not Applicable | • default |

In questo caso, il percorso generale per il debug consiste nell'esaminare i log del gestore del cluster. CloudWatch (Cerca il gruppo di log denominato.) `<env-name>/cluster-manager`

Problemi possibili:

- Se i log contengono il testo`Insufficient permissions`, assicurati che il ServiceAccount nome utente fornito al momento della creazione dello stack res sia digitato correttamente.

  Esempio di riga di registro:

  ```
  Insufficient permissions to modify computer account:
   CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
   000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - È possibile accedere al ServiceAccount nome utente fornito durante la RES distribuzione dalla SecretsManager console. Trova il segreto corrispondente in Secrets Manager e scegli Recupera testo normale. Se il nome utente non è corretto, scegli Modifica per aggiornare il valore segreto. Termina le istanze correnti di cluster-manager e vdc-controller. Le nuove istanze verranno visualizzate in uno stato stabile.
  - Il nome utente deve essere "ServiceAccount" se si utilizzano le risorse create dallo stack di risorse esterne fornito. Se il `DisableADJoin` parametro è stato impostato su False durante la distribuzione diRES, assicurati che l'utente "ServiceAccount" disponga delle autorizzazioni per creare oggetti Computer in AD.
- Se il nome utente utilizzato era corretto, ma i log contengono il testo**`Invalid credentials`**, la password inserita potrebbe essere errata o scaduta.

  Esempio di riga di registro:

  ```
  {'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
   'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
   data 532, v4563'}
  ```

  - Puoi leggere la password che hai inserito durante la creazione dell'ambiente accedendo al segreto che memorizza la password nella console Secrets Manager. Seleziona il segreto (ad esempio`<env_name>directoryserviceServiceAccountPassword`) e scegli Recupera testo normale.
  - Se la password nel segreto non è corretta, scegli Modifica per aggiornarne il valore nel segreto. Termina le istanze correnti di cluster-manager e vdc-controller. Le nuove istanze utilizzeranno la password aggiornata e si presenteranno in uno stato stabile.

- Se la password è corretta, è possibile che sia scaduta nell'Active Directory connessa. Dovrai prima reimpostare la password in Active Directory e quindi aggiornare il segreto. È possibile reimpostare la password dell'utente in Active Directory dalla console Directory Service:
  1. Scegli l'ID di directory appropriato
  2. Scegli Azioni, Reimposta la password dell'utente, quindi compila il modulo con il nome utente (ad esempio, "ServiceAccount«) e la nuova password.
  3. Se la password appena impostata è diversa dalla password precedente, aggiorna la password nel segreto del Secret Manager corrispondente (ad esempio,`<env_name>directoryserviceServiceAccountPassword`.
  4. Termina le istanze correnti di cluster-manager e vdc-controller. Le nuove istanze verranno visualizzate in uno stato stabile.

.....

## Il progetto non viene visualizzato nel menu a discesa quando si modifica lo stack software per aggiungerlo

Questo problema può essere correlato al seguente problema associato alla sincronizzazione dell'account utente con AD. Se si verifica questo problema, verifica l'errore "`<user-home-init> account not available yet. waiting for user to be synced`" nel gruppo di CloudWatch log Amazon cluster-manager per determinare se la causa è la stessa o correlata.

.....

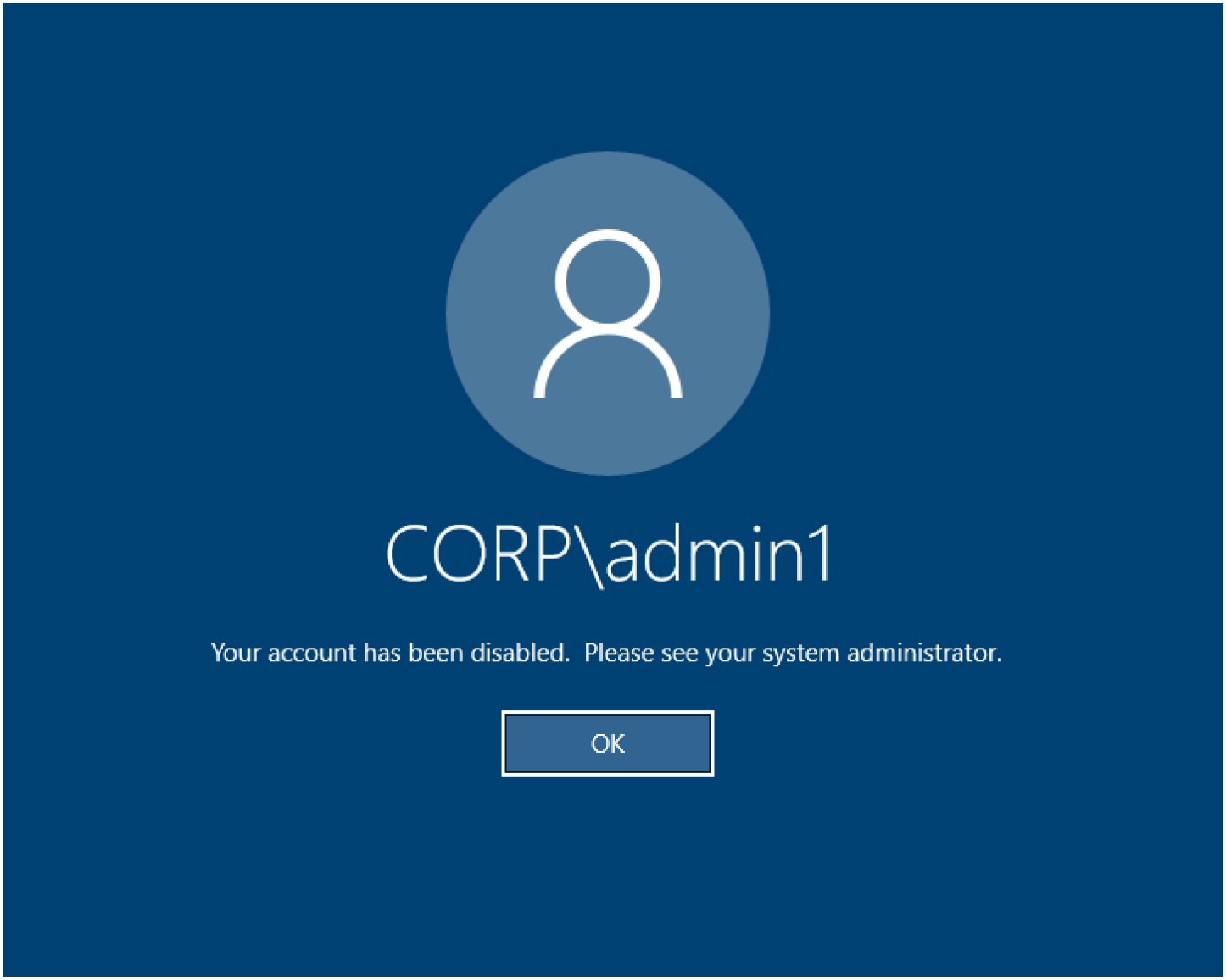
## Il CloudWatch log di Amazon cluster-manager mostra «< user-home-init > account non ancora disponibile in attesa della sincronizzazione dell'utente» (dove l'account è un nome utente)

L'SQSabbonato è occupato e bloccato in un ciclo infinito perché non può accedere all'account utente. Questo codice viene attivato quando si tenta di creare un filesystem home per un utente durante la sincronizzazione dell'utente.

Il motivo per cui non è possibile accedere all'account utente potrebbe essere che non RES è stato configurato correttamente per l'AD in uso. Un esempio potrebbe essere che il `ServiceAccountCredentialsSecretArn` parametro utilizzato nella creazione RES dell'ambiente BI/ non era il valore corretto.

.....

Il desktop di Windows al tentativo di accesso dice «Il tuo account è stato disabilitato. Rivolgiti al tuo amministratore»




Se l'utente non è in grado di accedere nuovamente a una schermata bloccata, ciò potrebbe indicare che l'utente è stato disabilitato nella configurazione AD RES dopo aver effettuato correttamente l'accesso tramiteSSO.

L'SSOaccesso dovrebbe fallire se l'account utente è stato disabilitato in AD.

.....

## DHCPProblemi relativi alle opzioni con la configurazione AD esterna/del cliente

Se riscontri un errore durante l'utilizzo di desktop virtuali Windows "`The connection has been closed. Transport error`" RES con il tuo Active Directory, controlla nel CloudWatch log di dcv-connection-gateway Amazon qualcosa di simile al seguente:

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }

Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Se utilizzi un controller di dominio AD per DHCP le tue opzioniVPC, devi:

1. Aggiungilo AmazonProvided DNS ai due controller di dominioIPs.
2. Imposta il nome di dominio su ec2.internal.

Un esempio è mostrato qui. Senza questa configurazione, il desktop di Windows restituirà l'errore Transport, perchéRES/DCVcerca ip-10-0-x-xx.ec2.internal hostname.


.....

## Errore Firefox MOZILLA _ PKIX ERROR _ REQUIRED _ TLS _ FEATURE _ MISSING

Quando si utilizza il browser Web Firefox, è possibile che venga visualizzato il messaggio di errore del tipo MOZILLA _ PKIX _ ERROR _ REQUIRED _ TLS _ _ FEATURE _ _ MISSING quando si tenta di connettersi a un desktop virtuale.

La causa è che il server RES web è configurato con TLS + Stapling On ma non risponde con Stapling Validation (vedi https://support.mozilla. org/en-US/questions/1372483.

Puoi risolvere questo problema seguendo le istruzioni su: / mozilla_pkix_error_required_tls_feature_missing. https://really-simple-ssl.com

.....

## Eliminazione di Env

Argomenti

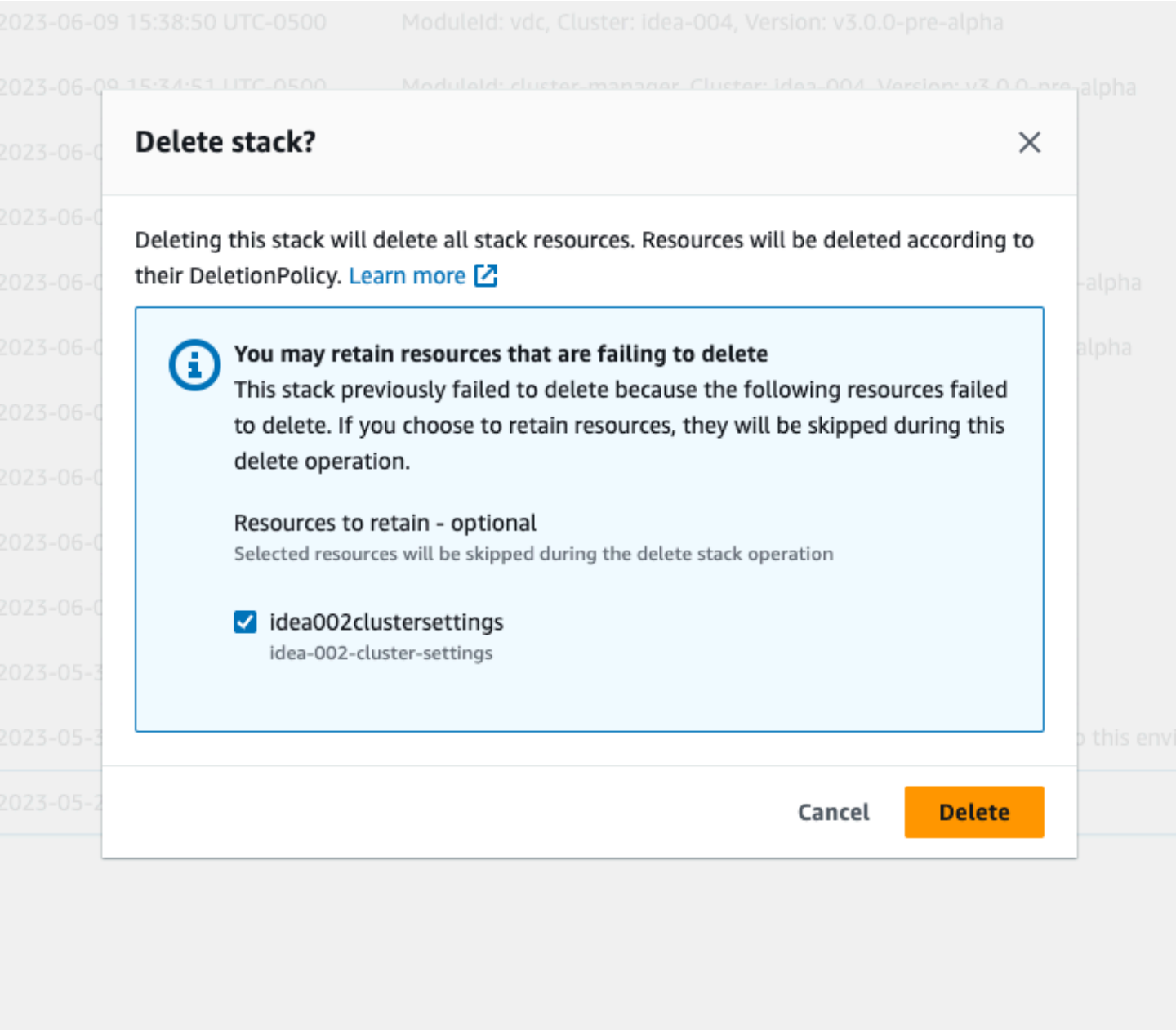
- res-xxx-cluster si trova nello stato "DELETE_FAILED" e non può essere eliminato manualmente a causa dell'errore «Il ruolo non è valido o non può essere assunto»
- Raccolta di registri
- Scaricamento VDI dei registri
- Scaricamento dei log da istanze Linux EC2
- Scaricamento dei registri dalle istanze di Windows EC2
- Raccolta dei ECS log relativi all'errore WaitCondition

.....

### res-xxx-cluster si trova nello stato "DELETE_FAILED" e non può essere eliminato manualmente a causa dell'errore «Il ruolo non è valido o non può essere assunto»

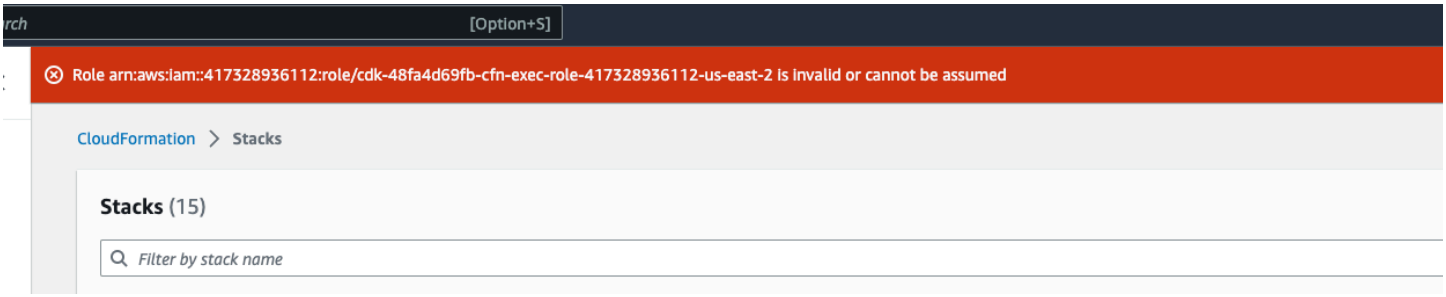
Se noti che lo stack res-xxx-cluster "" è nello stato "DELETE_FAILED" e non può essere eliminato manualmente, puoi effettuare le seguenti operazioni per eliminarlo.

Se vedi lo stack nello stato "DELETE_FAILED", prova innanzitutto a eliminarlo manualmente. Potrebbe apparire una finestra di dialogo che conferma Delete Stack. Scegli Elimina.



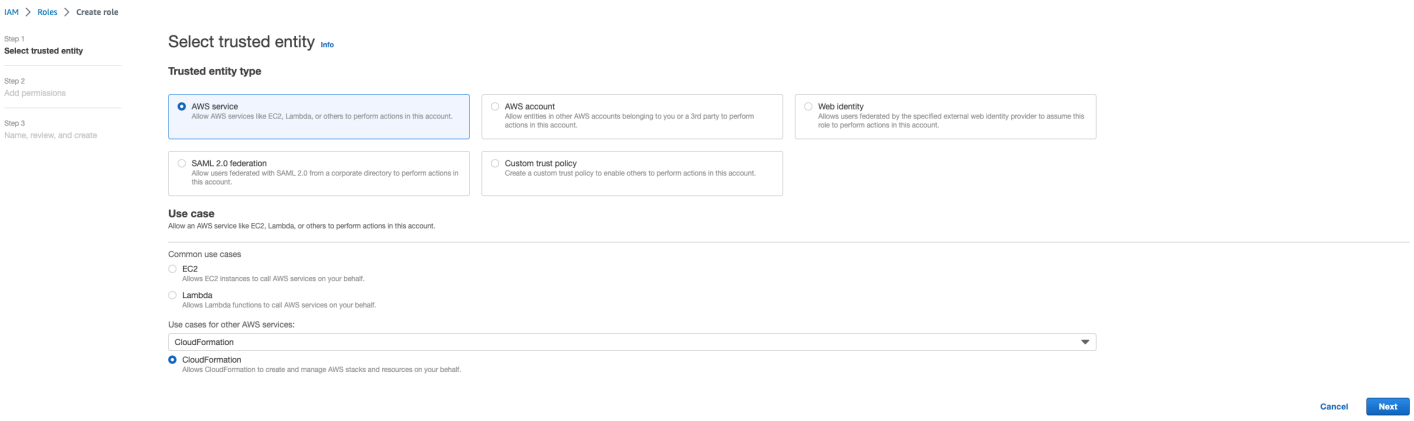

A volte, anche se elimini tutte le risorse dello stack richieste, potresti comunque visualizzare il messaggio che richiede di selezionare le risorse da conservare. In tal caso, seleziona tutte le risorse come «risorse da conservare» e scegli Elimina.

È possibile che venga visualizzato un errore simile a `Role: arn:aws:iam::... is Invalid or cannot be assumed`

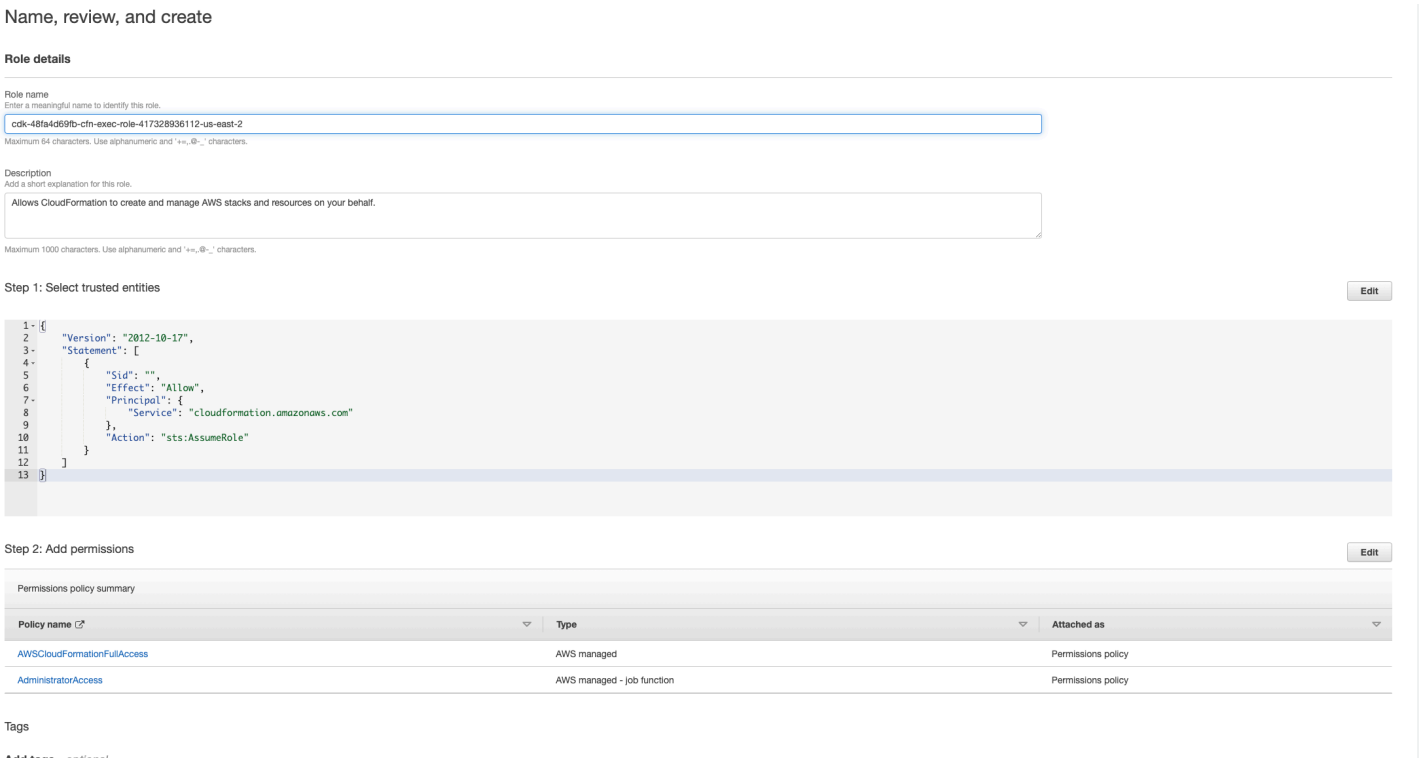



Ciò significa che il ruolo richiesto per eliminare lo stack è stato eliminato prima dello stack. Per ovviare a questo problema, copia il nome del ruolo. Vai alla IAM console e crea un ruolo con quel nome usando i parametri mostrati qui, che sono:

- Per il tipo di entità attendibile scegli AWS il servizio.
- Per il caso d'uso, in `Use cases for other AWS services` Scegli`CloudFormation`.




Scegli Next (Successivo). Assicurati di concedere le autorizzazioni al ruolo `AWSCloudFormationFullAccess` " e `AdministratorAccess` ". La tua pagina di recensione dovrebbe avere il seguente aspetto:




Quindi torna alla CloudFormation console ed elimina lo stack. Ora dovresti essere in grado di eliminarlo dopo aver creato il ruolo. Infine, vai alla IAM console ed elimina il ruolo che hai creato.

.....

## Raccolta di registri

### Accesso a un'EC2istanza dalla console EC2

- Segui queste istruzioni per accedere alla tua EC2 istanza Linux.
- Segui queste istruzioni per accedere alla tua EC2 istanza Windows. Quindi apri Windows PowerShell per eseguire qualsiasi comando.

### Raccolta dei registri degli host dell'infrastruttura

1. Cluster-manager: recupera i log per il gestore del cluster dai seguenti punti e li allega al ticket.
   a. Tutti i log del gruppo di log. CloudWatch `<env-name>/cluster-manager`
   b. Tutti i log presenti `/root/bootstrap/logs` nella directory dell'istanza. `<env-name>-cluster-manager` EC2 Segui le istruzioni riportate in «Accesso a un'EC2istanza dalla EC2 console» all'inizio di questa sezione per accedere alla tua istanza.

2. Controller VDC: recupera i log del controller vdc dai seguenti punti e allegali al ticket.
   a. Tutti i log del gruppo di log. CloudWatch `<env-name>/vdc-controller`
   b. Tutti i log presenti `/root/bootstrap/logs` nella directory dell'istanza. `<env-name>-vdc-controller` EC2 Segui le istruzioni riportate in «Accesso a un'EC2istanza dalla EC2 console» all'inizio di questa sezione per accedere alla tua istanza.

Uno dei modi per ottenere facilmente i log è seguire le istruzioni contenute nella Scaricamento dei log da istanze Linux EC2 sezione. Il nome del modulo sarebbe il nome dell'istanza.

Raccolta di VDI registri

Identifica l'EC2istanza Amazon corrispondente

Se un utente avviasse una sessione VDI con nome di sessione`VDI1`, il nome corrispondente dell'istanza sulla EC2 console Amazon sarebbe`<env-name>-VDI1-<user name>`.

Raccogli i VDI log di Linux

Accedi all'EC2istanza Amazon corrispondente dalla EC2 console Amazon seguendo le istruzioni collegate a «Accesso a un'EC2istanza dalla EC2 console» all'inizio di questa sezione. Ottieni tutti i log `/var/log/dcv/` nelle directory `/root/bootstrap/logs` e sull'istanza VDI AmazonEC2.

Uno dei modi per ottenere i log sarebbe caricarli su s3 e poi scaricarli da lì. Per questo, puoi seguire questi passaggi per ottenere tutti i log da una directory e poi caricarli:

1. Segui questi passaggi per copiare i log dcv nella directory: `/root/bootstrap/logs`

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Ora, segui i passaggi elencati nella prossima sezione Scaricamento VDI dei registri per scaricare i log.

Raccogli i registri di Windows VDI

Accedi all'EC2istanza Amazon corrispondente dalla EC2 console Amazon seguendo le istruzioni collegate a «Accesso a un'EC2istanza dalla EC2 console» all'inizio di questa sezione. Ottieni tutti i log `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` nella directory dell'istanza. VDI EC2

Uno dei modi per ottenere i log sarebbe caricarli su S3 e poi scaricarli da lì. Per farlo, segui i passaggi elencati nella sezione successiva-. Scaricamento VDI dei registri

.....

## Scaricamento VDI dei registri

1. Aggiorna il IAM ruolo dell'VDIEC2istanza per consentire l'accesso a S3.
2. Vai alla EC2 console e seleziona la tua VDI istanza.
3. Seleziona il IAM ruolo che sta utilizzando.
4. Nella sezione Politiche di autorizzazione dal menu a discesa Aggiungi autorizzazioni, scegli Allega politiche, quindi seleziona la politica FullAccessAmazonS3.
5. Scegli Aggiungi autorizzazioni per allegare quella politica.
6. Dopodiché, segui i passaggi elencati di seguito in base al VDI tipo di file per scaricare i log. Il nome del modulo sarebbe il nome dell'istanza.
   a. Scaricamento dei log da istanze Linux EC2per Linux.
   b. Scaricamento dei registri dalle istanze di Windows EC2per Windows.
7. Infine, modifica il ruolo per rimuovere la `AmazonS3FullAccess` politica.

> **Note**
>
> Tutti VDIs usano lo stesso IAM ruolo che è `<env-name>-vdc-host-role-<region>`

.....

## Scaricamento dei log da istanze Linux EC2

Accedi all'EC2istanza da cui desideri scaricare i log ed esegui i seguenti comandi per caricare tutti i log in un bucket s3:

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
```

```
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

Dopodiché, vai alla console S3, seleziona il bucket con il nome `<environment_name>-cluster-<region>-<aws_account_number>` e scarica il file precedentemente caricato. `<module_name>_logs.tar.gz`

.....

## Scaricamento dei registri dalle istanze di Windows EC2

Accedi all'EC2istanza da cui desideri scaricare i log ed esegui i seguenti comandi per caricare tutti i log in un bucket S3:

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

Dopodiché, vai alla console S3, seleziona il bucket con il nome `<environment_name>-cluster-<region>-<aws_account_number>` e scarica il file precedentemente caricato. `<module_name>_logs.zip`

.....

## Raccolta dei ECS log relativi all'errore WaitCondition

1. Vai allo stack distribuito e seleziona la scheda Risorse.

2. Espandi Deploy → ResearchAndEngineeringStudio→ Installer → Tasks → → CreateTaskDefCreateContainer→ LogGroupe seleziona il gruppo di log per aprire i log. CloudWatch
3. Prendi il registro più recente da questo gruppo di log.

.....

# Ambiente dimostrativo

Argomenti

- Errore di accesso all'ambiente demo durante la gestione della richiesta di autenticazione al provider di identità

.....

## Errore di accesso all'ambiente demo durante la gestione della richiesta di autenticazione al provider di identità

Problema

Se tenti di accedere e ricevi un «Errore imprevisto durante la gestione della richiesta di autenticazione al provider di identità», le tue password potrebbero essere scadute. Potrebbe essere la password dell'utente con cui stai tentando di accedere o il tuo account di Active Directory Service.

Attenuazione

1. Reimposta le password degli utenti e degli account di servizio nella console del servizio Directory.
2. Aggiorna le password degli account di servizio in Secrets Manager in modo che corrispondano alla nuova password che hai inserito sopra:
   - per lo stack Keycloak: -... PasswordSecret - -... RESExternal - DirectoryService-... con descrizione: Password per Microsoft Active Directory
   - perRES: res- ServiceAccountPassword -... con descrizione: password dell'account del servizio Active Directory Service
3. Vai alla EC2console e termina l'istanza del gestore del cluster. Le regole di Auto Scaling attiveranno automaticamente la distribuzione di una nuova istanza.

.....

# Problemi noti



## Problemi noti 2024.x

.....

### (2024.08) I desktop virtuali non riescono a montare il bucket Amazon S3 di lettura/scrittura con bucket root e prefisso personalizzato ARN

Descrizione del bug

Research and Engineering Studio 2024.08 non riesce a montare i bucket S3 di lettura/scrittura su un'istanza di infrastruttura desktop virtuale (VDI) quando si utilizza un bucket root ARN

(ovveroarn:aws:s3:::example-bucket) e un prefisso personalizzato (nome del progetto o nome del progetto e nome utente).

Le configurazioni dei bucket che non sono interessate da questo problema includono:

- bucket di sola lettura
- bucket di lettura/scrittura con un prefisso come parte del bucket ARN (ovvero) e prefisso personalizzato (nome del progetto o nome del progetto e nome utentearn:aws:s3:::example-bucket/example-folder-prefix)
- bucket di lettura/scrittura con un bucket root, ma senza prefisso personalizzato ARN

Dopo aver effettuato il provisioning di un'VDIistanza, il bucket non verrà montato nella directory di montaggio specificata per quel bucket S3. Sebbene sia presente la directory di montaggio su, la directory sarà vuota e non conterrà il contenuto corrente del bucket. VDI Quando scrivi un file nella directory utilizzando il terminale, l'errore `Permission denied, unable to write a file` verrà generato e il contenuto del file non verrà caricato nel bucket S3 corrispondente.

Versioni interessate

2024.08

Mitigazione

1. Per scaricare lo script di patch e il file di patch (`patch.pyands3_mount_custom_prefix_fix.patch`), esegui il seguente comando, sostituendolo `<output-directory>` con la directory in cui desideri scaricare lo script e il file di patch e `<environment-name>` con il nome del tuo RES ambiente:

   a. La patch si applica solo alla versione RES 2024.08.

   b. Lo script di patch richiede AWS CLIv2, Python 3.9.16 o superiore e Boto3.

   c. Configura AWS CLI l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni Amazon S3 per scrivere nel bucket creato da. RES

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
 ${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. Passa alla directory in cui vengono scaricati lo script e il file di patch. Eseguite il seguente comando di patch:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. Per terminare l'istanza di Virtual Desktop Controller (vdc-controller) per il tuo ambiente, esegui i seguenti comandi. (La `ENVIRONMENT_NAME` variabile è già stata impostata sul nome dell'RESambiente nel primo passaggio.)

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> Per le VPC configurazioni private, se non l'hai già fatto, per la `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` funzione assicurati di aggiungere il `Environment variable` nome `AWS_STS_REGIONAL_ENDPOINTS` e il valore di`regional`. Per ulteriori informazioni, consulta Prerequisiti del bucket Amazon S3 per distribuzioni isolate VPC.

4. Dopo che il gruppo target che inizia con il nome sarà *`<RES-EnvironmentName>`*`-vdc-ext` diventato sano, VDIs sarà necessario lanciarne uno nuovo che abbia i bucket S3 di lettura/scrittura con root bucket ARN e prefisso personalizzato montati correttamente.

.....

## (2024.06) L'applicazione dell'istantanea non riesce quando il nome del gruppo AD contiene spazi

Problema

RES2024.06 non riesce ad applicare le istantanee delle versioni precedenti se i gruppi AD contengono spazi nei nomi.

I CloudWatch log del gestore del cluster (nel gruppo di `<environment-name>/cluster-manager` log) includeranno il seguente errore durante la sincronizzazione AD:

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

L'errore deriva dall'accettazione RES solo di nomi di gruppo che soddisfano i seguenti requisiti:

- Può contenere solo ASCII lettere minuscole e maiuscole, cifre, trattino (-), punto (.) e trattino basso (_)
- Non è consentito utilizzare un trattino (-) come primo carattere
- Non può contenere spazi.

Versioni interessate

2024.06

Mitigazione

1. Per scaricare lo script e il file di patch (patch.py e groupname_regex.patch), esegui il comando seguente, sostituendolo `<output-directory>` con la directory in cui desideri inserire i file e `<environment-name>` con il nome del tuo ambiente: RES

   a. La patch si applica solo alla versione 2024.06 RES

   b. Lo script di patch richiede AWS CLIv2, Python 3.9.16 o superiore e Boto3.

   c. Configura il AWS CLI file per l'account e la regione in cui RES viene distribuito e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da: RES

   ```
   OUTPUT_DIRECTORY=<output-directory>
   ```

```
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. Vai alla directory in cui vengono scaricati lo script e il file di patch. Eseguite il seguente comando di patch:

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Per riavviare l'istanza di Cluster Manager per il tuo ambiente, esegui i seguenti comandi: Puoi anche terminare l'istanza dalla Amazon EC2 Management Console.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> La patch consente ai nomi dei gruppi AD di contenere ASCII lettere minuscole e maiuscole, cifre, trattino (-), punto (.), trattino basso (_) e spazi con una lunghezza totale compresa tra 1 e 30, inclusi.

.....

## (2024.04-2024.04.02) Limite di autorizzazione fornito non associato al ruolo delle istanze IAM VDI

Il problema

Le sessioni di desktop virtuale non ereditano correttamente la configurazione dei limiti di autorizzazione del progetto. Ciò è dovuto al fatto che il limite delle autorizzazioni definito dal IAMPermissionBoundary parametro non viene assegnato correttamente a un progetto durante la creazione di quel progetto.

Versioni interessate

2024.04 - 2024.04.02

Mitigazione

Segui questi passaggi per consentire di VDIs ereditare correttamente il limite delle autorizzazioni assegnato a un progetto:

1. Per scaricare lo script e il file di patch (patch.py e vdi_host_role_permission_boundary.patch), esegui il comando seguente, sostituendolo con la directory locale in cui desideri inserire i file: `<output-directory>`

   a. La RES patch si applica solo alla versione 2024.04.02. Se utilizzi la versione 2024.04 o 2024.04.01, puoi seguire i passaggi elencati nel documento pubblico per gli aggiornamenti minori delle versioni per aggiornare l'ambiente alla versione 2024.04.02.

   b. Lo script di patch richiede AWS CLIv2), Python 3.9.16 o superiore e Boto3.

   c. Configura il AWS CLI file per l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da. RES

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Vai alla directory in cui vengono scaricati lo script e il file di patch. Eseguite il seguente comando patch, sostituendolo `<environment-name>` con il nome del vostro RES ambiente:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Riavvia l'istanza di cluster-manager nel tuo ambiente eseguendo questo comando, sostituendolo `<environment-name>` con il nome dell'ambiente. RES Puoi anche terminare l'istanza dalla Console di EC2 gestione Amazon.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

## (2024.04.02 e versioni precedenti) NVIDIA Le istanze di Windows in ap-southeast-2 (Sydney) non vengono avviate

Il problema

Amazon Machine Images (AMIs) viene utilizzato per avviare desktop virtuali (VDIs) RES con configurazioni specifiche. Ciascuno AMI ha un ID associato che varia in base alla regione. L'AMIID configurato RES per avviare le istanze Windows Nvidia in ap-southeast-2 (Sydney) non è attualmente corretto.

AMI-ID `ami-0e190f8939a996caf` per questo tipo di configurazione dell'istanza è elencato erroneamente in ap-southeast-2 (Sydney). AMIAl suo posto dovrebbe essere usato un ID`ami-027cf6e71e2e442f4`.

Gli utenti riceveranno il seguente errore quando tentano di avviare un'istanza con l'impostazione predefinita `ami-0e190f8939a996caf`AMI.

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id ‘[ami-0e190f8939a996caf]’ does not exist
```

Passaggi per riprodurre il bug, incluso un file di configurazione di esempio:

- RESImplementa nella regione ap-southeast-2.

- Avvia un'istanza utilizzando lo stack software (ID) NVIDIA predefinito di Windows. AMI `ami-0e190f8939a996caf`

Versioni interessate

Tutte le RES versioni 2024.04.02 o precedenti sono interessate

Mitigazione

La seguente mitigazione è stata testata nella RES versione 2024.01.01:

- Registra un nuovo stack software con le seguenti impostazioni
  - AMIID: `ami-027cf6e71e2e442f4`
  - Sistema operativo: Windows
  - GPUProduttore: NVIDIA
  - Min. Dimensione di archiviazione (GB): 30
  - Min. RAM(GB): 4
- Usa questo stack software per avviare istanze di Windows NVIDIA

.....

## (2024.04 e 2024.04.01) errore di eliminazione in RES GovCloud

Il problema

Durante il flusso di lavoro di RES eliminazione, `UnprotectCognitoUserPool` Lambda disattiva la protezione dalla cancellazione per i pool di utenti di Cognito che verranno successivamente eliminati. L'esecuzione Lambda viene avviata da. `InstallerStateMachine`

A causa delle differenze di AWS CLI versione predefinite tra Commercial e GovCloud le regioni, la `update_user_pool` chiamata in Lambda avrà esito negativo nelle GovCloud regioni.

I clienti riceveranno il seguente errore quando tenteranno di eseguire l'eliminazione RES nelle GovCloud aree geografiche:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
```

```
VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Procedura per riprodurre il bug:

- Implementa RES in una regione GovCloud
- Elimina lo stack RES

Versioni interessate

RESversione 2024.04 e 2024.04.01

Mitigazione

La seguente mitigazione è stata testata nella RES versione 2024.04:

- Apri la `UnprotectCognitoUserPool` Lambda
  - Convenzione di denominazione: *`<env-name>`*`-InstallerTasksUnprotectCognitoUserPool-...`
- Impostazioni di runtime -> Modifica -> Seleziona Runtime `Python 3.11` -> Salva.
- Apri CloudFormation.
- Elimina RES pila -> esci da Retain Installer Resource UNCHECKED -> Elimina.

.....

## (2024.04 - 2024.04.02) Il desktop virtuale Linux potrebbe rimanere bloccato nello stato "" al riavvio RESUMING

Il problema

I desktop virtuali Linux possono rimanere bloccati nello stato "RESUMING" quando vengono riavviati dopo un arresto manuale o programmato.

Dopo il riavvio dell'istanza, AWS Systems Manager non esegue alcun comando remoto per creare una nuova DCV sessione e il seguente messaggio di registro non è presente nei log di vdc-controller (nel gruppo di CloudWatch log): `<environment-name>/vdc/controller` CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Versioni interessate

2024.04 - 2024.04.02

Mitigazione

Per ripristinare i desktop virtuali bloccati nello stato "RESUMING":

1. SSHnell'istanza problematica dalla EC2 console.
2. Esegui i seguenti comandi sull'istanza:

```
sudo su -
/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
configure_post_reboot.sh
sudo reboot
```

3. Attendi il riavvio dell'istanza.

Per evitare che i nuovi desktop virtuali riscontrino lo stesso problema:

1. Per scaricare lo script e il file di patch (patch.py e vdi_stuck_in_resuming_status.patch), esegui il comando seguente, sostituendolo con la directory in cui desideri inserire i file: `<output-directory>`

> **Note**
>
> - La patch RES si applica solo alla versione 2024.04.02.
> - Lo script di patch richiede AWS CLIv2, Python 3.9.16 o superiore e Boto3.
> - Configura il AWS CLI file per l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da. RES

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Vai alla directory in cui vengono scaricati lo script e il file di patch. Eseguite il seguente comando di patch, sostituendolo `<environment-name>` con il nome dell'RESAmbiente e `<aws-region>` con la regione in cui RES è distribuito:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Per riavviare l'istanza VDC del Controller per il tuo ambiente, esegui i comandi seguenti, sostituendoli `<environment-name>` con il nome dell'RESAmbiente:

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

## (2024.04.02 e versioni precedenti) Non riesce a sincronizzare gli utenti AD il cui SAMAccountName attributo include lettere maiuscole o caratteri speciali

Il problema

RESnon riesce a sincronizzare gli utenti AD dopo SSO la configurazione per almeno due ore (due cicli di sincronizzazione AD). I CloudWatch log del gestore del cluster (nel gruppo di `<environment-name>/cluster-manager` log) includono il seguente errore durante la sincronizzazione AD:

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

L'errore deriva dall'accettazione RES solo di un SAMAccount nome utente che soddisfi i seguenti requisiti:

- Può contenere solo ASCII lettere minuscole, cifre, punto (.), trattino basso (_).
- Non è consentito inserire un punto o un carattere di sottolineatura come primo o ultimo carattere.
- Non può contenere due punti continui o caratteri di sottolineatura (ad esempio.., __, ._, _.).

Versioni interessate

2024.04.02 e precedenti

Mitigazione

1. Per scaricare lo script e il file di patch (patch.py e samaccountname_regex.patch), esegui il comando seguente, sostituendolo <output-directory> con la directory in cui desideri inserire i file:

   > **Note**
   >
   > - La patch si applica solo alla versione 2024.04.02. RES
   > - Lo script di patch richiede AWS CLIv2, Python 3.9.16 o superiore e Boto3.
   > - Configura il AWS CLI file per l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da. RES

   ```
   OUTPUT_DIRECTORY=<output-directory>

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
    ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
   ```

2. Vai alla directory in cui vengono scaricati lo script e il file di patch. Eseguite il seguente comando patch, sostituendolo <environment-name> con il nome del vostro RES ambiente:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Per riavviare l'istanza di Cluster Manager per il tuo ambiente, esegui i seguenti comandi, sostituendoli <environment-name> con il nome dell'RESambiente. Puoi anche terminare l'istanza dalla Console di EC2 gestione Amazon.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

## (2024.04.02 e versioni precedenti) La chiave privata per accedere all'host bastion non è valida

### Il problema

Quando un utente scarica la chiave privata per accedere all'host bastion dal portale RES web, la chiave non è ben formattata: più righe vengono scaricate come una singola riga, il che rende la chiave non valida. L'utente riceverà il seguente errore quando tenta di accedere all'host bastion con la chiave scaricata:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

### Versioni interessate

2024.04.02 e precedenti

### Mitigazione

Ti consigliamo di utilizzare Chrome per scaricare le chiavi, poiché questo browser non è interessato.

In alternativa, il file delle chiavi può essere riformattato creando una nuova riga dopo `-----BEGIN PRIVATE KEY-----` e un'altra riga appena prima. `-----END PRIVATE KEY-----`

.....

## (2024.06 e versioni precedenti) I membri del gruppo non sono stati sincronizzati durante la sincronizzazione AD RES

Descrizione del bug

I membri del gruppo non si sincronizzeranno correttamente RES se GroupOU è diverso dall'UserOU.

REScrea un filtro ldapsearch quando tenta di sincronizzare gli utenti di un gruppo AD. Il filtro corrente utilizza erroneamente il parametro userOU anziché il parametro GroupOU. Il risultato è che la ricerca non restituisce alcun utente. Questo comportamento si verifica solo nei casi in cui UsersOU e GroupOU sono diversi.

Versioni interessate

Questo problema riguarda tutte le RES versioni 2024.06 o precedenti

Attenuazione

Segui questi passaggi per risolvere il problema:

1. Per scaricare lo script patch.py e il file group_member_sync_bug_fix.patch, esegui i comandi seguenti, sostituendoli `<output-directory>` con la directory locale in cui desideri scaricare i file e con la versione a cui desideri applicare la patch: `<res_version>` RES

   > **Note**
   >
   > - Lo script di patch richiede AWS CLIv2, Python 3.9.16 o superiore e Boto3.
   > - Configura il AWS CLI file per l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da. RES
   > - La patch supporta solo le RES versioni 2024.04.02 e 2024.06. Se si utilizza la versione 2024.04 o la 2024.04.01, è possibile seguire i passaggi elencati per aggiornare l'ambiente alla versione 2024.04.02 prima Aggiornamenti di versione minori di applicare la patch.

- RESVersione: 2024.04.02 RES

  Link per il download della patch: 2024.04.02_group_member_sync_bug_fix.patch

- RESVersioneRES: 2024.06

  Link per il download della patch: 2024.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. Accedere alla directory in cui vengono scaricati lo script e il file della patch. Eseguite il seguente comando patch, sostituendolo <environment-name> con il nome del vostro RES ambiente:

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. Per riavviare l'istanza di cluster-manager per il tuo ambiente, esegui i seguenti comandi:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

## (2024.06 e versioni precedenti) CVE -2024-6387, RegreSSHion, vulnerabilità di sicurezza in e Ubuntu RHEL9 VDIs

Descrizione del bug

CVE-2024-6387, soprannominatoregreSSHion, è stato identificato nell'Open server. SSH Questa vulnerabilità consente agli aggressori remoti e non autenticati di eseguire codice arbitrario sul server di destinazione, presentando un grave rischio per i sistemi che utilizzano Open per comunicazioni sicure. SSH

InfattiRES, la configurazione standard prevede l'accesso ai desktop virtuali attraverso l'host bastion, e l'host bastion non è interessato da SSH questa vulnerabilità. Tuttavia, l'impostazione predefinita AMI (Amazon Machine Image) che forniamo RHEL9 e Ubuntu2024 VDIs (Virtual Desktop Infrastructure) nelle ALLRESversioni utilizza una SSH versione Open vulnerabile alla minaccia alla sicurezza.

Ciò significa che le versioni esistenti RHEL9 e Ubuntu2024 VDIs potrebbero essere sfruttabili, ma l'aggressore richiederebbe l'accesso all'host bastion.

Maggiori dettagli sul problema sono disponibili qui.

Versioni interessate

Questo problema riguarda tutte le RES versioni 2024.06 o precedenti.

Attenuazione

Entrambi RHEL9 e Ubuntu hanno rilasciato patch per Open SSH che risolvono la vulnerabilità di sicurezza. Questi possono essere recuperati utilizzando il rispettivo gestore di pacchetti della piattaforma.

Se disponi di Ubuntu RHEL9 o di UbuntuVDIs, ti consigliamo di seguire le PATCHEXISTINGVDIsistruzioni riportate di seguito. Per applicare le patch futureVDIs, consigliamo di seguire le PATCHFUTUREVDIsistruzioni. Queste istruzioni descrivono come eseguire uno script per applicare l'aggiornamento della piattaforma sul tuoVDIs.

PATCH EXISTING VDIs

1. Esegui il seguente comando che patcherà tutti gli Ubuntu esistenti e RHEL9VDIs:

a. Lo script di patch richiede AWS CLIv2.

b. Configura il AWS CLI per l'account e la regione in cui RES è distribuito e assicurati di disporre delle autorizzazioni di AWS Systems Manager per inviare un comando Systems Manager Run.

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. È possibile verificare che lo script sia stato eseguito correttamente nella pagina Esegui comando. Fai clic sulla scheda Cronologia dei comandi, seleziona l'ID del comando più recente e verifica che tutte le istanze IDs abbiano un SUCCESS messaggio.

PATCH FUTURE VDIs

1. Per scaricare lo script e il file di patch (patch.py e update_openssh.patch) esegui i seguenti comandi, sostituendoli `<output-directory>` con la directory in cui desideri scaricare i file e `<environment-name>` con il nome del tuo ambiente: RES

> **Note**
>
> - La patch si applica solo alla versione 2024.06. RES
> - Lo script di patch richiede AWS CLIv2), Python 3.9.16 o superiore e Boto3.
> - Configura la tua copia di AWS CLI per l'account e la regione in cui RES viene distribuita e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da. RES

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Esegui il seguente comando patch:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. Riavvia l'istanza VDC Controller per il tuo ambiente con i seguenti comandi:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Important**
>
> Le patch future VDIs sono supportate solo RES nelle versioni 2024.06 e successive. Per applicare le patch future VDIs in RES ambienti con versioni precedenti alla 2024.06, aggiorna prima l'RESambiente alla 2024.06 utilizzando le istruzioni disponibili all'indirizzo:. Principali aggiornamenti delle versioni

.....

# Note

Ogni EC2 istanza Amazon 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 EC2 istanze Amazon senza RDP e senza bisogno di RDP licenze. Se sono necessarie licenze aggiuntive di Remote Desktop Services, l'utente Remote Desktop CALs deve essere acquistato da Microsoft o da un rivenditore di licenze Microsoft. Gli utenti di Remote Desktop CALs con Software Assurance attiva godono dei vantaggi della mobilità delle licenze e possono essere portati in ambienti tenant AWS predefiniti (condivisi). Per informazioni sull'acquisto di licenze senza i vantaggi di Software Assurance o License Mobility, consulta questa sezione di. FAQ

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le offerte e le pratiche AWS attuali di prodotti, 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 CHANGELOGfile.md nel repository. GitHub

| Data | Modifica |
| --- | --- |
| ottobre 2024 | • Versione di rilascio 2024.10: è stato aggiunto il supporto per:<br>  • Limiti dell'ambiente.<br>  • Profili di condivisione del desktop.<br>  • Interruzione automatica dell'interfaccia desktop virtuale. |
| agosto 2024 | • Versione di rilascio 2024.08: è stato aggiunto il supporto per —<br>  • montaggio di bucket Amazon S3 su istanze Linux Virtual Desktop Infrastructure ()VDI. Per informazioni, consulta Bucket Amazon S3.<br>  • autorizzazioni di progetto personalizzate, un modello di autorizzazione avanzato che consente la personalizzazione dei ruoli esistenti e l'aggiunta di ruoli personali zzati. Per informazioni, consulta Policy di autorizzazione.<br>• Guida per l'utente: ha ampliato la sezione. Risoluzione dei problemi |
| Giugno 2024 | • Versione di rilascio 2024.06: supporto per Ubuntu, autorizzazioni del proprietario del progetto.<br>• Guida per l'utente: aggiunta Crea un ambiente demo |

| Data | Modifica |
| --- | --- |
| aprile 2024 | Versione di rilascio 2024.04: modelli RES pronti per il lancio del progetto AMIs e |
| Marzo 2024 | Argomenti aggiuntivi per la risoluzione dei problemi, conservazione dei CloudWatch log, disinstallazione delle versioni secondarie |
| Febbraio 2024 | Versione di rilascio 2024.01.01: modello di distribuzione aggiornato |
| Gennaio 2024 | Versione di rilascio 2024.01 |
| Dicembre 2023 | GovCloud indicazioni e modelli aggiunti |
| Novembre 2023 | Rilascio iniziale |

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.