



Guida per l'utente

# Studio di ricerca e ingegneria



# Studio di ricerca e ingegneria: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

---

# Table of Contents

Panoramica di .....	1
Funzionalità e vantaggi .....	1
Concetti e definizioni .....	3
Panoramica dell'architettura .....	5
Diagramma architetturale .....	5
AWS servizi inclusi in questo prodotto .....	7
Ambiente dimostrativo .....	10
Crea uno stack dimostrativo con un clic .....	10
Prerequisiti .....	10
Crea risorse e parametri di input .....	11
Fasi successive alla distribuzione .....	12
Pianifica la tua implementazione .....	14
Costo .....	14
Sicurezza .....	14
Ruoli IAM .....	15
Gruppi di sicurezza .....	15
Crittografia dei dati .....	15
Considerazioni sulla sicurezza del prodotto .....	16
Quote .....	19
Quote per i AWS servizi relativi a questo prodotto .....	19
AWS CloudFormation quote .....	19
Pianificazione della resilienza .....	20
Supportato Regioni AWS .....	20
Implementa il prodotto .....	22
Prerequisiti .....	22
Crea un messaggio Account AWS con un utente amministrativo .....	23
Crea una coppia di chiavi SSH Amazon EC2 .....	23
Aumentare le quote di servizio .....	23
Crea un dominio personalizzato (opzionale) .....	24
Crea dominio (GovCloud solo) .....	24
Fornire risorse esterne .....	25
Configura LDAPS nel tuo ambiente (opzionale) .....	26
Account di servizio per Microsoft Active Directory .....	27
Configurazione di un VPC privato (opzionale) .....	28

Crea risorse esterne .....	40
Fase 1: Avviare il prodotto .....	46
Passaggio 2: accedi per la prima volta .....	54
Aggiorna il prodotto .....	56
Principali aggiornamenti delle versioni .....	56
Aggiornamenti di versione minori .....	56
Disinstalla il prodotto .....	58
Usando il Console di gestione AWS .....	58
Usando AWS Command Line Interface .....	58
Eliminazione del shared-storage-security-group .....	58
Eliminazione dei bucket Amazon S3 .....	59
Guida alla configurazione .....	60
Gestione delle identità .....	60
Configurazione dell'identità Amazon Cognito .....	60
Sincronizzazione con Active Directory .....	67
Configurazione dell'SSO con IAM Identity Center .....	75
Configurazione del provider di identità per SSO .....	79
Impostazione delle password per gli utenti .....	89
Creazione di sottodomini .....	89
Crea un certificato ACM .....	90
CloudWatch Registri Amazon .....	91
Impostazione di limiti di autorizzazione personalizzati .....	92
Configura RES-Ready AMIs .....	96
Prepara un ruolo IAM per accedere all'ambiente RES .....	97
Crea il componente EC2 Image Builder .....	99
Prepara la tua ricetta per EC2 Image Builder .....	103
Configurazione dell'infrastruttura EC2 Image Builder .....	106
Configurazione della pipeline di immagini di Image Builder .....	107
Esegui la pipeline di immagini di Image Builder .....	108
Registra un nuovo stack software in RES .....	108
Guida per amministratori .....	109
Gestione dei segreti .....	109
Monitoraggio e controllo dei costi .....	112
Dashboard dei costi .....	116
Prerequisiti .....	116
Progetti con tabella del budget assegnato .....	117

Analisi dei costi nel grafico temporale .....	118
Scaricare in CSV .....	121
Gestione della sessione .....	122
Pannello di controllo .....	123
Sessioni .....	124
Pile di software ( ) AMIs .....	127
Debug .....	134
Impostazioni del desktop .....	135
Gestione dell'ambiente .....	137
Stato dell'ambiente .....	138
Impostazioni ambientali .....	138
Utenti .....	139
Gruppi .....	140
Progetti .....	140
Policy di autorizzazione .....	149
File system .....	169
Gestione degli snapshot .....	171
Bucket Amazon S3 .....	177
Usa il prodotto .....	194
accesso SSH .....	194
Desktop virtuali .....	194
Avvia un nuovo desktop .....	195
Accedi al tuo desktop .....	196
Controlla lo stato del desktop .....	197
Modificare un desktop virtuale .....	198
Recupera le informazioni sulla sessione .....	199
Pianifica i desktop virtuali .....	200
Arresto automatico VDI .....	204
Desktop condivisi .....	205
Condividi un desktop .....	206
Accedere a un desktop condiviso .....	207
Browser di file .....	207
Caricare uno o più file .....	208
Eliminare uno o più file .....	209
Gestisci i preferiti .....	209
Modificare i file .....	210

---

Trasferimento dei file .....	211
Risoluzione dei problemi .....	213
Debug e monitoraggio generali .....	216
Utili fonti di informazioni sui registri e sugli eventi .....	217
Aspetto tipico della console Amazon EC2 .....	222
Debug di Windows DCV .....	224
Trova informazioni sulla versione di Amazon DCV .....	225
Problema RunBooks .....	225
Problemi di installazione .....	228
Problemi di gestione delle identità .....	237
Archiviazione .....	241
Snapshot .....	245
Infrastruttura .....	246
Avvio di desktop virtuali .....	248
Componente del desktop virtuale .....	255
Eliminazione di Env .....	261
Ambiente dimostrativo .....	269
Problemi noti .....	271
Problemi noti 2024.x .....	272
Note .....	297
Revisioni .....	298
.....	ccci

# Panoramica di

## Important

Questa versione della Guida per l'utente riguarda la versione 2025.03 di Research and Engineering Studio on AWS. Per la versione attuale, consulta la Guida per l'[AWS utente di Research and Engineering Studio on](#).

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

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

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

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

## Funzionalità e vantaggi

Research and Engineering Studio on AWS offre le seguenti funzionalità:

## Interfaccia utente basata sul Web

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

## Configurazione basata su progetti

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

## Integrazione con l'infrastruttura di gestione delle identità esistente

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

## Archiviazione persistente e accesso ai dati condivisi

Per fornire agli utenti l'accesso ai dati condivisi tra sessioni di desktop virtuali, connessi ai file system esistenti all'interno di RES. I servizi di storage supportati includono Amazon Elastic File System per desktop Linux e Amazon FSx for 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 progetti RES per monitorare i costi di ogni progetto. Se superi il budget, puoi limitare l'avvio delle sessioni VDI.

## Concetti e definizioni

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

### Browser di file

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

### File system

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

### Amministratore globale

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

### Progetto

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

### Autorizzazioni basate sul progetto

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

### Membro del progetto

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

## Proprietario del progetto

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

## Pila di software

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

## Host VDI

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

Per un riferimento generale dei AWS termini, consulta il [AWS glossario](#) nella Guida generale.AWS

# Panoramica dell'architettura

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

## Diagramma architetturale

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

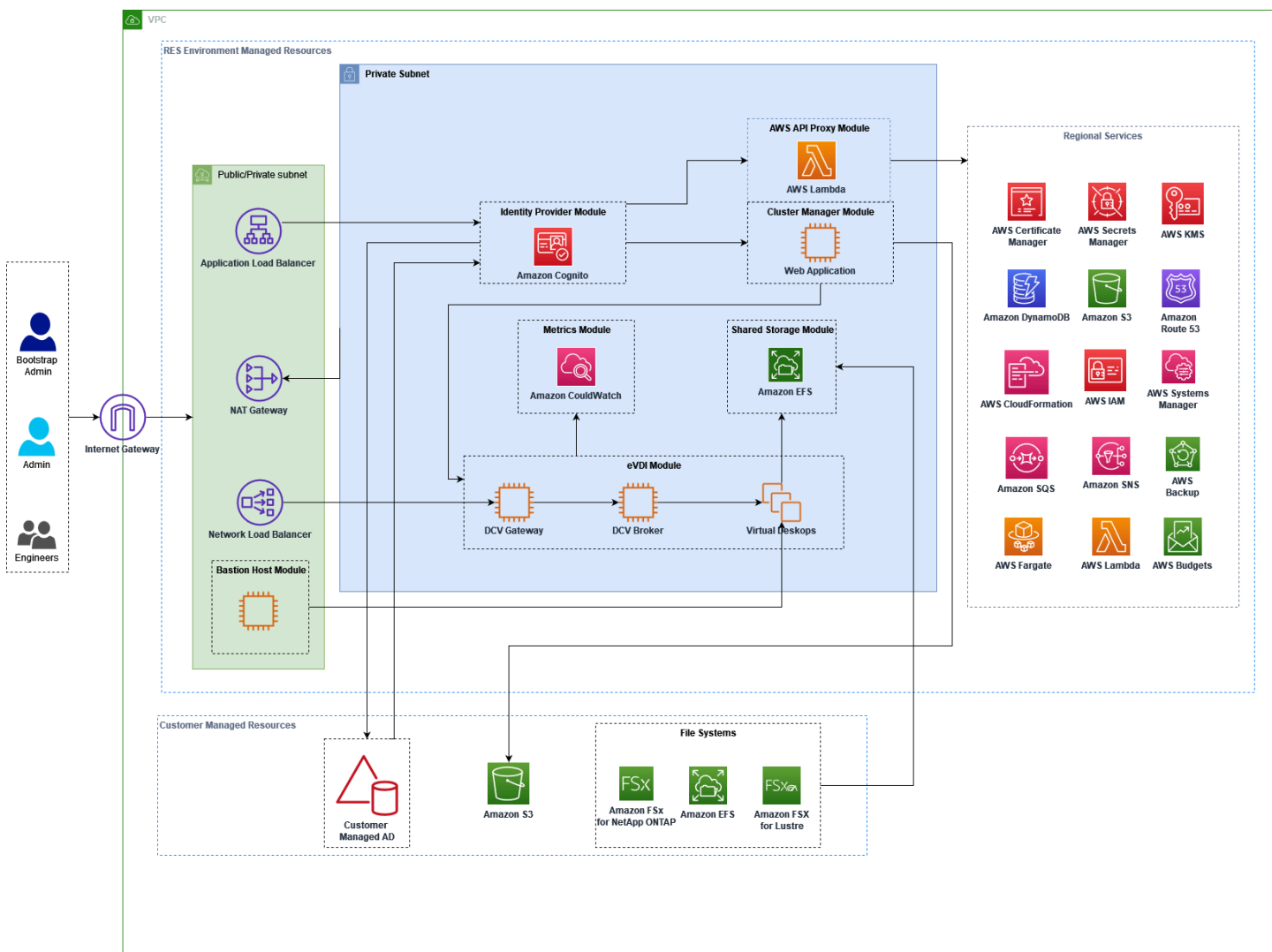


Figura 1: Studio di ricerca e ingegneria sull' AWS architettura

**Note**

AWS CloudFormation le risorse vengono create a partire da AWS Cloud Development Kit (AWS CDK) costrutti.

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

1. RES installa componenti per il portale web e:

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

Amazon CloudWatch riceve i parametri dai componenti eVDI.

c. Componente Bastion Host

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

2. RES installa componenti in sottoreti private dietro un gateway NAT. Gli amministratori accedono alle sottoreti private tramite l'Application Load Balancer (ALB) o il componente Bastion Host.

3. Amazon DynamoDB memorizza la configurazione dell'ambiente.

4. AWS Certificate Manager (ACM) genera e archivia un certificato pubblico per l'Application Load Balancer (ALB).

**Note**

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

5. Amazon Elastic File System (EFS) ospita il /home file system predefinito montato su tutti gli host di infrastruttura applicabili e le sessioni eVDI Linux.

6. RES utilizza Amazon Cognito per creare un utente bootstrap iniziale chiamato 'clusteradmin' e invia credenziali temporanee all'indirizzo e-mail fornito durante l'installazione. 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
<a href="#">Amazon Elastic Compute Cloud</a>	Core	Fornisce i servizi di elaborazione sottostanti per creare desktop virtuali con il sistema operativo e lo stack software scelti.
<a href="#">Elastic Load Balancing</a>	Core	Gli host Bastion, cluster-manager e VDI vengono creati nei gruppi di Auto Scaling dietro il sistema di bilanciamento del carico. ELB bilancia il traffico proveniente dal portale web tra gli host RES.
<a href="#">Amazon Virtual Private Cloud</a>	Core	Tutti i componenti principali del prodotto vengono creati all'interno del tuo VPC.
<a href="#">Amazon Cognito</a>	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.
<a href="#">Amazon Elastic File System</a>	Core	Fornisce il /home file system per il browser di file e gli host VDI, nonché per i file system esterni condivisi.

AWS servizio	Tipo	Descrizione
<a href="#">Amazon DynamoDB</a>	Core	Memorizza dati di configurazione come utenti, gruppi, progetti, file system e impostazioni dei componenti.
<a href="#">AWS Systems Manager</a>	Core	Memorizza i documenti per l'esecuzione di comandi per la gestione delle sessioni VDI.
<a href="#">AWS Lambda</a>	Core	Supporta funzionalità del prodotto come l'aggiornamento delle impostazioni all'interno della tabella DynamoDB, l'avvio dei flussi di lavoro di sincronizzazione con Active Directory e l'aggiornamento dell'elenco dei prefissi.
<a href="#">Amazon CloudWatch</a>	Supporta	Fornisce metriche e registri delle attività per tutti gli EC2 host Amazon e le funzioni Lambda.
<a href="#">Amazon Simple Storage Service</a>	Supporta	Memorizza i file binari delle applicazioni per il bootstrap e la configurazione degli host.
<a href="#">AWS Key Management Service</a>	Supporta	Utilizzato per la crittografia a riposo con code Amazon SQS, tabelle DynamoDB e argomenti Amazon SNS.
<a href="#">Gestione dei segreti AWS</a>	Supporto	Archivia le credenziali degli account di servizio in Active Directory e i certificati autofirmati per VDI.

AWS servizio	Tipo	Descrizione
<a href="#">AWS CloudFormation</a>	Supporto	Fornisce un meccanismo di distribuzione per il prodotto.
<a href="#">AWS Identity and Access Management</a>	Supportare	Limita il livello di accesso per gli host.
<a href="#">Amazon Route 53</a>	Supportare	Crea una zona ospitata privata per risolvere il load balancer interno e il nome di dominio dell'host bastion.
<a href="#">Amazon Simple Queue Service</a>	Supporto	Crea code di attività per supportare esecuzioni asincrone.
<a href="#">Amazon Simple Notification Service</a>	Supportare	Supporta il modello di abbonamento alla pubblicazione tra componenti VDI come il controller e gli host.
<a href="#">AWS Fargate</a>	Supporto	Installa, aggiorna ed elimina gli ambienti utilizzando le attività di Fargate.
<a href="#">Amazon FSx File Gateway</a>	Facoltativo	Fornisce un file system condiviso esterno.
<a href="#">Amazon FSx per NetApp ONTAP</a>	Facoltativo	Fornisce un file system condiviso esterno.
<a href="#">AWS Certificate Manager</a>	Facoltativo	Genera un certificato affidabile e per il tuo dominio personalizzato.
<a href="#">AWS Backup</a>	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 CloudFormation stack crea tutti i componenti richiesti da Research and Engineering Studio.

Tempo di implementazione: ~90 minuti

### Prerequisiti

#### Argomenti

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

### Crea un file Account AWS con un utente amministrativo

Devi avere un account Account AWS con un utente amministrativo:

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene 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 chiavi SSH Amazon EC2

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

## Aumentare le quote di servizio

Consigliamo di [aumentare le quote di servizio](#) per:

- [Amazon VPC](#)
  - Aumenta la quota di indirizzi IP elastici per gateway NAT da cinque a otto
  - Aumentate il numero di gateway NAT per zona di disponibilità da cinque a dieci
- [Amazon EC2](#)
  - Aumentare l'elastico EC2-VPC 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 Console di gestione AWS e apri la 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	Predefinita	Description
EnvironmentName	<i>&lt;res-demo&gt;</i>	Un nome univoco assegnato all'ambiente RES che inizia con res-, non più lungo di

Parametro	Predefinita	Description
		11 caratteri e senza lettere maiuscole.
AdministratorEmail		L'indirizzo e-mail dell'utente che completa la configurazione 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'infrastruttura.
Cliente IPCidr	<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 a SSH nell'host bastion.

#### 4. Seleziona Crea stack.

## Fasi successive alla distribuzione

1. Ora puoi accedere all'ambiente demo utilizzando l'utente clusteradmin e la password temporanea inviata all'e-mail dell'amministratore che hai inserito durante la configurazione. Ti viene richiesto di creare una nuova password al primo accesso.

2. Se desideri utilizzare la funzione «Accedi con l'SSO dell'organizzazione», devi prima reimpostare le password per ogni utente con cui desideri accedere. È possibile reimpostare le password degli utenti dal 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, digita la nuova password che desideri e quindi scegli Reimposta password.
3. Dopo aver reimpostato le password degli utenti, procedi alla pagina di accesso con accesso singolo per accedere all'ambiente.

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 Explorer](#) per 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 utilizzato. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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, consulta [Considerazioni sulla sicurezza per i servizi di questo prodotto](#). Per ulteriori informazioni sulla AWS sicurezza, visita [Cloud AWS Sicurezza](#).

## Ruoli IAM

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

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

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

## Gruppi di sicurezza

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

## Crittografia dei dati

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

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

## 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
<a href="#">Amazon Elastic Compute Cloud</a>	Core	Fornisce i servizi di elaborazione di base per creare desktop virtuali con il sistema operativo e lo stack software scelti.
<a href="#">Elastic Load Balancing</a>	Core	Gli host Bastion, cluster-manager e VDI vengono creati nei gruppi di Auto Scaling dietro il sistema di bilanciamento del carico. ELB bilancia il traffico proveniente dal portale web tra gli host RES.
<a href="#">Amazon Virtual Private Cloud</a>	Core	Tutti i componenti principali del prodotto vengono creati all'interno del tuo VPC.
<a href="#">Amazon Cognito</a>	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.
<a href="#">Amazon Elastic File System</a>	Core	Fornisce il /home file system per il browser di file e gli host

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

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

AWS informazioni sulla sicurezza del servizio	Tipo di servizio	Come viene utilizzato il servizio in RES
<a href="#">AWS Certificate Manager</a>	Facoltativo	Genera un certificato affidabile e per il tuo dominio personalizzato.
<a href="#">AWS Backup</a>	Facoltativo	Offre funzionalità di backup per host Amazon EC2, file system e DynamoDB.

## Quote

Le 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 AWS i 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 [lanci lo stack](#) di questo prodotto. Account AWS Comprendendo queste quote, è possibile evitare errori di limitazione che impedirebbero di implementare correttamente questo prodotto. Per ulteriori informazioni, consulta le [AWS CloudFormation quote](#) nella Guida per l'AWS CloudFormation utente.

## Pianificazione della resilienza

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

Le impostazioni ASG possono essere personalizzate all'interno della console Amazon EC2 all'indirizzo. <https://console.aws.amazon.com/ec2/> Per impostazione 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 informazioni ASGs, consulta [Ridimensionare le dimensioni del gruppo Auto Scaling nella Guida per l'utente](#) di Amazon EC2 Auto Scaling.

## 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 (2025.03)
Stati Uniti orientali (Virginia settentrionale)	us-east-1	sì	sì
Stati Uniti orientali (Ohio)	us-east-2	sì	sì

Nome Regione	Regione	Versioni precedenti	Versione più recente (2025.03)
Stati Uniti occidentali (California settentrionale)	us-west-1	sì	sì
Stati Uniti occidentali (Oregon)	us-west-2	sì	sì
Asia Pacifico (Tokyo)	ap-northeast-1	sì	sì
Asia Pacifico (Seoul)	ap-northeast-2	sì	sì
Asia Pacifico (Mumbai)	ap-south-1	sì	sì
Asia Pacifico (Singapore)	ap-southeast-1	sì	sì
Asia Pacifico (Sydney)	ap-southeast-2	sì	sì
Canada (Centrale)	ca-central-1	sì	sì
Europa (Francoforte)	eu-central-1	sì	sì
Europa (Milan)	eu-south-1	sì	sì
Europa (Irlanda)	eu-west-1	sì	sì
Europa (Londra)	eu-west-2	sì	sì
Europa (Parigi)	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](#)
- [Crea risorse esterne](#)
- [Fase 1: Avviare il prodotto](#)
- [Passaggio 2: accedi per la prima volta](#)

## Prerequisiti

### Argomenti

- [Crea un messaggio Account AWS con un utente amministrativo](#)
- [Crea una coppia di chiavi SSH Amazon EC2](#)
- [Aumentare le quote di servizio](#)
- [Crea un dominio personalizzato \(opzionale\)](#)
- [Crea dominio \(GovCloud solo\)](#)
- [Fornisci risorse esterne](#)
- [Configura LDAPS nel tuo ambiente \(opzionale\)](#)
- [Configurare un account di servizio per Microsoft Active Directory](#)
- [Configurazione di un VPC privato \(opzionale\)](#)

## Crea un messaggio Account AWS con un utente amministrativo

È necessario disporre di 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 o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene 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 chiavi SSH Amazon EC2

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

## Aumentare le quote di servizio

Consigliamo di [aumentare le quote di servizio](#) per:

- [Amazon VPC](#)
  - Aumenta la quota di indirizzi IP elastici per gateway NAT da cinque a otto.
  - Aumentate il numero di gateway NAT per zona di disponibilità da cinque a dieci.
- [Amazon EC2](#)
  - Aumentare l'elastico EC2-VPC 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 AWS i servizi di questo prodotto](#).

## Crea un dominio personalizzato (opzionale)

Ti consigliamo di utilizzare un dominio personalizzato per il prodotto in modo da avere un URL intuitivo. Puoi fornire un dominio personalizzato e, facoltativamente, fornire un relativo certificato.

Esiste un processo nello stack di risorse esterne per creare un certificato per un dominio personalizzato fornito dall'utente. Puoi saltare questi passaggi se hai un dominio e desideri utilizzare le funzionalità di generazione di certificati dello stack di risorse esterne.

In alternativa, segui questi passaggi per registrare un dominio utilizzando Amazon Route 53 e importare un certificato per il dominio che utilizza AWS Certificate Manager.

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

## Crea dominio (GovCloud solo)

Se 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. Distribuisci lo [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'`CertificateARNOutput`. Nota il nuovo ARN segreto e aggiungi due tag al segreto in modo da `vdc-gateway` poter accedere al valore segreto:
  - a. `res: = ModuleName virtual-desktop-controller`
  - b. `res: EnvironmentName = [nome dell'ambiente]` (potrebbe essere `res-demo`.)
4. Nell'account della GovCloud partizione, crea un segreto con il valore dell'`output.PrivateKeySecretArn`. Nota il nuovo ARN segreto e aggiungi due tag al segreto in modo da `vdc-gateway` poter accedere al valore segreto:
  - a. `res: = ModuleName virtual-desktop-controller`
  - b. `res: EnvironmentName = [nome dell'ambiente]` (potrebbe essere `res-demo`.)

## Fornisci risorse esterne

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

- Rete (VPC, sottoreti pubbliche e sottoreti private)

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

- Archiviazione (Amazon EFS)

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

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

Il servizio di directory autentica gli utenti nell'ambiente RES.

- Un segreto che contiene il nome utente e la password dell'account del servizio Active Directory formattati come coppia chiave-valore (nome utente, password)

Research and Engineering Studio accede ai [segreti](#) forniti dall'utente, inclusa la password dell'account del servizio, utilizzando. [Gestione dei segreti AWS](#)

**⚠ Warning**

È necessario fornire un indirizzo e-mail valido per tutti gli utenti di Active Directory (AD) che si desidera sincronizzare.

**ℹ Tip**

Se stai distribuendo un ambiente demo e non disponi di queste risorse esterne, puoi utilizzare le ricette AWS High Performance Compute per generare le risorse esterne. Consulta la sezione seguente per distribuire [Crea risorse esterne](#) le risorse nel tuo account.

Per le distribuzioni dimostrative nella regione AWS GovCloud (Stati Uniti occidentali), dovrai completare i passaggi preliminari indicati in. [Crea dominio \(GovCloud solo\)](#)

## Configura LDAPS nel tuo ambiente (opzionale)

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

1. Segui i passaggi forniti in [Come abilitare LDAPS lato server](#) per il tuo. AWS Managed Microsoft AD Puoi saltare questo passaggio se hai già abilitato LDAPS.
2. Dopo aver verificato che LDAPS è configurato su AD, esporta il certificato AD:
  - a. Vai al tuo server Active Directory.
  - b. Apri PowerShell come amministratore.
  - c. Esegui `certmgr .msc` per aprire l'elenco dei certificati.
  - d. Apri l'elenco dei certificati aprendo prima Trusted Root Certification Authorities e poi Certificati.
  - e. Seleziona e tieni premuto (o fai clic con il pulsante destro del mouse) sul certificato con lo stesso nome del server AD e scegli Tutte le attività, quindi Esporta.
  - f. Seleziona X.509 con codifica Base-64 (.CER) e scegli Avanti.
  - g. Seleziona una directory, quindi scegli Avanti.
3. Crea un segreto in Gestione dei segreti AWS:

Quando crei il tuo segreto nel Secrets Manager, seleziona `Other type of secrets` (Altro tipo di segreti) in `secret type` (Tipo di segreto) e incolla il certificato codificato PEM nel campo `Plaintext` (Testo normale).

4. Annotate l'ARN creato e inseritelo come `DomainTLSCertificateSecretARN` parametro in.

[Fase 1: Avviare il prodotto](#)

## Configurare un account di servizio per Microsoft Active Directory

Se scegli Microsoft Active Directory (AD) come origine dell'identità per RES, hai un account di servizio nell'AD che consente l'accesso programmatico. È necessario trasmettere un codice segreto con le credenziali dell'account di servizio come parte dell'installazione di RES. L'account di servizio è responsabile delle seguenti funzioni:

- Sincronizzazione degli utenti dall'AD: RES deve sincronizzare gli utenti dall'AD per consentire loro di accedere al portale web. Il processo di sincronizzazione utilizza l'account del servizio per interrogare l'AD utilizzando LDAP per determinare quali utenti e gruppi sono disponibili.
- Unisciti al dominio AD: si tratta di un'operazione opzionale per i desktop virtuali Linux e gli host dell'infrastruttura in cui l'istanza si unisce al dominio AD. In RES, questa operazione viene controllata con il `DisableADJoin` parametro. Questo parametro è impostato su `False` per impostazione predefinita, il che significa che i desktop virtuali Linux tenteranno di aggiungere il dominio AD nella configurazione predefinita.
- Connessione all'AD: i desktop virtuali e gli host dell'infrastruttura Linux si conetteranno al dominio AD se non vi aderiscono (`DisableADJoin= True`). Affinché questa funzionalità funzioni, il Service Account necessita anche dell'accesso in lettura per utenti `UsersOU` e `GroupsOU` gruppi.

L'account di servizio richiede le seguenti autorizzazioni:

- Per sincronizzare gli utenti e connettersi ad AD → Accesso in lettura per utenti e gruppi in modalità `UsersOU` e `GroupsOU`.
- Per entrare nel dominio AD → crea `Computer` oggetti in `ComputersOU`.

Lo script in [https://github.com/aws-samples/aws-hpc-recipes/blob/main/recipes/res/res\\_demo\\_env/assets/service\\_account.ps1](https://github.com/aws-samples/aws-hpc-recipes/blob/main/recipes/res/res_demo_env/assets/service_account.ps1) fornisce un esempio di come concedere le autorizzazioni appropriate all'account di servizio. Puoi modificarlo in base al tuo AD.

## Configurazione di un VPC privato (opzionale)

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

### Argomenti

- [Preparare le immagini delle macchine Amazon \(AMIs\)](#)
- [Configurazione degli endpoint VPC](#)
- [Connect ai servizi senza endpoint VPC](#)
- [Imposta i parametri di distribuzione di un VPC privato](#)

### Preparare le immagini delle macchine Amazon (AMIs)

1. Scarica [le dipendenze](#). Per l'implementazione in un VPC isolato, l'infrastruttura RES richiede la disponibilità di dipendenze senza l'accesso pubblico a Internet.
2. Crea un ruolo IAM con accesso in sola lettura e identità affidabile di Amazon S3 come Amazon EC2.
  - a. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
  - b. Da Ruoli, scegli Crea ruolo.
  - c. Nella pagina Seleziona un'entità attendibile:
    - In Tipo di entità attendibile, scegli Servizio AWS.
    - Per Caso d'uso in Servizio o caso d'uso, scegli EC2 e scegli Avanti.
  - d. In Aggiungi autorizzazioni, seleziona le seguenti politiche di autorizzazione, quindi scegli Avanti:
    - Amazon S3 ReadOnlyAccess
    - Amazon SSMManaged InstanceCore
    - EC2InstanceProfileForImageBuilder
  - e. Aggiungi un nome e una descrizione del ruolo, quindi scegli Crea ruolo.
3. Crea il componente EC2 image builder:

- a. Apri la console EC2 Image Builder <https://console.aws.amazon.com/imagebuilder> all'indirizzo.
- b. In Risorse salvate, scegli Componenti e scegli Crea componente.
- c. Nella pagina Crea componente, inserisci i seguenti dettagli:
  - Per Tipo di componente, scegli Costruisci.
  - Per i dettagli del componente, scegli:

Parametro	Inserimento utente
Sistema operativo (OS) di immagine	Linux
Versioni del sistema operativo compatibili	Amazon Linux 2 o Windows 10 e 11 RHEL8 RHEL9
Nome componente	Inserisci un nome come: <i>&lt;research-and-engineering-studio-infrastructure&gt;</i>
Versione del componente	Consigliamo di iniziare con 1.0.0.
Description	Inserimento utente opzionale.

- d. Nella pagina Crea componente, scegli Definisci il contenuto del documento.
  - i. Prima di inserire il contenuto del documento di definizione, è necessario un URI del file per il file tar.gz. Carica il file tar.gz fornito da RES in un bucket Amazon S3 e copia l'URI del file dalle proprietà del bucket.
  - ii. Immetti i seguenti dati:

#### Note

AddEnvironmentVariables è facoltativo e puoi rimuoverlo se non hai bisogno di variabili di ambiente personalizzate negli host dell'infrastruttura. Se si stanno http\_proxy configurando variabili di https\_proxy ambiente, i no\_proxy parametri sono necessari per impedire all'istanza di utilizzare il proxy

per interrogare localhost, gli indirizzi IP dei metadati dell'istanza e i servizi che supportano gli endpoint VPC.

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

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region

phases:
  - name: build
      steps:
        - name: DownloadRESInstallScripts
          action: S3Download
          onFailure: Abort
          maxAttempts: 3
          inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
        - name: RunInstallScript
```

```

    action: ExecuteBash
    onFailure: Abort
    maxAttempts: 3
    inputs:
      commands:
        - 'cd /root/bootstrap/res_dependencies'
        - 'tar -xf res_dependencies.tar.gz'
        - 'cd all_dependencies'
        - '/bin/bash install.sh'
  - name: AddEnvironmentVariables
    action: ExecuteBash
    onFailure: Abort
    maxAttempts: 3
    inputs:
      commands:
        - |
          echo -e "
            http_proxy=http://<ip>:<port>
            https_proxy=http://<ip>:<port>

no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.

```

```

{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com,ecs.
{{ AWSRegion }}.amazonaws.com,.execute-api.{{ 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 o Red Hat Enterprise Linux (RHEL)
	Origine dell'immagine	Avvio rapido (gestito da Amazon)
	Nome dell'immagine	Amazon Linux 2 x86, Red Hat Enterprise Linux 8 x86 o Red Hat Enterprise Linux 9 x86
	Opzioni di controllo automatico delle versioni	Usa l'ultima versione del sistema operativo disponibili.

Sezione	Parametro	Inserimento utente
Configurazione dell'istanza	–	Mantieni tutto nelle impostazioni predefinite e assicurati che Rimuovi l'agente SSM dopo l'esecuzione della pipeline non sia selezionato.
Directory di lavoro	Percorso della directory di lavoro	/root/bootstrap/res_dipende nze
Componenti	Costruisci componenti	Cerca e seleziona quanto segue: <ul style="list-style-type: none"> <li>• Gestito da Amazon: -2- linux aws-cli-version</li> <li>• Gestito da Amazon: amazon-cloudwatch- agent-linux</li> <li>• Di tua proprietà: componente Amazon EC2 creato in precedenz a. Inserisci il tuo Account AWS ID e la tua corrente Regione AWS nei campi.</li> </ul>
	Componenti di test	Cerca e seleziona: <ul style="list-style-type: none"> <li>• Gestito da Amazon: simple-boot-test-linux</li> </ul>

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
Ambito generale	Nome	Immettere un nome appropriato, ad esempio res-infra-linux-x 86.
	Descrizione	Aggiungi una descrizione opzionale.
	Ruolo IAM	Seleziona il ruolo IAM creato in precedenza.
AWS infrastruttura	Tipo di istanza	Scegli t3.medium.
	VPC, sottorete e gruppi di sicurezza	<p>Seleziona un'opzione che consenta l'accesso a Internet e l'accesso al bucket Amazon S3. Se devi creare un gruppo di sicurezza, puoi crearne uno dalla console Amazon EC2 con i seguenti input:</p> <ul style="list-style-type: none"> <li>• VPC: seleziona lo stesso VPC utilizzato per la configurazione dell'infrastruttura. Questo VPC deve avere accesso a Internet.</li> <li>• Regola in entrata: <ul style="list-style-type: none"> <li>• Tipo: SSH</li> <li>• Source (Origine): personalizzata</li> <li>• Blocco CIDR: 0.0.0.0/0</li> </ul> </li> </ul>

d. Scegli Crea configurazione dell'infrastruttura.

6. Crea una nuova pipeline EC2 Image Builder:

- a. Vai a Image pipelines e scegli Crea pipeline di immagini.
  - b. Nella pagina Specificare i dettagli della pipeline, immettete quanto segue e scegliete Avanti:
    - Nome della tubazione e descrizione opzionale
    - Per Programma di costruzione, imposta un programma o scegli Manuale se desideri avviare manualmente il processo di cottura AMI.
  - c. Nella pagina Scegli la ricetta, scegli Usa ricetta esistente e inserisci il nome della ricetta creato in precedenza. 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'ambiente RES distribuito, in modo che RES possa avviare correttamente le istanze host dell'infrastruttura da essa. Utilizzando le impostazioni predefinite del servizio, l'immagine di output verrà creata nella regione in cui viene utilizzato il servizio EC2 Image Builder.
    - Se desideri implementare RES in più regioni, puoi scegliere Crea nuove impostazioni di distribuzione e aggiungervi altre regioni.
  - g. Controlla le tue selezioni e scegli Crea pipeline.
7. Esegui la pipeline EC2 Image Builder:
- a. Da Image pipelines, trova e seleziona la pipeline che hai creato.
  - b. Scegliete Azioni e selezionate Esegui pipeline.
- La pipeline può impiegare da 45 minuti a un'ora per creare un'immagine AMI.
8. Annota l'ID AMI per l'AMI generato e usalo come input per il parametro InfrastructureHost AMI [in the section called "Fase 1: Avviare il prodotto"](#).

## Configurazione degli endpoint VPC

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

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

Servizio AWS	Nome del servizio
<a href="#">Application Auto Scaling</a>	com.amazonaws. <i>region</i> .scalabilità automatica delle applicazioni
<a href="#">AWS CloudFormation</a>	com.amazonaws. <i>region</i> .formazione di nuvole
<a href="#">Amazon CloudWatch</a>	com.amazonaws. <i>region</i> .monitoraggio
<a href="#">CloudWatch Registri Amazon</a>	com.amazonaws. <i>region</i> .registri
<a href="#">Amazon DynamoDB</a>	com.amazonaws. <i>region</i> .dynamodb (richiede un endpoint gateway)
<a href="#">Amazon EC2</a>	com.amazonaws. <i>region</i> .ec2
<a href="#">Amazon ECR</a>	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
<a href="#">Amazon Elastic File System</a>	com.amazonaws. <i>region</i> .filesystem elastico
<a href="#">Elastic Load Balancing</a>	com.amazonaws. <i>region</i> .bilanciamento elastico del carico
<a href="#">Amazon EventBridge</a>	com.amazonaws. <i>region</i> .eventi
Amazon FSx	com.amazonaws. <i>region</i> .fsx

Servizio AWS	Nome del servizio
<a href="#">AWS Key Management Service</a>	com.amazonaws. <i>region</i> .kms
<a href="#">Flusso di dati Amazon Kinesis</a>	com.amazonaws. <i>region</i> .kinesis-stream
<a href="#">AWS Lambda</a>	com.amazonaws. <i>region</i> .lambda
<a href="#">Amazon S3</a>	<p>com.amazonaws. <i>region</i>.s3 (richiede un endpoint gateway creato per impostazione predefinita in RES.)</p> <p>Sono necessari endpoint di interfaccia Amazon S3 aggiuntivi per il montaggio incrociato di bucket in un ambiente isolato. Vedi <a href="#">Accesso agli endpoint dell'interfaccia Amazon Simple Storage Service</a>.</p>
<a href="#">Gestione dei segreti AWS</a>	com.amazonaws. <i>region</i> . gestore dei segreti
<a href="#">Servizio Amazon Elastic Container</a>	com.amazonaws. <i>region</i> .ecs
<a href="#">Amazon SES</a>	com.amazonaws. <i>region</i> .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.)
<a href="#">AWS Security Token Service</a>	com.amazonaws. <i>region</i> .sts
<a href="#">Amazon SNS</a>	com.amazonaws. <i>region</i> .sns
<a href="#">Amazon SQS</a>	com.amazonaws. <i>region</i> .sqs
<a href="#">AWS Systems Manager</a>	com.amazonaws. <i>region</i> messaggi.ec2
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> messaggi.ssm

## Connect ai servizi senza endpoint VPC

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

1. Avvia un'istanza Linux nella sottorete pubblica del VPC che utilizzerai per la distribuzione RES.
  - Famiglia Linux: Amazon Linux 2 o Amazon Linux 3
  - Architettura: x86
  - Tipo di istanza: t2.micro o versione successiva
  - Gruppo di sicurezza: TCP sulla porta 3128 da 0.0.0.0/0
2. Connect all'istanza per configurare un server proxy.
  - a. Apri la connessione http.
  - b. Consenti la connessione ai seguenti domini da tutte le sottoreti pertinenti:
    - .amazonaws.com (per servizi generici) AWS
    - .amazoncognito.com (per Amazon Cognito)
    - .awsapps.com (per Identity Center)
    - .signin.aws (per Identity Center)
    - .amazonaws-us-gov.com (per Gov Cloud)
  - c. Nega tutte le altre connessioni.
  - d. Attiva e avvia il server proxy.
  - e. Annota la PORTA su cui il server proxy ascolta.
3. Configura la tabella delle rotte per consentire l'accesso al server proxy.
  - a. Vai alla tua console VPC e identifica le tabelle di routing per le sottoreti che utilizzerai per gli host dell'infrastruttura e gli host VDI.
  - b. Modifica la tabella di routing per consentire a tutte le connessioni in entrata di accedere all'istanza del server proxy creata nei passaggi precedenti.
  - c. 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'istanza EC2 del server proxy e assicurati che consenta le connessioni TCP in entrata sulla PORTA su cui il server proxy è in ascolto.

## Imposta i parametri di distribuzione di un VPC privato

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

Parametro	Input
InfrastructureHostAMI	Utilizza l'ID AMI dell'infrastruttura creato in <a href="#">the section called “Preparare le immagini delle macchine Amazon (AMIs)”</a> .
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 il tuo VPC CIDR per consentire l'accesso a tutti gli indirizzi IP VPC.
HttpProxy	Esempio: <code>http://10.1.2.3:123</code>
HttpsProxy	Ad esempio: <code>http://10.1.2.3:123</code>
NoProxy	Esempio:

```
127.0.0.1,169.254.169.254,169.254.17
0.2,localhost,us-east-1.res,us-east-
1.vpce.amazonaws.com,us-east-1.elb.a
mazonaws.com,s3.us-east-1.amazonaws.
com,s3.dualstack.us-east-1.amazonaws
```

## Parametro

## Input

```
.com,ec2.us-east-1.amazonaws.com,ec2.us-east-1.api.aws,ec2messages.us-east-1.amazonaws.com,ssm.us-east-1.amazonaws.com,ssmmessages.us-east-1.amazonaws.com,kms.us-east-1.amazonaws.com,secretsmanager.us-east-1.amazonaws.com,sqs.us-east-1.amazonaws.com,elasticloadbalancing.us-east-1.amazonaws.com,sns.us-east-1.amazonaws.com,logs.us-east-1.amazonaws.com,logs.us-east-1.api.aws,elasticfilesystem.us-east-1.amazonaws.com,fsx.us-east-1.amazonaws.com,dynamodb.us-east-1.amazonaws.com,api.ecr.us-east-1.amazonaws.com,.dkr.ecr.us-east-1.amazonaws.com,kinesis.us-east-1.amazonaws.com,.data-kinesis.us-east-1.amazonaws.com,.control-kinesis.us-east-1.amazonaws.com,events.us-east-1.amazonaws.com,cloudformation.us-east-1.amazonaws.com,sts.us-east-1.amazonaws.com,application-autoscaling.us-east-1.amazonaws.com,monitoring.us-east-1.amazonaws.com,ecs.us-east-1.amazonaws.com,.execute-api.us-east-1.amazonaws.com
```

## Crea risorse esterne

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

È possibile [scaricare il modello di ricette](#) prima della distribuzione.

Tempo di implementazione: circa 40-90 minuti

1. [Accedi a Console di gestione AWS e apri la CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.](https://console.aws.amazon.com/cloudformation)

**Note**

Assicurati di essere nel tuo account amministratore.

2. Avvia [il modello](#) nella console.

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

3. Immettete i parametri del modello:

Parametro	Predefinito	Descrizione
DomainName	corp.res.com	Dominio utilizzato per Active Directory. Il valore predefinito viene fornito nel LDIF file che configura gli utenti bootstrap. Se desideri utilizzare gli utenti predefiniti, lascia il valore come predefinito. Per modificare il valore, aggiorna e fornisci un LDIF file separato. Non è necessario che ciò corrisponda al dominio utilizzato per Active Directory.
SubDomain (GovCloud solo)		Questo parametro è facoltativo per le regioni commerciali, ma obbligatorio per GovCloud le regioni.  Se fornisci un SubDomain, il parametro avrà il prefisso DomainName fornito. Il nome di dominio Active

Parametro	Predefinito	Descrizione
		Directory fornito diventerà un sottodominio.
AdminPassword		<p>La password per l'amministratore di Active Directory (nome utenteAdmin). Questo utente viene creato in Active Directory per la fase iniziale di bootstrap e non viene utilizzato dopo.</p> <p>Importante: il formato di questo campo può essere (1) una password in testo semplice o (2) l'ARN di un AWS segreto formattato o in coppia. key/value <code>{"password": "somepassword"}</code></p> <p>Nota: la password per questo utente deve soddisfare i <a href="#">requisiti di complessità della password per Active Directory</a>.</p>

Parametro	Predefinito	Descrizione
ServiceAccountPassword		<p>Password utilizzata per creare un account di servizio (ReadOnlyUser ). Questo account viene utilizzato per la sincronizzazione.</p> <p>Importante: il formato di questo campo può essere (1) una password in testo semplice o (2) l'ARN di un AWS segreto formattato o in coppia. key/value <code>{"password": "somepassword"}</code></p> <p>Nota: la password per questo utente deve soddisfare i <a href="#">requisiti di complessità della password per Active Directory</a>.</p>
Coppia di chiavi		<p>Connette le istanze amministrative utilizzando un client SSH.</p> <p>Nota: AWS Systems Manager Session Manager può essere utilizzato anche per connettersi alle istanze.</p>

Parametro	Predefinito	Descrizione
LDIFS3Percorso	<code>aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif</code>	<p>Il percorso Amazon S3 di un file LDIF importato durante la fase di avvio della configurazione di Active Directory. Per ulteriori informazioni, consulta <a href="#">LDIF Support</a>. Il parametro viene precompilato con un file che crea un numero di utenti in Active Directory.</p> <p>Per visualizzare il file, consultate il file <a href="#">res.ldif</a> disponibile in. GitHub</p>
ClientIpCidr		<p>L'indirizzo IP da cui accederai al sito. Ad esempio, puoi selezionare il tuo indirizzo IP e <code>[IPADDRESS]/32</code> utilizzarlo per consentire l'accesso solo dal tuo host. È possibile aggiornarlo dopo la distribuzione.</p>
ClientPrefixList		<p>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 <a href="#">Utilizzare gli elenchi di prefissi gestiti dal cliente</a>.</p>

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

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

## Fase 1: Avviare il prodotto

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

Tempo di implementazione: circa 60 minuti

È possibile [scaricare il CloudFormation modello](#) per questo prodotto prima di distribuirlo.

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

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

### Note

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

Il AWS CloudFormation modello implementa Research and Engineering Studio AWS in. Cloud AWS È necessario soddisfare i [prerequisiti](#) prima di avviare lo stack.

1. [Accedi Console di gestione AWS e apri la CloudFormation console all'indirizzo /cloudformazione. https://console.aws.amazon.com](https://console.aws.amazon.com/cloudformation/)
2. [Avvia il modello.](#)

[Per implementarlo in AWS GovCloud \(Stati Uniti occidentali\), avvia questo modello.](#)

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

### Note

Questo prodotto utilizza il servizio Amazon Cognito, che al momento non è disponibile in tutti. Regioni AWS È 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	Predefinita	Description
EnvironmentName	<i>&lt;res-demo&gt;</i>	Un nome univoco assegnato all'ambiente RES che inizia con res-, non più lungo di 11 caratteri e senza lettere maiuscole.
AdministratorEmail		L'indirizzo e-mail dell'utente che completa la configurazione del prodotto. Questo utente funge anche da utente Break-Glass in caso di errore di integrazione Single Sign-On di Active Directory.
InfrastructureHostAMI	Ami- <i>[numbers or letters only]</i>	(Facoltativo) È possibile fornire un ID AMI personalizzato da utilizzare per tutti gli host dell'infrastruttura. Attualmente OSes sono supportati Amazon Linux 2 RHEL8 RHEL9, Windows Server 2019 e 2022 (x86) e Windows 10 e 11. Per ulteriori informazioni, consulta <a href="#">Preparare le immagini delle macchine Amazon (AMIs)</a> .
SSHKeyCoppia		La key pair utilizzata per connettersi agli host dell'infrastruttura.

Parametro	Predefinita	Description
ClientIP	<code>x.x.x.0/24</code> o <code>.0/32</code> <code>x.x.x</code>	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 a SSH nell'host bastion.
IAMPermissionConfine		(Facoltativo) È possibile fornire un ARN di policy gestito che verrà allegato come limite di autorizzazione a tutti i ruoli creati in RES. Per ulteriori informazioni, consulta <a href="#">Impostazione di limiti di autorizzazione personalizzati</a> .
VpcId		ID per il VPC in cui verranno avviate le istanze.
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 o un accesso limitato a Internet, seleziona false.

Parametro	Predefinita	Description
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 o 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 istanze VDI. Se più di due sono state create dallo stack di rete esterno, seleziona tutte quelle create.

Parametro	Predefinita	Description
ActiveDirectoryName	<i>corp.res.com</i>	Dominio per l'Active Directory. Non è necessario che corrisponda al nome di dominio del portale.
ADShortNome	<i>corp</i>	Il nome breve per Active Directory. Viene anche chiamato nome NetBIOS.
Base LDAP	<i>DC=corp,DC=res,DC=com</i>	Un percorso LDAP verso la base all'interno della gerarchia LDAP.
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 ARN segreto che contiene il nome utente e la password per l'utente di Active Directory, formattati come coppia nome ServiceAccount utente:password. key/value
Utenti: OU		Unità organizzativa all'interno di AD per gli utenti che effettueranno la sincronizzazione.

Parametro	Predefinita	Description
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.
Dominio: TLSCertificateSecretArn		(Facoltativo) Fornisci un ARN segreto del certificato TLS di dominio per abilitare la comunicazione TLS con AD.
EnableLdapIDMapping		Determina se i numeri UID e GID vengono generati da SSSD o se vengono utilizzati i numeri forniti dall'AD. Impostare su True per utilizzare UID e GID generati da SSSD o su False per utilizzare UID e GID forniti dall'AD. Nella maggior parte dei casi questo parametro deve essere impostato su True.

Parametro	Predefinita	Description
Disabilita ADJoin	False	Per evitare che gli host Linux entrino a far parte del dominio della directory , impostate True. Altrimenti, lascia l'impostazione predefinita False.
ServiceAccountUserDN		Fornisci il nome distinto (DN) dell'utente dell'account di servizio in Directory.
SharedHomeFilesystemID		Un ID EFS da utilizzare per il file system home condiviso per gli host VDI Linux.
CustomDomainNameforWebApp		(Facoltativo) Sottodominio utilizzato dal portale web per fornire collegamenti alla parte web del sistema.
CustomDomainNameforVDI		(Facoltativo) Sottodominio utilizzato dal portale Web per fornire collegamenti per la parte VDI del sistema.

Parametro	Predefinita	Description
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. <a href="#">Guida alla configurazione</a>
CertificateSecretARNforVDI		(Facoltativo) Questo segreto ARN archivia 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.

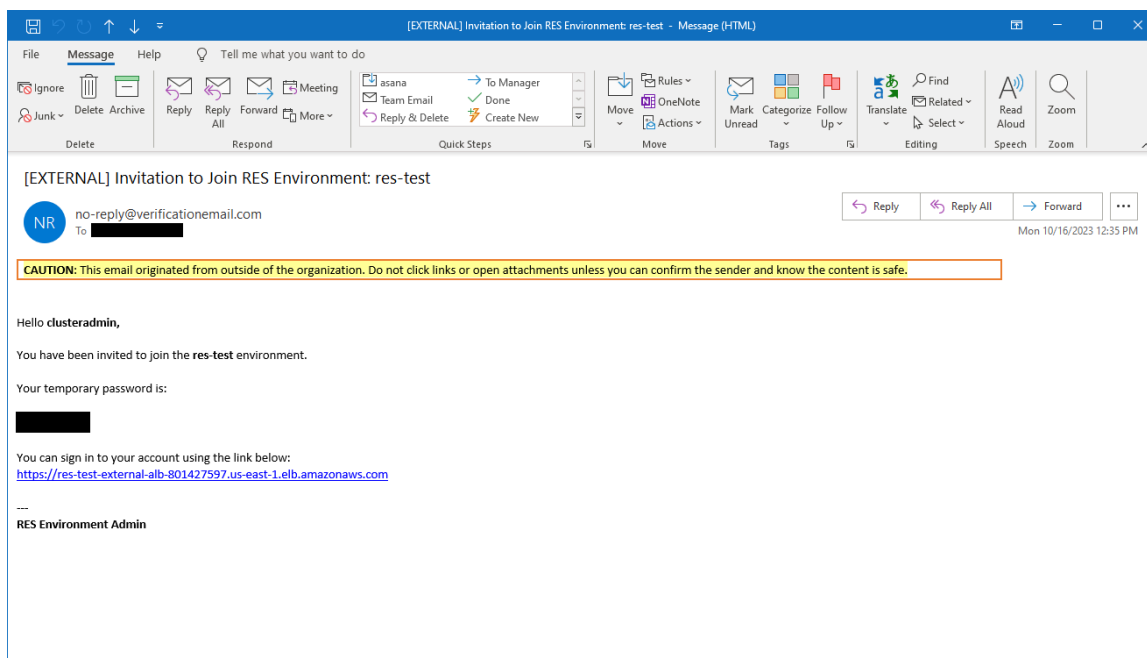
Parametro	Predefinita	Description
PrivateKeySecretARNforVDI		(Facoltativo) Questo segreto ARN memorizza la chiave privata per il certificato del tuo portale web. Se imposti un nome di dominio del portale per le tue risorse esterne automatizzate, puoi trovare questo valore nella scheda Output dello stack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

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

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

## Passaggio 2: accedi per la prima volta

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



Dopo aver effettuato l'accesso per la prima volta, puoi configurare le impostazioni nel portale web per connetterti al provider SSO. Per informazioni sulla configurazione successiva all'implementazione, consulta [Guida 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) offre due metodi per aggiornare il prodotto, a seconda che l'aggiornamento della versione sia principale o secondario.

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

## Argomenti

- [Principali aggiornamenti delle versioni](#)
- [Aggiornamenti di versione minori](#)

## Principali aggiornamenti delle versioni

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

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

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

## Aggiornamenti di versione minori

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

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

Ad esempio: "Description": "RES\_2024.1"

Per effettuare un aggiornamento secondario della versione:

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

## Disinstalla il prodotto

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

## Usando il Console di gestione AWS

1. Accedi alla [AWS CloudFormation console](#).
2. Nella pagina Stacks, seleziona lo stack di installazione di questo prodotto.
3. Scegliere Delete (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 Console di gestione AWS e apri la console Amazon EFS all'indirizzo <https://console.aws.amazon.com/efs/>.

2. Elimina tutti i file system associati a `<RES-stack-name>-shared-storage-security-group`. In alternativa, è possibile riassegnare questi file system a un altro gruppo di sicurezza per conservare i dati.
3. Accedi a Console di gestione AWS 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 Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli Bucket dal pannello di navigazione.
3. Individua i `stack-name` bucket S3.
4. Seleziona ogni bucket Amazon S3, quindi scegli Empty. Devi svuotare ogni bucket.
5. Seleziona il bucket S3 e scegli Elimina.

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

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

### Note

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

# Guida alla configurazione

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

## Argomenti

- [Gestione delle identità](#)
- [Creazione di sottodomini](#)
- [Crea un certificato ACM](#)
- [CloudWatch Registri Amazon](#)
- [Impostazione di limiti di autorizzazione personalizzati](#)
- [Configura RES-Ready AMIs](#)

## Gestione delle identità

Research and Engineering Studio può utilizzare qualsiasi provider di identità conforme a SAML 2.0. Per utilizzare Amazon Cognito come directory utente nativa che consente agli utenti di accedere al portale Web e a Linux con identità utente VDI Cognito, consulta. [Configurazione degli utenti di Amazon Cognito](#) Se hai distribuito RES utilizzando risorse esterne o prevedi di utilizzare IAM Identity Center, vedi. [Configurazione del single sign-on \(SSO\) con IAM Identity Center](#) Se disponi di un provider di identità personale conforme a SAML 2.0, consulta. [Configurazione del provider di identità per il Single Sign-On \(SSO\)](#)

## Argomenti

- [Configurazione degli utenti di Amazon Cognito](#)
- [Sincronizzazione con Active Directory](#)
- [Configurazione del single sign-on \(SSO\) con IAM Identity Center](#)
- [Configurazione del provider di identità per il Single Sign-On \(SSO\)](#)
- [Impostazione delle password per gli utenti](#)

## Configurazione degli utenti di Amazon Cognito

Research and Engineering Studio (RES) ti consente di configurare Amazon Cognito come directory utente nativa. Ciò consente agli utenti di accedere al portale Web basato su Linux con le identità

utente di Amazon VDI Cognito. Gli amministratori possono importare più utenti nel pool di utenti utilizzando un file csv da Console. AWS Per maggiori dettagli sull'importazione di utenti in blocco, consulta [Importazione di utenti in pool di utenti da un file CSV](#) nella Amazon Cognito Developer Guide. RES supporta l'utilizzo combinato di una directory utente nativa basata su Amazon Cognito e dell'SSO.

## Configurazione amministrativa

In qualità di amministratore RES, per configurare l'ambiente RES per utilizzare Amazon Cognito come directory utente, attiva il pulsante Usa Amazon Cognito come directory utente nella pagina di gestione delle identità, accessibile dalla pagina Gestione dell'ambiente. Per consentire agli utenti di registrarsi autonomamente, attiva il pulsante Autoregistrazione utente sulla stessa pagina.

RES > Environment Management > Identity Management

### Identities Management

Manage user identities

#### AWS Cognito Directory

Cognito user pool metadata. Use this for debugging issues related to the Cognito user pool.

<b>Provider Name</b> cognito-idp	<b>User Pool Id</b> <a href="#">us-west-1_CT13SJMAD</a>	<b>Domain URL</b> <a href="https://res-cafar-9ef59aa3-ff5a-4e94-8938-76861e1ef7c1.auth.us-west-1.amazoncognito.com">https://res-cafar-9ef59aa3-ff5a-4e94-8938-76861e1ef7c1.auth.us-west-1.amazoncognito.com</a>
-------------------------------------	--	--

**Provider URL**  
[https://cognito-idp.us-west-1.amazonaws.com/us-west-1\\_CT13SJMAD](https://cognito-idp.us-west-1.amazonaws.com/us-west-1_CT13SJMAD)

**Use AWS Cognito as user directory**  
Enable this for small scale user cases involving 50 or less users. User sign in through their username and password. Recommended for small teams or for demo purposes.  
 Enabled

**User self registration**  
Let anyone sign up for a Cognito user account through the UI  
 Enabled

## Flusso di accesso up/sign degli utenti

Se l'autoregistrazione degli utenti è abilitata, puoi fornire agli utenti l'URL della tua applicazione web. Lì, gli utenti troveranno un'opzione che dice Non sei ancora un utente? Registrati qui

## Research and Engineering Studio

res-new (us-west-2)

**Username**  
Enter your account's username

**Password**  
Enter your account's password

**Sign In**

[Forgot Password?](#)

[Not a user yet? Sign up here](#)

[Verify account](#)

Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

## Flusso di registrazione

Utenti che scelgono [Non sei ancora un utente? Registrati qui](#) e ti verrà chiesto di inserire la loro email e la password per creare un account.

## Create account

**Email**

**Password**

Minimum 8 characters with numbers and special symbols (@#\$\$\*&)

**Re-enter password**

**Create account**

Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

Come parte del flusso di registrazione, agli utenti verrà chiesto di inserire il codice di verifica ricevuto nell'e-mail per completare la procedura di registrazione.

## Verify email address

*To verify your email, we've sent a verification code to your email.*

**Email**

**Verification Code**  
Enter the verification code

**Verify**

[Resend verification code](#)

Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

Se l'iscrizione automatica è disattivata, gli utenti non vedranno il link di registrazione. Gli amministratori devono configurare gli utenti in Amazon Cognito al di fuori di RES. (Vedi [Creazione di account utente come amministratore](#) nella Amazon Cognito Developer Guide.)

## Research and Engineering Studio

res-new (us-west-2)

**Username**  
Enter your account's username

**Password**  
Enter your account's password

**Sign In**

[Forgot Password?](#)

Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

## Opzioni della pagina di accesso

Se sia l'SSO che Amazon Cognito sono abilitati, verrà visualizzata l'opzione Accedi con l'SSO dell'organizzazione. Quando gli utenti fanno clic su tale opzione, verranno reindirizzati alla pagina di accesso SSO. Per impostazione predefinita, gli utenti si autenticheranno con Amazon Cognito se è abilitato.

## Research and Engineering Studio

res-new(us-west-2)

**Username**  
Enter your account's username

**Password**  
Enter your account's password

**Sign In**

[Forgot Password?](#)

[Not a user yet? Sign up here](#)

[Verify account](#)

[Sign in with organization SSO](#)

Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

## Vincoli

- Il nome del tuo gruppo Amazon Cognito può contenere un massimo di sei lettere; sono accettate solo lettere minuscole.
- La registrazione ad Amazon Cognito non consentirà due indirizzi e-mail con lo stesso nome utente ma un indirizzo di dominio diverso.
- Se Active Directory e Amazon Cognito sono abilitati e il sistema rileva un nome utente duplicato, solo gli utenti di Active Directory potranno effettuare l'autenticazione. Gli amministratori devono adottare misure per non configurare nomi utente duplicati tra Amazon Cognito e il relativo Active Directory.

- Gli utenti di Cognito non potranno avviare sistemi basati su Windows VDI poiché RES non supporta l'autenticazione basata su Amazon Cognito per le istanze Windows.

## Sincronizzazione

RES sincronizza il suo database con le informazioni su utenti e gruppi di Amazon Cognito ogni ora. A tutti gli utenti che appartengono al gruppo «amministratori» verrà concesso il privilegio sudo nel proprio VDI.

Puoi anche avviare la sincronizzazione manualmente dalla console Lambda.

Avvia il processo di sincronizzazione manualmente:

1. Aprire la [console Lambda](#).
2. Cerca la Lambda di sincronizzazione Cognito. Questa Lambda segue questa convenzione di denominazione: `{RES_ENVIRONMENT_NAME}_cognito-sync-lambda`
3. Seleziona Test.
4. Nella sezione Evento di test, scegli il pulsante Test in alto a destra. Il formato del corpo dell'evento non ha importanza.

## Considerazioni sulla sicurezza per Cognito

Prima della versione 2024.12, la [registrazione delle attività degli utenti](#), che fa parte della funzionalità del piano Amazon Cognito Plus, era abilitata per impostazione predefinita. L'abbiamo rimossa dalla nostra implementazione di base per ridurre i costi per i clienti che vogliono provare RES. Puoi riattivare questa funzionalità se necessario per allinearla alle impostazioni di sicurezza cloud della tua organizzazione.

## Sincronizzazione con Active Directory

### Configurazione di runtime

Tutti i parametri CFN relativi ad Active Directory (AD) sono opzionali durante l'installazione.

**Active Directory details - Optional****ActiveDirectoryName - Optional**

Please provide the Fully Qualified Domain Name (FQDN) for your Active Directory. For example, developer.res.hpc.aws.dev

**ADShortName - Optional**

Please provide the short name in Active directory

**LDAPBase - Optional**

Please provide the Active Directory base string Distinguished Name (DN) For example, dc=developer,dc=res,dc=hpc,dc=aws,dc=dev

**LDAPConnectionURI - Optional**

Please provide the active directory connection URI (e.g. ldap://www.example.com)

**ServiceAccountCredentialsSecretArn - Optional**

Directory Service Root (Service Account) Credentials Secret ARN. The username and password for the Active Directory ServiceAccount user formatted as a username:password key/value pair.

**UsersOU - Optional**

Please provide Users Organization Unit in your active directory for example, OU=Users,DC=RES,DC=example,DC=internal

**GroupsOU - Optional**

Please provide user groups Organization Unit in your active directory

**SudoersGroupName - Optional**

Please provide group name of users who will be able to sudo in your active directory

**ComputersOU - Optional**

Please provide Organization Unit for compute and storage servers in your active directory

**DomainTLSCertificateSecretArn - Optional**

AD Domain TLS Certificate Secret ARN

**EnableLdapIDMapping - Optional**

Set to False to use the uidNumbers and gidNumbers for users and group from the provided AD. Otherwise set to True.

**DisableADJoin - Optional**

Set to True to prevent linux hosts from joining the Directory Domain. Otherwise set to False

**ServiceAccountUserDN - Optional**

Provide the Distinguished name (DN) of the service account user in the Active Directory

Per qualsiasi ARN segreto fornito in fase di esecuzione (ad esempio ServiceAccountCredentialsSecretArn o DomainTLSCertificateSecretArn), assicurati di aggiungere i seguenti tag al segreto per RES per ottenere le autorizzazioni per leggere il valore segreto:

- chiave: `res:EnvironmentName`, valore: *<your RES environment name>*
- chiave: `res:ModuleName`, valore: `directoryservice`

Tutti gli aggiornamenti della configurazione AD nel portale web verranno rilevati automaticamente durante la successiva sincronizzazione AD programmata (ogni ora). Gli utenti potrebbero dover riconfigurare l'SSO dopo aver modificato la configurazione AD (ad esempio, se passano a un AD diverso).

Dopo l'installazione iniziale, gli amministratori possono visualizzare o modificare la configurazione AD nel portale web RES nella pagina di gestione delle identità:

### Active Directory Domain [↗](#)

Configuration setting for a specific AD domain

[Start AD Synchronization](#)

Latest AD synchronization completed at 3/5/2025, 3:01:16 PM

<p><b>Domain Name</b> corp.res.com</p> <p><b>LDAP Connection URI</b> ldap://corp.res.com</p> <p><b>Users OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p> <p><b>Groups Filter</b> -</p> <p><b>Enable LDAP ID Mapping</b> true</p>	<p><b>Short Name (NETBIOS)</b> CORP</p> <p><b>Service Account User DN</b> <a href="#">🔗</a> CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com</p> <p><b>Users Filter</b> -</p> <p><b>Sudoers Group Name</b> RESAdministrators</p> <p><b>Disable AD Join</b> false</p>	<p><b>LDAP Base</b> dc=corp,dc=res,dc=com</p> <p><b>Service Account Credentials Secret ARN</b> <a href="#">🔗</a> arn:aws:secretsmanager:us-east-1:905418417732:secret:CredentialsSecret-res-deploy-RESExternal-GZBJSYJBLAW4-DirectoryService-1AUMFPSAPKV6E-TVYM7Q</p> <p><b>Groups OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p> <p><b>Computers OU</b> OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p> <p><b>Domain TLS Certificate Secret ARN</b> -</p>
---	--	--

### Active Directory Synchronization ✕

**Active Directory Name**  
Type the name for the Active Directory. It does not need to match the portal domain name.

**Short Name (NETBIOS)**  
Provide the short name for the Active Directory. This is also called the netBIOS name.

**Service Account User DN**  
Provide the distinguished name (DN) of the service account user in Directory.

**Service Account Credentials Secret ARN**  
Provide a Secret ARN which contains the username and password for the Active Directory ServiceAccount user, formatted as a username:password key/value pair.

The secret should contain the username and password in the format username:password.

**LDAP Connection URI**  
Specify the connection URI for the Active Directory server.

**LDAP Base**  
Specify the LDAP path within the directory hierarchy.

**Disable Active Directory Join**  
To prevent Linux hosts from joining the directory domain, check the box. Otherwise, leave in the default setting of unchecked.

**Enable LDAP ID Mapping**  
Determines if UID and GID numbers are generated by SSSD or if the numbers provided by the AD are used. Check to use SSSD generated UID and GID, or uncheck to use UID and GID provided by the AD. For most cases this parameter should be checked.

**Organizational Units (OU)**  
Provide the Organizational Unit within AD that will sync.

**Users OU**

**Groups OU**

**Computers OU**

**Sudoers Group Name**  
Provide the group name that contains all users with sudoer access on instances at install and administrator access on RES.

**► Additional Settings**

Cancel Submit

## Impostazioni aggiuntive

### Filtri

Gli amministratori possono filtrare gli utenti o i gruppi da sincronizzare utilizzando le opzioni Filtro utenti e Filtro gruppi. I filtri devono seguire la [sintassi del filtro LDAP](#). Un esempio di filtro è:

```
(sAMAccountname=<user>)
```

### Parametri SSSD personalizzati

Gli amministratori possono fornire un dizionario di coppie chiave-valore contenente parametri e valori SSSD da scrivere [domain\_type/DOMAIN\_NAME] nella sezione del file di configurazione SSSD sulle istanze del cluster. RES applica automaticamente gli aggiornamenti SSSD: riavvia il servizio SSSD sulle istanze del cluster e attiva il processo di sincronizzazione AD. Per una descrizione completa del file di configurazione SSSD, consulta le pagine man di Linux per. SSSD

#### Additional SSSD Configuration - optional

Provide additional SSSD configs for your AD domain.

Key	Value
ldap_id_mapping	true
join_active_directory	true

[Add Parameter](#)

I parametri e i valori SSSD devono essere compatibili con la configurazione RES SSSD come descritto qui:

- `id_provider` è impostato internamente da RES e non deve essere modificato.
- Le configurazioni relative ad `ADldap_uri`, tra cui `ldap_search_base`, `ldap_default_bind_dn` e `ldap_default_authtok` sono impostate in base alle altre configurazioni AD fornite e non devono essere modificate.

L'esempio seguente abilita il livello di debug per i log SSSD:

**Additional SSSD Configuration - optional**

Provide additional SSSD configs for your AD domain.

Key	Value
ldap_id_mapping	true
join_active_directory	true
debug_level	0xFFFF0

[Remove](#)

[Add Parameter](#)

Come avviare o interrompere manualmente la sincronizzazione (versione 2025.03 e successive)

Vai alla pagina di gestione delle identità e scegli il pulsante Avvia sincronizzazione AD nel contenitore del dominio Active Directory per attivare una sincronizzazione AD su richiesta.

**Active Directory Domain** **Start AD Synchronization**

Configuration setting for a specific AD domain

**Domain Name**

corp.res.com

**Short Name (NETBIOS)**

CORP


**LDAP Base**

dc=corp,dc=res,dc=com

**LDAP Connection URI**

ldap://corp.res.com

**Service Account User DN**

 CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com
**Service Account Credentials Secret ARN**

 arn:aws:secretsmanager:us-west-2:590184128708:secret:RESServiceAccountCredentialsSecret-ISyIRg
**Users OU**

OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Users Filter**

-

**Groups OU**

OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Groups Filter**

-

**Sudoers Group Name**

RESAdministrators

**Computers OU**

OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Enable LDAP ID Mapping**

true

**Disable AD Join**

false

**Domain TLS Certificate Secret ARN**

-

**Additional SSSD Configuration**

-

Per interrompere una sincronizzazione AD in corso, seleziona il pulsante Arresta sincronizzazione AD nel contenitore del dominio Active Directory.

**Active Directory Domain** 

AD Synchronization in progress...

**Stop AD Synchronization**

Configuration setting for a specific AD domain

Latest AD synchronization initialized at 2/20/2025, 3:20:19 PM

**Domain Name**

corp.res.com

**Short Name (NETBIOS)**



CORP

**LDAP Base**

dc=corp,dc=res,dc=com

**LDAP Connection URI**

ldap://corp.res.com

**Service Account User DN**

 CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com
**Service Account Credentials Secret ARN**

 arn:aws:secretsmanager:us-west-2:590184128708:secret:RESServiceAccountCredentialsSecret-ISyIRg
**Users OU**

OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Users Filter**

-

**Groups OU**

OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Groups Filter**

-

**Sudoers Group Name**

RESAdministrators

**Computers OU**

OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com

**Enable LDAP ID Mapping**

true

**Disable AD Join**

false

**Domain TLS Certificate Secret ARN**

-

**Additional SSSD Configuration**

-

Puoi anche controllare lo stato di sincronizzazione AD e l'ora di sincronizzazione più recente nel contenitore del dominio Active Directory.

### Active Directory Domain ↗

Configuration setting for a specific AD domain

Start AD Synchronization

Latest AD synchronization completed at 2/20/2025, 3:21:00 PM

<p><b>Domain Name</b> corp.res.com</p>	<p><b>Short Name (NETBIOS)</b> CORP</p>	<p><b>LDAP Base</b> dc=corp,dc=res,dc=com</p>
<p><b>LDAP Connection URI</b> ldap://corp.res.com</p>	<p><b>Service Account User DN</b>  CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com</p>	<p><b>Service Account Credentials Secret ARN</b>  arn:aws:secretsmanager:us-west-2:590184128708:secret:RESServiceAccountCredentialsSecret-ISylRg</p>
<p><b>Users OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p>	<p><b>Users Filter</b> -</p>	<p><b>Groups OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p>
<p><b>Groups Filter</b> -</p>	<p><b>Sudoers Group Name</b> RESAdministrators</p>	<p><b>Computers OU</b> OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com</p>
<p><b>Enable LDAP ID Mapping</b> true</p>	<p><b>Disable AD Join</b> false</p>	<p><b>Domain TLS Certificate Secret ARN</b> -</p>
<p><b>Additional SSSD Configuration</b> -</p>		

Come eseguire manualmente la sincronizzazione (release 2024.12 e 2024.12.01)

Il processo di sincronizzazione di Active Directory è stato spostato dall'infra host Cluster Manager a un'unica attività Amazon Elastic Container Service (ECS) dietro le quinte. L'esecuzione del processo è pianificata ogni ora e puoi trovare un'attività ECS in esecuzione nella console Amazon ECS sotto il `<res-environment-name>-ad-sync-cluster` cluster mentre è in corso.

Per avviarlo manualmente:

1. Vai alla [console Lambda](#) e cerca la lambda chiamata. `<res-environment>-scheduled-ad-sync`
2. Apri la funzione Lambda e vai a Test
3. Nell'Event JSON inserisci quanto segue:

```

{
  "detail-type": "Scheduled Event"
}
```

4. Scegli Test (Esegui test).

5. Osserva i log dell'attività AD Sync in esecuzione in → Gruppi di log CloudWatch→.  
<environment-name>/ad-sync Vedrai i log di ciascuna delle attività ECS in esecuzione.  
Seleziona il più recente per visualizzare i log.

#### Note

- Se modifichi i parametri AD o aggiungi filtri AD, RES aggiungerà i nuovi utenti in base ai nuovi parametri specificati e rimuoverà gli utenti che erano stati precedentemente sincronizzati e non sono più inclusi nello spazio di ricerca LDAP.
- RES non può rimuovere un user/group elemento assegnato attivamente a un progetto. È necessario rimuovere gli utenti dai progetti per fare in modo che RES li rimuova dall'ambiente.

## Configurazione SSO

Dopo aver fornito la configurazione AD, gli utenti devono configurare Single Sign-On (SSO) per poter accedere al portale web RES come utenti AD. La configurazione SSO è stata spostata dalla pagina Impostazioni generali alla nuova pagina di gestione delle identità. Per ulteriori informazioni sulla configurazione dell'SSO, consulta. [Gestione delle identità](#)

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

Se non disponi già di un centro di identità collegato all'Active Directory gestita, inizia con [Fase 1: configurare un centro di identità](#). Se hai già un centro di identità collegato all'Active Directory gestita, inizia con [Fase 2: Connect a un centro di identità](#).

#### Note

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

## Fase 1: configurare un centro di identità

### Abilitazione di IAM Identity Center

1. Accedi 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. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli Aggiungi applicazione.
4. In Preferenze di configurazione, scegli Ho un'applicazione che voglio configurare.
5. In Tipo di applicazione, scegli SAML 2.0.
6. Scegli Next (Successivo).
7. Inserisci il nome visualizzato e la descrizione che desideri utilizzare.
8. In Metadati IAM Identity Center, copia il link per il file di metadati IAM Identity Center SAML. Ne avrai bisogno per configurare IAM Identity Center con il portale RES.
9. In Proprietà dell'applicazione, inserisci l'URL di avvio dell'applicazione. Ad esempio, <your-portal-domain>/sso.
10. In URL ACS dell'applicazione, inserite l'URL di reindirizzamento dal portale RES. Per trovarlo:
  - a. In Gestione dell'ambiente, scegli Impostazioni generali.
  - b. Seleziona la scheda Identity provider.
  - c. In Single Sign-On, troverai l'URL di reindirizzamento SAML.
11. In Application SAML Audience, inserisci l'URN di Amazon Cognito.

Per creare l'urna:

- a. Dal portale RES, apri Impostazioni generali.
- b. 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 inserito l'URN di Amazon Cognito, 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, scegli Indirizzo e-mail.
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 IAM Identity Center

1. Dall'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'ambiente RES

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. Scegli SAML.
  - b. In Nome del fornitore, inserisci un nome intuitivo.
  - c. Scegli Inserisci l'URL dell'endpoint del documento di metadati.
  - d. Inserisci l'URL che hai copiato durante. [Configurazione dell'applicazione in IAM Identity Center](#)
  - e. In Attributo email del fornitore, inserisci 'email'.
  - f. Seleziona Invia.
5. Aggiorna la pagina e verifica che lo stato sia visualizzato come abilitato.

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

Research and Engineering Studio si integra con qualsiasi provider di identità SAML 2.0 per autenticare l'accesso degli utenti al portale RES. Questi passaggi forniscono indicazioni per l'integrazione con il provider di identità SAML 2.0 scelto. Se intendi utilizzare IAM Identity Center, consulta [Configurazione del single sign-on \(SSO\) con IAM Identity Center](#).

### Note

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


### Argomenti

- [Configura il tuo provider di identità](#)
- [Configura RES per utilizzare il tuo provider di identità](#)
- [Configurazione del provider di identità in un ambiente non di produzione](#)
- [Eseguire il debug dei problemi di SAML IdP](#)

## Configura il tuo provider di identità

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

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


 Note

A seconda dell'IdP, l'URL di reindirizzamento SAML potrebbe avere un nome diverso:

- URL dell'applicazione
- URL dell'Assertion Consumer Service (ACS)
- URL vincolante POST ACS

Per ottenere l'URL

1. Accedi a RES come amministratore o amministratore del cluster.
  2. Passa a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
  3. Scegli SAML Redirect URL.
- URI SAML Audience: l'ID univoco dell'entità di audience SAML sul lato del fornitore di servizi.

 Note

A seconda dell'IdP, l'URI SAML Audience potrebbe avere un nome diverso:

- ClientID
- Applicazione SAML Audience
- ID dell'entità SP

Fornisci l'input nel seguente formato.

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

Per trovare il tuo URI SAML Audience

1. Accedi a RES come amministratore o amministratore del cluster.
  2. Passa a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
  3. Scegli User Pool Id.
3. L'asserzione SAML pubblicata su RES deve avere quanto segue fields/claims impostato sull'indirizzo e-mail dell'utente:
- Oggetto o NameID SAML
  - Posta elettronica SAML
4. Il tuo IdP si aggiunge fields/claims all'asserzione SAML, in base alla configurazione. RES richiede questi campi. La maggior parte dei provider compila automaticamente questi campi per impostazione predefinita. Fai riferimento ai seguenti input e valori dei campi se devi configurarli.
- AudienceRestriction— Impostato su. `urn:amazon:cognito:sp:user-pool-id` Sostituiscilo `user-pool-id` con l'ID del tuo pool di utenti Amazon Cognito.

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

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

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

- **SubjectConfirmationData**— Imposta Recipient sull'`saml2/idpresponseendpoint` del pool di utenti e sull'`InResponseToID` della richiesta SAML originale.

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

- **AuthnStatement**— Configura come segue:

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

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

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

Per ottenere l'URL del dominio

1. Accedi a RES come amministratore o amministratore del cluster.
  2. Passa a Gestione dell'ambiente ⇒ Impostazioni generali ⇒ Identity Provider.
  3. Scegli l'URL del dominio.
6. Se il tuo IdP accetta un certificato di firma per stabilire un rapporto di fiducia con Amazon Cognito, scarica il certificato di firma Amazon Cognito e caricalo nel tuo IdP.

Per ottenere il certificato di firma

1. Apri la console Amazon Cognito nella [Guida introduttiva a Console di gestione AWS](#)

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.

### Cognito user pool sign-in Info

Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

**Cognito user pool sign-in options**  
User name  
Email

**User name requirements**  
User names are not case sensitive

### Federated identity provider sign-in (1) Info

Your app users can sign-in through external social identity providers like Facebook, Google, Amazon, or Apple, and through your on-prem directories via SAML or Open ID Connect.

Search identity providers by name

Identity provider	Identity provider type	Created time	Last updated time
<input type="radio"/> <a href="#">idc</a>	SAML	2 weeks ago	3 hours ago

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

#### Note

Questo non si applica a Keycloak e IDC.

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

## Configura RES per utilizzare il tuo provider di identità

Per completare la configurazione Single Sign-On per RES

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

## Environment Settings

View and manage environment settings. [View Environment Status](#)

Environment Name res-gaenv1	AWS Region us-east-1	S3 Bucket res-gaenv1-cluster-us-east-1-088837573664
--------------------------------	-------------------------	--

< General Network **Identity Provider** Directory Service Analytics Metrics CloudWatch Logs SES EC2 Bac >

### Identity Provider

Provider Name cognito-idp	User Pool Id us-east-1_reuFsm8SE	Administrators Group Name administrators-cluster-group
Managers Group Name managers-cluster-group	Domain URL https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazoncognito.com	Provider URL https://cognito-idp.us-east-1.amazonaws.com/us-east-1_reuFsm8SE

### Single Sign-On

Status Enabled	SAML Redirect URL https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazoncognito.com/saml2/idpresponse	OIDC Redirect URL https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazoncognito.com/oauth2/idpresponse
-------------------	---	--

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

## Single Sign On Configuration ✕

### Identity Provider

Choose the third-party identity provider that you would like to configure.

**SAML**  
Configure trust between Cognito and a SAML 2.0-compatible identity provider.

**OIDC**  
Configure trust between Cognito and an OIDC identity provider,

### Provider Name

Name used for the provider in cognito

### Metadata Document Source

Provide a SAML metadata document. This document is issued by your SAML provider.

Upload metadata document

Enter metadata document endpoint URL

### Metadata document

### Provider Email Attribute

The Email attribute used to map email between your idp and the Amazon Cognito user pool

### Refresh Token Expiration (hours)

Must be between 1 and 87600 (10 years)

- Per Identity Provider, scegli SAML.
- Per Provider Name, inserisci un nome univoco per il tuo provider di identità.

**Note**

I seguenti nomi non sono consentiti:

- Cognito
- IdentityCenter

- In Origine del documento di metadati, scegli l'opzione appropriata e carica il documento XML con metadati o fornisci l'URL dal provider di identità.
  - Per Provider Email Attribute, inserisci il valore di testo. `email`
  - Seleziona Invia.
- Ricarica la pagina delle impostazioni dell'ambiente. Il Single Sign-On è abilitato se la configurazione è corretta.

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

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

- Nome del provider: non può essere modificato
- Documento o URL di metadati: può essere modificato
- Attributo email del provider: può essere modificato

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

- Passa alla console Amazon Cognito.
- Dalla navigazione, scegli Pool di utenti.
- Seleziona il tuo pool di utenti per visualizzare la panoramica del pool di utenti.
- Dalla scheda Esperienza di accesso, accedi a Federated Identity Provider e apri il provider di identità configurato.
- 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.

**Attribute mapping (1)** [Info](#) Edit

View, add, and edit attribute mappings between SAML and your user pool. < 1 > ⚙

User pool attribute	SAML attribute
email	email

**Metadata document** [Info](#) Replace metadata

View and update your SAML metadata. This document is issued by your SAML provider. It includes the issuer's name, expiration information, and keys that can be used to validate the response from the identity provider.

<p><b>Metadata document source</b> Enter metadata document endpoint URL</p>	<p><b>Metadata document endpoint URL</b> https://portal.sso.us-west-2.amazonaws.com/saml/metadata/MDg4ODM3NTczNjY0X2lucy04M2EyYTcyMGUzZTFIMDI4</p>
---	--

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 a Filtri e inserisci i seguenti parametri:
    - Nome dell'attributo: `key`
    - Valore — `identity-provider.cognito.sso_idp_provider_email_attribute`
  - d. Scegli 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.

▼ Scan or query items

Scan  Query

Select a table or index: Table - res-jan19.cluster-settings

Select attribute projection: All attributes

▼ Filters **6**

Attribute name	Type	Condition	Value	
key	String	Equal to	identity-provider	Remove

Add filter

**7** Run Reset

Completed. Read capacity units consumed: 13

Items returned (1)

Item	Value
key (String)	identity-provider.cognito.s...

Edit String dialog: email

Save

## Eseguire il debug dei problemi di SAML IdP

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

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

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

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

## Impostazione delle password per gli utenti

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

### Note

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

1. 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 CNAME come 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 il VDC, recupera l'indirizzo NLB.
  - a. Apri la [AWS CloudFormation console](#).
  - b. Scegli <environment-name>-vdc.
  - c. Scegli Risorse e apri. <environmentname>-vdc-external-nlb
  - d. Copia il nome DNS dal NLB.
8. Apri la [console Route 53](#).
9. Trova il tuo dominio e scegli Crea record.
10. In Nome del record, inseriscivdc.

11. In Record type (Tipo di record), seleziona CNAME.
12. Per l'NLB, inserisci il DNS.
13. Scegli Crea record.

## Crea un certificato ACM

Per impostazione predefinita, RES ospita il portale Web con un sistema di bilanciamento del carico delle applicazioni utilizzando il dominio `amazonaws.com`. Per utilizzare il tuo dominio, dovrai configurare un SSL/TLS certificato pubblico fornito da te o richiesto da AWS Certificate Manager (ACM). Se utilizzi ACM, riceverai un nome di AWS risorsa che dovrai fornire come parametro per crittografare il SSL/TLS canale 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 distribuisce lo stack di risorse esterne. [Crea risorse esterne](#)

Per creare un certificato per domini personalizzati:

1. Dalla console, apri [AWS Certificate Manager](#) per richiedere un certificato pubblico. Se stai distribuendo in AWS GovCloud (Stati Uniti occidentali), crea il certificato nel tuo account di GovCloud partizione.
2. Scegli Richiedi un certificato pubblico e scegli Avanti.
3. In Nomi di dominio, richiedi un certificato per entrambi `*.PortalDomainName` e `PortalDomainName`.
4. In Metodo di convalida, scegli Convalida DNS.
5. Scegli Richiedi.
6. Dall'elenco dei certificati, apri i certificati richiesti. Lo stato di ogni certificato sarà In attesa di convalida.

### Note

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

7. Esegui una delle seguenti 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 chiave e il valore CNAME. Dall'account di partizione commerciale, utilizza i valori per creare un nuovo record nella Public Hosted Zone. Lo stato del certificato dovrebbe cambiare in Emesso.

8. Copia il nuovo ARN del certificato da immettere come parametro per.  
ACMCertificateARNforWebApp

## CloudWatch Registri Amazon

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

CloudWatch Gruppi di log	Retention
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-endpoints	Non scadono mai
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-manager-scheduled-ad-sync	Non scadono mai
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-settings	Non scadono mai
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -oauth-credentials	Non scadono mai
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -self-signed-certificate	Non scadono mai
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -update-cluster-prefix-list	Non scadono mai

CloudWatch Gruppi di log	Retention
<code>/aws/lambda/ &lt;installation-stack-name&gt;-vdc-scheduled-event-transformer</code>	Non scadono mai
<code>/aws/lambda/ &lt;installation-stack-name&gt;-vdc-update-cluster-manager-client-scope</code>	Non scadono mai
<code>/&lt;installation-stack-name&gt; /cluster-manager</code>	3 mesi
<code>/&lt;installation-stack-name&gt; /vdc/controller</code>	3 mesi
<code>/&lt;installation-stack-name&gt; /vdc/dcv-broker</code>	3 mesi
<code>/&lt;installation-stack-name&gt; /vdc/dcv-connection-gateway</code>	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 da RES aggiungendo limiti di autorizzazione personalizzati. Un limite di autorizzazione personalizzato può essere definito come parte dell' CloudFormation installazione RES fornendo l'ARN del limite di autorizzazione come parte del parametro Boundary. IAMPermission Nessun limite di autorizzazione viene impostato su alcun ruolo RES se questo parametro viene lasciato vuoto. Di seguito è riportato l'elenco delle azioni che i ruoli RES richiedono per operare. Assicurati che qualsiasi limite di autorizzazione che intendi utilizzare in modo esplicito consenta le seguenti azioni:

```
[
  {
```

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

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

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

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

## Configura RES-Ready AMIs

Con le Amazon Machine Images (AMI) pronte per RESS, puoi preinstallare le dipendenze RES per le istanze di desktop virtuali (VDI) sulle tue AMI personalizzate. L'uso di AMI pronte per RESS migliora i tempi di avvio delle istanze VDI utilizzando le immagini predefinite. Utilizzando EC2 Image Builder, puoi creare e AMIs registrare i tuoi stack software come nuovi. 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 un ruolo IAM per accedere all'ambiente RES](#)
- [Crea il componente EC2 Image Builder](#)
- [Prepara la tua ricetta per EC2 Image Builder](#)
- [Configurazione dell'infrastruttura EC2 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 un ruolo IAM per accedere all'ambiente RES

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

Il tuo ruolo richiede:

- Relazioni affidabili che includono il servizio Amazon EC2.
- Amazon SSMManaged InstanceCore e EC2 InstanceProfileForImageBuilder le politiche.
- Una policy RES personalizzata con accesso limitato a DynamoDB e Amazon S3 all'ambiente RES distribuito.

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

1. Inizia creando una nuova policy da allegare al tuo ruolo: IAM -> Policies -> Create policy
2. Seleziona JSON dall'editor delle politiche.
3. Copia e incolla la politica mostrata qui nell'editor, sostituendola `us-east-1` con quella desiderata Regione AWS, `111122223333` con l'ID del tuo AWS account e `{RES-EnvironmentName}` con il tuo RES, EnvironmentName ove applicabile.

Politica RES:

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RES DynamoDB Access",
      "Effect": "Allow",
      "Action": "dynamodb:GetItem",
      "Resource": "arn:aws:dynamodb:us-east-1:111122223333:table/{RES-EnvironmentName}.cluster-settings",
      "Condition": {
        "ForAllValues:StringLike": {
          "dynamodb:LeadingKeys": [
            "global-settings.gpu_settings.*",
            "global-settings.package_config.*",
            "cluster-manager.host_modules.*",
            "identity-provider.cognito.enable_native_user_login"
          ]
        }
      }
    },
    {
      "Sid": "RES S3 Access",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": [
        "arn:aws:s3:::{RES-EnvironmentName}-cluster-us-east-1-111122223333/idea/vdc/res-ready-install-script-packages/*",
        "arn:aws:s3:::research-engineering-studio-us-east-1/host_modules/*"
      ]
    }
  ]
}
```

4. Scegli Avanti e fornisci un nome e una descrizione facoltativa per completare la creazione della politica.
5. Per creare il ruolo, inizia andando su IAM -> Roles -> Create role.
6. In Trusted Entity Type, seleziona "AWS service».

7. Seleziona EC2 nel menu a discesa Servizio o caso d'uso.
8. Nella sezione Caso d'uso, seleziona EC2, quindi scegli Avanti.
9. Cerca e seleziona il nome della policy che hai creato in precedenza.
10. Scegli Avanti e fornisci un nome e una descrizione opzionale per completare la creazione del ruolo.
11. Seleziona il tuo nuovo ruolo e verifica che la relazione Trust corrisponda a quanto segue:

Entità di relazione affidabile:

JSON

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

## Crea il componente EC2 Image Builder

Segui le istruzioni per [creare un componente utilizzando la console Image Builder](#) nella Guida per l'utente di Image Builder.

Inserisci i dettagli del componente:

1. Per Tipo, scegli Costruisci.
2. Per il sistema operativo (OS) Image, scegli Linux o Windows.
3. Per Nome componente, inserisci un nome significativo, ad esempio **research-and-engineering-studio-vdi-*<operating-system>***.
4. Inserisci il numero di versione del componente e, facoltativamente, aggiungi una descrizione.

5. Per il documento di definizione, inserisci il seguente file di definizione. Se si verificano errori, il file YAML è sensibile allo spazio ed è la causa più probabile.

## Linux

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

phases:
  - name: build
    steps:
      - name: PrepareRESBootstrap
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
```

```

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

```

```
inputs:
  delaySeconds: 0
```

## Windows

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

phases:
  - name: build
    steps:
      - name: CreateRESBootstrapFolder
        action: CreateFolder
        onFailure: Abort
        maxAttempts: 3
```

```

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

```

6. Crea eventuali tag opzionali e scegli Crea componente.

## Prepara la tua ricetta per EC2 Image Builder


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

RES supporta i seguenti sistemi operativi di immagini:

- Amazon Linux 2 (x86 e ARM64)
- Ubuntu 22.04.3 (x86)
- RHEL 8 (x86) e 9 (x86)
- Windows Server 2019, 2022 (x86)
- Windows 10, 11 (x86)

Create a new recipe

1. Apri la console EC2 Image Builder <https://console.aws.amazon.com/imagebuilder> all'indirizzo.
2. In Risorse salvate, scegli Ricette di immagini.
3. Scegli Crea ricetta di immagine.
4. Inserisci un nome univoco e un numero di versione.
5. Seleziona un'immagine di base supportata da RES.
6. In Configurazione dell'istanza, installa un agente SSM se non è preinstallato. Inserisci le informazioni in Dati utente e qualsiasi altro dato utente necessario.

 Note

Per informazioni su come installare un agente SSM, consulta:

- [Installazione manuale dell'agente SSM su istanze EC2](#) per Linux.
- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2](#) per Windows Server.

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

### ⚠ Important

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

**Components (2)** [Info](#) [Create component](#)

You can select a maximum of 20 components (including build and test) for a recipe. Drag the components up and down to sort the sequence after selection. Components cannot be modified or replaced after a recipe is created. Automatic version choices are provided for each component.

**Build components (2)** [Expand all](#)

Build components are software scripts that define a sequence of steps for downloading, installing, and configuring software packages. They also define validation steps.

- aws-cli-version-2-linux**  
Use latest version Amazon managed
- res-vdi-ubuntu**  
Version 1.0.0 Owned by me

**Input parameters**  
Component parameters are plain text values, and are logged in AWS CloudTrail. We recommend that you use [AWS Secrets Manager](#) or the [AWS Systems Manager Parameter Store](#) to store your secrets.

Parameter name	Description	Value
AWSAccountID	RES Environment AWS Account ID	<input type="text"/> Enter value ⊗ Parameter is required.
RESEnvName	RES Environment Name	<input type="text"/> Enter value ⊗ Parameter is required.
RESEnvRegion	RES Environment Region	<input type="text"/> Enter value ⊗ Parameter is required.
RESEnvReleaseVersion	RES Release Version	<input type="text"/> Enter value ⊗ Parameter is required.

[Add build components](#)

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

### Modify a recipe

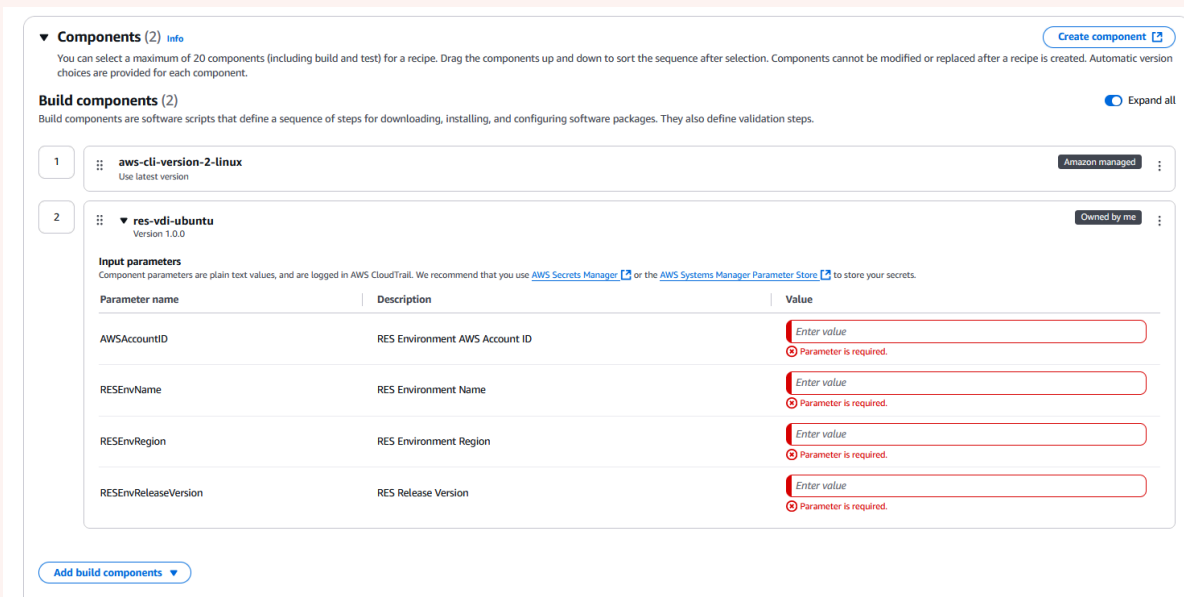
Se disponi di una ricetta EC2 Image Builder esistente, puoi utilizzarla aggiungendo i seguenti componenti:

- Per le ricette basate su Linux, aggiungi il componente di `aws-cli-version-2-linux` compilazione gestito da Amazon alla ricetta. Gli script di installazione RES utilizzano il AWS CLI per fornire l'accesso VDI ai valori di configurazione per le impostazioni del cluster DynamoDB. Windows non richiede questo componente.

2. Aggiungi il componente EC2 Image Builder creato per il tuo ambiente Linux o Windows e inserisci i valori dei parametri richiesti. I seguenti parametri sono input obbligatori: AWSAccount ID, RESEnv Nome, RESEnv Regione e. RESEnv ReleaseVersion

### Important

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



**Components (2)** [Info](#) [Create component](#)

You can select a maximum of 20 components (including build and test) for a recipe. Drag the components up and down to sort the sequence after selection. Components cannot be modified or replaced after a recipe is created. Automatic version choices are provided for each component.

**Build components (2)** [Expand all](#)

Build components are software scripts that define a sequence of steps for downloading, installing, and configuring software packages. They also define validation steps.

Parameter name	Description	Value
AWSAccountID	RES Environment AWS Account ID	<input type="text" value="Enter value"/> Parameter is required.
RESEnvName	RES Environment Name	<input type="text" value="Enter value"/> Parameter is required.
RESEnvRegion	RES Environment Region	<input type="text" value="Enter value"/> Parameter is required.
RESEnvReleaseVersion	RES Release Version	<input type="text" value="Enter value"/> Parameter is required.

[Add build components](#)

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

## Configurazione dell'infrastruttura EC2 Image Builder

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

- Per creare una nuova configurazione dell'infrastruttura, consulta [Creare una configurazione dell'infrastruttura](#).
- Per utilizzare una configurazione dell'infrastruttura esistente, [aggiorna una configurazione dell'infrastruttura](#).

Per configurare l'infrastruttura Image Builder:

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

## Configurazione della pipeline di immagini di Image Builder

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

Create a new Image Builder pipeline

1. Aprire la console Image Builder all'indirizzo. <https://console.aws.amazon.com/imagebuilder>
2. 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 in [Prepara la tua ricetta per EC2 Image Builder](#). Verifica che i dettagli della ricetta siano corretti.
6. Per Definisci il processo di creazione dell'immagine, scegli il flusso di lavoro predefinito o personalizzato a seconda del caso d'uso. Nella maggior parte dei casi, i flussi di lavoro predefiniti sono sufficienti. Per ulteriori informazioni, consulta [Configurare i flussi di lavoro di immagini per la pipeline EC2 Image Builder](#).
7. Per Definisci la configurazione dell'infrastruttura, scegli Scegli la configurazione dell'infrastruttura esistente e seleziona la configurazione dell'infrastruttura creata in. [Configurazione dell'infrastruttura EC2 Image Builder](#) Verifica che i dettagli dell'infrastruttura siano corretti.

8. Per Definisci le impostazioni di distribuzione, scegli Crea impostazioni di distribuzione utilizzando i valori predefiniti del servizio. L'immagine di output deve risiedere nello stesso ambiente Regione AWS RES. Utilizzando le impostazioni predefinite del servizio, l'immagine verrà creata nella regione in cui viene utilizzato Image Builder.
9. Esamina i dettagli della pipeline e scegli Crea pipeline.

### Modify an existing Image Builder pipeline

1. Per utilizzare una pipeline esistente, modifica i dettagli in modo da utilizzare la ricetta creata in. [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 AMI ID, inserisci l'ID AMI dell'immagine di output incorporata [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](#)
- [Monitoraggio e controllo dei costi](#)
- [Dashboard di analisi dei costi](#)
- [Gestione della sessione](#)
- [Gestione dell'ambiente](#)

## Gestione dei segreti

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

Nome segreto	Description	RES generato	Amministratore inserito
<code>&lt;envname&gt; -sso-client-secret</code>	Single Sign-On OAuth2 Client Secret per l'ambiente	✓	
<code>&lt;envname&gt; -vdc-client-secret</code>	vdc ClientSecret	✓	
<code>&lt;envname&gt; -vdc-client-id</code>	vdc ClientId	✓	
<code>&lt;envname&gt; -vdc-gateway-certificate-private-key</code>	Chiave privata del certificato autofirmato per il dominio	✓	

Nome segreto	Description	RES generato	Amministratore inserito
<i>&lt;envname&gt;</i> - vdc-gateway- certificate- certificate	Certificato autofirmato per dominio	✓	
<i>&lt;envname&gt;</i> -cluster- manager- client-secret	gestore di cluster ClientSecret	✓	
<i>&lt;envname&gt;</i> -cluster- manager- client-id	gestore di cluster ClientId	✓	
<i>&lt;envname&gt;</i> - external- private-key	Chiave privata del certificato autofirmato per il dominio	✓	
<i>&lt;envname&gt;</i> - external- certificate	Certificato autofirmato per dominio	✓	
<i>&lt;envname&gt;</i> - internal- private-key	Chiave privata del certificato autofirmato per il dominio	✓	
<i>&lt;envname&gt;</i> - internal- certificate	Certificato autofirmato per dominio	✓	

Nome segreto	Description	RES generato	Amministratore inserito
<code>&lt;envname&gt;-director-service-ServiceAccountUserDN</code>	L'attributo Distinguished Name (DN) dell' ServiceAccount utente.	✓	

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

Chiave	Origine
<code>identity-provider.cognito.sso_client_secret</code>	
<code>vdc.dcv_connection_gateway.certificate.certificate_secret_arn</code>	stack
<code>vdc.dcv_connection_gateway.certificate.private_key_secret_arn</code>	stack
<code>cluster.load_balancers.internal_alb.certificates.private_key_secret_arn</code>	stack
<code>directoryservice.root_username_secret_arn</code>	
<code>vdc.client_secret</code>	stack
<code>cluster.load_balancers.external_alb.certificates.certificate_secret_arn</code>	stack
<code>cluster.load_balancers.internal_alb.certificates.certificate_secret_arn</code>	stack
<code>directoryservice.root_password_secret_arn</code>	
<code>cluster.secretsmanager.kms_key_id</code>	

Chiave	Origine
<code>cluster.load_balancers.external_alb. certificates.private_key_secret_arn</code>	stack
<code>cluster-manager.client_secret</code>	

## 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 dei [the section called "AWS servizi inclusi in questo prodotto"](#).

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

1. Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo. <https://console.aws.amazon.com/costmanagement/>
2. Scegli i tag di allocazione dei costi.
3. Cerca e seleziona i `res:EnvironmentName` tag `res:Project` and.
4. Selezionare Attiva.

**Billing** ×

Home

- ▼ Billing
  - Bills
  - Payments
  - Credits
  - Purchase orders
  - Cost & usage reports
  - Cost categories
  - Cost allocation tags** 2
  - Free tier
  - Billing Conductor
- ▼ Cost Management
  - Cost explorer
  - Budgets
  - Budgets reports
  - Savings Plans
- ▼ Preferences
  - Billing preferences
  - Payment preferences
  - Consolidated billing
  - Tax settings
- ▼ Permissions

**Cost allocation tags** Info

Cost allocation tags activated: 3 Download CSV

User-defined cost allocation tags | AWS generated cost allocation tags

**User-defined cost allocation tags (2/47)** Info Undo Deactivate Activate 4

Find cost allocation tags 11 matches

res × Clear filters

<input type="checkbox"/>	Tag key	Status	Last updated date	Last used month
<input type="checkbox"/>	res:BackupPlan	Inactive	-	November 2023
<input type="checkbox"/>	res:ClusterName	Inactive	-	November 2023
<input type="checkbox"/>	res:DCVSessionUUID	Inactive	-	November 2023
<input type="checkbox"/>	res:EndpointName	Inactive	-	November 2023
<input checked="" type="checkbox"/>	res:EnvironmentName	Inactive	-	November 2023
<input type="checkbox"/>	res:ModuleId	Inactive	-	November 2023
<input type="checkbox"/>	res:ModuleName	Inactive	-	November 2023
<input type="checkbox"/>	res:ModuleVersion	Inactive	-	November 2023
<input type="checkbox"/>	res:NodeType	Inactive	-	November 2023
<input checked="" type="checkbox"/>	res:Project	Inactive	-	November 2023

### Note

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

Per creare un budget per le risorse RES:

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

The screenshot shows the AWS Budgets 'Choose budget type' wizard. The interface is divided into a sidebar and a main content area. The sidebar on the left contains navigation links for 'Billing' and 'Cost Management'. The main content area is titled 'Choose budget type' and includes a progress indicator with five steps: 'Step 1: Choose budget type', 'Step 2: Set your budget', 'Step 3: Configure alerts', 'Step 4 - Optional: Attach actions', and 'Step 5: Review'. The 'Budget setup' section offers two options: 'Use a template (simplified)' and 'Customize (advanced)'. The 'Budget types' section lists four options: 'Cost budget - Recommended', 'Usage budget', 'Savings Plans budget', and 'Reservation budget'. The 'Cost budget - Recommended' option is selected. At the bottom right, there are 'Cancel' and 'Next' buttons.

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 X

Cancel Apply filter

Add filter

**Advanced options**

**Aggregate costs by**  
Unblended costs

**Supported charge types**

Upfront reservation fees X    Recurring reservation charges X    Other subscription costs X

Taxes X    Support charges X    Discounts X

Cancel Previous Next

15. Opzionale. Aggiungi una soglia di avviso.
16. Scegli Next (Successivo).
17. Opzionale. 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, consulta [the 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.

Title	Project Code	Status	Budgets	Groups	Updated On
project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 <span style="color: red;">⚠ Budget Exceeded</span> Limit: 500.00 USD, Forecasted: 3945.34 USD	<ul style="list-style-type: none"> <li>DemoUsers</li> <li>DemoAdmins</li> <li>ProductUsers</li> </ul>	10/31/2023, 12:44:12 PM

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

## Dashboard di analisi dei costi

La dashboard di analisi dei costi consente agli amministratori RES di monitorare i budget e i costi dei progetti nel tempo dal portale RES. I costi possono essere filtrati a livello di progetto.

### Argomenti

- [Prerequisiti](#)
- [Progetti con tabella del budget assegnato](#)
- [Analisi dei costi nel grafico temporale](#)
- [Scaricare in CSV](#)

## Prerequisiti

Per utilizzare il dashboard dei costi per Research and Engineering Studio, devi prima:

- [Crea un progetto](#).
- Crea un [budget](#) nella console [AWS Billing and Cost Management](#).

- Allega il budget al progetto (vedi [Modifica un progetto](#)).
- Attiva il grafico di analisi dei costi per i conti con nuove implementazioni RES. A tale scopo, seguire queste fasi:
  1. Implementa una [VDI](#) per il progetto che hai creato. Questa operazione esegue il provisioning del `res:Project` tag nel [AWS Cost Explorer](#), operazione che può richiedere fino a 24 ore.
  2. Dopo la creazione del tag, viene attivato il pulsante **Abilita tag**. Scegli il pulsante per attivare i tag in Cost Explorer. Questo processo potrebbe richiedere altre 24 ore.

**Cost analysis onboarding** Info

To start tracking expenses incurred over a period of time, take the following steps.

**Step 1 - Launch desktop**

Launch your first desktop within this account and wait up to 24 hours for cost allocation tags to create.

[Launch desktop](#)

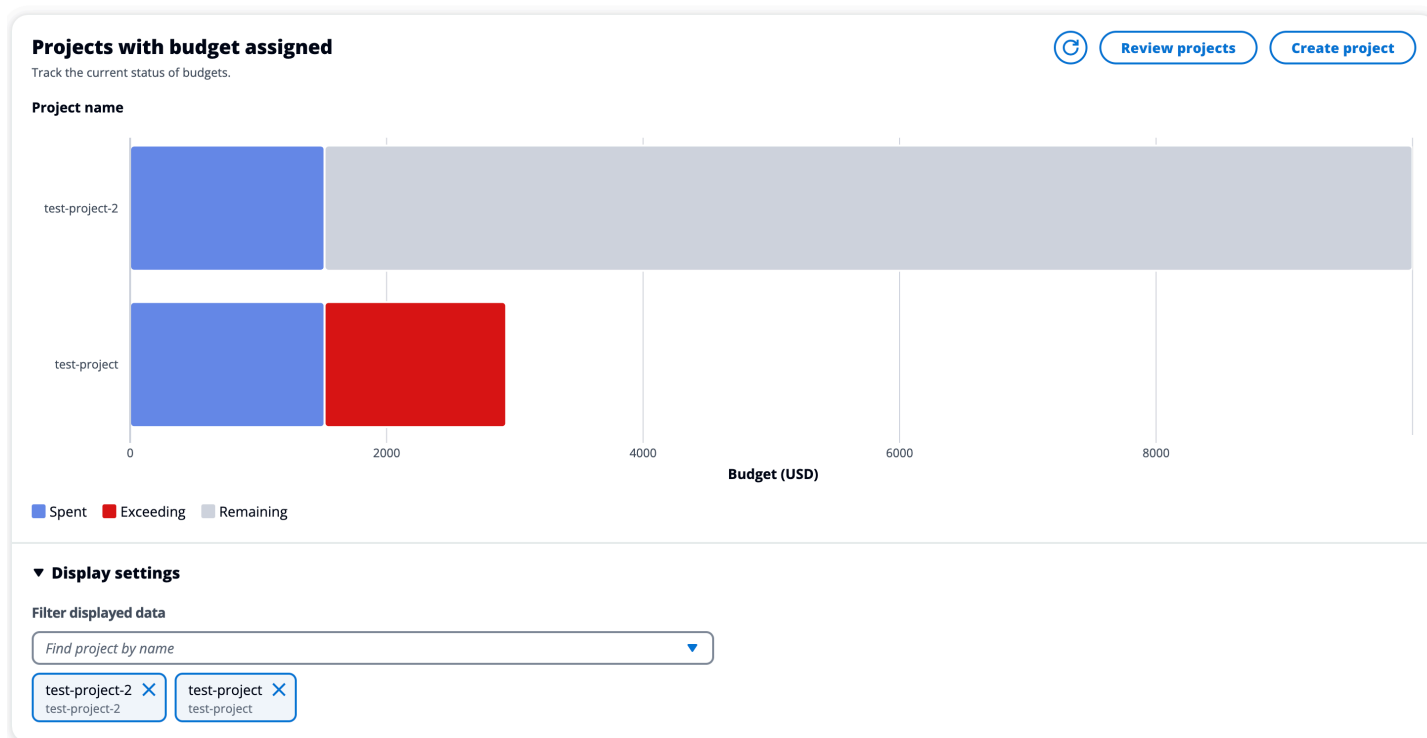
**Step 2 - Enable cost tags**

Once tags are created, enable cost allocation tags for the web portal and wait another 24 hours for data to display.

[Enable tags](#)

## Progetti con tabella del budget assegnato

Il grafico Progetti con budget assegnato mostra lo stato del budget dei progetti in ambiente RES a cui sono stati assegnati dei budget. Per impostazione predefinita, il grafico mostra i primi 5 progetti per importo del budget. Puoi selezionare progetti specifici nel menu a discesa **Filtra dati visualizzati** che carica l'elenco completo dei progetti assegnati al budget.

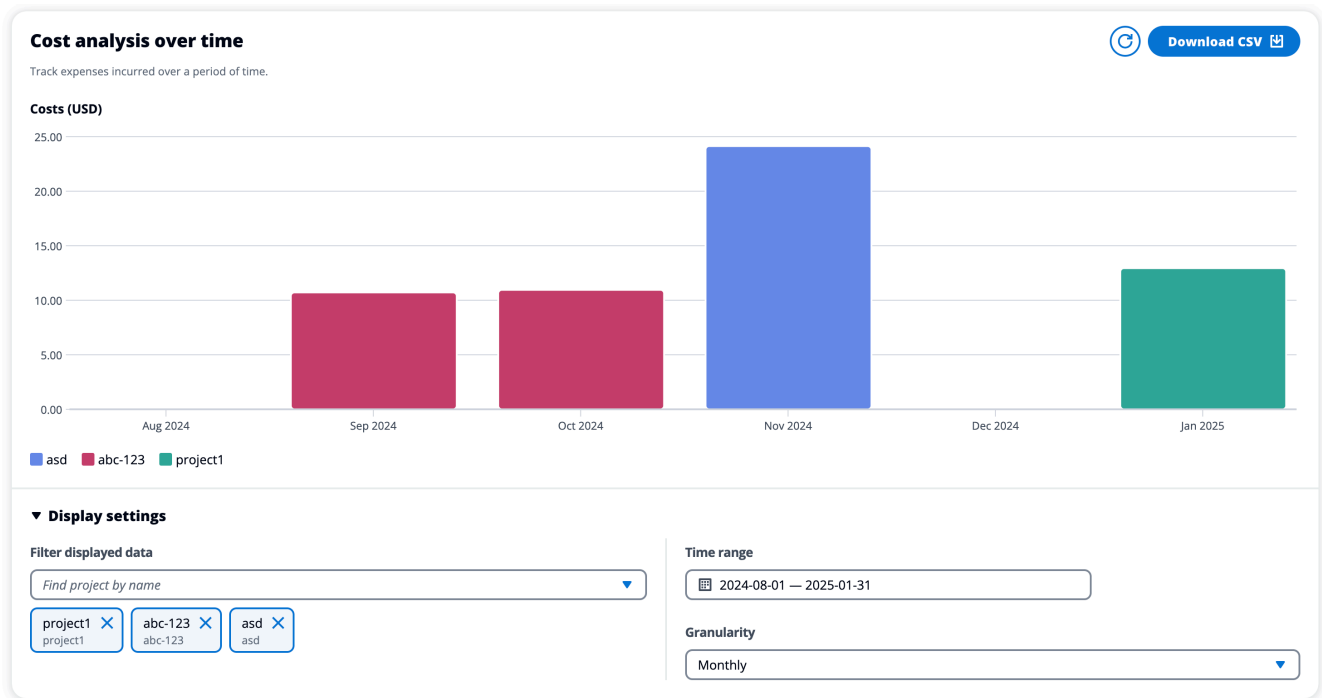


Il grafico mostra gli importi spesi, rimanenti ed eccedenti per ogni budget in valuta USD. Passa il mouse su una barra per mostrare gli importi esatti in USD per ciascuna categoria. Puoi anche aprire le pagine Progetti e Crea progetto scegliendo rispettivamente i pulsanti Rivedi progetti e Crea progetto nell'angolo in alto a destra.



## Analisi dei costi nel grafico temporale

Il grafico dell'analisi dei costi nel tempo mostra la ripartizione dei costi per progetto in un periodo di tempo specificato. Per impostazione predefinita, il grafico mostra i dati per ciascuno degli ultimi 6 mesi. Visualizza i primi 5 progetti per costo totale nell'intervallo di tempo selezionato con la granularità selezionata. Tutti gli altri progetti selezionati oltre ai primi 5 sono aggregati in una categoria Altro.

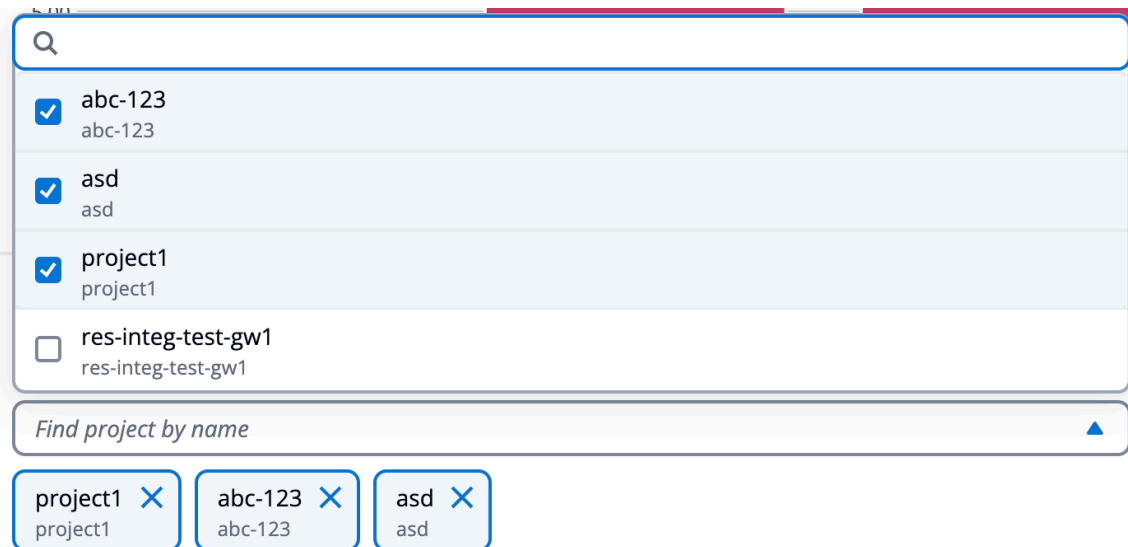


## Filtri

È possibile filtrare per progetto, intervallo di tempo e granularità per personalizzare l'analisi dei costi sulla base della visualizzazione del grafico temporale. Se vengono selezionate combinazioni di filtri non valide, verrà visualizzata una finestra modale che offre la possibilità di tornare alla configurazione precedente o accettare un suggerimento per la combinazione di filtri aggiornata.

## Progetto

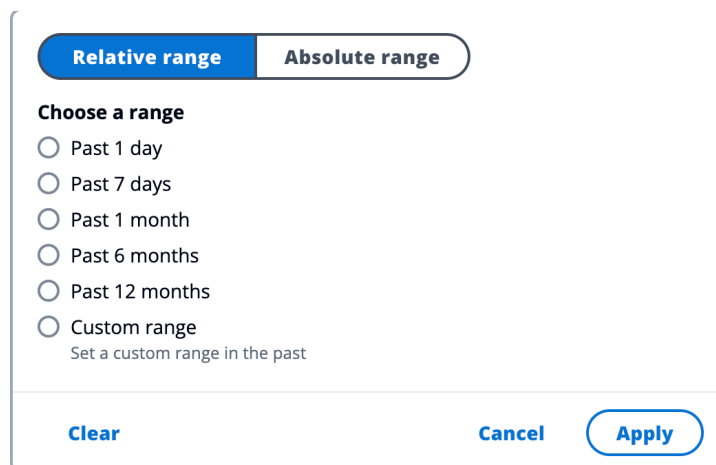
Quando si sceglie il menu a discesa Filtra i dati visualizzati, viene visualizzato un elenco completo dei progetti nell'ambiente RES corrente. Vedi il nome del progetto, con il codice del progetto visualizzato sotto.



The screenshot shows a search interface with a search bar at the top containing a magnifying glass icon. Below the search bar is a list of four items, each with a checkbox and a label: 'abc-123', 'asd', 'project1', and 'res-integ-test-gw1'. The first three items have their checkboxes checked, while the last one is unchecked. Below the list is a text input field with the placeholder text 'Find project by name' and a small upward-pointing triangle on the right. At the bottom, there are three filter tags: 'project1', 'abc-123', and 'asd', each with a blue 'X' icon to its right.

## Specificare l'intervallo di tempo

È possibile scegliere di utilizzare un intervallo assoluto o un intervallo relativo quando si specifica un intervallo di date. Quando si seleziona un intervallo relativo, le date vengono calcolate utilizzando unità di tempo complete. Ad esempio, se si seleziona l'opzione Ultimi 6 mesi nel febbraio 2025, si otterrà un intervallo di tempo compreso tra 8/1/25 e 1/31/25.



The screenshot shows a dialog box for selecting a date range. At the top, there are two tabs: 'Relative range' (which is selected and highlighted in blue) and 'Absolute range'. Below the tabs, the text 'Choose a range' is followed by a list of radio button options: 'Past 1 day', 'Past 7 days', 'Past 1 month', 'Past 6 months', 'Past 12 months', and 'Custom range'. Under 'Custom range', there is a sub-label 'Set a custom range in the past'. At the bottom of the dialog, there are three buttons: 'Clear', 'Cancel', and 'Apply' (which is highlighted in blue).

Relative range Absolute range

< August 2024 September 2024 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3	1	2	3	4	5	6	7
4	5	6	7	8	9	10	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28
25	26	27	28	29	30	31	29	30					

Start date: 2024/08/01 End date: 2025/01/31

Clear Cancel Apply

## Granularity (Granularità)

Puoi scegliere di visualizzare i dati con una granularità mensile, giornaliera o oraria. La granularità oraria supporta solo un intervallo di date fino a 14 giorni. La granularità giornaliera supporta solo un intervallo di date fino a 14 mesi.

Monthly ✓

Daily

Hourly

Monthly ▲

## Scaricare in CSV

Per esportare la visualizzazione corrente dell'analisi dei costi, scegli Scarica CSV in alto a destra nel grafico Analisi dei costi nel tempo. Il file CSV scaricato contiene le informazioni sui costi per ogni progetto selezionato per il periodo di tempo specificato, nonché i totali dei costi per progetto e per periodo di tempo.

The screenshot shows the Microsoft Excel interface. The 'Home' ribbon is active, displaying options for Paste, Font (Calibri, size 12), Paragraph (bullet points, indent), and Styles (background color, text color). A yellow warning banner reads: 'Possible Data Loss Some features might be lost if you save this workbook in the current format'. Below the ribbon, the formula bar shows 'res:Project' for cell A1. The spreadsheet contains the following data:

	A	B	C	D	E	F
1	res:Project	asd(\$)	abc-123(\$)	project1(\$)	Total costs(\$)	
2	res:Project total	24.136179	21.67188038	12.9429946	58.75105397	
3	8/1/24				0	
4	9/1/24		10.7180966		10.7180966	
5	10/1/24		10.95378378		10.95378378	
6	11/1/24	24.136179			24.13617901	
7	12/1/24				0	
8	1/1/25			12.9429946	12.94299457	
9						
10						
11						
12						
13						

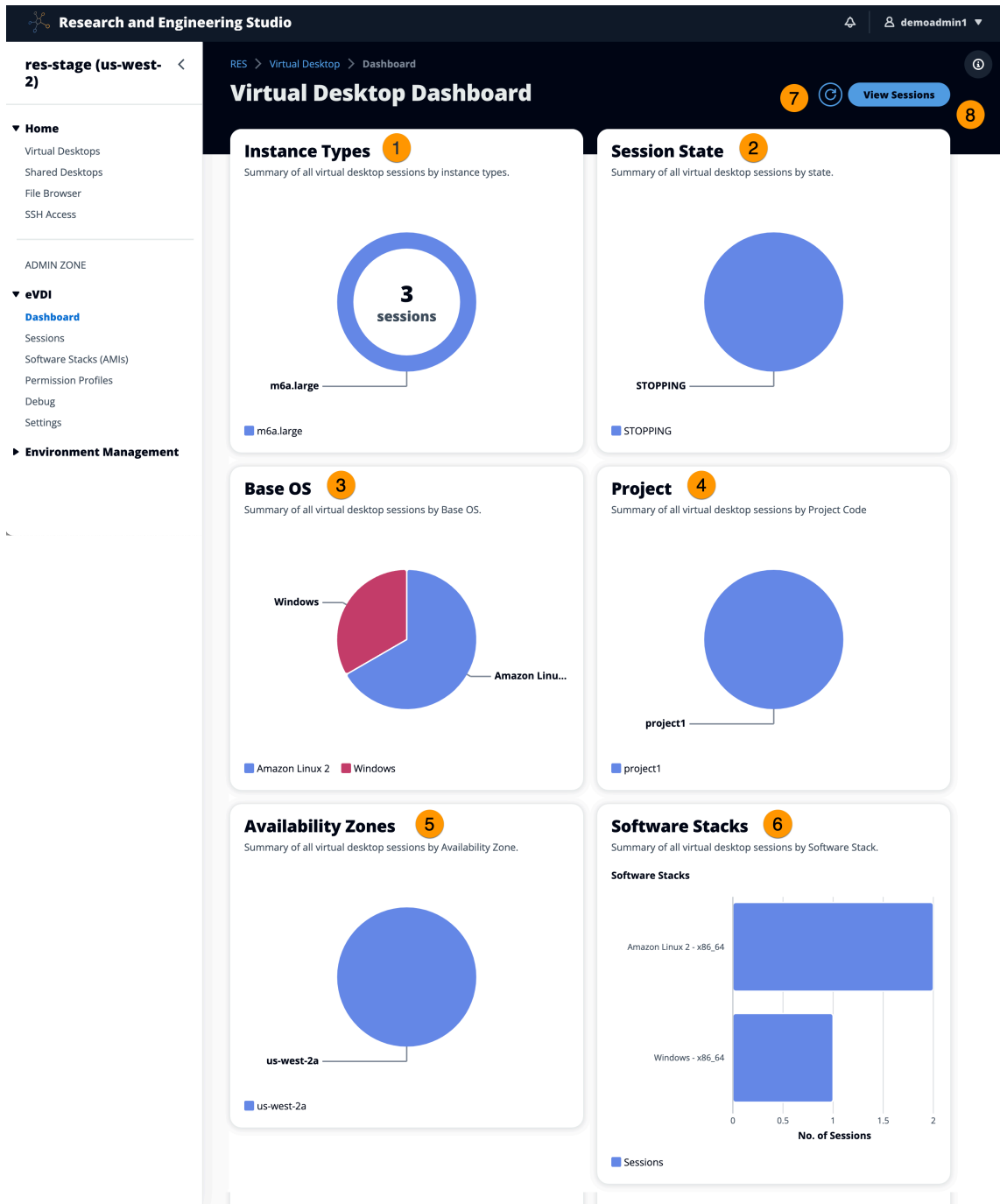
## Gestione della sessione

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

### Argomenti

- [Pannello di controllo](#)
- [Sessioni](#)
- [Stack software \(\) AMIs](#)
- [Debug](#)
- [Impostazioni del desktop](#)

# Pannello di controllo



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 all'interno di Research and Engineering Studio. Dalla pagina Sessioni, è possibile filtrare e visualizzare le informazioni sulla sessione o creare una nuova sessione.

RES > Virtual Desktops > Sessions

### Sessions (2)

Virtual Desktop sessions for all users. End-users see these sessions as Virtual Desktops.

Created ▾ Last 1 month **1** Actions **2** Create Session **3**

Search **4** All States ▾ All Operating Systems ▾ < 1 >

<input type="checkbox"/>	Session Name	Owner	Base OS	Instance Ty...	State	Project	Created On
<input checked="" type="checkbox"/> <b>5</b>	demoadmin1aml21	demoadmin1	Amazon Linux 2	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:31:50 AM
<input type="checkbox"/>	demoadmin1windows1	demoadmin1	Windows	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:38:23 AM

< 1 >

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. Stop/Hibernate Sessione/i
  - c. Stop/Hibernate Sessione/i di forza
  - 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.

## Creazione di una sessione

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

**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

**Show Advanced Options**

Cancel Submit

## Dettagli della sessione

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

RES > Virtual Desktop > Sessions > 8765705b-8919-48ba-901a-19e2c49cf043

## Session: demoadmin1aml21

### General Information

Session Name demoadmin1aml21	Owner demoadmin1	State Stopped
---------------------------------	---------------------	------------------

< **Details** | Server | Software Stack | Project | Permissions | Schedule | Monitoring | Session R >

### Session Details

RES Session Id 8765705b-8919-48ba-901a-19e2c49cf043	DCV Session Id bd63e69a-e75a-427b-b4c8-39d7c43b95ad	Description -
Session Type VIRTUAL	Hibernation Enabled No	Created On 9/27/2023, 8:31:50 AM
Updated On 9/29/2023, 11:01:20 PM		

## Stack software ( ) AMIs

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

RES > Virtual Desktops > Software Stacks (AMIs)

## Software Stacks

Manage your Virtual Desktop Software Stacks

1  All Operating Systems 3 4 Register Software Stack

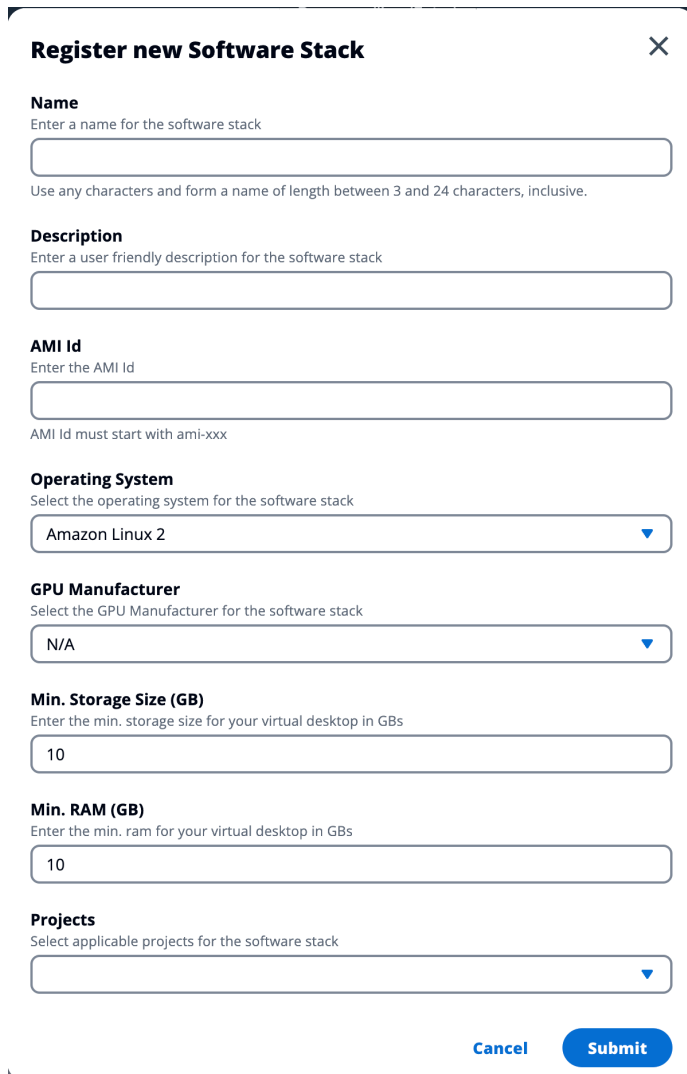
	Name	Description	AMI ID	Base OS	Root Volume Size	Min RAM	GPU Manufacturer	Created On
2	<input type="radio"/> CentOS7 - ARM64	CentOS7 - ARM64	ami-07f692d95b2b9c8c5	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> CentOS7 - x86_64	CentOS7 - x86_64	ami-00f8e2c955f7fa9b	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> RHEL8 - x86_64	RHEL8 - x86_64	ami-0b530377951178d6b	RedHat Enterprise Linux 8	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> UBUNTU2204 - x86_64	UBUNTU2204 - x86_64	ami-073ffe13d826b778	Ubuntu 22.04	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> RHEL7 - x86_64	RHEL7 - x86_64	ami-0bb2449c2217c9b0	RedHat Enterprise Linux 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> Windows - x86_64	Windows - x86_64	ami-0667133d0dc6089e1	Windows	30GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> Windows - AMD	Windows - AMD	ami-05df91be1d294f195	Windows	30GB	4GB	AMD	6/7/2024, 11:25:20 AM
	<input type="radio"/> Windows - NVIDIA	Windows - NVIDIA	ami-00d7af9d003819a90	Windows	30GB	4GB	NVIDIA	6/7/2024, 11:25:20 AM
	<input type="radio"/> RHEL9 - x86_64	RHEL9 - x86_64	ami-099f85c24d27c2a7	RedHat Enterprise Linux 9	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> Amazon Linux 2 - ARM64	Amazon Linux 2 - ARM64	ami-04ed2b27d86c17f09	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
	<input type="radio"/> Amazon Linux 2 - x86_64	Amazon Linux 2 - x86_64	ami-0ee5c62243ab25259	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM

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. Scegliete il pulsante di opzione accanto a uno stack di software, quindi utilizzate il menu Azioni per modificare lo stack e assegnarlo a un progetto.
4. Scegli il pulsante Registra lo stack software per creare un nuovo stack.

## Registra un nuovo stack software

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. Seleziona 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

**GPU Manufacturer**  
Select the GPU Manufacturer for the software stack

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

**Min. RAM (GB)**  
Enter the min. ram for your virtual desktop in GBs

**Projects**  
Select applicable projects for the software stack

Cancel Submit

## Assegna uno stack software a un progetto

Quando crei un nuovo stack software, puoi assegnare lo stack ai progetti. Tuttavia, 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. Nella pagina Software Stacks, selezionate il pulsante di opzione relativo allo stack di software che desiderate aggiungere a un progetto.
2. Scegli Azioni.
3. Scegli Modifica.
4. Utilizza il menu a discesa Progetti per selezionare il progetto.

**Update Software Stack: RHEL8 - x86\_64** ✕

**Stack Name**  
Enter a name for the Software Stack.  
RHEL8 - x86\_64  
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  
RHEL8 - x86\_64

**Projects**  
Select applicable projects for the software stack

**Tenancy**  
The type of tenancy  
Shared

**Allowed Instance Families and Types**  
Select instance families and types allowed for this software stack  
m6a ✕ t3 ✕

Cancel Submit

5. Seleziona Invia.

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

## Modifica l'elenco delle istanze VDI dello stack software

Per ogni stack software registrato, è possibile scegliere le famiglie e i tipi di istanze consentiti. L'elenco delle opzioni per ogni stack software viene filtrato in base alle opzioni definite nelle impostazioni del desktop. Qui puoi trovare e modificare le famiglie e i tipi di istanze consentiti globali.

**Research and Engineering Studio** admin1

res-deploy (us-east-2)

Review the virtual desktop settings

Module Name	Module ID	Version
virtual-desktop-controller	vdc	2024.12.01

**General** | Notifications | **Server** | Controller | Broker | Connection Gateway | CloudWatch Logs

### Session

Idle Timeout	CPU Utilization Threshold	Enforce Schedule
43200 minutes	30 %	Yes
Transition State	Allowed Sessions Per User	
Stop	5	

### DCV Host

Allowed Security Groups	Max Root Volume Size
-	1000 GB
Allowed Instance Families and Types	Denied Instance Types
<ul style="list-style-type: none"><li>g4ad</li><li>g4dn</li><li>g5</li><li>m6a</li><li>t3</li><li>m6g</li></ul>	-

Per modificare l'attributo Allowed Instance Families and Types di uno stack software:

1. Nella pagina Software Stacks, scegliete il pulsante di opzione per lo stack di software.
2. Scegli Azioni, quindi seleziona Modifica stack.
3. Scegli le famiglie e i tipi di istanze desiderati dall'elenco a discesa in Famiglie e tipi di istanze consentiti.

### Update Software Stack: RHEL8 - x86\_64

**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

**Projects**  
Select applicable projects for the software stack

test X

**Tenancy**  
The type of tenancy

**Allowed Instance Families and Types**  
Select instance families and types allowed for this software stack

t3 X m6a X

Cancel Submit

#### 4. Selezionare Invia.

##### Note

Se l'insieme globale di famiglie e tipi di istanze consentiti include una famiglia di istanze e un tipo di istanza all'interno di tale famiglia (ad esempio t3 et3 .large), le opzioni disponibili per l'attributo Allowed Instance Families and Types di uno stack software includeranno solo la famiglia di istanze.

##### Important

- Quando un'istanza type/family viene eliminata dall'elenco Consenti a livello di ambiente, dovrebbe essere rimossa automaticamente da tutti gli stack software.
- Le istanze types/families aggiunte a livello di ambiente non vengono aggiunte automaticamente agli stack software.

## Visualizza i dettagli dello stack software

Dalla pagina Software Stacks, selezionate il nome dello stack software per visualizzarne i dettagli. Puoi anche selezionare il pulsante di opzione per uno stack di software, scegliere Azioni e selezionare Modifica per modificare lo stack di software.

## Supporto per la locazione VDI

Quando si registra un nuovo stack software o si modifica uno stack software esistente, è possibile selezionare la locazione per il programma VDI avviato da questo stack di software. Sono supportate le seguenti tre locazioni:

- Condiviso (impostazione predefinita): viene eseguito VDI con istanze hardware condivise
- Istanza dedicata: eseguita VDI con istanze dedicate
- Host dedicato: esegui VDI con un host dedicato

### 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

50

**Min. RAM (GB)**  
Enter the min. ram for your virtual desktop in GBs

10

**Projects**  
Select applicable projects for the software stack

▼

**Tenancy**  
The type of tenancy

Shared ▼

Quando si seleziona il tipo di locazione dell'host dedicato, è necessario selezionare anche l'affinità di tenancy e il tipo di host di destinazione. Sono supportati i seguenti tipi di host di destinazione:

- Host Resource Group - Gruppo di risorse host creato in AWS License Manager
- Host ID: un ID host specifico

**Tenancy**

The type of tenancy

Dedicated Host

**Tenancy Affinity**

The relationship between an instance and a dedicated host

Off

**Target Host By**

The type of target host

Host Resource Group

**Host Resource Group ARN**

The ARN of the dedicated resource group

**Tenancy**

The type of tenancy

Dedicated Host

**Tenancy Affinity**

The relationship between an instance and a dedicated host

Host

**Target Host By**

The type of target host

Host ID

**Tenancy Host ID**

The ID of the dedicated host

Per specificare eventuali licenze autogestite richieste al VDI al momento del lancio con l'host tenancy dedicato, associate le licenze alla vostra AMI seguendo le istruzioni [Associating self-managed licenses e nella AMIs](#) License Manager User Guide.AWS

## 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.

▼ Home

- Virtual Desktops
- Shared Desktops
- File Browser
- SSH Access

---

ADMIN ZONE

▼ eVDI

- Dashboard
- Sessions
- Software Stacks (AMIs)
- Permission Profiles
- Debug**
- Settings

View hosts and sessions registered with NICE DCV Broker

**VD Host** | **VD Sessions**

```

{ 1 item
  "servers": [ 1 item
    { 15 items
      "id": "aXAtMTAtMy0xNTctMTk0LmNvcnAucmVzLmNvbS0xMC4zLjE1Ny4xOTQ1NmRmYjJmNWYyYTQ4NDYyN2E1MzgwZDU4YjIzM2I2Zjg="
      "ip": "10.3.157.194"
      "hostname": "ip-10-3-157-194.corp.res.com"
      "default_dns_name": "ip-10-3-157-194.corp.res.com"
      "port": null
      "endpoints": [ 4 items
        { 3 items
          "port": 8443
        }
      ]
    }
  ]
}

```

## Impostazioni del desktop

È possibile utilizzare la pagina Impostazioni del desktop per configurare le risorse associate ai desktop virtuali.

RES > Virtual Desktops > Settings

### Virtual Desktop Settings

Review the virtual desktop settings

Module Name	Module ID	Version
virtual-desktop-controller	vdc	2025.03b1

**General** | Notifications | **Server** | Controller | Broker | Connection Gateway | CloudWatch Logs

**Session** ✎

Idle Timeout 43200 minutes	CPU Utilization Threshold 30 %	Enforce Schedule Yes
Transition State Stop		

**DCV Host** ✎

Allowed Security Groups -	Max Root Volume Size 1000 GB
Allowed Instance Families and Types <ul style="list-style-type: none"> <li>t3</li> <li>g4dn</li> <li>g4ad</li> <li>g5</li> <li>m6a</li> <li>m6g</li> </ul>	Denied Instance Types -

### Ambito generale

La scheda Generale consente di accedere a impostazioni quali:

#### RAPIDO

Abilita QUIC a favore del TCP come protocollo di streaming predefinito per tutti i desktop virtuali.

## Tipo di sessione DCV predefinito

Il tipo di sessione DCV predefinito utilizzato per tutti i desktop virtuali. Questa impostazione non si applica ai desktop creati in precedenza. Ciò si applicherà solo nei casi in cui il tipo di istanza e il sistema operativo supportino i tipi di sessione virtuale o console.

## Sessioni consentite predefinite per utente per progetto

Il valore predefinito per il numero consentito di sessioni VDI per utente per progetto.

## Server

La scheda Server consente di accedere a impostazioni quali:

### Timeout di inattività della sessione DCV

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

### Avviso di timeout di inattività

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

### Soglia di utilizzo della CPU

L'utilizzo della CPU da considerare inattivo.

### 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 ambiente RES. Le combinazioni di famiglie di istanze e dimensioni delle istanze sono entrambe accettate. Ad esempio, se si specifica 'm7a', tutte le dimensioni della famiglia m7a saranno disponibili per l'avvio come sessioni VDI. Se si specifica 'm7a.24xlarge', solo m7a.24xlarge sarà disponibile per l'avvio come sessione VDI. Questo elenco riguarda tutti i progetti presenti nell'ambiente.

RES &gt; Virtual Desktops &gt; Settings

## Virtual Desktop Settings

Review the virtual desktop settings

Module Name	Module ID	Version
virtual-desktop-controller	vdc	2025.03b1

**General**

Notifications

Server

Controller

Broker

Connection Gateway

CloudWatch Logs

### General

#### QUIC

Quick UDP Internet Connections (QUIC) is a protocol that attempts to improve streaming in higher latency environments.

Toggle on to activate QUIC in favor of TCP as the default streaming protocol for all your virtual desktops

Disabled

#### Subnet AutoRetry

Enabled

#### Default DCV Session Type

Default setting will only apply in cases where Instance Type and Operating System supports either Virtual or Console Session Types.

Console

#### eVDI Subnets

- subnet-0631e566e706ad31e
- subnet-00d930afd7485c9a5

#### Randomize Subnets

Disabled

#### Default Allowed Sessions Per User Per Project

Default value for allowed sessions per user per project.

5 

## Gestione dell'ambiente

Dalla sezione Gestione dell'ambiente di Research and Engineering Studio, 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 dell'ambiente](#)
- [Utenti](#)
- [Gruppi](#)
- [Progetti](#)
- [Policy di autorizzazione](#)
- [File system](#)
- [Gestione degli snapshot](#)

- [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.

**Research and Engineering Studio** demoadmin4

RES > Environment Management > Status

### Environment Status

[View Environment Settings](#)

#### Modules

Environment modules and status

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

#### Infrastructure Hosts

Cluster hosts and status

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

## Impostazioni dell'ambiente

La pagina delle impostazioni ambientali mostra i dettagli della configurazione del prodotto, come:

- Ambito generale

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

- Provider di identità

Visualizza informazioni come lo stato del Single Sign-On.

- Rete

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

- Directory Service

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

## 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.

The screenshot shows the 'Users' page in the Research and Engineering Studio. The page title is 'Users' and the subtitle is 'Environment user management'. There is a search bar and a '1' icon. The 'Actions' menu is open, showing options like 'Set as Admin User' and 'Disable User' with a '2' icon. The table below lists the users:

	Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
<input checked="" type="radio"/>	demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	• IDEAUUsers • DemoUsers
<input type="radio"/>	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	• SAUsers
<input type="radio"/>	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	• DemoAdmins • AWS Delegated Administrators • IDEAUUsers
<input type="radio"/>	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	• ProductUsers

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, consulta [Guida alla configurazione](#).

The screenshot shows the 'Groups' management interface in the Research and Engineering Studio. The main table lists the following groups:

Title	Group Name	Type	Role	Status	GID
IDEAUsers	IDEAUsers	external	user	Enabled	4000
SAdmins	SAdmins	external	user	Enabled	3035
AWS Delegated Administrators	AWS Delegated Administrators	external	admin	Enabled	3999

Below the table, the 'Users in IDEAUsers' section is expanded, showing a list of users:

Username	UID	GID	Email	Is Sudo?	Role	Is Active	Status	Groups	Syn
demoadmin1	3000	3000	demoadmin1@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> <li>DemoAdmins</li> <li>AWS Delegated Administrators</li> <li>IDEAUsers</li> </ul>	10/3
demoadmin4	3003	3003	demoadmin4@demo	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> <li>DemoAdmins</li> <li>AWS Delegated Administrators</li> <li>IDEAUsers</li> <li>SAdmins</li> </ul>	10/3

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

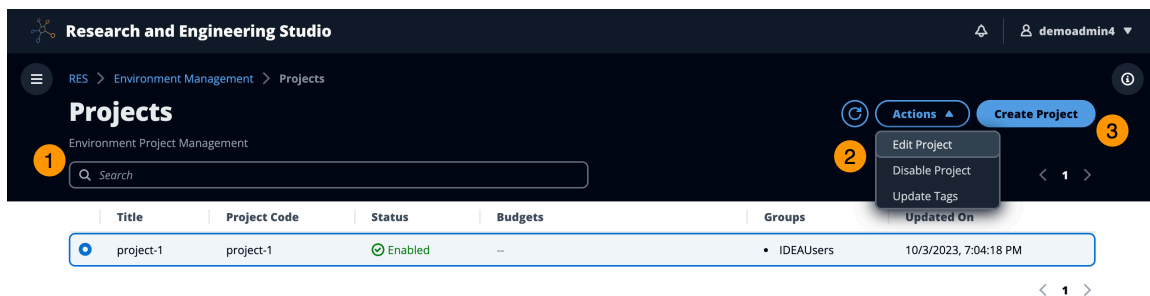
I progetti costituiscono un limite per desktop virtuali, team e budget. Quando crei un progetto, ne definisci le impostazioni, come il nome, la descrizione e la configurazione dell'ambiente. I progetti includono in genere uno o più ambienti, che possono essere personalizzati per soddisfare i requisiti

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](#)
- [Disabilita un progetto](#)
- [Elimina 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
  - d. Elimina un 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, vedere [Aggiungi 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), EFS, FSx per lo storage di volumi Lustre, FSx NetApp ONTAP o EBS.

È importante notare che il file system home condiviso, EFS, FSx for Lustre e FSx NetApp ONTAP possono essere condivisi tra più progetti e. VDI Tuttavia, l'opzione di storage su volumi EBS richiederà che ogni VDI di quel progetto abbia una propria home directory che non sia condivisa tra altri progetti. VDI

RES > Virtual Desktop > Projects > Create new Project

## Create new Project

### Project Definition

**Title**  
Enter a user friendly project title.

**Project ID**  
Enter a project-id.

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (\_), or periods (.). Must be between 3 and 40 characters long.

**Description**  
Enter the project description.

**Allowed sessions per user**  
Maximum number of sessions a user can launch in this project

**Enable budget assignment and tracking**  
To track budget status in the cost dashboard, specify the budget created in AWS Budgets

### Resource Configurations

**Storage resources**  
Add file systems and/or S3 buckets to the project.

**Home directory filesystem**  
Select the filesystem that will be used to create the user home directories on Linux desktops.

► **Advanced Options**

5. Assegna ai and/or gruppi di utenti il ruolo appropriato («Membro del progetto» o «Proprietario del progetto»). Scopri [profili di autorizzazioni predefiniti](#) le azioni che ogni ruolo può intraprendere.
6. Seleziona 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. Quando scegli un budget per il progetto, potrebbero verificarsi alcuni secondi di ritardo nel caricamento delle opzioni del menu a discesa del budget: se non vedi il budget che hai appena creato, seleziona il pulsante di aggiornamento accanto al menu a discesa.

Per informazioni sulle opzioni avanzate, consulta. [Aggiungi un modello di lancio](#)

## 4. Seleziona Invia.

RES > Virtual Desktop > Projects > Edit Project

### Edit Project

**Project Definition**

**Title**  
Enter a user friendly project title.

**Project ID**  
Enter a project-id.  
  
Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (\_), or periods (.). Must be between 3 and 40 characters long.

**Description**  
Enter the project description.

**Allowed sessions per user**  
Maximum number of sessions a user can launch in this project

**Enable budget assignment and tracking**  
To track budget status in the cost dashboard, specify the budget created in AWS Budgets

**Resource Configurations**

▼ **Advanced Options**

**Add Policies**  
Select applicable policies for the Project.

**Add Security Groups**  
Select applicable security groups for the Project.

► **Linux**

► **Windows**

## Disabilita un progetto

Per disabilitare un progetto:

1. Seleziona un progetto nell'elenco dei progetti.
2. Dal menu Azioni, scegli Disabilita progetto.

Research and Engineering Studio

RES > Environment Management > Projects

### Projects

Environment Project Management.

- Edit Project
- Disable Project
- Update Tags
- Delete Project

	Title	Project Code	Status	Budgets	Groups	Users	
<input type="radio"/>	deleteProject2	004	Enabled	--	• group_1	• admin1	1/28/2025, 2:12:38 AM
<input checked="" type="radio"/>	disableProject	002	Enabled	--	• group_1	• admin1	1/28/2025, 4:03:18 PM
<input type="radio"/>	test	001	Enabled	--	• group_1	• admin1	1/27/2025, 12:59:53 AM

◀ 1 ▶

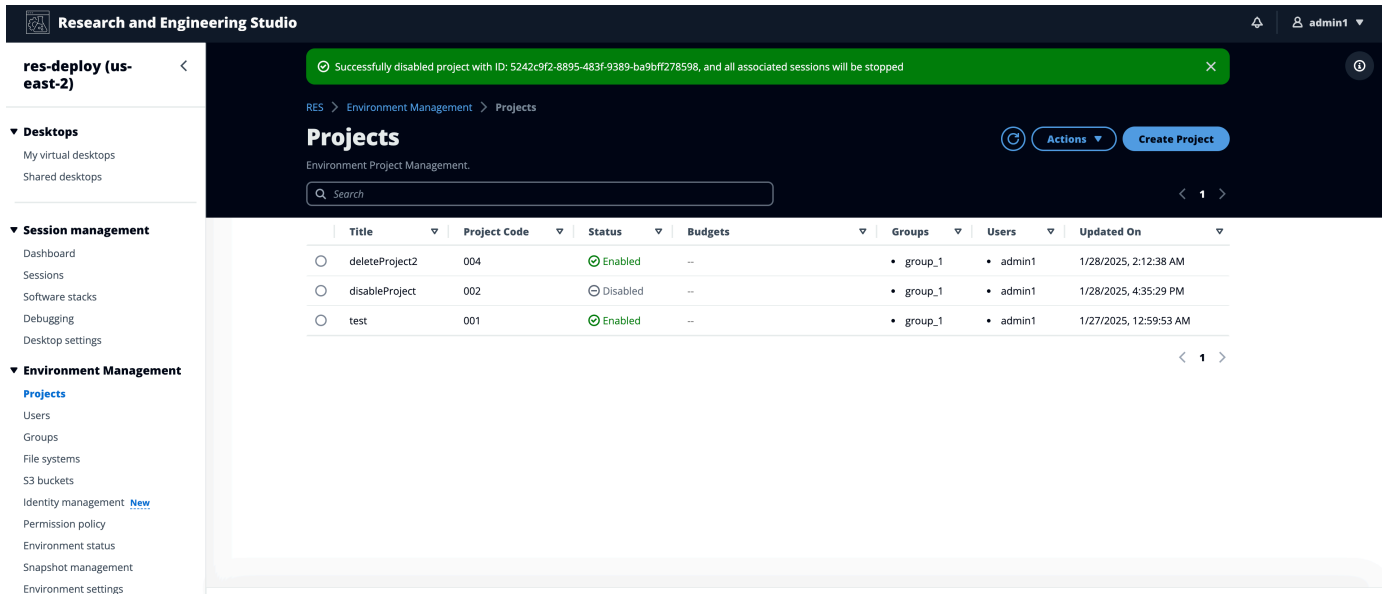
◀ 1 ▶

▼ **Desktops**  
My virtual desktops  
Shared desktops

▼ **Session management**  
Dashboard  
Sessions  
Software stacks  
Debugging  
Desktop settings

▼ **Environment Management**  
**Projects**  
Users  
Groups  
File systems  
S3 buckets  
Identity management [New](#)  
Permission policy  
Environment status  
Snapshot management  
Environment settings

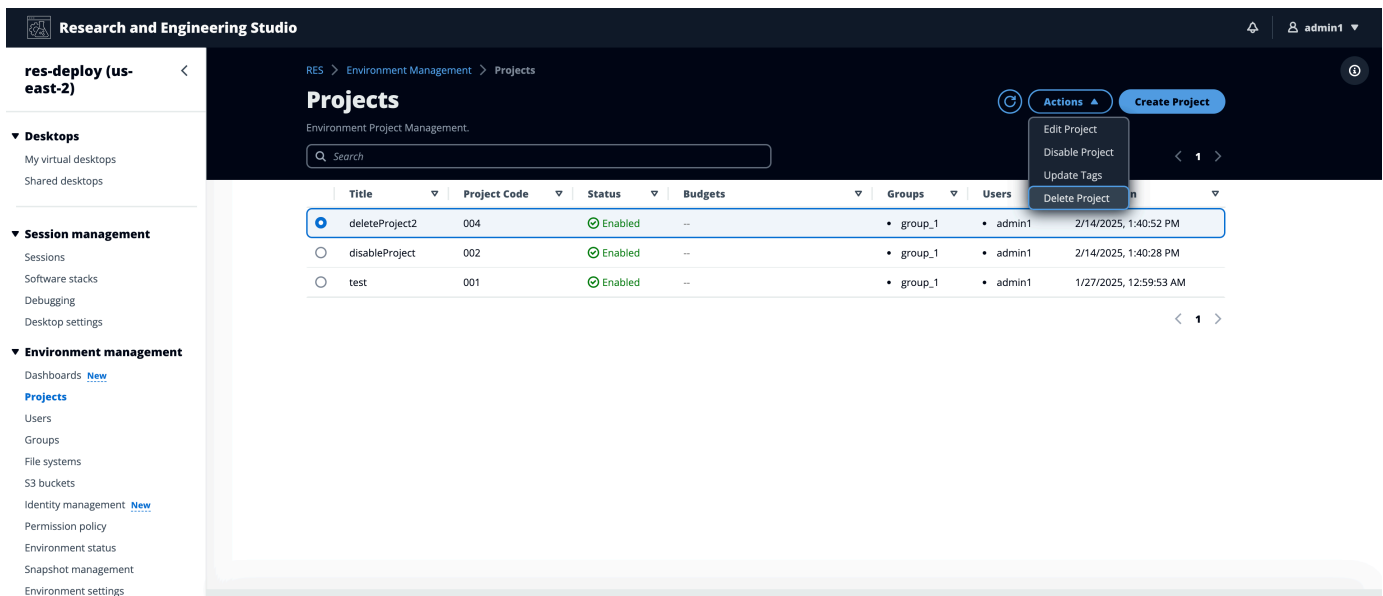
- Se un progetto è disabilitato, tutte le sessioni VDI associate a quel progetto vengono interrotte. Queste sessioni non possono essere riavviate mentre il progetto è disabilitato.



## Elimina un progetto

Per eliminare un progetto:

- Seleziona un progetto nell'elenco dei progetti.
- Dal menu Azioni, scegli Elimina progetto.



- Viene visualizzato un pop-up di conferma. Inserisci il nome del progetto, quindi scegli Sì per eliminarlo.

## Delete Project: test-proj-deletion



Are you sure you want to delete this project?

All associated sessions will be terminated. This action cannot be undone.

**To confirm deletion, enter the name of the project in the text input field.**

*test-proj-deletion*

Cancel

Yes

- Se un progetto viene eliminato, tutte le sessioni VDI associate a quel progetto vengono terminate.

The screenshot shows the 'Research and Engineering Studio' interface. A green notification bar at the top states: 'Project with ID: ea231a4c-7e01-4d1c-8590-55703918c87e has been deleted successfully'. Below this, the 'Projects' section is visible, showing a table of active projects. The table has columns for Title, Project Code, Status, Budgets, Groups, Users, and Updated On. Two projects are listed: 'disableProject' and 'test'.

Title	Project Code	Status	Budgets	Groups	Users	Updated On
disableProject	002	Enabled	--	group_1	admin1	1/28/2025, 4:40:03 PM
test	001	Enabled	--	group_1	admin1	1/27/2025, 12:59:53 AM

## Aggiungere o rimuovere tag da un progetto

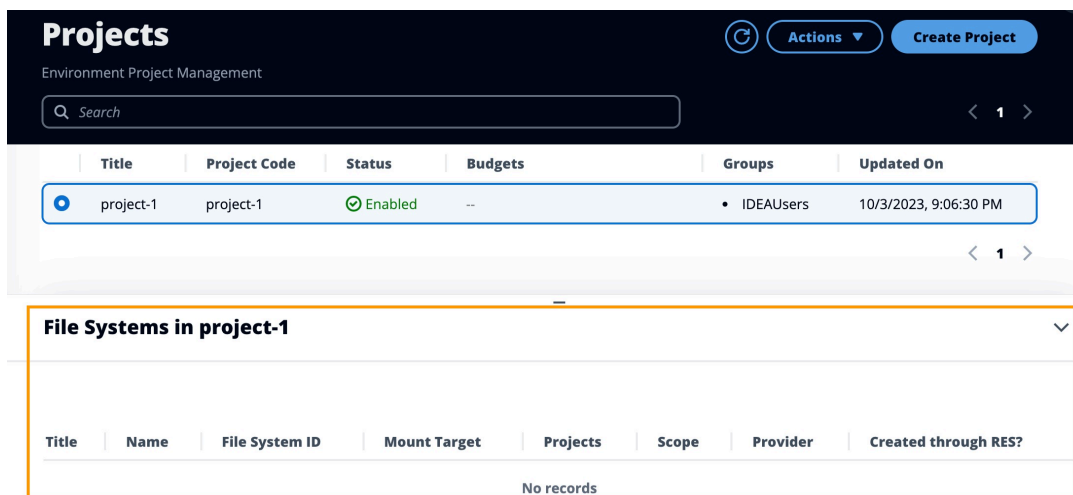
I tag di progetto assegneranno tag a tutte le istanze create nell'ambito di quel progetto.

- Seleziona un progetto nell'elenco dei progetti.
- Dal menu Azioni, scegli Aggiorna tag.

- Scegli Aggiungi tag e inserisci un valore per Chiave.
- 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.



The screenshot shows the 'Projects' management interface. At the top, there's a search bar and a 'Create Project' button. Below is a table of projects with columns: Title, Project Code, Status, Budgets, Groups, and Updated On. One project, 'project-1', is selected. Below the table, a section titled 'File Systems in project-1' is expanded, showing a table with columns: Title, Name, File System ID, Mount Target, Projects, Scope, Provider, and Created through RES?. The table currently displays 'No records'.

## Aggiungi un modello di lancio

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

### Aggiungi politiche

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

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

Per ulteriori informazioni sui ruoli IAM, consulta [Politiche e autorizzazioni](#) in IAM.

## Aggiunta di gruppi di sicurezza

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

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

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

## Aggiungi script di avvio

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

### Esegui script all'avvio di VDI

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

### Esegui lo script quando VDI è configurato

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

Gli script supportano le seguenti opzioni:

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

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

**▼ Linux**

**Run Script When VDI Starts**  
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="https://sample.samplecontent.com/sample"/>	<input type="text"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="file:///root/bootstrap/latest/launch/script"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

**Run Script when VDI is Configured**  
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

**▼ Windows**

**Run Script When VDI Starts**  
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

**Run Script when VDI is Configured**  
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

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. Autorizzazioni di gestione delle sessioni VDI che consistono in «Crea sessione» che consente a un utente designato di creare una sessione VDI all'interno del proprio progetto e «Creazione/terminazione della 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](#)
- [Autorizzazioni per la gestione delle sessioni VDI](#)
- [Gestione dei profili di autorizzazione](#)
- [profili di autorizzazioni predefiniti](#)
- [Limiti dell'ambiente](#)
- [profili di condivisione del desktop](#)

## 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.

### Team Configurations

**Groups** [Info](#)

group\_1 ▼

group\_2 ▼

[Add group](#)

No users attached. Click 'Add user' below to get started.

[Add user](#)

**Permission profile** [Info](#)

Project Owner ▼ [Remove](#)

⚠ Users/groups assigned to this permission profile can grant themselves or others higher privileges for this project by re-assigning personnel to a different permission profile

Project Member ▼ [Remove](#)

[Cancel](#) [Submit](#)

## 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.

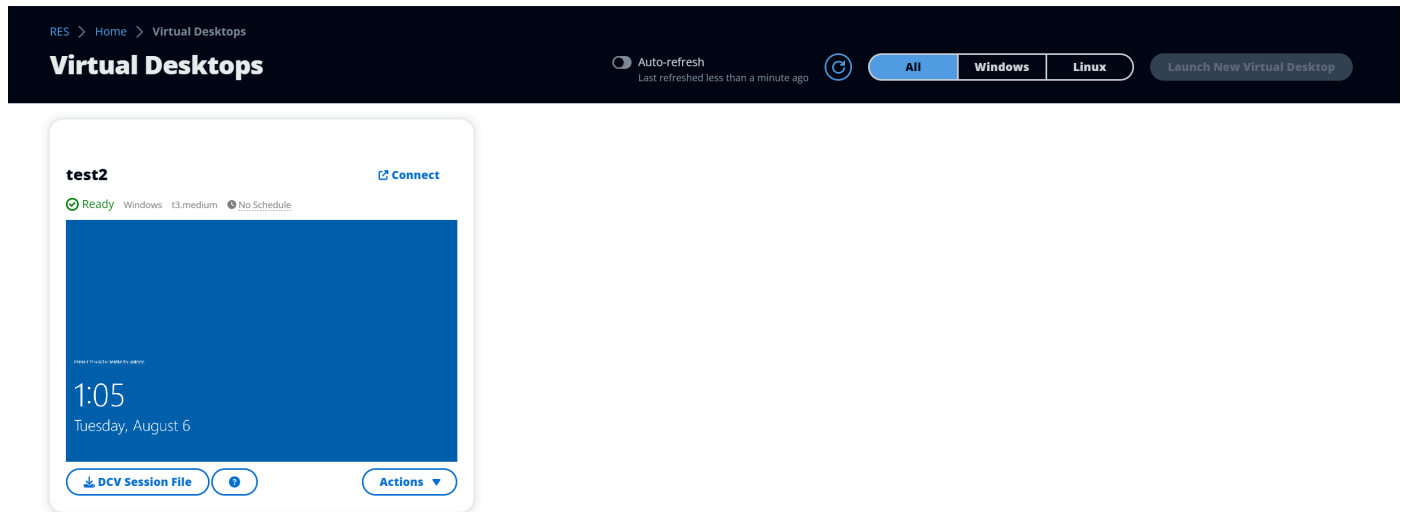
Title	Project Code	Status	Budgets	Groups	Users	Updated On
project2	Project2	Enabled	--	• group_2	• user1	7/15/2024, 11:45:22 AM
project3	Project3	Enabled	--	• group_1 • group_2	-	7/15/2024, 8:05:20 AM

## Autorizzazioni per la gestione delle sessioni VDI

### Creazione di una sessione

Controlla se un utente è autorizzato o meno ad avviare la propria sessione VDI 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.

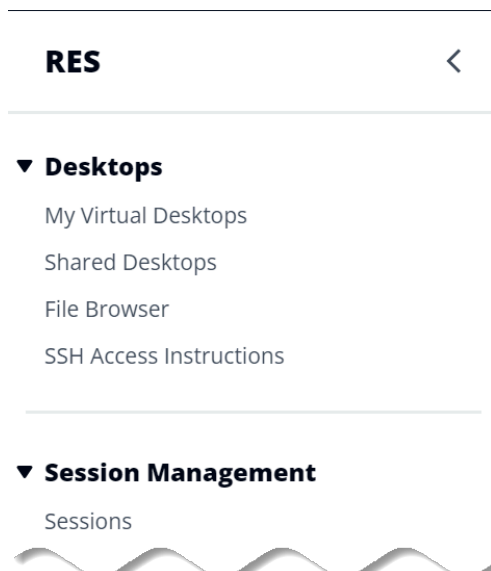
Se un utente non amministratore non dispone delle autorizzazioni per creare una sessione, il pulsante Avvia nuovo desktop virtuale verrà disabilitato per lui come illustrato di seguito:



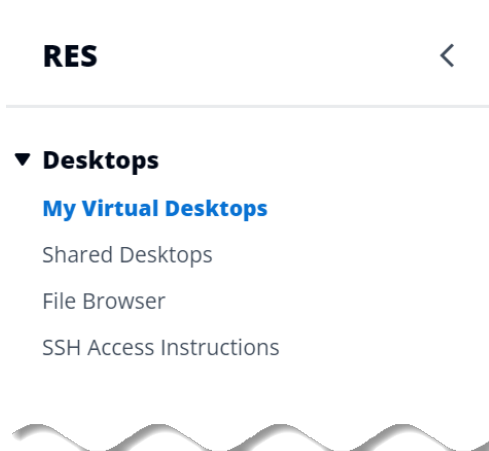
## Crea o termina le sessioni di altri utenti

Consente agli utenti non amministratori di accedere alla pagina Sessioni dal riquadro di navigazione a sinistra. Questi utenti saranno in grado di avviare sessioni VDI 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 amministratore RES, 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 Politica di autorizzazione nel riquadro di navigazione a sinistra. Da questa pagina è possibile creare, aggiornare, elencare, visualizzare ed eliminare i profili di autorizzazione.

	Role ID	Role name	Description	Latest update	Affected projects
<input type="radio"/>	project_owner	Project Owner	Default Permission Profile for Project Owner	2 weeks ago	0
<input type="radio"/>	project_member	Project Member	Default Permission Profile for Project Member	2 weeks ago	10

### Visualizza i profili di autorizzazione

- 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.

RES > Permission Profiles > Project Owner

## Project Owner

Edit Delete

### General Settings

<b>Profile ID</b> project_owner	<b>Description</b> Default Permission Profile for Project Owner	<b>Creation date</b> 3 weeks ago
		<b>Latest update</b> 3 weeks ago

**Permissions** | Affected projects

### Permissions (4)

Permissions granted to this permission profile.

#### Project management permissions (selected 2/2)

<b>Update project membership</b> Update users and groups associated with a project. Enabled	<b>Update project status</b> Enable or disable a project. Enabled
---	---

#### VDI session management permissions (selected 2/2)

<b>Create session</b> Create your own session. Users can always terminate their own sessions with or without this permission. Enabled	<b>Create/Terminate other's session</b> Create/Terminate another user's session within a project. Enabled
---	---

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

RES > Permission Profiles > Project Owner

## Project Owner

Edit Delete

### General Settings

<b>Profile ID</b> project_owner	<b>Description</b> Default Permission Profile for Project Owner	<b>Creation date</b> 2 months ago
		<b>Latest update</b> 4 hours ago

**Permissions** | **Affected projects**

### Affected projects (2)

List of projects using this permission profile.

Project name	Groups	Users
<a href="#">Project1</a>	1	2
<a href="#">Project3</a>	2	0

## 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.

The screenshot shows the 'Create permission profile' form in the RES application. The breadcrumb trail is 'RES > Permission Profiles > Create Profile'. The form is titled 'Create permission profile' and is divided into two main sections: 'Permission profile definition' and 'Permissions'.

**Permission profile definition**

**Profile name**  
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

**Profile description**  
Optionally add more details to describe the specific profile

**Permissions**  
Permissions granted to this permission profile.

**Project management permissions**

<b>Update project membership</b> Update users and groups associated with a project. <input type="checkbox"/>	<b>Update project status</b> Enable or disable a project. <input type="checkbox"/>
--	--

**VDI session management permissions**

<b>Create session</b> Create a session within a project. <input type="checkbox"/>	<b>Create/Terminate other's session</b> Create/Terminate another user's session within a project. <input type="checkbox"/>
---	--

At the bottom right of the form, there are two buttons: 'Cancel' and 'Create profile'.

## 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.

RES > Permission Profiles > Project Member > Edit

## Edit Project Member

### Permission profile definition

**Profile name**  
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

**Profile description**  
Optionally add more details to describe the specific profile

### Permissions

Permissions granted to this permission profile.

#### Project management permissions

**Update project membership**  
Update users and groups associated with a project.

**Update project status**  
Enable or disable a project.

#### VDI session management permissions

**Create session**  
Create your own session. Users can always terminate their own sessions with or without this permission.

**Create/Terminate other's session**  
Create/Terminate another user's session within a project.

[Cancel](#) [Save changes](#)

## 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.

**Research and Engineering Studio** admin1

1 permission profile deleted successfully. This deletion did not impact any ongoing projects.

RES > Permission Profiles

### Permission Profiles

Create and manage permission profiles.

Profile name	Description	Creation date	Latest update	Affected projects
<a href="#">Project Owner</a>	Default Permission Profile for Project Owner	2 months ago	3 minutes ago	2
<a href="#">Project Member</a>	Default Permission Profile for Project Member	2 months ago	2 months ago	2

## profili di autorizzazioni predefiniti

Ogni progetto RES include 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.

Permissions	Description	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

Permissions	Description	Membro del progetto	Proprietario del progetto
	questa autorizzazione.		
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 disabilita a un progetto.		X

## Limiti dell'ambiente

I limiti dell'ambiente consentono agli amministratori di Research and Engineering Studio (RES) di configurare le autorizzazioni che avranno effetto a livello globale per tutti gli utenti. Ciò include autorizzazioni come le autorizzazioni File Browser e SSH, le autorizzazioni desktop e le impostazioni avanzate del desktop.

Engineering Studio clusteradmin

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making any changes, [read Info](#)

### Environment boundaries

- File browser and SSH permissions (enabled 1/2)
- Desktop permissions (enabled 11/11)
  - Display**  
View the remote desktop. This permission is critical, review implications before disabling.
  - Pointer**  
View mouse of remote desktop. This permission is critical, review implications before disabling.
  - Mouse**  
Use local mouse on remote desktop. This permission is critical, review implications before disabling.
  - Audio Out**  
Playback audio from remote desktop. This permission is critical, review implications before disabling.
  - Keyboard**  
Use the local keyboard on remote desktop. This permission is critical, review implications before disabling.
  - Keyboard SAS**  
Use the Secure Attention Sequence (Ctrl+Alt+Del). This permission is critical, review implications before disabling.
  - Screenshot**  
Save screenshot of remote desktop.
  - Clipboard Copy**  
Copy from remote desktop to local clipboard.
  - Clipboard Paste**  
Copy from local clipboard to remote desktop.
  - File Upload**  
Upload files to remote desktop storage.
  - File Download**  
Download files from remote desktop storage.
- Desktop advanced settings (enabled 8/8)

[Project roles](#) | [Desktop sharing profiles](#)

## Configurazione dell'accesso al file browser

Gli amministratori RES possono attivare o disattivare i dati di accesso 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.

**Research and Engineering Studio**

res-new (us-east-1) <

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making

### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

**File browser and SSH permissions (enabled 0/2)**

- Access data**  
Display File browser in the navigation menu and access data via web portal.
- SSH access**  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

- Desktop permissions (enabled 12/12)**
- Desktop advanced settings (enabled 8/8)**

Quando la funzionalità Access data 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 dell'accesso SSH

Gli amministratori possono abilitare o disabilitare SSH per l'ambiente RES dalla sezione Limiti dell'ambiente. L'accesso SSH a VDI è facilitato tramite un host bastion. Quando attivi questo interruttore, RES implementa un bastion host e rende visibile agli utenti la pagina delle istruzioni di accesso SSH. Quando si disattiva l'interruttore, RES disabilita l'accesso SSH, chiude l'host bastion e rimuove la pagina delle istruzioni di accesso SSH per gli utenti. Questo interruttore è disattivato per impostazione predefinita.

### Note

Quando RES implementa un bastion host, aggiunge un'istanza Amazon t3.medium EC2 nel tuo account. AWS Sei responsabile di tutti gli addebiti associati a questa istanza. Per ulteriori informazioni, consulta la [pagina dei prezzi di Amazon EC2](#).

## Per abilitare l'accesso SSH

1. Nella console RES, nel riquadro di navigazione a sinistra, scegli Gestione dell'ambiente, quindi Politica di autorizzazione. In Limiti ambientali, seleziona l'interruttore di accesso SSH.

**Research and Engineering Studio**

res-new (us-east-1) <

- ▼ Desktops
  - My Virtual Desktops
  - Shared Desktops
- ▼ Session Management
  - Dashboard
  - Sessions
  - Software Stacks
  - Debugging
  - Desktop Settings
- ▼ Environment Management
  - Projects
  - Users
  - Groups
  - File Systems
  - S3 Buckets
  - Identity Management
  - Permission policy**
  - Environment Status
  - Snapshot Management
  - General Settings

RES > Environment Management > Permission policy

### Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making any changes, ensure you understand the cascading effects of permissions.

#### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled permissions listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

▼ File browser and SSH permissions (enabled 0/2)

- Access data  
Display File browser in the navigation menu and access data via web portal.
- SSH access  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

▶ Desktop permissions (enabled 12/12)

▶ Desktop advanced settings (enabled 8/8)

2. Attendi che l'accesso SSH sia abilitato.

**Research and Engineering Studio**

res-new (us-east-1) <

- ▼ Desktops
  - My Virtual Desktops
  - Shared Desktops
- ▼ Session Management
  - Dashboard
  - Sessions
  - Software Stacks
  - Debugging
  - Desktop Settings
- ▼ Environment Management
  - Projects
  - Users
  - Groups
  - File Systems
  - S3 Buckets
  - Identity Management
  - Permission policy**
  - Environment Status
  - Snapshot Management
  - General Settings

RES > Environment Management > Permission policy

### Permission policy

Manage user permissions throughout the environment.

**SSH access is being enabled. The application will auto-reload once the change takes effect.**

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making any changes, ensure you understand the cascading effects of permissions.

#### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled permissions listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

▼ File browser and SSH permissions (enabled 1/2)

- Access data  
Display File browser in the navigation menu and access data via web portal.
- SSH access  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

▶ Desktop permissions (enabled 12/12)

▶ Desktop advanced settings (enabled 8/8)

### 3. Una volta aggiunto l'host Bastion, l'accesso SSH è abilitato.

**Research and Engineering Studio**

res-new (us-east-1) <

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making

### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

**File browser and SSH permissions (enabled 1/2)**

- Access data**  
Display File browser in the navigation menu and access data via web portal.
- SSH access**  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

**Desktop permissions (enabled 12/12)**

**Desktop advanced settings (enabled 8/8)**

**Environment Management**

- Projects
- Users
- Groups
- File Systems
- S3 Buckets
- Identity Management
- Permission policy**
- Environment Status
- Snapshot Management
- General Settings


La pagina delle istruzioni di accesso SSH è visibile agli utenti dal pannello di navigazione a sinistra.

**Research and Engineering Studio**

res-new (us-east-1) <

RES > Home > SSH Access

## SSH Access



### Access environment using Linux / MacOS

Follow the below steps to connect to the cluster using Terminal on your Linux or MacOS laptop/workstation:

#### Step 1: Download my Private Key

Download the private key file, and save it your `~/.ssh` directory.

[Download Private Key](#)

#### Step 2: Modify key permissions

Run: `chmod 600 ~/.ssh/admin1_res-new_privatekey.pem`

#### Step 3: Connect to the cluster

Run: `ssh -i ~/.ssh/admin1_res-new_privatekey.pem admin1@3.92.72.222`

#### Optional Step 4: Create SSH config

If you don't want your session to be automatically closed after a couple of minutes of inactivity, edit: `~/.ssh/config` and add:

```
Host res-new-us-east-1
  User admin1
  Hostname 3.92.72.222
  ServerAliveInterval 10
  ServerAliveCountMax 2
  IdentityFile ~/.ssh/admin1_res-new_privatekey.pem
```

Once updated, you can simply run below to connect to your cluster:  
`ssh res-new-us-east-1`

### Access environment using Wind

Follow the below steps to connect to the cluster us

#### Step 1: Download my PuTTY private key

[Download Private Key](#)

#### Step 2: Configure PuTTY

- [Download PuTTY](#)
- As hostname, enter `3.92.72.222`
- Navigate to Connection > SSH > Auth and enter `admin1` under "Private Key used for Authentication"
- Save your session
- Click connect/open to access the cluster

#### Optional Step 3: Enable KeepAlive

If you don't want your session to be automatically closed and add "3" as "Seconds between KeepAlives"

## Per disabilitare l'accesso SSH

1. Nella console RES, nel riquadro di navigazione a sinistra, scegli Gestione dell'ambiente, quindi Politica di autorizzazione. In Limiti ambientali, seleziona l'interruttore di accesso SSH.

**Research and Engineering Studio**

res-new (us-east-1) <

- ▼ **Desktops**
  - My Virtual Desktops
  - Shared Desktops
  - SSH Access Instructions
- ▼ **Session Management**
  - Dashboard
  - Sessions
  - Software Stacks
  - Debugging
  - Desktop Settings
- ▼ **Environment Management**
  - Projects
  - Users
  - Groups
  - File Systems
  - S3 Buckets
  - Identity Management
  - Permission policy**
  - Environment Status
  - Snapshot Management
  - General Settings

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making

### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

▼ **File browser and SSH permissions (enabled 1/2)**

- Access data**  
Display File browser in the navigation menu and access data via web portal.
- SSH access**  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

- ▶ **Desktop permissions (enabled 12/12)**
- ▶ **Desktop advanced settings (enabled 8/8)**

2. Attendi che l'accesso SSH sia disabilitato.

**Research and Engineering Studio**

res-new (us-east-1) <

- ▼ **Desktops**
  - My Virtual Desktops
  - Shared Desktops
  - SSH Access Instructions
- ▼ **Session Management**
  - Dashboard
  - Sessions
  - Software Stacks
  - Debugging
  - Desktop Settings
- ▼ **Environment Management**
  - Projects
  - Users
  - Groups
  - File Systems
  - S3 Buckets
  - Identity Management
  - Permission policy**
  - Environment Status
  - Snapshot Management
  - General Settings

SSH access is being disabled. The application will auto-reload once the change takes effect.

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making

### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

▼ **File browser and SSH permissions (enabled 0/2)**

- Access data**  
Display File browser in the navigation menu and access data via web portal.
- SSH access**  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.

**Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)

- ▶ **Desktop permissions (enabled 12/12)**
- ▶ **Desktop advanced settings (enabled 8/8)**

3. Una volta completato il processo, l'accesso SSH è disabilitato.

**Research and Engineering Studio**

res-new (us-east-1) <

- ▼ **Desktops**
  - My Virtual Desktops
  - Shared Desktops
- ▼ **Session Management**
  - Dashboard
  - Sessions
  - Software Stacks
  - Debugging
  - Desktop Settings
- ▼ **Environment Management**
  - Projects
  - Users
  - Groups
  - File Systems
  - S3 Buckets
  - Identity Management
  - Permission policy**
  - Environment Status
  - Snapshot Management
  - General Settings

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

**Permission policy key concepts**  
Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making

### Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

- ▼ **File browser and SSH permissions (enabled 0/2)**
  - Access data**  
Display File browser in the navigation menu and access data via web portal.
  - SSH access**  
Access data and desktop via Secure Shell (SSH), displaying 'SSH access instructions' in the navigation menu. Disabling SSH removes the menu item as well.
- Info**  
Enabling SSH access adds the Bastion host automatically, which may take minutes. Disabling SSH terminates the host. [View module status](#)
- ▶ **Desktop permissions (enabled 12/12)**
- ▶ **Desktop advanced settings (enabled 8/8)**

## Configurazione delle autorizzazioni del desktop

Gli amministratori possono attivare o disattivare le autorizzazioni del desktop per gestire globalmente la funzionalità VDI di tutti i proprietari di sessioni. 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.

Engineering Studio

RES > Environment Management > Permission policy

## Permission policy

Manage user permissions throughout the environment.

Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making any changes, [read Info](#)

### Environment boundaries

- ▶ File browser and SSH permissions (enabled 1/2)
- ▼ Desktop permissions (enabled 11/11)
  - Display  
View the remote desktop. This permission is critical, review implications before disabling.
  - Pointer  
View mouse of remote desktop. This permission is critical, review implications before disabling.
  - Mouse  
Use local mouse on remote desktop. This permission is critical, review implications before disabling.
  - Audio Out  
Playback audio from remote desktop. This permission is critical, review implications before disabling.
  - Keyboard  
Use the local keyboard on remote desktop. This permission is critical, review implications before disabling.
  - Keyboard SAS  
Use the Secure Attention Sequence (Ctrl+Alt+Del). This permission is critical, review implications before disabling.
  - Screenshot  
Save screenshot of remote desktop.
  - Clipboard Copy  
Copy from remote desktop to local clipboard.
  - Clipboard Paste  
Copy from local clipboard to remote desktop.
  - File Upload  
Upload files to remote desktop storage.
  - File Download  
Download files from remote desktop storage.
- ▶ Desktop advanced settings (enabled 8/8)

[Project roles](#) | [Desktop sharing profiles](#)

## 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.

Project roles | **Desktop sharing profiles**

## Desktop sharing profiles (3)



Actions ▾

Create profile

Find profile by ID

< 1 > ⚙️

	Profile ID	Profile name	Description	Latest update
<input type="radio"/>	observer_profile	View Only Profile	This profile grants view only access on the DCV Se...	2 days ago
<input type="radio"/>	reviewer_2	Reviewer-2	The studio of Jadé Fadojutimi, the British artist,...	27 seconds ago
<input type="radio"/>	reviewer	Admin Profile	This profile grants the same access as the Admin o...	24 hours ago

### Profile definition

#### Profile name

Assign a name to the profile.

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)

- |   |  |  |
|---|--|--|
| <p><input checked="" type="checkbox"/> <b>Display</b><br/>Receive visual data from the NICE DCV server</p> <p><input checked="" type="checkbox"/> <b>Pointer</b><br/>View NICE DCV server mouse position events and pointer shapes</p> <p><input checked="" type="checkbox"/> <b>Mouse</b><br/>Input from the client mouse to the NICE DCV server</p> <p><input checked="" type="checkbox"/> <b>Audio Out</b><br/>Receive audio from the NICE DCV server to the client</p> <p><input checked="" type="checkbox"/> <b>Unsupervised Access</b><br/>Allow a user to connect to session without supervision</p> | <p><input checked="" type="checkbox"/> <b>Keyboard</b><br/>Input from the client keyboard to the NICE DCV server</p> <p><input checked="" type="checkbox"/> <b>Keyboard SAS</b><br/>Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well</p> <p><input checked="" type="checkbox"/> <b>Screenshot</b><br/>Save a screenshot of the remote desktop</p> | <p><input checked="" type="checkbox"/> <b>Clipboard Copy</b><br/>Copy data from the NICE DCV server to the client clipboard</p> <p><input checked="" type="checkbox"/> <b>Clipboard Paste</b><br/>Copy data to the NICE DCV server from the client clipboard</p> <p><input checked="" type="checkbox"/> <b>File Upload</b><br/>Upload files to the session storage</p> <p><input checked="" type="checkbox"/> <b>File Download</b><br/>Download files from the session storage</p> |
|---|--|--|

#### ► Desktop advanced settings (enabled 8/8)

Cancel

Save changes

## 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.

Edit
Actions ▲
Create profile

Desktop sharing profile ID	Title	Description	Created On
<input checked="" type="radio"/> testprofile_1	testProfile_1		9/15/2024, 9:29:55
<input type="radio"/> 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.

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)

<input checked="" type="checkbox"/> <b>Display</b> Receive visual data from the NICE DCV server	<input checked="" type="checkbox"/> <b>Keyboard</b> Input from the client keyboard to the NICE DCV server	<input type="checkbox"/> <b>Clipboard Copy</b> Copy data from the NICE DCV server to the client clipboard
<input checked="" type="checkbox"/> <b>Pointer</b> View NICE DCV server mouse position events and pointer shapes	<input checked="" type="checkbox"/> <b>Keyboard SAS</b> Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well	<input type="checkbox"/> <b>Clipboard Paste</b> Copy data to the NICE DCV server from the client clipboard
<input checked="" type="checkbox"/> <b>Mouse</b> Input from the client mouse to the NICE DCV server	<input checked="" type="checkbox"/> <b>Screenshot</b> Save a screenshot of the remote desktop	<input checked="" type="checkbox"/> <b>File Upload</b> Upload files to the session storage
<input checked="" type="checkbox"/> <b>Audio Out</b> Receive audio from the NICE DCV server to the client		<input checked="" type="checkbox"/> <b>File Download</b> Download files from the session storage
<input checked="" type="checkbox"/> <b>Unsupervised Access</b> Allow a user to connect to session without supervision		

▶ Desktop advanced settings (enabled 8/8)

Cancel
Save changes

# File system

	Title	Name	File System ID	Scope	Provider
<input type="radio"/>	Shared Storage - Home	home	fs-0b4ce6b191491f3e4	cluster	efs
<input type="radio"/>	FSx Lustre	fsx_lustre	fs-0a9042e216f9e3109	project	fsx_lustre
<input type="radio"/>	FSx ONTAP	fsx_ontap	fs-0105118574b6e9890	project	fsx_netapp_ontap
<input type="radio"/>	efs home	efs_home	fs-0df4c9ac93b975142	project	efs

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. Quando viene selezionato un file system, è possibile espandere il riquadro nella parte inferiore dello schermo per visualizzare i dettagli del file system.

## Argomenti

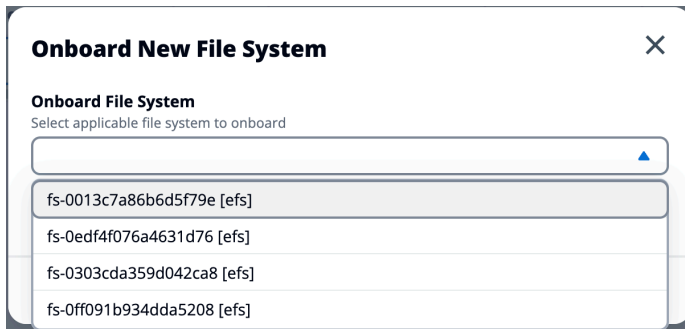
- [Incorpora un file system](#)

## Incorpora un file system

### Note

Per eseguire correttamente l'onboard di un file system, è necessario che condivida lo stesso VPC e almeno una delle sottoreti RES. È inoltre necessario assicurarsi di avere il gruppo di sicurezza configurato correttamente in modo da VDI avere accesso ai contenuti del 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 file system tramite i propri. VDI. VDI monterà il filesystem nel punto di montaggio selezionato durante l'onboarding di un filesystem.

4. Seleziona 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 degli snapshot

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.

The screenshot displays the 'Snapshot Management' interface. At the top, there is a breadcrumb trail: 'RES > Environment Management > Snapshot Management'. The main title is 'Snapshot Management'. Below this, there are two main sections: 'Created Snapshots' and 'Applied Snapshots'. Each section has a search bar, a table with columns 'S3 Bucket Name', 'Snapshot Path', 'Status', and 'Created On', and a 'No records' message. The 'Created Snapshots' section has a 'Create Snapshot' button, and the 'Applied Snapshots' section has an 'Apply Snapshot' button. Orange callout boxes with numbers 1, 2, 3, and 4 highlight the 'Created Snapshots' title, the 'Create Snapshot' button, the 'Applied Snapshots' title, and the 'Apply Snapshot' button respectively.

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 Policy del bucket, scegli Modifica.
4. Aggiungi la seguente dichiarazione alla policy del bucket. Sostituire questi valori con i propri valori:
  - *111122223333*-> l'ID del tuo AWS account
  - *{RES\_ENVIRONMENT\_NAME}*-> il nome del tuo ambiente RES
  - *us-east-1*-> la tua AWS regione
  - *amzn-s3-demo-bucket*-> il nome del tuo bucket S3

**⚠ Important**

Esistono stringhe di versione limitate supportate da AWS. Per ulteriori informazioni, consulta [https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\\_policies\\_elements\\_version.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html).

**JSON**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Export-Snapshot-Policy",
      "Effect": "Allow",
      "Principal": {
        "AWS":
          "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-role"
      }
    }
  ]
}
```

```

    },
    "Action": [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:AbortMultipartUpload",
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "AllowSSLRequestsOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "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. Seleziona Invia.

**Create New Snapshot** ✕

**S3 Bucket Name**  
Enter the name of an existing S3 bucket where the snapshot should be stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

**Snapshot Path**  
Enter a path at which the snapshot should be stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamation marks (!), asterisks (\*), single quotes ('), parentheses (), and hyphens (-).

Cancel Submit

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

## Applica un'istantanea

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

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

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

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

Per aggiungere autorizzazioni al bucket:

1. Seleziona il bucket che hai creato dall'elenco dei bucket.
2. Seleziona la scheda Autorizzazioni.
3. In Policy del bucket, scegli Modifica.
4. Aggiungi la seguente dichiarazione alla policy del bucket. Sostituire questi valori con i propri valori:

- *111122223333*-> l'ID del tuo AWS account
- *{RES\_ENVIRONMENT\_NAME}*-> il nome del tuo ambiente RES
- *us-east-1*-> la tua AWS regione
- *amzn-s3-demo-bucket*-> il nome del tuo bucket S3

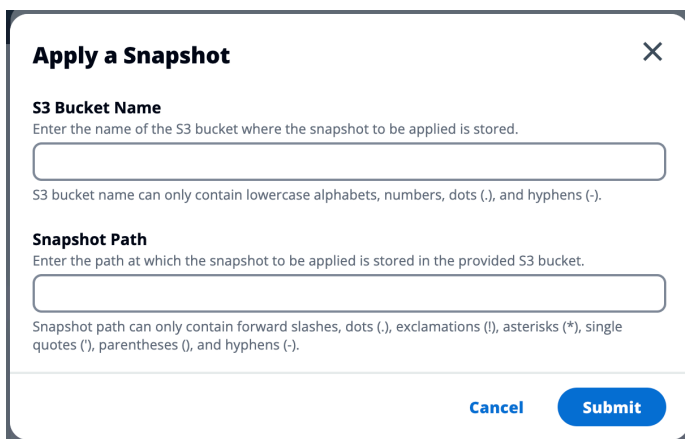
JSON

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

```
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "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. Seleziona Invia.



**Apply a Snapshot** ×

**S3 Bucket Name**  
Enter the name of the S3 bucket where the snapshot to be applied is stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

**Snapshot Path**  
Enter the path at which the snapshot to be applied is stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamation marks (!), asterisks (\*), single quotes ('), parentheses (), and hyphens (-).

Cancel Submit

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

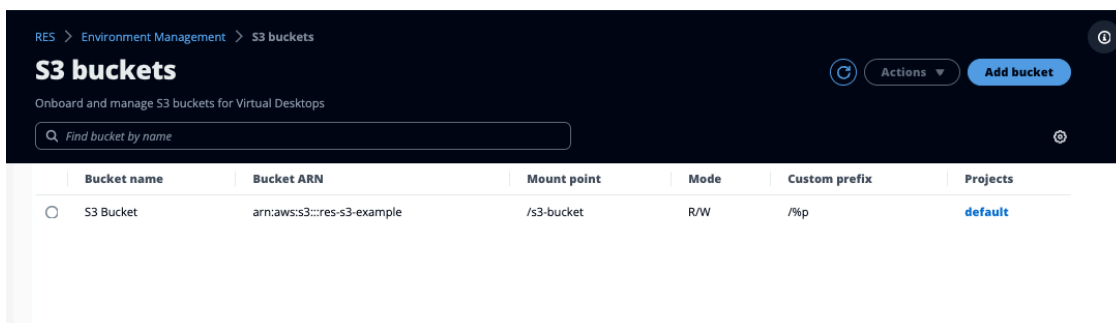
## Bucket Amazon S3

Research and Engineering Studio (RES) supporta il montaggio di [bucket Amazon S3](#) su istanze Linux Virtual Desktop Infrastructure (VDI). Gli amministratori RES possono inserire i bucket S3 in RES,

collegarli ai progetti, modificarne la configurazione e rimuovere i bucket nella scheda S3 bucket in Gestione ambientale.

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

1. Usa Aggiungi bucket per inserire un bucket S3 in 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.

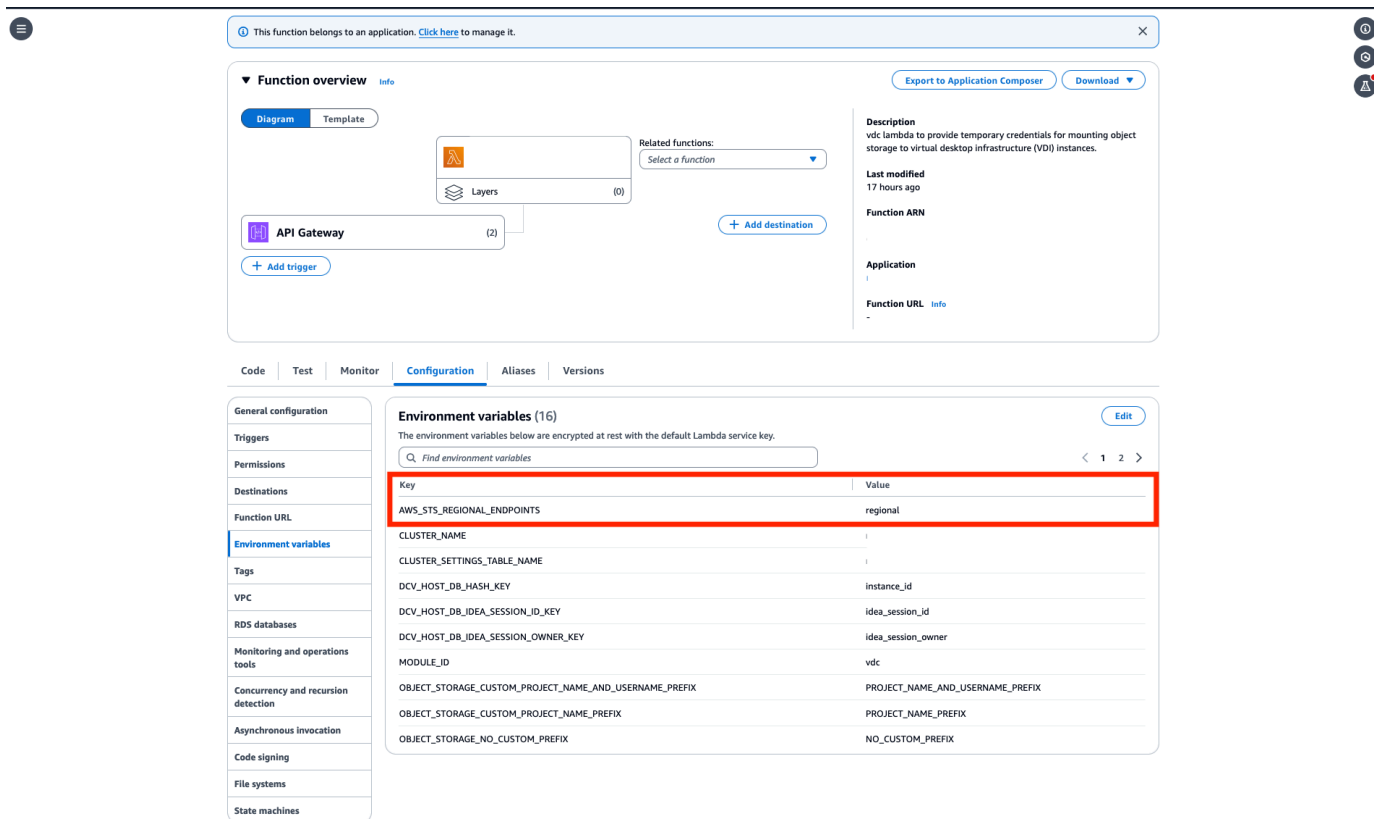
## Argomenti

- [Prerequisiti del bucket Amazon S3 per distribuzioni VPC isolate](#)
- [Aggiungi un bucket Amazon S3](#)
- [Modifica un bucket Amazon S3](#)
- [Rimuovere un bucket Amazon S3](#)
- [Isolamento dei dati](#)
- [Accesso a diversi bucket di account](#)
- [Prevenzione dell'esfiltrazione dei dati in un VPC privato](#)
- [Risoluzione dei problemi](#)
- [Abilitazione CloudTrail](#)

## Prerequisiti del bucket Amazon S3 per distribuzioni VPC isolate

Se stai implementando Research and Engineering Studio in un VPC isolato, segui questi passaggi per aggiornare i parametri di configurazione lambda dopo aver distribuito RES nel tuo account. 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.



The screenshot shows the AWS Lambda console configuration page for a function. The 'Environment variables' section is highlighted with a red box, showing a table of variables. The variable 'AWS\_STS\_REGIONAL\_ENDPOINTS' with the value 'regional' is highlighted.

Key	Value
AWS_STS_REGIONAL_ENDPOINTS	regional
CLUSTER_NAME	
CLUSTER_SETTINGS_TABLE_NAME	
DCV_HOST_DB_HASH_KEY	instance_id
DCV_HOST_DB_IDEA_SESSION_ID_KEY	idea_session_id
DCV_HOST_DB_IDEA_SESSION_OWNER_KEY	idea_session_owner
MODULE_ID	vdc
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_AND_USERNAME_PREFIX	PROJECT_NAME_AND_USERNAME_PREFIX
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_PREFIX	PROJECT_NAME_PREFIX
OBJECT_STORAGE_NO_CUSTOM_PREFIX	NO_CUSTOM_PREFIX

4. Sul lato sinistro, scegli Variabili di 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. Scegli Save (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 nome del bucket, ARN e punto di montaggio.

### Important

- L'ARN, il punto di montaggio e la modalità del bucket forniti non possono essere modificati dopo la creazione.
- L'ARN del bucket 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 dati](#) Per ulteriori informazioni relative all'isolamento dei dati con modalità specifiche, consulta.

4. In Opzioni avanzate, puoi fornire un ruolo IAM ARN per montare i bucket per l'accesso tra account. Segui i passaggi indicati [Accesso a diversi bucket di account](#) per creare il ruolo IAM 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 VDI esistenti di un progetto. Solo le sessioni avviate dopo che il progetto è stato associato al bucket monteranno il bucket.
6. Seleziona Invia.

RES > Environment Management > S3 buckets > Add bucket

## Add bucket

Currently only available for Linux desktops

### Bucket setup

**Bucket display name**  
Type a user friendly name to display

**Bucket ARN**  
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

**Mount point**  
Type the directory path where the bucket will be mounted

**Mode**

Read only (R)  
Allow user only to read or copy stored data

Read and write (R/W)  
Allow users to read or copy stored data and write or edit

**Custom prefix**  
Enable the system to create a prefix automatically

**Advanced settings - optional**

**IAM role ARN**  
To access the bucket, paste the IAM role Amazon Resource Name (ARN) copied in Identity and Access Management (IAM)

### Project association

**Projects - optional**  
Associate the bucket with the following projects. To add a new project, go to Create Project.

Cancel Submit

## 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 VDI (Virtual Desktop Infrastructure) esistenti di quel progetto. Il bucket verrà montato solo nelle sessioni VDI avviate in un progetto 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.

RES > Environment Management > S3 buckets > Edit bucket

### Edit S3 Bucket

**Bucket setup**

**Bucket display name**  
Type a user friendly name to display

S3 Bucket

**Project association**

**Projects - optional**  
Choose the projects to associate to the bucket

default

Cancel 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 le sessioni VDI esistenti perderanno l'accesso al contenuto di quel bucket alla scadenza delle credenziali di quella sessione (~1 ora).

## Isolamento dei dati

Quando aggiungi un bucket S3 a RES, 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 ARN (Amazon Resource Name). Ad esempio, se un amministratore aggiunge un bucket a RES utilizzando l'`arn:aws:s3:::bucket-name/example-data/ARN` e lo associa al Progetto A e al Progetto B, gli utenti che eseguono l' VDI avviato 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 bucket ARN, 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 bucket ARN, come descritto sopra. Questa modalità dispone di opzioni aggiuntive per consentire agli amministratori di fornire prefissi basati 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`

RES > Environment Management > S3 buckets > Add bucket

### Add bucket

Currently only available for Linux desktops

**Bucket setup**

**Bucket display name**  
Type a user friendly name to display

**Bucket ARN**  
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

**Mount point**  
Type the directory path where the bucket will be mounted

**Mode**

Read only (R)  
Allow user only to read or copy stored data

Read and write (R/W)  
Allow users to read or copy stored data and write or edit

**Custom prefix**  
Enable the system to create a prefix automatically

No custom prefix

No custom prefix  
Will not create a dedicated directory

`/%p`  
Create a dedicated directory by project

`/%p/%u`  
Create a dedicated directory by project name and user name

**Projects - optional**  
Associate the bucket with the following projects. To add a new project, go to Create Project.

Cancel Submit

## 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 a RES utilizzando l'`arn:aws:s3:::bucket-name`ARN `No custom prefix` con `selected` e lo associa al Progetto A e al Progetto B, gli utenti che eseguono i VDI avvio 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 a RES utilizzando l'`arn:aws:s3:::bucket-name`ARN `/%p` con `selected` e un Mount Point `/bucket` di 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 ha scritto l'utente A. Tuttavia, se l'utente B avvia un VDI nel Progetto B e lo cerca `/bucket`, non vedrà 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. VDI

## 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 a RES utilizzando l'`arn:aws:s3:::bucket-name`ARN `/%p/%u` con `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 `/bucket`. A differenza dello scenario precedente con il solo `%p` isolamento, l'utente B in questo caso non vedrà il file scritto dall'utente A 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. VDI

## Accesso a diversi bucket di account

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

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

1. Accedi alla console di AWS gestione per l'account RES che deve accedere al bucket S3 (account A).
2. Apri la console IAM:
  - a. Vai alla dashboard IAM.
  - b. Nel riquadro di navigazione, scegli Policy.
3. Crea una policy:
  - a. Scegli Crea policy.
  - b. Seleziona la scheda JSON.
  - c. Incolla la seguente politica JSON (*amzn-s3-demo-bucket* sostituiscila con il nome del bucket S3 situato nell'account B):

JSON

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

```
    ]
  }
]
}
```

- 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 console IAM:
    - a. Vai alla dashboard IAM.
    - b. Nel riquadro di navigazione, seleziona Ruoli.
  6. Crea un ruolo:
    - a. Scegli Crea ruolo.
    - b. Scegli la politica di fiducia personalizzata come tipo di entità affidabile.
    - c. Incolla la seguente politica JSON (**111122223333** sostituiscila con l'ID account effettivo dell'account A, **ENVIRONMENT\_NAME** con il nome dell'ambiente della distribuzione RES e **us-east-1** con la AWS regione in cui viene distribuito RES):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS":
          "arn:aws:iam::111122223333:role/<ENVIRONMENT_NAME>-vdc-custom-
          credential-broker-lambda-role"
      },
      "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. Controlla il ruolo e scegli Crea ruolo.
  9. Usa il ruolo IAM in RES:
    - a. Copia l'ARN del ruolo IAM che hai creato.
    - b. Accedi alla console RES.
    - c. Nel riquadro di navigazione a sinistra, scegli S3 Bucket.
    - d. Scegli Aggiungi bucket e compila il modulo con l'ARN del bucket S3 multiaccount.
    - e. Scegli le impostazioni avanzate (menu a discesa opzionale).
    - f. Inserisci il ruolo ARN nel campo ARN del ruolo IAM.
    - 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 policy per concedere al ruolo IAM dell'Account A l'accesso al bucket (sostituiscilo **111122223333** con l'ID account effettivo dell'Account A e **amzn-s3-demo-bucket** con il nome del bucket S3):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ]
    }
  ]
}
```

- c. Scegli Save (Salva).

## Prevenzione dell'esfiltrazione dei dati in un VPC privato

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

1. Apri la console Amazon VPC:
  - a. Accedi alla console di AWS gestione.

- b. Apri la console Amazon VPC all'indirizzo. <https://console.aws.amazon.com/vpc/>
2. Crea un endpoint VPC 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 in cui desideri creare l'endpoint.
    - b. Per le sottoreti, seleziona entrambe le sottoreti private utilizzate per le sottoreti VDI durante la distribuzione.
    - c. Per Abilita nome DNS, assicurati che l'opzione sia selezionata. Ciò consente di risolvere il nome host DNS privato nelle interfacce di rete degli 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 (sostituiscila *amzn-s3-demo-bucket* con il nome del tuo bucket S3 *111122223333* e *444455556666* con l' AWS account appropriato a IDs cui desideri avere accesso):

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3::amzn-s3-demo-bucket",
        "arn:aws:s3::amzn-s3-demo-bucket/*"
      ]
    }
  ],
}
```

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalAccount": [
      "111122223333",
      "444455556666"
    ]
  }
}
```

## 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 endpoint VPC 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 un VDI, esistono alcune posizioni in cui è possibile verificare la presenza di errori. Segui i passaggi seguenti.

### 1. Controlla i registri VDI:

- a. Accedere alla console di AWS gestione.
- b. Apri la console EC2 e vai a Istanze.
- c. Seleziona l'istanza VDI che hai lanciato.
- d. Connect al 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 CloudWatch log del gateway API di Custom Credential Broker:
  - 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-lambda-vdc-custom-credential-broker-api-gateway-access-logs<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 all'API Gateway per le credenziali personalizzate necessarie per montare i bucket S3.

Come modificare la configurazione del ruolo IAM di un bucket dopo l'onboarding

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: shared-storage.<filesystem\_id>.s3\_bucket.iam\_role\_arn Inserire sostituendolo <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 l'ARN del ruolo IAM corretto.

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 l'ARN del ruolo IAM corretto.
  - c. Scegli Salva per aggiungere l'articolo.
7. Riavvia le istanze VDI:

Riavvia l'istanza per assicurarti VDI che gli ARN interessati dal ruolo IAM errato vengano montati 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 ruolo IAM 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

- [accesso SSH](#)
- [Desktop virtuali](#)
- [Desktop condivisi](#)
- [Browser di file](#)

## accesso SSH

Per utilizzare SSH per accedere all'host bastion:

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

## Desktop virtuali

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

### Sistemi operativi supportati

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

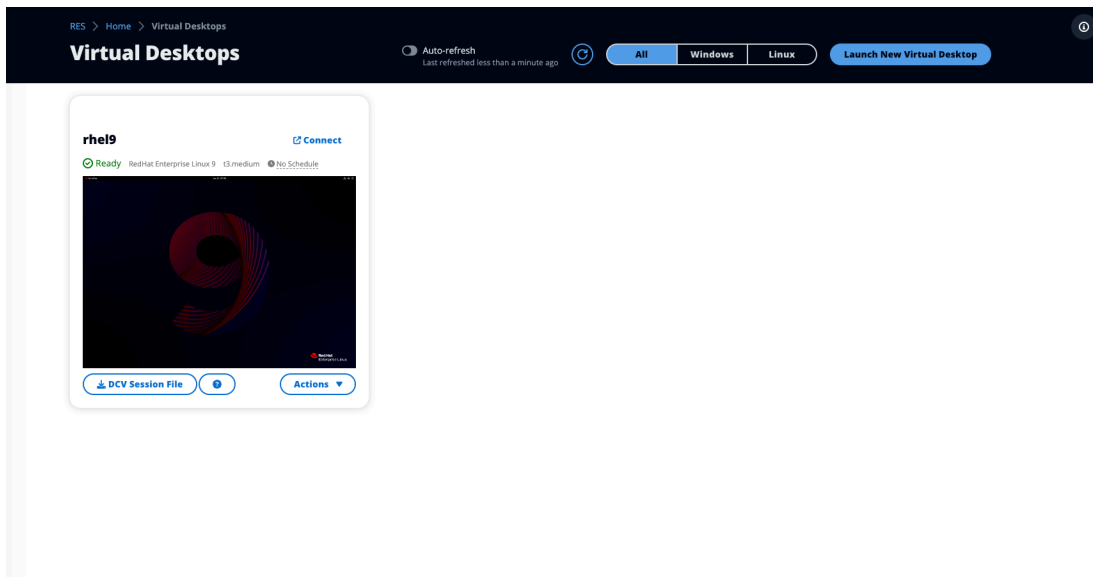
- Amazon Linux 2 (x86 e ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL 8 (x86) e 9 (x86)
- Windows Server 2019, 2022 (x86)
- Windows 10, 11 (x86)

## Argomenti

- [Avvia un nuovo desktop](#)
- [Accedi al tuo desktop](#)
- [Controlla lo stato del tuo desktop](#)
- [Modificare un desktop virtuale](#)
- [Recupera le informazioni sulla sessione](#)
- [Pianifica i desktop virtuali](#)
- [Interfaccia desktop virtuale \(autostop\)](#)

## 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. Seleziona Invia.

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

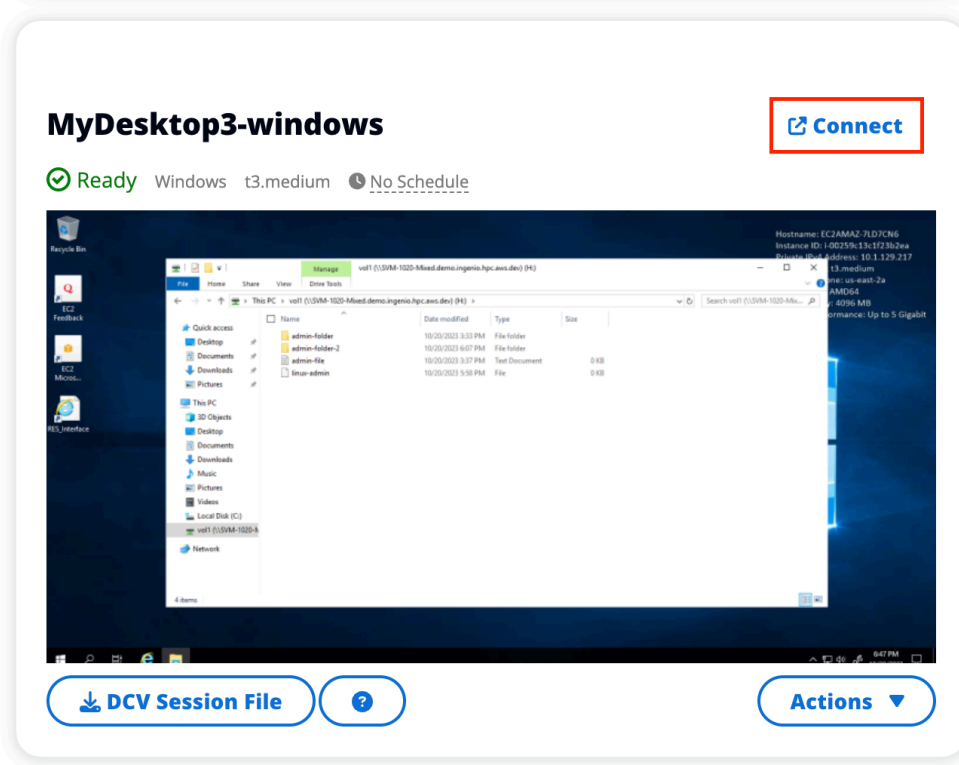
## Accedi al tuo desktop

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

### Web connection

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

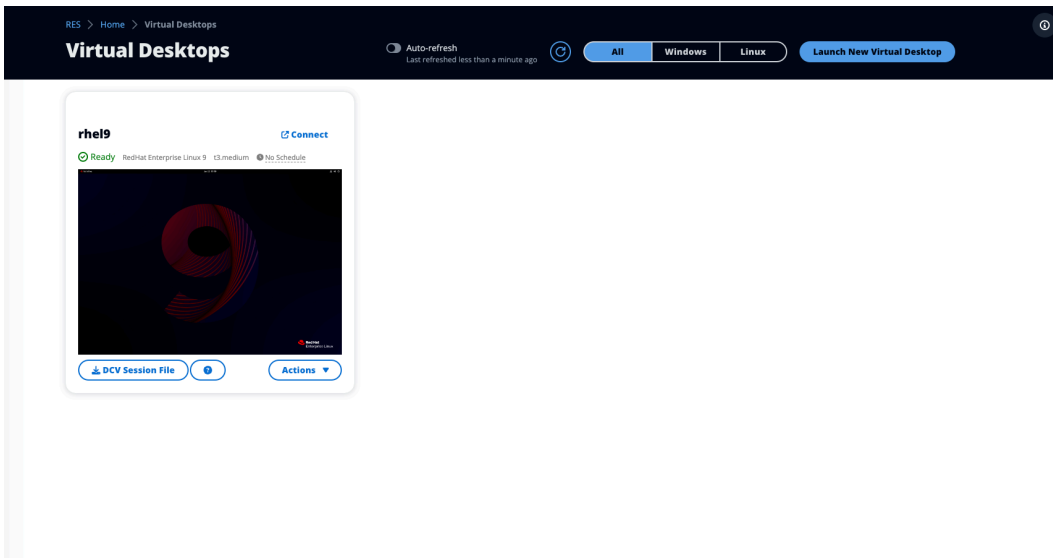
- Scegli Connect o scegli la miniatura per accedere al desktop direttamente tramite il browser.



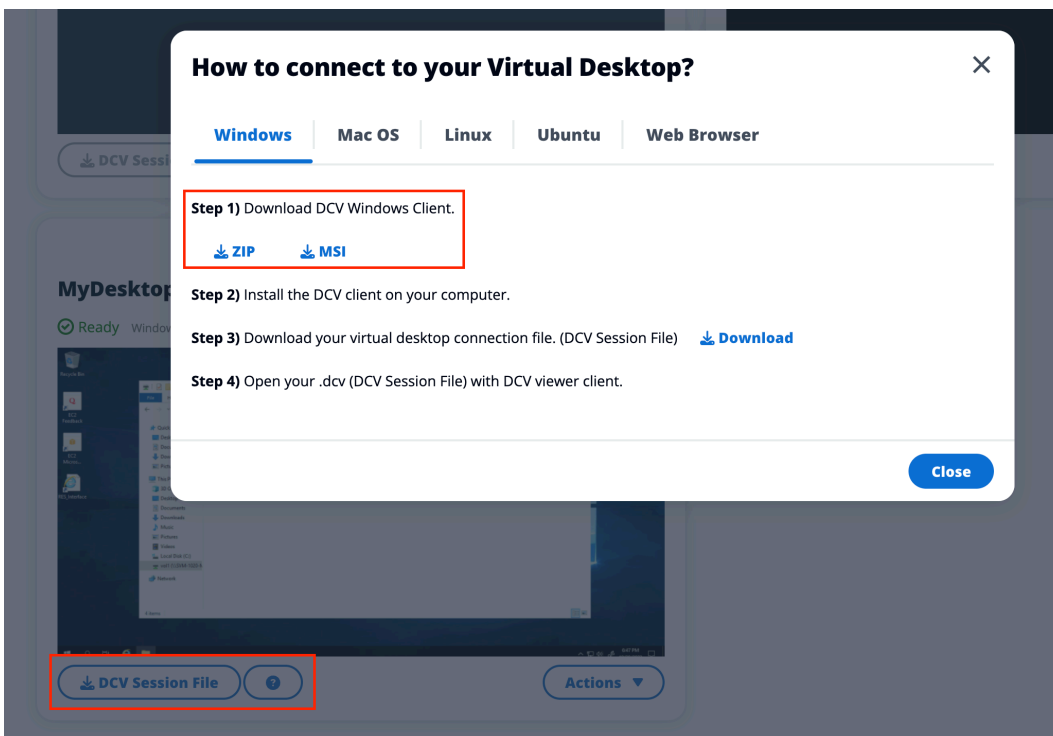
### DCV connection

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

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



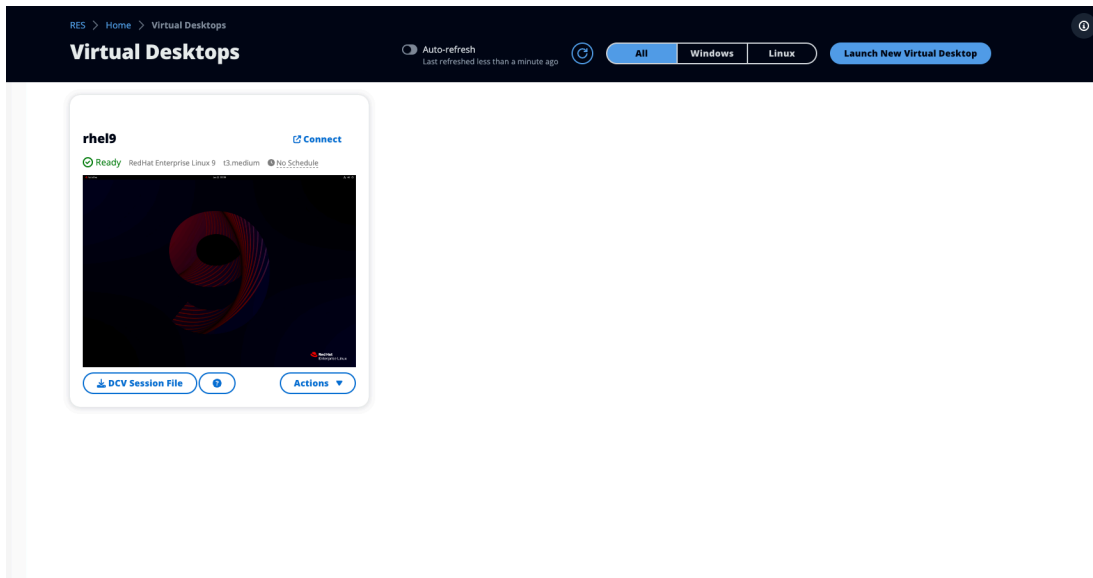
2. Per le istruzioni di installazione, scegli il? icona.



## Controlla lo stato del 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 RES prima di terminare.

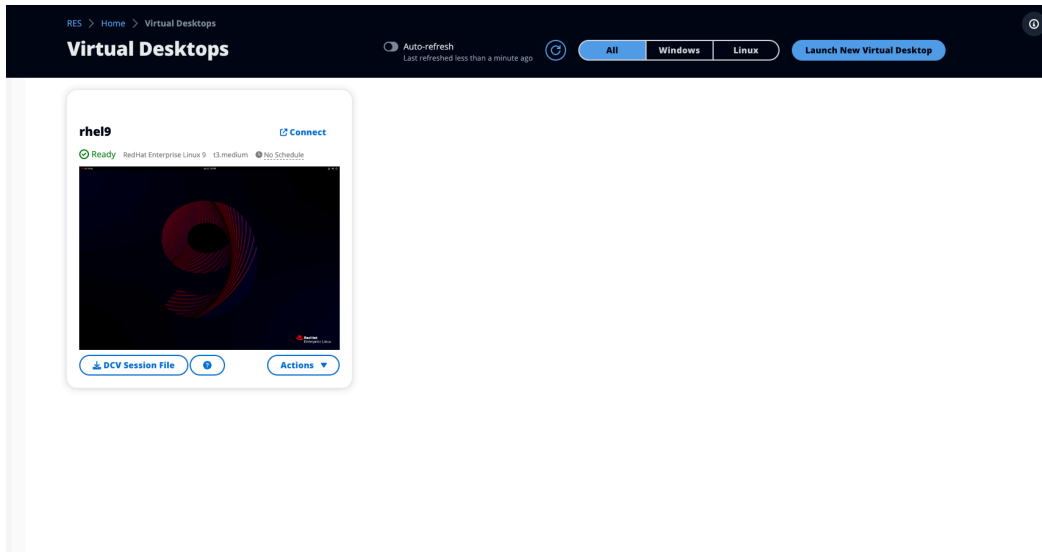
- Ibernazione

Lo stato del desktop verrà salvato in memoria. Al riavvio del desktop, le applicazioni verranno riattivate 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).

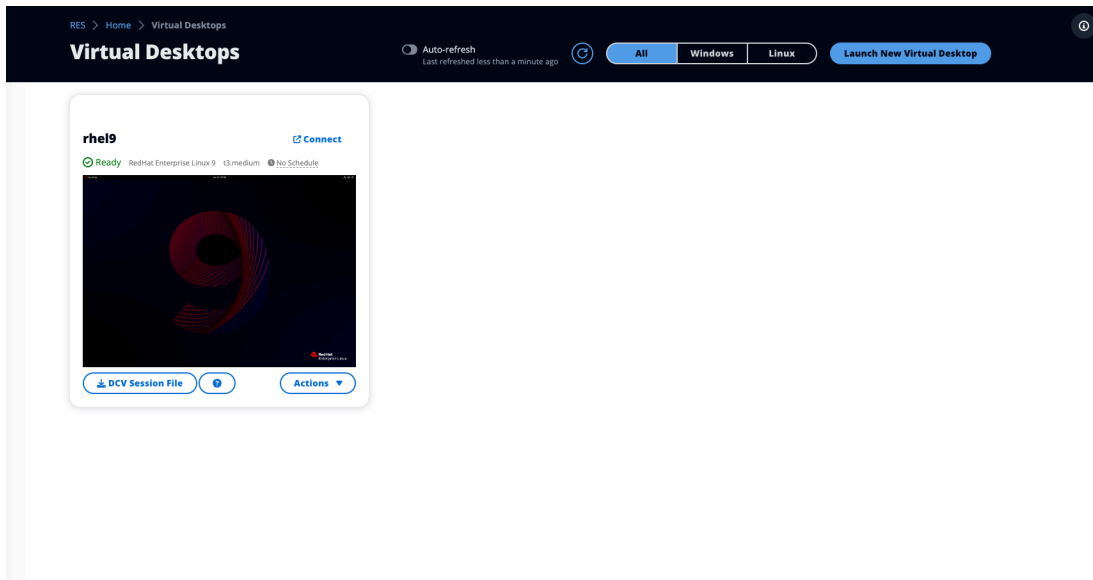
#### Note

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. Seleziona 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

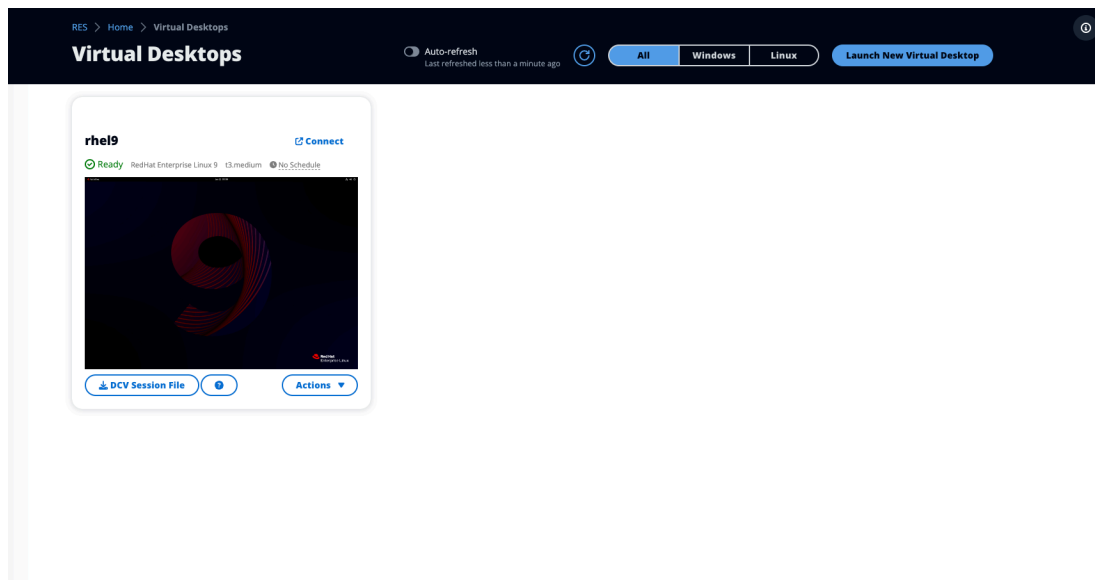
Per impostazione predefinita, i desktop virtuali sono programmati per arrestarsi automaticamente il sabato e la domenica. Le pianificazioni sui singoli desktop possono essere modificate utilizzando le finestre Pianifica a cui si accede dal menu Azioni sui singoli desktop, come illustrato nella sezione successiva. Per ulteriori informazioni, [Impostazione delle pianificazioni predefinite in tutto l'ambiente](#) consulta questa sezione. I desktop possono anche fermarsi se inattivi per contribuire a ridurre i costi. Vedi [Interfaccia desktop virtuale \(autostop\)](#) per saperne di più su VDI Autostop.

### Argomenti

- [Impostazione di pianificazioni desktop individuali](#)
- [Impostazione delle pianificazioni predefinite in tutto l'ambiente](#)

## Impostazione di pianificazioni desktop individuali

1. Scegli Azioni.



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

## Impostazione delle pianificazioni predefinite in tutto l'ambiente

La pianificazione predefinita può essere aggiornata in [DynamoDB](#):

1. Cerca la tabella delle impostazioni del cluster del tuo ambiente: `<env-name>.cluster-settings`

2. Seleziona Esplora elementi.
3. In Filtri inserisci i due filtri seguenti:

#### Filtro 1

- Nome dell'attributo = **key**
- Condizione = **Contains**
- Tipo = **String**
- Valore = **vdc.dcv\_session.schedule**

#### Filtro 2

- Nome dell'attributo = **key**
- Condizione = **Contains**
- Tipo = **String**
- Valore = **type**

filters - optional

Attribute name	Condition	Type	Value	
key	Contains	String	vdc.dcv_session.schedule	Remove
key	Contains	String	type	Remove

[Add filter](#)

[Run](#) [Reset](#)

Verranno visualizzate sette voci che rappresentano i tipi di pianificazione predefiniti per ogni giorno del modulo `vdc.dcv_session.schedule.<day>.type`. I valori validi sono:

- NO\_SCHEDULE
  - STOP\_ALL\_DAY
  - START\_ALL\_DAY
  - WORKING\_HOURS
  - CUSTOM\_SCHEDULE
4. Se CUSTOM\_SCHEDULE è impostata, è necessario fornire orari di inizio e fine personalizzati. A tale scopo, utilizzate il seguente filtro nella tabella delle impostazioni del cluster:

- Nome dell'attributo = **key**
  - Condizione = **Contains**
  - Tipo = **String**
  - Valore = **vdc.dcv\_session.schedule**
5. Cerca l'elemento formattato come `vdc.dcv_session.schedule.<day>.start_up_time` e `vdc.dcv_session.schedule.<day>.shut_down_time` per i rispettivi giorni in cui desideri impostare la tua pianificazione personalizzata. All'interno dell'elemento, elimina la voce Null e sostituiscila con una voce String come segue:
- Nome dell'attributo = **value**
  - Valore = **<The time>**
  - Tipo = **String**

Il valore dell'ora deve essere formattato come XX:XX utilizzando un orologio a 24 ore. Ad esempio, le 9:00 sarebbero le 09:00 mentre le 17:00 sarebbero le 17:00. L'ora inserita corrisponde sempre all'ora locale della AWS regione in cui è installato l'ambiente RES.

## Interfaccia desktop virtuale (autostop)

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

1. Timeout di inattività: le sessioni inattive per questo periodo con un utilizzo della CPU inferiore alla soglia verranno scadute.
2. Soglia di utilizzo della CPU: 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.

## Update Session Settings ✕

**Idle Timeout (minutes)**  
1440  
Sessions idle for this time with CPU utilization below the threshold will time out

**CPU Utilization Threshold (%)**  
60  
Sessions under this threshold are considered idle

**Transition State**  
Stop ▼  
Sessions will transition to this state after idle timeout

**Enforce Schedule**  
  
Enable to allow schedule to resume a session that has been stopped for being idle

**Allowed Sessions Per User**  
5  
Maximum sessions allowed per user

Cancel Submit

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.

RES > Home > Shared Desktops

## Shared Desktops (2)

List of Virtual Desktops shared with you. Unless user has Admin or Owner profile, session owner must be connected in order for them to connect.

Session Created ▾ Last 1 month

Search [ ] All States ▾ All Operating Systems ▾

Name	Session Owner	Base OS	Instance Type	State	Permission Expiry	Download DCV File	Join Session
DemoSession	demouser2	Amazon Linux 2	m6a.large	Ready	10/26/2023, 5:00:00 PM	Download	Connect
MyDesktop6-linux-gs	demoadmin1	Amazon Linux 2	t3.medium	Ready	10/22/2023, 5:00:00 PM	Download	Connect

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.

RES > Home > Virtual Desktops

## Virtual Desktops

Auto-refresh Last refreshed less than a minute ago

All Windows Linux Launch New Virtual Desktop

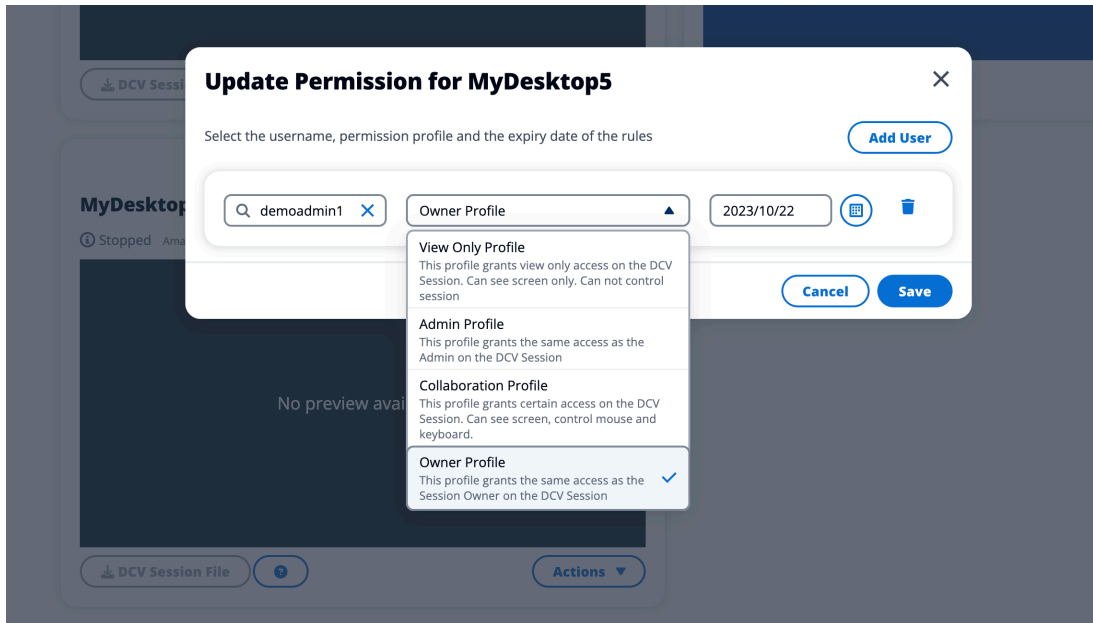
rhel9 [Connect](#)

Ready Redhat Enterprise Linux 9 t3.medium No Schedule

Download DCV Session File Actions

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

#### 4. Scegli Save (Salva).



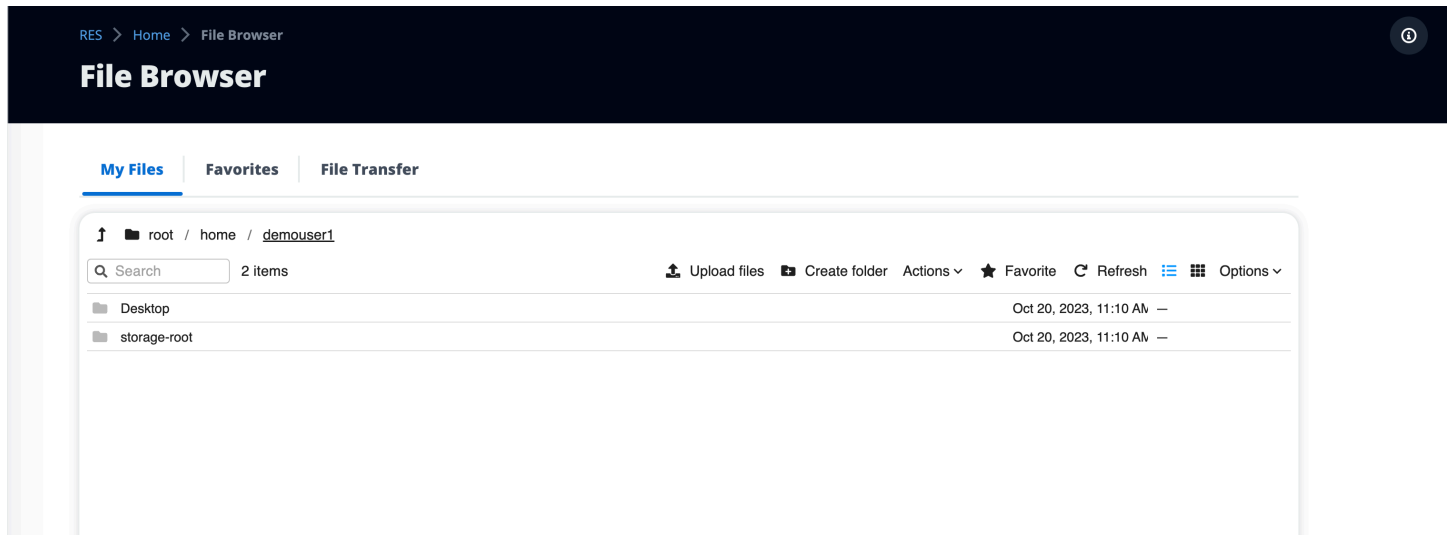
Per ulteriori informazioni sulle autorizzazioni, vedere. [the section called "Policy di autorizzazione"](#)

## 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 istruzioni riportate in [Accedi al tuo desktop](#).

## Browser di file

Il file browser consente di accedere al file system EFS globale condiviso tramite il portale web. È possibile gestire tutti i file disponibili a cui si è autorizzati ad accedere sul filesystem sottostante. Si tratta dello stesso file system condiviso dai desktop virtuali Linux. L'aggiornamento dei file sul desktop virtuale equivale all'aggiornamento di un file tramite il terminale o il browser di file basato sul Web.

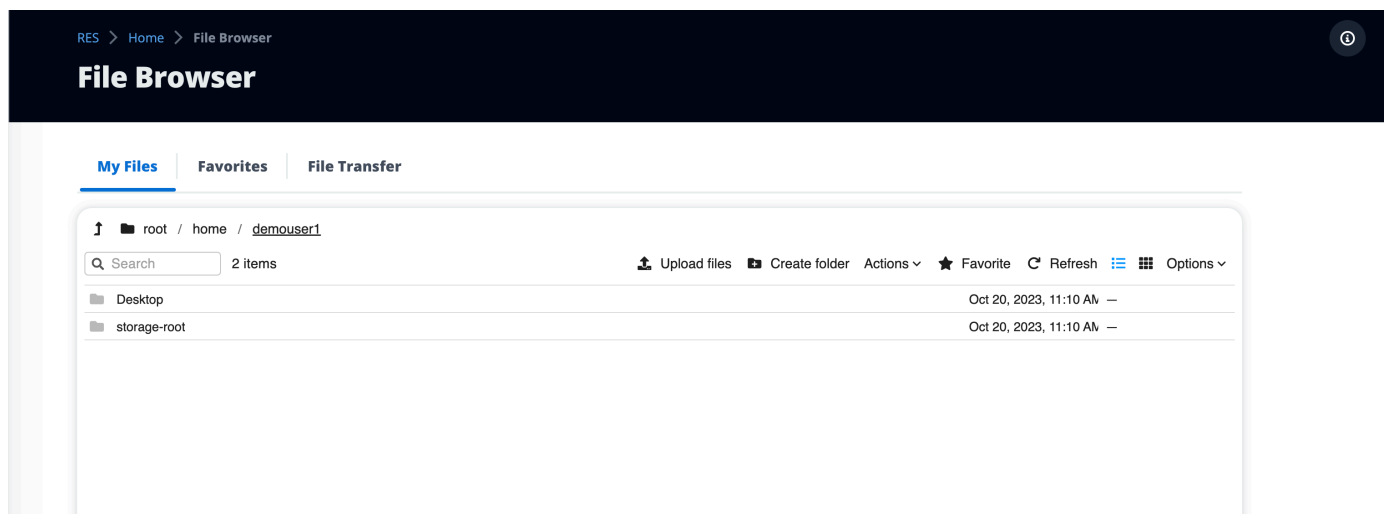


## Argomenti

- [Carica file](#)
- [Elimina uno o più file](#)
- [Gestisci i preferiti](#)
- [Modifica i file](#)
- [Trasferimento dei file](#)

## Carica file

1. Scegli Carica file.

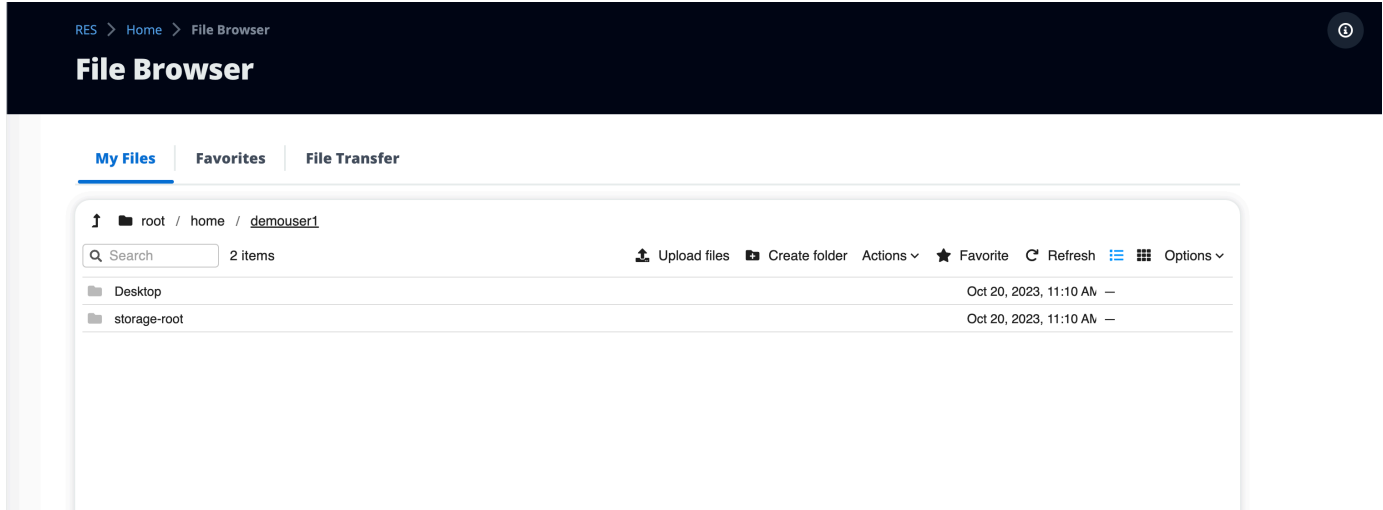


2. Rilascia i file o cerca i file da caricare.

### 3. Scegli Carica (n) file.

## Elimina uno o più file

### 1. Seleziona i file che desideri eliminare.



### 2. Scegli Azioni.

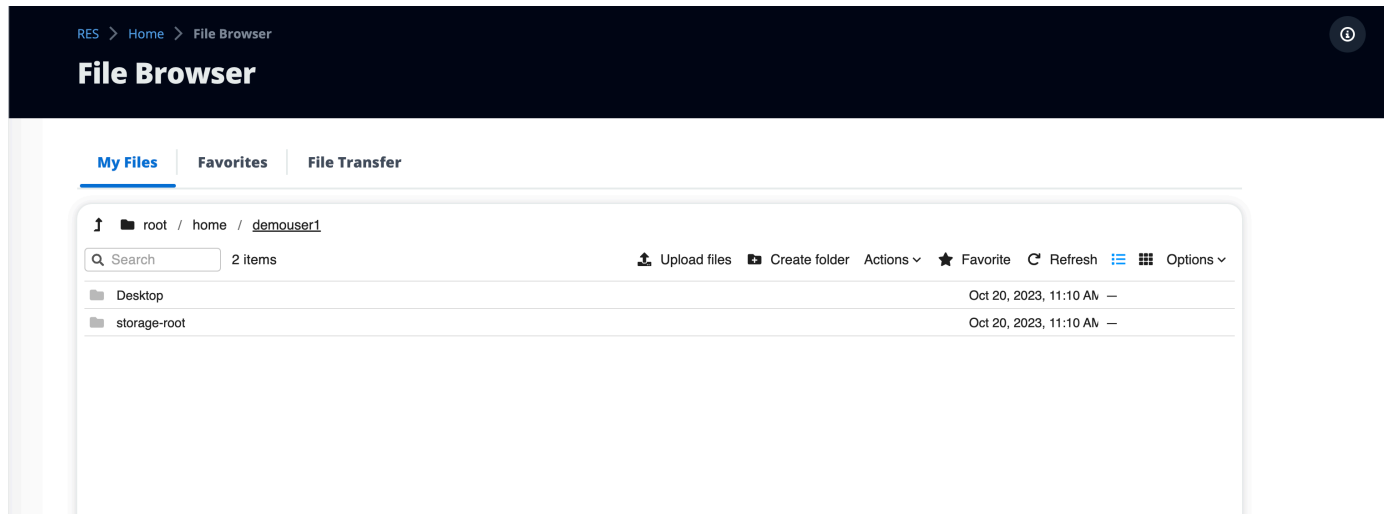
### 3. Seleziona Elimina file.

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.

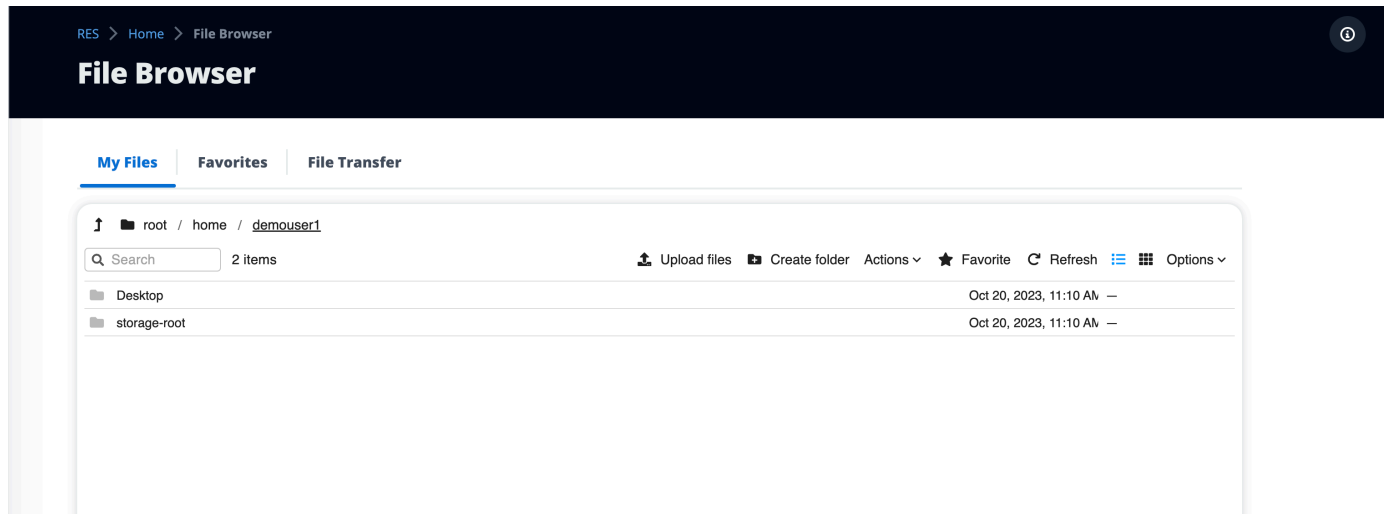
### Note

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

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

RES &gt; Home &gt; 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	Logon Type
SFTP	Key File
User	Key File
demouser3	/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

- [Debug e monitoraggio generali](#)
- [Problema RunBooks](#)
- [Problemi noti](#)

## Contenuti dettagliati:

- [Debug e monitoraggio generali](#)
  - [Utili fonti di informazioni sui registri e sugli eventi](#)
    - [Dove trovare le variabili di ambiente](#)
    - [File di log sull'ambiente \(istanze Amazon EC2\)](#)
    - [CloudFormation pile](#)
    - [Guasti di sistema dovuti a un problema e rilevati dall'attività di gruppo di Amazon EC2 Auto Scaling](#)
  - [Aspetto tipico della console Amazon EC2](#)
    - [Host dell'infrastruttura](#)
    - [Host dell'infrastruttura e desktop virtuali](#)
    - [Host in uno stato terminato](#)
    - [Utili comandi di riferimento relativi ad Active Directory \(AD\)](#)
  - [Debug di Windows DCV](#)
  - [Trova informazioni sulla versione di Amazon DCV](#)
- [Problema RunBooks](#)
  - [Problemi di installazione](#)
    - [Voglio configurare domini personalizzati dopo aver installato RES](#)
    - [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 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 del blocco CIDR 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 CREATE\\_FAILED AdDomainAdminNode](#)
- [Problemi di gestione delle identità](#)
  - [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 in RES](#)
  - [Utente non disponibile durante la creazione di una sessione](#)
  - [Il limite di dimensione è stato superato \(errore nel registro del gestore del CloudWatch cluster\)](#)
- [Archiviazione](#)
  - [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 riesco ad accedervi dagli read/write host VDI](#)
    - [Esempi di casi d'uso per la gestione delle autorizzazioni](#)
  - [Ho creato Amazon FSx for NetApp ONTAP da RES, ma non è stato aggiunto al mio dominio](#)
- [Snapshot](#)
  - [Lo stato di un'istantanea è Fallito](#)
  - [Uno snapshot non viene applicato con i log che indicano che le tabelle non possono essere importate.](#)
- [Infrastruttura](#)
  - [Gruppi target di Load Balancer senza istanze integre](#)
- [Avvio di desktop virtuali](#)
  - [L'account di accesso per Windows Virtual Desktop è impostato su Amministratore](#)
  - [Il certificato scade quando si utilizza una risorsa esterna CertificateRenewalNode](#)

- [Un desktop virtuale che funzionava in precedenza 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»](#)
  - [VDIs bloccato nello stato di Provisioning](#)
  - [VDIs entra nello stato di errore dopo l'avvio](#)
  - [Componente del desktop virtuale](#)
    - [L'istanza Amazon EC2 viene ripetutamente visualizzata come terminata nella console](#)
    - [L'istanza vdc-controller è ciclica a causa del mancato accesso al modulo AD/eVDI mostra Failed API Health Check](#)
    - [Il progetto non viene visualizzato nel menu a discesa quando si modifica lo stack software per aggiungerlo](#)
    - [Il CloudWatch log di Amazon cluster-manager mostra «< user-home-init > account non ancora disponibile in attesa della sincronizzazione dell'utente» \(dove l'account è un nome utente\)](#)
    - [Il desktop di Windows al tentativo di accesso dice «Il tuo account è stato disabilitato. Rivolgiti al tuo amministratore»](#)
    - [Problemi relativi alle opzioni DHCP con external/customer la configurazione AD](#)
    - [Errore Firefox MOZILLA\\_PKIX\\_ERROR\\_REQUIRED\\_TLS\\_FEATURE\\_MISSING](#)
  - [Eliminazione di Env](#)
    - [res-xxx-cluster impila 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 dei registri](#)
    - [Scaricamento dei registri VDI](#)
    - [Scaricamento dei log dalle istanze Linux EC2](#)
    - [Scaricamento dei log dalle istanze di Windows EC2](#)
    - [Raccolta dei log ECS relativi all'errore WaitCondition](#)
  - [Ambiente dimostrativo](#)
    - [Errore di accesso all'ambiente demo durante la gestione della richiesta di autenticazione al provider di identità](#)
    - [Il keycloak dello stack demo non funziona](#)
- 
- [Problemi noti 2024.x](#)

- [Problemi noti 2024.x](#)
  - [\(2024.12 e 2024.12.01\) Errore Regex durante la registrazione di un nuovo utente Cognito](#)
  - [\(2024.12.01 e versioni precedenti\) Errore di certificato errato non valido durante la connessione a VDI utilizzando un dominio personalizzato](#)
  - [\(2024.12 e 2024.12.01\) Gli utenti di Active Directory non possono accedere tramite SSH a Bastion Host](#)
  - [\(2024.10\) Arresto automatico VDI interrotto per ambienti RES implementati in ambienti isolati VPCs](#)
  - [\(2024.10 e versioni precedenti\) Errore nell'avvio di VDI for Graphic Enhanced di istanze](#)
  - [\(2024.08\) Preparazione dell'errore AMI dell'infrastruttura](#)
  - [\(2024.08\) I desktop virtuali non riescono a montare il bucket read/write Amazon S3 con ARN del bucket root e prefisso personalizzato](#)
  - [\(2024.06\) L'applicazione dello snapshot fallisce quando il nome del gruppo AD contiene spazi](#)
  - [\(2024.06 e versioni precedenti\) I membri del gruppo non erano sincronizzati con RES durante la sincronizzazione AD](#)
  - [\(2024.06 e versioni precedenti\) CVE-2024-6387, Regre, vulnerabilità di sicurezza in e Ubuntu SSHion RHEL9 VDI](#)
  - [\(2024.04-2024.04.02\) Limite di autorizzazione IAM fornito non associato al ruolo delle istanze VDI](#)
  - [\(2024.04.02 e versioni precedenti\) Le istanze Windows NVIDIA in ap-southeast-2 \(Sydney\) non vengono avviate](#)
  - [\(2024.04 e 2024.04.01\) Errore di eliminazione RES in GovCloud](#)
  - [\(2024.04 - 2024.04.02\) Il desktop virtuale Linux potrebbe rimanere bloccato nello stato «RIPRESA» al riavvio](#)
  - [\(2024.04.02 e versioni precedenti\) Non riesce a sincronizzare gli utenti AD il cui attributo SAMAccount Name include lettere maiuscole o caratteri speciali](#)
  - [\(2024.04.02 e versioni precedenti\) La chiave privata per l'accesso all'host bastion non è valida](#)

## Debug e monitoraggio generali

Questa sezione contiene informazioni su dove è possibile trovare le informazioni all'interno di RES.

- [Dove trovare le variabili di ambiente](#)
- [File di log sull'ambiente \(istanze Amazon EC2\)](#)
- [CloudFormation pile](#)
- [Guasti di sistema dovuti a un problema e rilevati dall'attività di gruppo di Amazon EC2 Auto Scaling](#)
- [Aspetto tipico della console Amazon EC2](#)
  - [Host dell'infrastruttura](#)
  - [Host dell'infrastruttura e desktop virtuali](#)
  - [Host in uno stato terminato](#)
  - [Utili comandi di riferimento relativi ad Active Directory \(AD\)](#)
- [Debug di Windows DCV](#)
- [Trova informazioni sulla versione di Amazon DCV](#)

## 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.

### Dove trovare le variabili di ambiente

Per impostazione predefinita, puoi trovare le variabili di ambiente, come il nome utente del proprietario della sessione, nelle seguenti posizioni:

- Linux: `/etc/environment`
- Windows: `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\environment_variables.json`

### File di log sull'ambiente (istanze Amazon EC2)

I file di log esistono sulle istanze Amazon EC2 utilizzate da RES. Il Session Manager SSM può essere utilizzato per aprire una sessione sull'istanza per l'esame di questi file.

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

- `/.log opt/idea/app/logs/application`

- /root/bootstrap/logs/
- /var/log/
- /var/log/sss/
- /var/log/messages
- /-data.log var/log/user
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

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

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

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

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

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

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

Su Windows, i file dei certificati NICE DCV si trovano 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 delle stringhe `error` ed `ERROR` e le contenga 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.

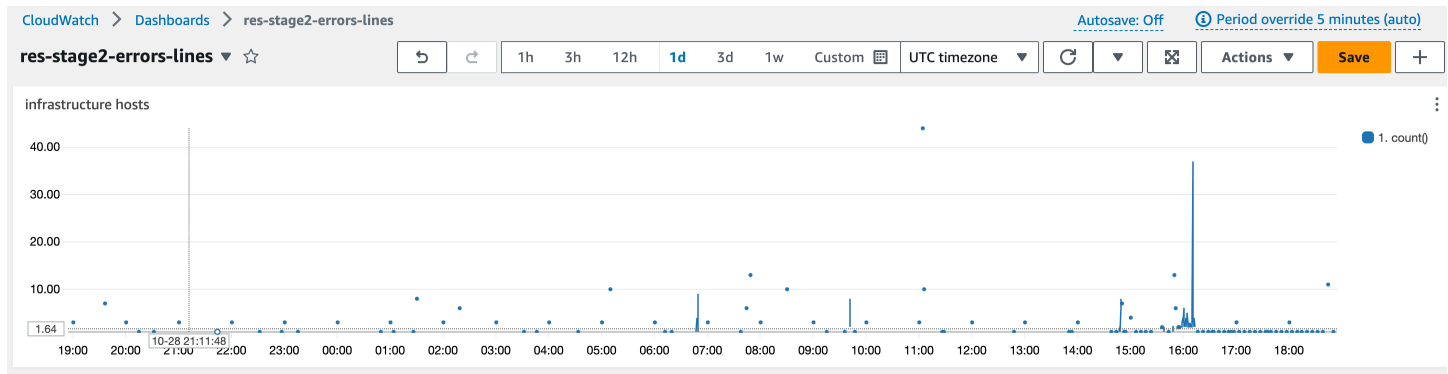
```
{
  "widgets": [
    {
      "type": "log",
      "x": 0,
      "y": 0,
      "width": 24,
      "height": 6,
      "properties": {
        "query": "SOURCE '/<envname>/vdc/controller' |
          SOURCE '/<envname>/cluster-manager' |
          SOURCE '/<envname>/vdc/dcv-broker' |
          SOURCE '/<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.

Pile RES:

- <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 rilevati dall'attività di gruppo di Amazon EC2 Auto Scaling

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

Ciascuno degli ASG (Instance Autoscaling Groups) dell'infrastruttura Amazon EC2 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 console Amazon EC2 e controlla la scheda Auto Scaling Group Activity dell'ASG correlato per determinare se le istanze Amazon EC2 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 sessione SSM 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 dall'ASG.

La console ASG potrebbe mostrare attività simili alle seguenti se si verifica questo problema.

The screenshot shows the 'Target groups' page in the Amazon EC2 console. The breadcrumb path is 'EC2 > Target groups > res-bicfn3-web-portal-e2958adc'. The main heading is 'res-bicfn3-web-portal-e2958adc'. Under 'Details', the 'Target type' is 'Instance' and the 'Protocol' is 'Port HTTPS: 8443'. The 'Health' summary shows 1 Healthy and 0 Unhealthy targets. Below this, a section titled 'Registered targets (1)' contains a table with the following data:

Instance ID	Name	Port	Zone	Health status	Health status details
I-Oba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1c	healthy	

## Aspetto tipico della console Amazon EC2

Questa sezione contiene schermate del sistema operativo in vari stati.

### Host dell'infrastruttura

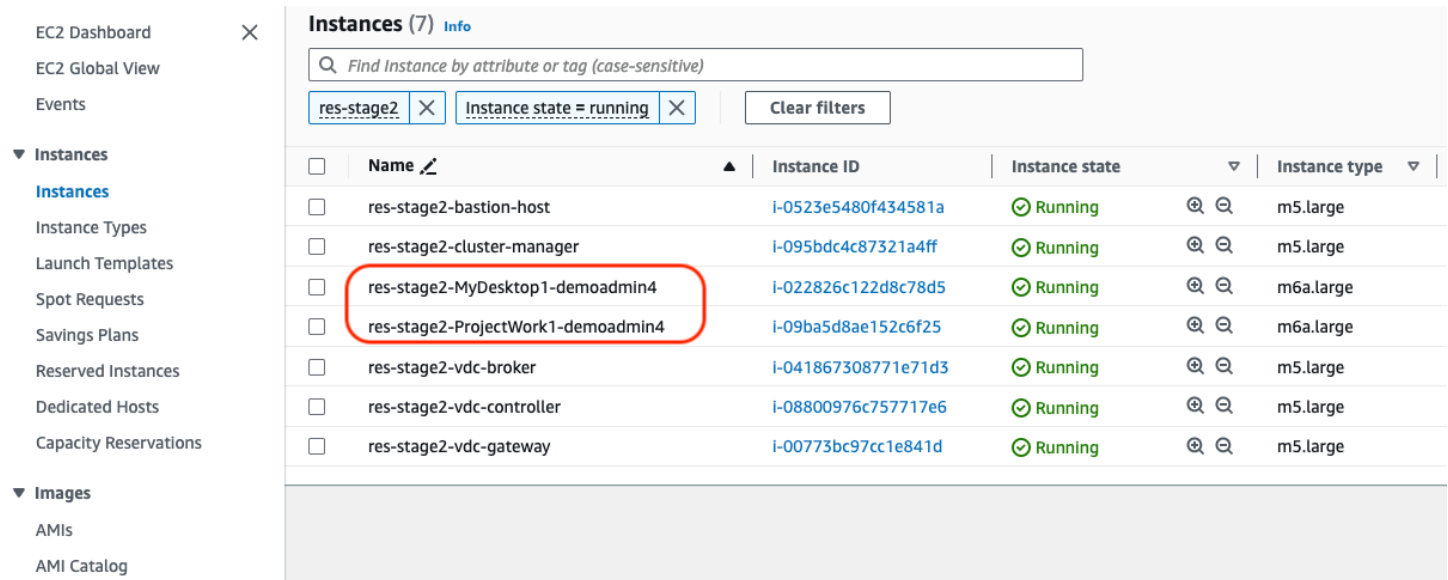
La console Amazon EC2, quando nessun desktop è in esecuzione, in genere ha un aspetto simile alla seguente. Le istanze mostrate sono gli host Amazon EC2 dell'infrastruttura RES. Il prefisso nel nome di un'istanza è il nome dell'ambiente RES.

The screenshot shows the 'Instances (5)' page in the Amazon EC2 console. The breadcrumb path is 'EC2 Dashboard > Instances'. The main heading is 'Instances (5) Info'. There is a search bar and filter buttons for 'res-stage2' and 'Instance state = running'. Below this, a table lists the instances with the following data:

Name	Instance ID	Instance state	Instance type
res-stage2-cluster-manager	I-095bdc4c87321a4ff	Running	m5.large
res-stage2-vdc-broker	I-041867308771e71d3	Running	m5.large
res-stage2-vdc-controller	I-08800976c757717e6	Running	m5.large
res-stage2-bastion-host	I-0523e5480f434581a	Running	m5.large
res-stage2-vdc-gateway	I-00773bc97cc1e841d	Running	m5.large

## Host dell'infrastruttura e desktop virtuali

Nella console Amazon EC2, 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.



The screenshot shows the Amazon EC2 console interface. On the left, there is a navigation menu with options like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMIs', and 'AMI Catalog'. The main area displays a table of instances under the heading 'Instances (7) Info'. The table has columns for 'Name', 'Instance ID', 'Instance state', and 'Instance type'. The instances listed are:

Name	Instance ID	Instance state	Instance type
res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

## Host in uno stato terminato

Quando la console Amazon EC2 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.

EC2 Dashboard		Instances (10) Info			
EC2 Global View		Find Instance by attribute or tag (case-sensitive)			
Events		res-stage2	Clear filters		
Instances	Name	Instance ID	Instance state	Instance type	
Instances	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large	
Instance Types	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large	
Launch Templates	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large	
Spot Requests	res-stage2-windows1-demoadmin4	i-092cdf6a7e52e9b9a	Terminated	m6a.large	
Savings Plans	res-stage2-rhel91-demoadmin4	i-0b3d134f606a53636	Terminated	m6a.large	
Reserved Instances	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large	
Dedicated Hosts	res-stage2-aml21-demoadmin4	i-023844b29c12b9393	Terminated	m6a.large	
Capacity Reservations	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large	
Images	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large	
AMIs	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large	
AMI Catalog					

## 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>
```

## Debug di Windows DCV

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 versione di Amazon DCV

Amazon DCV viene utilizzato per sessioni di desktop virtuali. [AWS Amazon DCV](#). Gli esempi seguenti mostrano come determinare la versione del software DCV installata.

### 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](#)
  - [Voglio configurare domini personalizzati dopo aver installato RES](#)
  - [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 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 del blocco CIDR 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 CREATE\\_FAILED AdDomainAdminNode](#)
- [Problemi di gestione delle identità](#)
  - [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 in RES](#)
  - [Utente non disponibile durante la creazione di una sessione](#)
  - [Il limite di dimensione è stato superato \(errore nel registro del gestore del CloudWatch cluster\)](#)
- [Archiviazione](#)
  - [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 riesco ad accedervi dagli read/write host VDI](#)
    - [Esempi di casi d'uso per la gestione delle autorizzazioni](#)
  - [Ho creato Amazon FSx for NetApp ONTAP da RES, ma non è stato aggiunto al mio dominio](#)
- [Snapshot](#)
  - [Lo stato di un'istantanea è Fallito](#)
  - [Uno snapshot non viene applicato con i log che indicano che le tabelle non possono essere importate.](#)
- [Infrastruttura](#)
  - [Gruppi target di Load Balancer senza istanze integre](#)
- [Avvio di desktop virtuali](#)
  - [L'account di accesso per Windows Virtual Desktop è impostato su Amministratore](#)
  - [Il certificato scade quando si utilizza una risorsa esterna CertificateRenewalNode](#)

- [Un desktop virtuale che funzionava in precedenza 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»](#)
- [VDIs bloccato nello stato di Provisioning](#)
- [VDIs entra nello stato di errore dopo l'avvio](#)
- [Componente del desktop virtuale](#)
  - [L'istanza Amazon EC2 viene ripetutamente visualizzata come terminata nella console](#)
  - [L'istanza vdc-controller è ciclica a causa del mancato accesso al modulo AD/eVDI mostra Failed API Health Check](#)
  - [Il progetto non viene visualizzato nel menu a discesa quando si modifica lo stack software per aggiungerlo](#)
  - [Il CloudWatch log di Amazon cluster-manager mostra «< user-home-init > account non ancora disponibile in attesa della sincronizzazione dell'utente» \(dove l'account è un nome utente\)](#)
  - [Il desktop di Windows al tentativo di accesso dice «Il tuo account è stato disabilitato. Rivolgiti al tuo amministratore»](#)
  - [Problemi relativi alle opzioni DHCP con external/customer la configurazione AD](#)
  - [Errore Firefox MOZILLA\\_PKIX\\_ERROR\\_REQUIRED\\_TLS\\_FEATURE\\_MISSING](#)
- [Eliminazione di Env](#)
  - [res-xxx-cluster impila 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 dei registri](#)
  - [Scaricamento dei registri VDI](#)
  - [Scaricamento dei log dalle istanze Linux EC2](#)
  - [Scaricamento dei log dalle istanze di Windows EC2](#)
  - [Raccolta dei log ECS relativi all'errore WaitCondition](#)
- [Ambiente dimostrativo](#)
  - [Errore di accesso all'ambiente demo durante la gestione della richiesta di autenticazione al provider di identità](#)
  - [Il keycloak dello stack demo non funziona](#)

## Problemi di installazione

### Argomenti

- [Voglio configurare domini personalizzati dopo aver installato RES](#)
- [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 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 del blocco CIDR 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 CREATE\\_FAILED AdDomainAdminNode](#)

.....

### Voglio configurare domini personalizzati dopo aver installato 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. Vai al sistema di bilanciamento del carico esterno RES nella AWS console sotto EC2 > Load Balancing > Load Balancers.
  - 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 SSL/TLS certificato predefinito 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`.  
Si tratta dell'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 nome DNS del bilanciamento del carico alb esterno. *<env-name>-external-alb*
4. Se l'SSO è già configurato nell'ambiente, riconfigura l'SSO con gli stessi input utilizzati inizialmente dal pulsante Gestione dell'ambiente > Gestione delle identità > Single Sign-On > Status > Modifica nel portale web RES.

## Aggiungi certificati al VDI

1. Concedi all'applicazione RES 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 l'accesso VDI.
  - e. Aggiorna il valore di.  
vdc.dcv\_connection\_gateway.certificate.certificate\_secret\_arn Questo è l'ARN del segreto che contiene il contenuto del certificato.
  - f. Aggiorna il valore di.  
vdc.dcv\_connection\_gateway.certificate.private\_key\_secret\_arn Questo è l'ARN del 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'ambiente RES. 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 ePRIVATE\_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 nome DNS del sistema di bilanciamento del carico nlb esterno:.
- <env-name>*-external-nlb

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

.....

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 di 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 CloudFormation stack sono stati creati correttamente

Se non è stato ricevuto un invito via e-mail dopo che gli 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 accessibile, elimina e ridistribuisce l'ambiente Research and Engineering Studio.

2. Controlla la console Amazon EC2 per le prove delle istanze cicliche.

Se ci sono istanze Amazon EC2 con il `<envname>` prefisso che appaiono come 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 le tue risorse esterne, verifica che il VPC, le sottoreti private e pubbliche e altri parametri selezionati siano stati creati dallo stack.

Se uno qualsiasi dei parametri non è corretto, potrebbe essere necessario eliminare e ridistribuire l'ambiente RES. Per ulteriori informazioni, consulta [Disinstalla il prodotto](#).

4. Se hai distribuito il prodotto con 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, avvia una sessione con SSM sull'istanza in esecuzione del vdc-controller.
2. Esegui `sudo su -`.
3. Esegui `systemctl status sssd`.

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

```
[root@ip-10-3-144-194.ec2.internal]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
 Main PID: 31248 (sss) Might see "inactive"/"failed" here
   CGroup: /system.slice/sss.service
           └─31248 /usr/sbin/sss -i --logger=files
             └─31249 /usr/libexec/sss/sss_be --domain corp.res.com --uid 0 --gid 0 --logger=files
               └─31251 /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger=files
                 └─31252 /usr/libexec/sss/sss_pam --uid 0 --gid 0 --logger=files

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

*Might see errors highlighted in RED here*

## Registro degli errori SSM

Per risolvere il problema:

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

Il problema potrebbe 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 dello stack RES.
  - `directoryservice.ldap_connection_uri`
  - `directoryservice.ldap_base`
  - `directoryservice.users.ou`
  - `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 Directory Service.

- ii. Seleziona l'ID della directory RES 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 `ilvdcvhostsecuritygroup`, ciò potrebbe essere dovuto a un'istanza Amazon EC2 che è stata lanciata in una sottorete o in un gruppo di sicurezza creato da RES utilizzando la Console. AWS

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

.....

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

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

## Esempio di errore:

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

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

.....

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

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

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

.....

## La creazione dello stack di risorse esterne (demo) non riesce con CREATE\_FAILED AdDomainAdminNode

Se la creazione dello stack dell'ambiente demo fallisce con il seguente errore, potrebbe essere dovuto all'applicazione di patch di Amazon EC2 avvenuta 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, controlla se RunCommand/Automation l'esecuzione di un documento SSM relativo all'applicazione di patch coincide con l'avvio di un'istanza.
3. Nei file di registro per le istanze Amazon EC2 dell'ambiente, esamina la registrazione dell'istanza locale per determinare se l'istanza è stata riavviata durante il provisioning.

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

.....

## Problemi di gestione delle identità

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

- [the section called “Configurazione dell'SSO con IAM Identity Center”](#)
- [the section called “Configurazione del provider di identità per 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 in RES](#)
- [Utente non disponibile durante la creazione di una sessione](#)
- [Il limite di dimensione è stato superato \(errore nel registro del gestore del CloudWatch cluster\)](#)

.....

### Non sono autorizzato a eseguire iam: PassRole

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

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 utente IAM 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 trasmettere 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 maggiori informazioni, consulta gli argomenti seguenti:

- Per scoprire come fornire l'accesso alle tue risorse su più AWS account di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta [Fornire l'accesso agli AWS account di proprietà di terze parti](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo dei ruoli e delle politiche basate sulle risorse per l'accesso tra account diversi, consulta [In che modo i ruoli IAM 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'integrazione SSO non è configurata correttamente. Per determinare il problema, controlla i registri delle istanze del controller e verifica la presenza di errori nelle impostazioni di configurazione.

Per controllare i log:

1. Apri la [CloudWatch console](#).
2. Da 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. Scegli Esegui.
6. Nella stringa restituita, verifica che i valori di configurazione SSO siano corretti. Se non sono corretti, modifica il valore della chiave `sso_enabled` su False.

### Edit item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#) 



Attribute name	Value
key - Partition key	identity-provider.cognito.sso_enabled
value	<input type="radio"/> True <input checked="" type="radio"/> False

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

---

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

Se un utente riceve l'errore «Utente non trovato» quando tenta di accedere all'interfaccia RES 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. RES si sincronizza ogni ora, quindi potrebbe essere necessario attendere e verificare che l'utente sia stato aggiunto dopo la sincronizzazione successiva. Per eseguire la sincronizzazione immediata, segui la procedura riportata di seguito. [Utente aggiunto in Active Directory, ma mancante in RES](#)
- Se l'utente è presente in RES:
  1. Assicurati che la mappatura degli attributi sia configurata correttamente. Per ulteriori informazioni, consulta [Configurazione del provider di identità per il Single Sign-On \(SSO\)](#).
  2. Assicurati che l'oggetto SAML e l'e-mail SAML corrispondano entrambi all'indirizzo e-mail dell'utente.

---

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

### Note

Questa sezione si applica a RES 2024.10 e versioni precedenti. Per RES 2024.12 e versioni successive, vedere. [Come eseguire manualmente la sincronizzazione \(release 2024.12 e 2024.12.01\)](#) Per RES 2025.03 e versioni successive, vedere. [Come avviare o interrompere manualmente la sincronizzazione \(versione 2025.03 e successive\)](#)

Se hai aggiunto un utente ad Active Directory ma non è presente in RES, è necessario attivare la sincronizzazione AD. La sincronizzazione AD viene eseguita ogni ora da una funzione Lambda che importa le voci AD nell'ambiente RES. 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 [console Amazon SQS](#).
2. Da Queues, seleziona. `<environment-name>-cluster-manager-tasks.fifo`
3. Scegli Invia e ricevi messaggi.
4. Per il corpo del messaggio, inserisci:  

```
{ "name": "adsync.sync-from-ad", "payload": {} }
```
5. Per 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 di ricerca ldap del tuo IDP.

.....

## Archiviazione

### 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 riesco ad accedervi dagli read/write host VDI](#)
- [Ho creato Amazon FSx for NetApp ONTAP da RES, ma non è stato aggiunto al 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 host VDI. Segui i passaggi seguenti per verificare che il file system sia nello stato richiesto.

### Amazon EFS

1. Vai alla [console Amazon EFS](#).
2. Verifica che lo stato del file system sia Disponibile.
3. Se lo stato del file system non è Disponibile, attendi prima di avviare gli host VDI.

### Amazon FSx ONTAP

1. Vai alla [FSx console Amazon](#).
2. Verifica che lo stato sia disponibile.
3. Se Status non è disponibile, attendi prima di avviare gli host VDI.

.....

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

I file system integrati su RES devono avere le regole di gruppo di sicurezza richieste configurate per consentire agli host VDI di montare i file system. Poiché questi file system vengono creati esternamente a RES, 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:

- Traffico NFS (porta: 2049) dagli host Linux VDC

- Traffico SMB (porta: 445) proveniente dagli host Windows VDC

.....

## Non riesco ad accedervi dagli read/write host VDI

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

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

### Esempi di casi d'uso per la gestione delle autorizzazioni

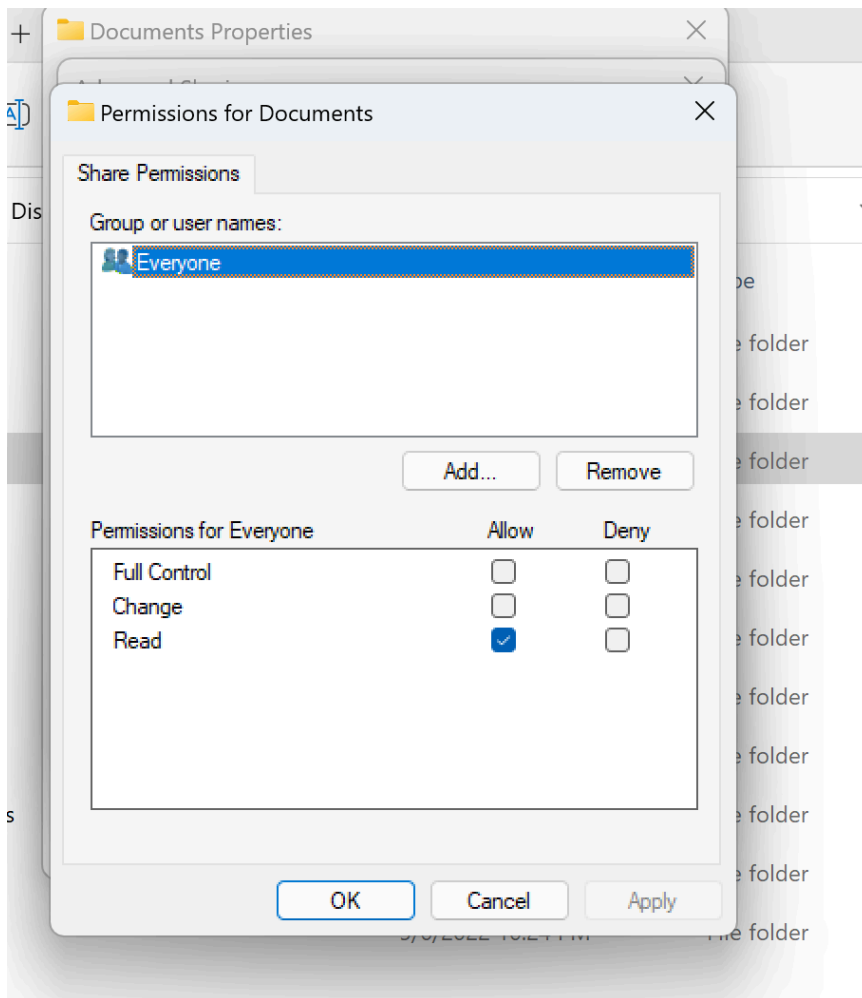
#### Utilizzo di volumi in stile UNIX con carichi di lavoro Linux

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

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

#### Utilizzo di volumi in stile NTFS 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



Se il volume verrà utilizzato da client Linux e Windows, è necessario impostare una mappatura dei nomi su SVM che assocerà qualsiasi nome utente Linux allo stesso nome utente con il formato del nome di dominio NetBIOS domain\username. 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 for NetApp ONTAP da RES, ma non è stato aggiunto al mio dominio

Attualmente, quando crei Amazon FSx for NetApp ONTAP dalla console RES, il file system viene fornito ma non entra a far parte del dominio. Per aggiungere la SVM del file system ONTAP creata al tuo dominio, consulta [Registrazione SVMs a Microsoft Active Directory](#) e segui i passaggi sulla console [Amazon FSx](#). Assicurati che [le autorizzazioni richieste siano delegate all'account Amazon](#)

[FSx Service](#) in AD. Una volta che l'SVM si è unito correttamente al dominio, vai su SVM Summary > Endpoints > SMB DNS name e copia il nome DNS perché ti servirà in seguito.

Dopo averlo aggiunto al dominio, modifica la chiave di configurazione DNS SMB 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 nome DNS SMB 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](#). I nuovi host VDI che utilizzano il file system saranno ora in grado di montare SVM e file system uniti al dominio.

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](#)
- [Uno snapshot non viene applicato con i log che indicano che le tabelle non possono essere importate.](#)

.....

## Lo stato di un'istantanea è Fallito

Nella pagina RES Snapshots, 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 lo stato delle varie tabelle sia ExportStatus COMPLETATO. 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 diventi su COMPLETATO in 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

- [Gruppi target di Load Balancer senza istanze integre](#)

## Gruppi target di Load Balancer senza istanze integre

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

I metodi per determinare l'origine del problema consistono innanzitutto nel controllare nella console Amazon EC2 eventuali istanze Amazon EC2 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 console Amazon EC2, non mostrano alcuna istanza integra registrata.

Di seguito è riportato un esempio di aspetto normale:

The screenshot shows the Amazon EC2 console interface for a target group. The breadcrumb navigation at the top is 'EC2 > Target groups > res-bicfn3-web-portal-e2958adc'. The main content area displays the following details:

- Details:** Target type: Instance; Protocol: Port HTTPS: 8443; Protocol version: HTTP1; VPC: vpc-011d10e23ad10cb8e.
- Summary Table:**

Total targets	1	Healthy	1	Unhealthy	0	Unused	0	Initial	0	Draining	0
---------------	---	---------	---	-----------	---	--------	---	---------	---	----------	---
- Registered targets (1):**

Instance ID	Name	Port	Zone	Health status	Health status details
I-Oba5d508631f20045	res-bicfn3-cluster-manager	8443	eu-central-1c	healthy	

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

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

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

- [L'account di accesso per Windows Virtual Desktop è impostato su Amministratore](#)
- [Il certificato scade quando si utilizza una risorsa esterna CertificateRenewalNode](#)
- [Un desktop virtuale che funzionava in precedenza 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»](#)
- [VDIs bloccato nello stato di Provisioning](#)
- [VDIs entra nello stato di errore dopo l'avvio](#)

.....

### L'account di accesso per Windows Virtual Desktop è impostato su Amministratore

Se è possibile avviare un desktop virtuale Windows nel portale Web RES ma il relativo account di accesso è impostato su Amministratore al momento della connessione, è possibile che il VDI di Windows non si sia unito correttamente ad Active Directory.

Per verificare, connettiti all'istanza Windows dalla console Amazon EC2 e controlla i log di bootstrap sotto. C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\ Un messaggio di errore che inizia con [Join AD] authorization failed: indica che l'istanza non è riuscita a unirsi all'AD. Controlla che Cluster Manager acceda CloudWatch con il nome del gruppo di log *<res-environment-name>*/cluster-manager per maggiori dettagli sull'errore:

- `Insufficient permissions to modify computer account`
  - Questo errore indica che il tuo account di servizio non dispone delle autorizzazioni appropriate per aggiungere computer all'AD. Controlla la [Configurare un account di servizio per Microsoft Active Directory](#) sezione per le autorizzazioni richieste dall'account di servizio.

## • Invalid Credentials

- Le credenziali del tuo account di servizio in AD sono scadute o hai fornito credenziali errate. Per controllare o aggiornare le credenziali del tuo account di servizio, accedi al segreto che memorizza la password nella [console Secrets Manager](#). Assicurati che l'ARN di questo segreto sia corretto nel campo Service Account Credentials Secret ARN in Active Directory Domain nella pagina Identity Management del tuo ambiente RES.

## Il certificato scade quando si utilizza una risorsa esterna CertificateRenewalNode

Se hai distribuito la [ricetta External Resources](#) e riscontri un errore "The connection has been closed. Transport error" durante la connessione a Linux VDIs, la causa più probabile è un certificato scaduto che non viene aggiornato automaticamente a causa di un percorso di installazione pip errato su Linux. I certificati scadono dopo 3 mesi.

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:

```
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702 WARN HTTP:Splicer Connection{id=341
client_address="x.x.x.x:50682"}: Error in connection task: TLS handshake error:
received fatal alert: CertificateUnknown | redacted:/res-demo/vdc/dcv-connection-
gateway | dcv-connection-gateway_10.3.146.195 |
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702 WARN HTTP:Splicer Connection{id=341
client_address="x.x.x.x:50682"}: Certificate error: AlertReceived(CertificateUnknown)
| redacted:/res-demo/vdc/dcv-connection-gateway | dcv-connection-gateway_10.3.146.195
|
```

Per risolvere il problema:

1. Nel tuo AWS account, accedi a [EC2](#). Se è presente un'istanza denominata\* - CertificateRenewalNode-\*, interrompi l'istanza.
2. Vai a [Lambda](#). Dovresti vedere una funzione Lambda denominata\* - CertificateRenewalLambda-\* , controlla il codice Lambda per qualcosa di simile alla seguente:

```
export HOME=/tmp/home
mkdir -p $HOME
```

```

cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
python3 ./get-pip.py
pip3 install boto3
eval $(python3 -c "from botocore.credentials import
InstanceMetadataProvider, InstanceMetadataFetcher; provider =
InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
num_attempts=2)); c = provider.load().get_frozen_credentials();
print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
git clone https://github.com/Neilpang/acme.sh.git
cd acme.sh

```

3. [Trova l'ultimo modello di stack di risorse esterne Certs qui.](#) Trova il codice Lambda nel modello: Risorse → → Proprietà CertificateRenewalLambda → Codice. Potresti trovare qualcosa di simile al seguente:

```

sudo yum install -y wget
export HOME=/tmp/home
mkdir -p $HOME
cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
mkdir -p pip
python3 ./get-pip.py --target $PWD/pip
$PWD/pip/bin/pip3 install boto3
eval $(python3 -c "from botocore.credentials import
InstanceMetadataProvider, InstanceMetadataFetcher; provider =
InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
num_attempts=2)); c = provider.load().get_frozen_credentials();
print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
VERSION=3.1.0
wget https://github.com/acmesh-official/acme.sh/archive/refs/tags/$VERSION.tar.gz -
O acme-$VERSION.tar.gz
tar -xvf acme-$VERSION.tar.gz

```

```
cd acme.sh-$VERSION
```

4. Sostituisci la sezione del passaggio 2 della funzione `*-CertificateRenewalLambda-*` Lambda con il codice del passaggio 3. Seleziona Deploy e attendi che la modifica al codice abbia effetto.
5. Per attivare manualmente la funzione Lambda, vai alla scheda Test e seleziona Test. Non è richiesto alcun input aggiuntivo. Questo dovrebbe creare un'istanza EC2 del certificato che aggiorni il certificato e PrivateKey i segreti in Secret Manager.
6. Termina l'istanza `dcv-gateway` esistente `<env-name>-vdc-gateway` e attendi che l'auto scaling group ne distribuisca automaticamente una nuova.

.....

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

Se una connessione desktop si chiude o non è più possibile connetterti ad essa, il problema potrebbe essere dovuto al guasto dell'istanza Amazon EC2 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 console Amazon EC2 deve essere utilizzata per determinare se l'istanza è stata interrotta o interrotta. Se è 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 Generale.
- Seleziona l'icona di modifica a destra del campo Sessioni consentite predefinite per utente per progetto e modifica il valore con il nuovo valore desiderato.
- Seleziona 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 server DCV relativo alla creazione di certificati sull'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 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.

## VDIs bloccato 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'ID AMI 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. AMIs gli id presi dal AWS Marketplace potrebbero non funzionare per le istanze desktop RES. 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'AMI personalizzata.

Per impostazione predefinita, gli script dei dati utente vengono eseguiti una sola volta all'avvio di un'istanza Amazon EC2. Se crei un'AMI da un'istanza di desktop virtuale esistente, quindi registri uno stack software con l'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 del desktop virtuale originale che hai usato per creare l'AMI ed esegui il seguente comando:

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

Quindi crea una nuova AMI dall'istanza. È possibile utilizzare la nuova AMI per registrare 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 dall'AMI non configurata correttamente.

.....

## VDIs entra nello stato di errore dopo l'avvio

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

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

1. La versione RES implementata è 2024.01 o successiva.
2. Durante la distribuzione dello stack RES l'attributo `EnableLdapIDMapping` è stato impostato su `True`
3. Il filesystem home specificato durante l'implementazione dello stack RES è stato utilizzato nella versione precedente a 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. SSM all'host del gestore del cluster.
2. `cd /home`.
3. `ls`- dovrebbe elencare le directory con nomi di directory che corrispondono ai nomi `utenteadmin1`, `admin2` come.. 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 l'utente dalla tabella DDB dell'utente (eccetto `clusteradmin`).
6. Avvia la sincronizzazione AD: esegui `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` nel gestore di cluster Amazon EC2.
7. Riavvia l'istanza VDI nello stato della pagina Web RES. Error Verifica che il VDI passi allo stato in circa 20 minuti. Ready

.....

## Componente del desktop virtuale

### Argomenti

- [L'istanza Amazon EC2 viene ripetutamente visualizzata come terminata nella console](#)
- [L'istanza vdc-controller è ciclica a causa del mancato accesso al modulo AD/eVDI mostra Failed API Health Check](#)
- [Il progetto non viene visualizzato nel menu a discesa quando si modifica lo stack software per aggiungerlo](#)
- [Il CloudWatch log di Amazon cluster-manager mostra «< user-home-init > account non ancora disponibile in attesa della sincronizzazione dell'utente» \(dove l'account è un nome utente\)](#)
- [Il desktop di Windows al tentativo di accesso dice «Il tuo account è stato disabilitato. Rivolgiti al tuo amministratore»](#)
- [Problemi relativi alle opzioni DHCP con external/customer la configurazione AD](#)
- [Errore Firefox MOZILLA\\_PKIX\\_ERROR\\_REQUIRED\\_TLS\\_FEATURE\\_MISSING](#)

.....

L'istanza Amazon EC2 viene ripetutamente visualizzata come terminata nella console

Se un'istanza dell'infrastruttura viene ripetutamente visualizzata come terminata nella console Amazon EC2, 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 console Amazon EC2, 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 accessi IAM collegate alle istanze dell'infrastruttura Amazon EC2. Se il controller vdc è in esecuzione ciclica e nel gruppo di CloudWatch log viene visualizzato il seguente errore, la causa potrebbe essere che un segreto non è 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'istanza Amazon EC2 e verifica che corrispondano all'elenco precedente.

.....

L'istanza vdc-controller è ciclica a causa del mancato accesso al modulo AD/eVDI mostra Failed API Health Check

Se il modulo eVDI non funziona, durante il controllo dello stato dell'ambiente verrà visualizzato quanto segue nella sezione Environment Status.

## Modules

Environment modules and status



Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	<a href="#">Config</a>	✔ Deployed	⊖ Not Applicable	-
Cluster	cluster	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Directory Service	directoryservice	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Analytics	analytics	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	<a href="#">App</a>	✔ Deployed	✔ Healthy	• default
eVDI	vdc	2023.10b1	<a href="#">App</a>	✔ Deployed	✘ Failed	• default
Bastion Host	bastion-host	2023.10b1	<a href="#">Stack</a>	✔ 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: AttrErr: 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 l'implementazione di RES 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 di RES, assicuratevi 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.

.....

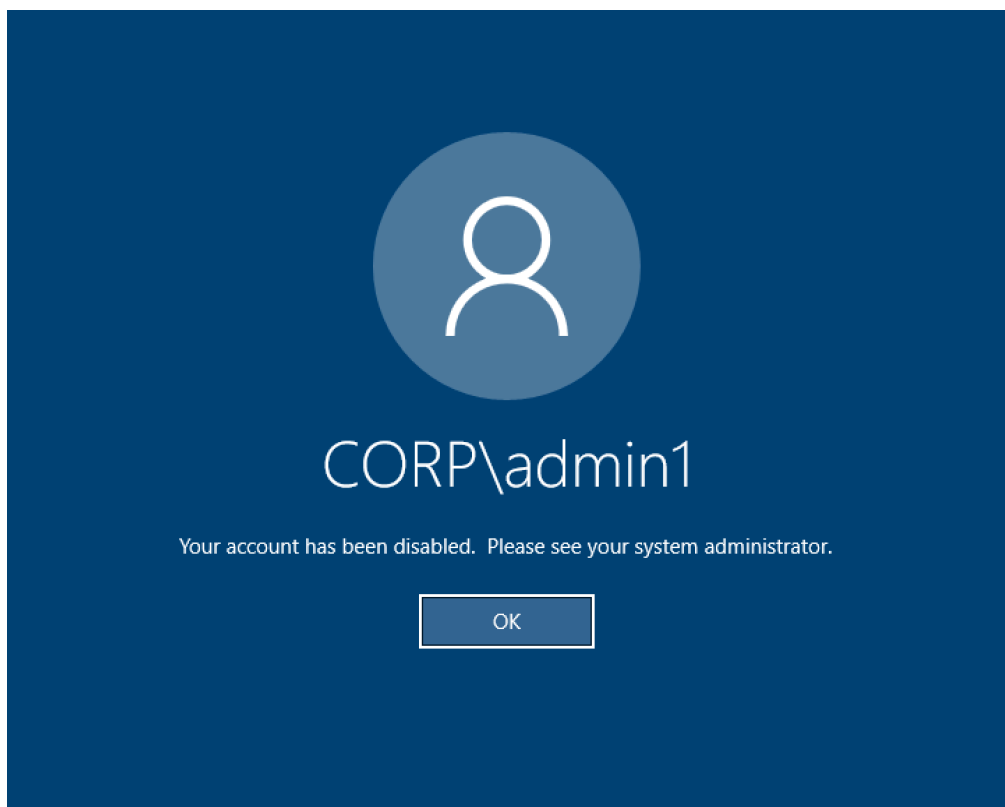
Il CloudWatch log di Amazon cluster-manager mostra «< user-home-init > account non ancora disponibile in attesa della sincronizzazione dell'utente» (dove l'account è un nome utente)

L'abbonato SQS 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 file system home per un utente durante la sincronizzazione dell'utente.

Il motivo per cui non è possibile accedere all'account utente potrebbe essere che RES non è stato configurato correttamente per l'AD in uso. Un esempio potrebbe essere che il ServiceAccountCredentialsSecretArn parametro utilizzato per la creazione BI/RES dell'ambiente 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 nell'AD configurato per RES dopo aver effettuato correttamente l'accesso tramite SSO.

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

.....

## Problemi relativi alle opzioni DHCP con external/customer la configurazione AD

Se riscontri un errore durante l'utilizzo "The connection has been closed. Transport error" di desktop virtuali Windows quando usi 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 le opzioni DHCP per il tuo VPC, devi:


1. Aggiungere AmazonProvided DNS ai due controller di dominio. IPs
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, perché RES/DCV cerca ip-10-0-x-xx.ec2.internal hostname.

#### Domain name

 ec2.internal

#### Domain name servers

 10.0.2.168, 10.0.3.228,  
AmazonProvidedDNS

## 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 web RES è configurato con TLS + Stapling On ma non risponde con Stapling Validation \(vedi https://support.mozilla.org/en-US/questions/1372483\).](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](https://really-simple-ssl.com)

## Eliminazione di Env

### Argomenti

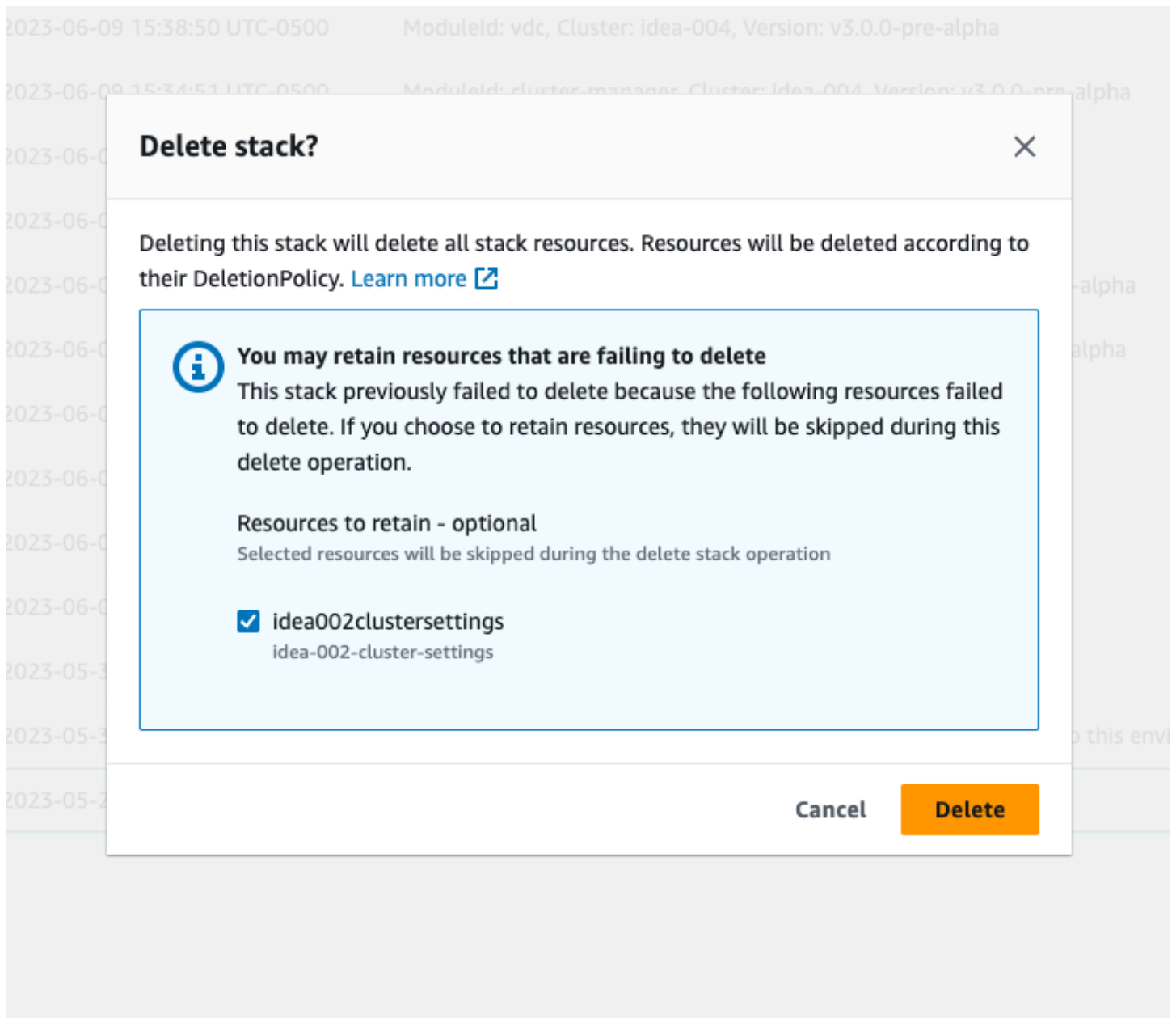
- [res-xxx-cluster impila nello stato «DELETE\\_FAILED» e non può essere eliminato manualmente a causa dell'errore «Il ruolo non è valido o non può essere assunto»](#)
- [Raccolta dei registri](#)
- [Scaricamento dei registri VDI](#)
- [Scaricamento dei log dalle istanze Linux EC2](#)
- [Scaricamento dei log dalle istanze di Windows EC2](#)
- [Raccolta dei log ECS relativi all'errore WaitCondition](#)

.....

res-xxx-cluster impila nello stato «DELETE\_FAILED» e non può essere eliminato manualmente a causa dell'errore «Il ruolo non è valido o non può essere assunto»

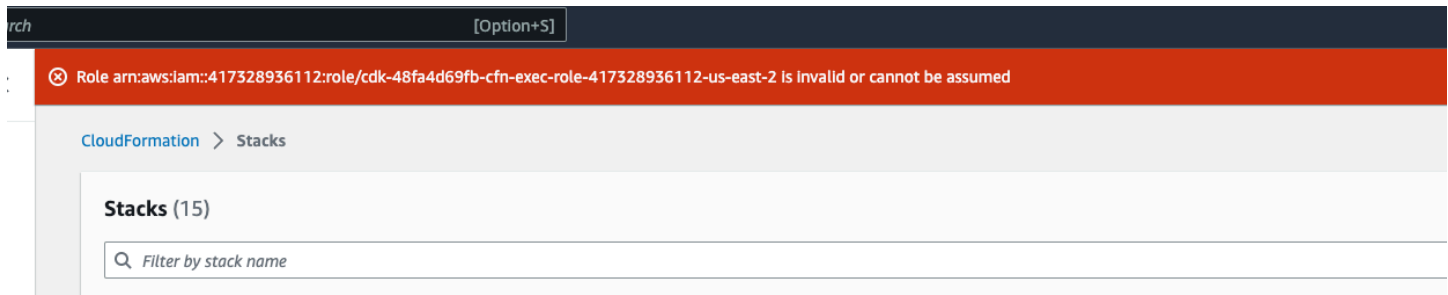
Se noti che lo stack "res-xxx-cluster" è nello stato «DELETE\_FAILED» e non può essere eliminato manualmente, puoi eseguire le seguenti operazioni per eliminarlo.

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.



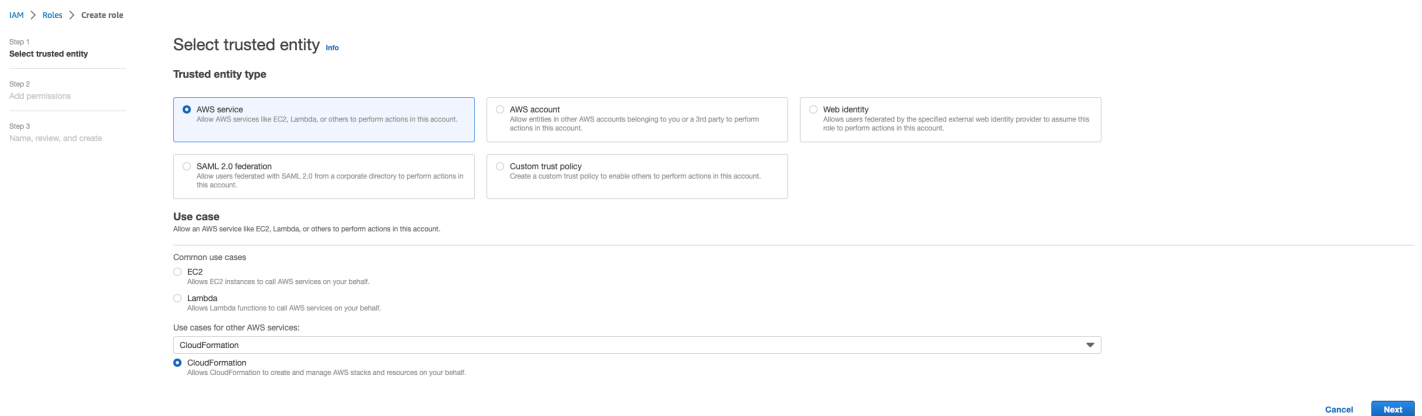
A volte, anche se elimini tutte le risorse dello stack richieste, potresti comunque visualizzare il messaggio che richiede di selezionare le risorse da conservare. In tal caso, seleziona tutte le risorse come «risorse da conservare» e scegli Elimina.

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 console IAM e crea un ruolo con quel nome utilizzando i parametri mostrati qui, che sono:

- Per il tipo di entità affidabile 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:

## Name, review, and create

## Role details

## Role name

Enter a meaningful name to identify this role.

cdk-48fa4d69b-cfn-exec-role-417328936112-us-east-2

Maximum 64 characters. Use alphanumeric and '+,=,@,\_' characters.

## Description

Add a short explanation for this role.

Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,=,@,\_' characters.

## Step 1: Select trusted entities

Edit

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "",
6-       "Effect": "Allow",
7-       "Principal": {
8-         "Service": "cloudformation.amazonaws.com"
9-       },
10-      "Action": "sts:AssumeRole"
11-     }
12-   ]
13- ]

```

## Step 2: Add permissions

Edit

## Permissions policy summary

Policy name	Type	Attached as
AWSCloudFormationFullAccess	AWS managed	Permissions policy
AdministratorAccess	AWS managed - job function	Permissions policy

## Tags

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

## Raccolta dei registri

### Accesso a un'istanza EC2 dalla console EC2

- Segui [queste istruzioni](#) per accedere alla tua istanza Linux EC2.
- Segui [queste istruzioni](#) per accedere alla tua istanza Windows EC2. 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 /root/bootstrap/logs nella directory sull'istanza <env-name>-cluster-manager EC2. Segui le istruzioni riportate in «Accesso a un'istanza EC2 dalla console EC2» 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 /root/bootstrap/logs nella directory sull'istanza <env-name>-vdc-controller EC2. Segui le istruzioni riportate in «Accesso a un'istanza EC2 dalla console EC2» all'inizio di questa sezione per accedere alla tua istanza.

Uno dei modi per ottenere facilmente i log è seguire le istruzioni contenute nella sezione.

[Scaricamento dei log dalle istanze Linux EC2](#) Il nome del modulo sarebbe il nome dell'istanza.

## Raccolta dei registri VDI

### Identifica l'istanza Amazon EC2 corrispondente

Se un utente avviasse una VDI con nome di sessioneVDI1, il nome corrispondente dell'istanza sulla console Amazon EC2 sarebbe. <env-name>-VDI1-<user name>

### Raccogli i log VDI di Linux

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

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 dei registri VDI](#) per scaricare i log.

### Raccogli i registri VDI di Windows

Accedi all'istanza Amazon EC2 corrispondente dalla console Amazon EC2 seguendo le istruzioni collegate a «Accesso a un'istanza EC2 dalla console EC2» all'inizio di questa sezione. Ottieni tutti i log nella \$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\ 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 dei registri VDI](#)

## Scaricamento dei registri VDI

1. Aggiorna il ruolo IAM dell'istanza VDI EC2 per consentire l'accesso a S3.
2. Vai alla console EC2 e seleziona la tua istanza VDI.
3. Seleziona il ruolo IAM 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 tipo di VDI in uso per scaricare i log. Il nome del modulo sarebbe il nome dell'istanza.
  - a. [Scaricamento dei log dalle istanze Linux EC2](#) per Linux.
  - b. [Scaricamento dei log dalle istanze di Windows EC2](#) per Windows.
7. Infine, modifica il ruolo per rimuovere la AmazonS3FullAccess politica.

### Note

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

## Scaricamento dei log dalle istanze Linux EC2

Accedi all'istanza EC2 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 log dalle istanze di Windows EC2

Accedi all'istanza EC2 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 log ECS 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. Recupera 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](#)
- [Il keycloak dello stack demo non funziona](#)

.....

## 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 - -... RESEExternal - DirectoryService-... con descrizione: Password per Microsoft Active Directory
  - per RES: res- ServiceAccountPassword -... con descrizione: password dell'account del servizio Active Directory Service

3. Vai alla [console EC2](#) e termina l'istanza del gestore del cluster. Le regole di Auto Scaling attiveranno automaticamente la distribuzione di una nuova istanza.

## Il keycloak dello stack demo non funziona

### Problema

Se il server keycloak si è bloccato e, al riavvio del server, l'IP dell'istanza è cambiato, ciò potrebbe aver provocato l'interruzione del keycloak: la pagina di accesso del portale RES non viene caricata o si blocca in uno stato di caricamento che non si risolve mai.

### Attenuazione

Dovrai eliminare l'infrastruttura esistente e ridistribuire lo stack Keycloak per ripristinare Keycloak a uno stato integro. Completare la procedura riportata di seguito.

1. Vai a Cloudformation. Lì dovreste vedere due pile relative al keycloak:
  - *<env-name>-RESSsoKeycloak-<random characters>*(Pila 1)
  - *<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-\**(Pila 2)
2. Elimina Stack1. Se viene richiesto di eliminare lo stack nidificato, selezionate Sì per eliminare lo stack nidificato.

Assicurati che lo stack sia stato eliminato completamente.

3. [Scarica il modello dello stack RES SSO Keycloak qui.](#)
4. Distribuisci questo stack manualmente con gli stessi valori di parametro dello stack eliminato. Distribuiscilo dalla CloudFormation console andando su Crea stack → Con nuove risorse (standard) → Scegli un modello esistente → Carica un file modello. Compila i parametri richiesti utilizzando gli stessi input dello stack eliminato. Puoi trovare questi input nello stack eliminato cambiando il filtro sulla CloudFormation console e andando alla scheda Parametri. Assicurati che il nome dell'ambiente, la key pair e gli altri parametri corrispondano ai parametri dello stack originale.
5. Una volta distribuito lo stack, l'ambiente è pronto per essere riutilizzato. Puoi trovarlo ApplicationUrl nella scheda Output dello stack distribuito.

## Problemi noti

- [Problemi noti 2024.x](#)
  - [\(2024.12 e 2024.12.01\) Errore Regex durante la registrazione di un nuovo utente Cognito](#)
  - [\(2024.12.01 e versioni precedenti\) Errore di certificato errato non valido durante la connessione a VDI utilizzando un dominio personalizzato](#)
  - [\(2024.12 e 2024.12.01\) Gli utenti di Active Directory non possono accedere tramite SSH a Bastion Host](#)
  - [\(2024.10\) Arresto automatico VDI interrotto per ambienti RES implementati in ambienti isolati VPCs](#)
  - [\(2024.10 e versioni precedenti\) Errore nell'avvio di VDI for Graphic Enhanced di istanze](#)
  - [\(2024.08\) Preparazione dell'errore AMI dell'infrastruttura](#)
  - [\(2024.08\) I desktop virtuali non riescono a montare il bucket read/write Amazon S3 con ARN del bucket root e prefisso personalizzato](#)
  - [\(2024.06\) L'applicazione dello snapshot fallisce quando il nome del gruppo AD contiene spazi](#)
  - [\(2024.06 e versioni precedenti\) I membri del gruppo non erano sincronizzati con RES durante la sincronizzazione AD](#)
  - [\(2024.06 e versioni precedenti\) CVE-2024-6387, Regre, vulnerabilità di sicurezza in e Ubuntu SSHion RHEL9 VDIs](#)
  - [\(2024.04-2024.04.02\) Limite di autorizzazione IAM fornito non associato al ruolo delle istanze VDI](#)
  - [\(2024.04.02 e versioni precedenti\) Le istanze Windows NVIDIA in ap-southeast-2 \(Sydney\) non vengono avviate](#)
  - [\(2024.04 e 2024.04.01\) Errore di eliminazione RES in GovCloud](#)
  - [\(2024.04 - 2024.04.02\) Il desktop virtuale Linux potrebbe rimanere bloccato nello stato «RIPRESA» al riavvio](#)
  - [\(2024.04.02 e versioni precedenti\) Non riesce a sincronizzare gli utenti AD il cui attributo SAMAccount Name include lettere maiuscole o caratteri speciali](#)
  - [\(2024.04.02 e versioni precedenti\) La chiave privata per l'accesso all'host bastion non è valida](#)

## Problemi noti 2024.x

### (2024.12 e 2024.12.01) Errore Regex durante la registrazione di un nuovo utente Cognito

#### Descrizione del bug

Se tenti di registrare utenti di AWS Cognito tramite il portale web che dispongono di prefissi e-mail che contengono «.», ad esempio <firstname>.<lastname>@<company>.com, ciò comporterà un errore che indica che il nome utente di Cognito non corrisponde al modello regex definito.

❌ Invalid parameters: Username doesn't match the regex pattern `^[a-z][-a-z0-9_]{0,31}$`. Username may only contain lower case ASCII letters (a-z), numbers (0-9), and the following special characters: underscore (`_`), and hyphen (`-`). The maximum length of username is 32.

Questo errore è causato dal fatto che RES genera automaticamente i nomi utente dal prefisso e-mail dell'utente. Tuttavia, i nomi utente con «.» non sono utenti validi per alcune distribuzioni Linux VDI supportate da RES. Questa correzione rimuove qualsiasi «.» nel prefisso e-mail durante la generazione di un nome utente in modo che il nome utente sia valido su RES Linux VDI.

#### Versioni interessate

Versioni RES 2024.12 e 2024.12.01

#### Mitigazione

1. Eseguite i seguenti comandi per scaricare `patch.py` e `cognito_sign_up_email_fix.patch` per la versione 2024.12 o `cognito_sign_up_email_fix.patch` per la versione 2024.12.01, sostituendoli <output-directory> con la directory in cui volete scaricare lo script e il file di patch e <environment-name> con il nome dell'ambiente RES:
  - a. La patch si applica a RES 2024.12 e 2024.12.01.
  - b. [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)

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

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>
RES_VERSION=<res-version> # either 2024.12 or 2024.12.01

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/cognito_sign_up_email_fix.patch --output
${OUTPUT_DIRECTORY}/cognito_sign_up_email_fix.patch
```

2. Vai alla directory in cui sono stati 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 ${RES_VERSION} --module cluster-manager --patch ${OUTPUT_DIRECTORY}/
cognito_sign_up_email_fix.patch
```

3. Riavvia l'istanza di Cluster Manager per il tuo ambiente. Puoi anche terminare l'istanza dalla console di gestione Amazon EC2.

```
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}
```

4. Verifica lo stato dell'istanza di Cluster Manager controllando l'attività del gruppo di auto scaling che inizia con il nome <RES-EnvironmentName>-cluster-manager-asg. Attendi che la nuova istanza venga lanciata correttamente.

.....

## (2024.12.01 e versioni precedenti) Errore di certificato errato non valido durante la connessione a VDI utilizzando un dominio personalizzato

### Descrizione del bug

Quando si distribuiscono la [ricetta External Resources](#) e RES con un nome di dominio del portale personalizzato, CertificateRenewalNode non riesce ad aggiornare il certificato TLS per la connessione VDI con il seguente errore in: `/var/log/user-data.log`

```
{
  "type": "urn:ietf:params:acme:error:unauthorized",
  "detail": "Error finalizing order :: OCSP must-staple extension is no longer
available: see https://letsencrypt.org/2024/12/05/ending-ocsp",
  "status": 403
}
```

Di conseguenza, si verificherà un errore che indica `net::ERR_CERT_DATE_INVALID` (Chrome) o `Error code: SSL_ERROR_BAD_CERT_DOMAIN` (FireFox) quando ci si connette al portale web VDI RES.

### Versioni interessate

2024.12.01 e versioni precedenti

### Mitigazione

1. Vai alla console EC2. Se è presente un'istanza denominata `CertificateRenewalNode-`, interrompi l'istanza.
2. Vai alla console Lambda. Apri il codice sorgente della funzione Lambda denominata `- CertificateRenewalLambda-`. Identifica la riga che inizia con `./acme.sh --issue --dns dns_aws --ocsp-must-staple --keylength 4096` e rimuovi `--ocsp-must-staple` argomento.
3. Seleziona Deploy e attendi che la modifica al codice abbia effetto.
4. Per attivare manualmente la funzione Lambda: vai alla scheda Test e seleziona Test. Non è richiesto alcun input aggiuntivo. Questo dovrebbe creare un'istanza EC2 del certificato che aggiorni il certificato e PrivateKey i segreti in Secret Manager. L'istanza verrà terminata automaticamente una volta aggiornati i segreti.
5. Termina l'istanza `dcv-gateway` esistente `<env-name>-vdc-gateway` e attendi che l'auto scaling group ne distribuisca automaticamente una nuova.

## Dettagli dell'errore

Let's Encrypt terminerà il supporto OCSP nel 2025. A partire dal 30 gennaio 2025, le richieste OCSP Must-Staple avranno esito negativo a meno che l'account richiedente non abbia precedentemente emesso un certificato contenente l'estensione OCSP Must Staple. [Consulta https://letsencrypt.org/2024/12/05/ending-ocsp/](https://letsencrypt.org/2024/12/05/ending-ocsp/) per maggiori dettagli.

.....

## (2024.12 e 2024.12.01) Gli utenti di Active Directory non possono accedere tramite SSH a Bastion Host

### Descrizione del bug

Gli utenti di Active Directory ricevono un errore di autorizzazione negata quando si connettono a Bastion Host seguendo le istruzioni del portale web RES.

L'applicazione Python in esecuzione su Bastion Host non riesce ad avviare il servizio SSSD a causa di una variabile di ambiente mancante. Di conseguenza, gli utenti AD sono sconosciuti al sistema operativo e non possono accedere.

### Versioni interessate

2024.12 e 2024.12.01

### Mitigazione

1. Connect all'istanza Bastion Host dalla console EC2.
2. Modifica `/etc/environment` e aggiungi `environment_name=<res-environment-name>` come nuova riga in `IDEA_CLUSTER_NAME`.
3. Eseguite i seguenti comandi sull'istanza:

```
source /etc/environment
sudo service supervisord restart
sudo systemctl restart supervisord
```

4. Prova a connetterti nuovamente a Bastion Host seguendo le istruzioni del portale web RES.
- .....

## (2024.10) Arresto automatico VDI interrotto per ambienti RES implementati in ambienti isolati VPCs

### Descrizione del bug

Con la versione 2024.10 RES, è stato aggiunto l'arresto automatico VDI VDI per coloro che sono inattivi per un certo periodo di tempo. Questa impostazione può essere configurata in Impostazioni del desktop → Server → Sessione.

L'arresto automatico VDI non è attualmente supportato per gli ambienti RES distribuiti in ambienti isolati. VPCs

### Versioni interessate

2024.10

### Mitigazione

Attualmente stiamo lavorando a una correzione che verrà inclusa in una versione futura. Tuttavia, è ancora possibile eseguire l'interruzione VDI manuale negli ambienti RES distribuiti in ambienti isolati VPCs.

.....

## (2024.10 e versioni precedenti) Errore nell'avvio di VDI for Graphic Enhanced di istanze

### Descrizione del bug

Quando una VDI Amazon Linux 2 - x86\_64, RHEL 8 - x86\_64 o RHEL 9 x86\_64 viene avviata su un tipo di istanza grafica avanzata (g4, g5), l'istanza rimarrà bloccata nello stato di provisioning. Ciò significa che l'istanza non raggiungerà mai lo stato «Pronto» e non sarà mai disponibile per la connessione.

Ciò accade perché l'X Server non crea correttamente le istanze sulle istanze. Dopo aver applicato questa patch, suggeriamo inoltre di aumentare la dimensione del volume root degli stack software per le istanze grafiche a 50 GB per garantire che ci sia spazio sufficiente per l'installazione di tutte le dipendenze.

### Versioni interessate

Tutte le versioni RES 2024.10 o precedenti.

## Mitigazione

1. Scarica [patch.py](#) e [graphic\\_enhanced\\_instance\\_types\\_fix.patch](#) sostituendoli `<output-directory>` con la directory in cui desideri scaricare lo script e il file di patch e con il nome del tuo ambiente RES nel comando seguente: `<environment-name>`
  - a. La patch si applica solo a RES 2024.10.
  - b. Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.
  - c. Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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/2024.10/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patches/graphic_enhanced_instance_types_fix.patch --
output ${OUTPUT_DIRECTORY}/graphic_enhanced_instance_types_fix.patch
```

2. Vai alla directory in cui sono stati 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 2024.10 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
graphic_enhanced_instance_types_fix.patch
```

3. Per terminare l'istanza di Virtual Desktop Controller (vdc-controller) per il tuo ambiente, esegui i seguenti comandi, sostituendo il nome dell'ambiente RES dove indicato.

```
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}
```

4. Avvia una nuova istanza dopo che il gruppo target che inizia con il nome è diventato integro. <RES-EnvironmentName>-vdc-ext Consigliamo che tutti i nuovi stack software registrati per le istanze grafiche abbiano almeno 50 GB di spazio di archiviazione.

## (2024.08) Preparazione dell'errore AMI dell'infrastruttura

### Descrizione del bug

Quando prepari le AMI utilizzando EC2 Image Builder secondo le istruzioni elencate nella Documentazione sui [prerequisiti](#), il processo di creazione fallisce e viene visualizzato il seguente messaggio di errore:

```
CmdExecution: [ERROR] Command execution has resulted in an error
```

Ciò è dovuto a errori nel file delle dipendenze fornito nella documentazione.

### Versioni interessate

2024.08

### Mitigazione

Crea nuove risorse EC2 Image Builder:

(Segui questi passaggi se non ti sei mai preparato AMIs per le istanze RES)

1. Scaricate il [res-infra-dependenciesfile.tar.gz aggiornato](#).
2. Segui i passaggi elencati in Prepare Amazon Machine Images (AMIs) nella pagina [Prerequisiti](#).

Riutilizzo delle precedenti risorse di EC2 Image Builder:

(Segui questi passaggi se ti sei preparato AMIs per le istanze RES)

1. Scaricate il [res-infra-dependenciesfile.tar.gz aggiornato](#).
2. Vai a EC2 Image Builder → Componenti → Fai clic sul componente creato per preparare RES. AMIs

3. Nota la posizione S3 elencata nella sezione Contenuto → Scarica RESInstall gli script, passo → input → source.
4. La posizione S3 trovata sopra contiene il file delle dipendenze utilizzato in precedenza, sostituisci questo file con il file scaricato nel primo passaggio.

.....

## (2024.08) I desktop virtuali non riescono a montare il bucket read/write Amazon S3 con ARN del bucket root e prefisso personalizzato

### Descrizione del bug

Research and Engineering Studio 2024.08 non riesce a montare i bucket read/write S3 su un'istanza VDI (Virtual Desktop Infrastructure) quando si utilizza un root bucket ARN (ovvero `arn: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 utente `arn:aws:s3:::example-bucket/example-folder-prefix`)
- bucket di lettura/scrittura con un ARN del bucket root, ma senza prefisso personalizzato

Dopo aver effettuato il provisioning di un'istanza VDI, il bucket non verrà montato nella directory di montaggio specificata per quel bucket S3. Sebbene sia presente la directory di montaggio sul VDI, la directory sarà vuota e non conterrà il contenuto corrente del bucket. Quando si scrive un file nella directory utilizzando il terminale, viene generato l'errore `Permission denied, unable to write a file` e il contenuto del file non viene 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 comando seguente,

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 ambiente RES:

- a. La patch si applica solo a RES 2024.08.
- b. [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)
- c. Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 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'ambiente RES 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 configurazioni VPC private, se non l'hai già fatto, per la `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` funzione assicurati di aggiungere il nome `AWS_STS_REGIONAL_ENDPOINTS` e il `Environment variable` valore di `regional`. Per ulteriori informazioni, consulta [Prerequisiti del bucket Amazon S3 per distribuzioni VPC isolate](#).

4. Dopo che il gruppo target che inizia con il nome sarà `<RES-EnvironmentName>-vdc-ext` diventato valido, VDI sarà necessario lanciarne uno nuovo con i bucket read/write S3 con ARN del root bucket e prefisso personalizzato montati correttamente.

.....

(2024.06) L'applicazione dello snapshot fallisce quando il nome del gruppo AD contiene spazi

**Problema**

RES 2024.06 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_.-]{1,20}:(user|group)$
```

L'errore deriva dal fatto che RES accetta solo nomi di gruppo che soddisfano i seguenti requisiti:

- Può contenere solo lettere ASCII 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 a RES 2024.06
  - b. [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)
  - c. Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 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 console di gestione Amazon EC2.

```
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 lettere ASCII minuscole e maiuscole, cifre, trattini (-), punto (.), trattini bassi (\_) e spazi con una lunghezza totale compresa tra 1 e 30, inclusi.

.....  
(2024.06 e versioni precedenti) I membri del gruppo non erano sincronizzati con RES durante la sincronizzazione AD

**Descrizione del bug**

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

RES crea 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**

Tutte le versioni RES 2024.06 o precedenti

**Mitigazione**

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 seguenti comandi, sostituendoli <output-directory> con la directory locale in cui desideri scaricare i file e con la versione di RES a cui desideri applicare le patch: <res\_version>

**Note**

- [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)
- Configura la AWS CLI per l'account e la regione in cui viene distribuito RES e assicurati di disporre delle autorizzazioni S3 per scrivere nel bucket creato da RES.

- La patch supporta solo le versioni RES 2024.04.02 e 2024.06. Se utilizzi 2024.04 o 2024.04.01, puoi seguire i passaggi elencati per aggiornare l'ambiente alla versione 2024.04.02 prima di [Aggiornamenti di versione minori](#) applicare la patch.

- Versione RES: RES 2024.04.02

[Link per il download della patch: 2024.04.02\\_group\\_member\\_sync\\_bug\\_fix.patch](#)

- Versione RES: RES 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. Vai 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 ambiente RES:

```
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, Regre, vulnerabilità di sicurezza in e Ubuntu SSHion RHEL9 VDIs

### Descrizione del bug

[CVE-2024-6387](#), soprannominato regreSSHion, è stato identificato nel server OpenSSH. 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 OpenSSH per comunicazioni sicure.

Per RES, la configurazione standard prevede il passaggio dall'host bastion a SSH nei desktop virtuali e l'host bastion non è interessato da questa vulnerabilità. Tuttavia, l'AMI (Amazon Machine Image) predefinita che forniamo RHEL9 e Ubuntu2024 VDIs (Virtual Desktop Infrastructure) in TUTTE le versioni RES utilizzano una versione OpenSSH 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 del bastione.

[Maggiori dettagli sul problema sono disponibili qui.](#)

### Versioni interessate

Tutte le versioni RES 2024.06 o precedenti.

### Mitigazione

Entrambi RHEL9 e Ubuntu hanno rilasciato patch per OpenSSH 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 Ubuntu VDIs, ti consigliamo di seguire le VDIs istruzioni PATCH EXISTING riportate di seguito. Per applicare patch future VDIs, consigliamo di seguire le VDIs istruzioni di PATCH FUTURE. Queste istruzioni descrivono come eseguire uno script per applicare l'aggiornamento della piattaforma sul tuo VDIs.

## PATCH ESISTENTE VDI

1. Esegui il seguente comando che patcherà tutti gli Ubuntu esistenti e RHEL9 VDI:
  - a. Lo script di patch richiede [AWS CLI v2](#).
  - b. Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 messaggio di SUCCESSO.

## PATCH FUTURE VDI

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 a RES 2024.06.
- [Lo script di patch richiede AWS CLI \(v2\), Python 3.9.16 o superiore e Boto3.](#)
- Configura la tua copia della AWS CLI per l'account e la regione in cui viene distribuito RES 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 del controller VDC 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 VDI sono supportate solo nelle versioni RES 2024.06 e successive. Per applicare patch future VDI negli ambienti RES con versioni precedenti alla 2024.06, è necessario prima aggiornare l'ambiente RES alla versione 2024.06 utilizzando le istruzioni disponibili all'indirizzo: [Principali aggiornamenti delle versioni](#)

.....

(2024.04-2024.04.02) Limite di autorizzazione IAM fornito non associato al ruolo delle istanze 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 parametro IAMPermission Boundary non viene assegnato correttamente a un progetto durante la creazione di tale progetto.

Versioni interessate

2024.04 - 2024.04.02

Mitigazione

Segui questi passaggi per consentire di VDI 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 patch si applica solo a RES 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 il tuo ambiente alla versione 2024.04.02](#).
  - b. [Lo script di patch richiede AWS CLI \(v2\), Python 3.9.16 o superiore e Boto3](#).
  - c. Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 ambiente RES:

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

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

```
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) Le istanze Windows NVIDIA in ap-southeast-2 (Sydney) non vengono avviate

Il problema

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

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

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

```
An error occurred (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:

- Implementa RES nella regione ap-southeast-2.

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

## Versioni interessate

Tutte le versioni RES 2024.04.02 o precedenti sono interessate

## Mitigazione

La seguente mitigazione è stata testata sulla versione RES 2024.01.01:

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

.....

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

### Il problema

Durante il flusso di lavoro di eliminazione RES, `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 versione AWS CLI predefinita tra Commercial e GovCloud Regions, la `update_user_pool` chiamata in Lambda avrà esito negativo nelle regioni. GovCloud

I clienti riceveranno il seguente errore quando tentano di eliminare RES nelle GovCloud regioni:

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

Versione RES 2024.04 e 2024.04.01

Mitigazione

La seguente mitigazione è stata testata sulla versione RES 2024.04:

- Apri la UnprotectCognitoUserPool Lambda
  - Convenzione di denominazione: `<env-name>-  
InstallerTasksUnprotectCognitoUserPool-...`
- Impostazioni di runtime -> Modifica -> Seleziona Runtime Python 3.11 -> Salva.
- Apri CloudFormation.
- Eliminare lo stack RES -> lasciare la voce Retain Installer Resource DESELEZIONATA -> Elimina.

.....

(2024.04 - 2024.04.02) Il desktop virtuale Linux potrebbe rimanere bloccato nello stato «RIPRESA» al riavvio

Il problema

I desktop virtuali Linux possono rimanere bloccati nello stato «RIPRESA» 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 sessione DCV 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 «RIPRESA»:

1. Accesso SSH all'istanza problematica dalla console EC2.
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 si applica solo a RES 2024.04.02.
- [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)
- Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 del vostro ambiente RES e <aws-region> con la regione in cui è distribuito RES:

```
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 Controller per il tuo ambiente, esegui i seguenti comandi, sostituendoli <environment-name> con il nome dell'ambiente RES:

```
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 attributo SAMAccount Name include lettere maiuscole o caratteri speciali

Il problema

RES non riesce a sincronizzare gli utenti AD dopo che l'SSO è stato configurato 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 dal fatto che RES accetta solo un SAMAccount nome utente che soddisfa i seguenti requisiti:

- Può contenere solo lettere ASCII 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 a RES 2024.04.02.
- [Lo script di patch richiede AWS CLI v2, Python 3.9.16 o superiore e Boto3.](#)
- Configura la AWS CLI per l'account e la regione in cui viene distribuito RES 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 ambiente RES:

```
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'ambiente RES. Puoi anche terminare l'istanza dalla console di gestione Amazon EC2.

```
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 l'accesso all'host bastion non è valida

Il problema

Quando un utente scarica la chiave privata per accedere all'host bastion dal portale web RES, 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-----

.....

## 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 l'accesso remoto alle EC2 istanze Amazon senza RDP e senza bisogno di licenze RDP. 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](#) delle domande frequenti.

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 AWS attuali offerte e pratiche di prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. AWS le responsabilità nei confronti dei propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

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

# Revisioni

[Per ulteriori informazioni, consultate il file ChangeLog.md nel repository.](#) GitHub

Data	Modifica
Marzo 2025	<ul style="list-style-type: none"><li>• Versione di rilascio 2025.03</li></ul> <p>Sezioni aggiunte:</p> <ul style="list-style-type: none"><li>• <a href="#">Disabilita un progetto.</a></li><li>• <a href="#">Elimina un progetto.</a></li><li>• <a href="#">Dashboard di analisi dei costi.</a></li></ul> <p>Sezioni modificate —</p> <ul style="list-style-type: none"><li>• <a href="#">Desktop virtuali.</a></li><li>• <a href="#">Stack software () AMLs.</a></li><li>• <a href="#">Configura RES-Ready AMLs.</a></li><li>• <a href="#">Impostazioni del desktop.</a></li><li>• <a href="#">Configurazione dell'accesso SSH.</a></li><li>• <a href="#">Sincronizzazione con Active Directory.</a></li></ul>
dicembre 2024	<ul style="list-style-type: none"><li>• Versione di rilascio 2024.12</li></ul> <p>Sezioni aggiunte:</p> <ul style="list-style-type: none"><li>• <a href="#">Sincronizzazione con Active Directory.</a></li><li>• <a href="#">Configurazione delle autorizzazioni del desktop.</a></li><li>• <a href="#">Configurazione dell'accesso al file browser.</a></li><li>• <a href="#">Configurazione dell'accesso SSH.</a></li><li>• <a href="#">Configurazione degli utenti di Amazon Cognito.</a></li></ul> <p>Sezioni modificate —</p> <ul style="list-style-type: none"><li>• <a href="#">Limiti dell'ambiente.</a></li></ul>

Data	Modifica
	<ul style="list-style-type: none"> <li>• <a href="#">Configurazione di un VPC privato (opzionale)</a>.</li> </ul>
ottobre 2024	<ul style="list-style-type: none"> <li>• Versione di rilascio 2024.10: aggiunto supporto per — <ul style="list-style-type: none"> <li>• <a href="#">Limiti dell'ambiente</a>.</li> <li>• <a href="#">profili di condivisione del desktop</a>.</li> <li>• <a href="#">Interfaccia desktop virtuale (autostop)</a>.</li> </ul> </li> </ul>
agosto 2024	<ul style="list-style-type: none"> <li>• Versione di rilascio 2024.08: aggiunto supporto per — <ul style="list-style-type: none"> <li>• montaggio di bucket Amazon S3 su istanze Linux Virtual Desktop Infrastructure (VDI). Per informazioni, consulta <a href="#">Bucket Amazon S3</a>.</li> <li>• autorizzazioni di progetto personalizzate, un modello di autorizzazione avanzato che consente la personalizzazione dei ruoli esistenti e l'aggiunta di ruoli personalizzati. Per informazioni, consulta <a href="#">Policy di autorizzazione</a>.</li> </ul> </li> <li>• Guida per l'utente: ha ampliato la sezione. <a href="#">Risoluzione dei problemi</a></li> </ul>
Giugno 2024	<ul style="list-style-type: none"> <li>• Versione di rilascio 2024.06: supporto per Ubuntu, autorizzazioni del proprietario del progetto.</li> <li>• Guida per l'utente: aggiunta <a href="#">Crea un ambiente demo</a></li> </ul>
aprile 2024	Versione di rilascio 2024.04: modelli pronti per RES-Ready AMIs e per il lancio del progetto

Data	Modifica
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.