



ユーザーガイド

# Research and Engineering Studio



# Research and Engineering Studio: ユーザーガイド

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

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

# Table of Contents

概要:	1
機能とメリット	1
概念と定義	3
アーキテクチャの概要	5
アーキテクチャ図	5
AWS この製品の サービス	7
デモ環境	11
ワンクリックデモスタックを作成する	11
前提条件	11
リソースと入力パラメータを作成する	12
デプロイ後のステップ	13
デプロイを計画する	15
Cost	15
セキュリティ	15
IAM ロール	16
セキュリティグループ	16
データ暗号化	16
製品セキュリティに関する考慮事項	17
クォータ	20
この製品の AWS サービスのクォータ	20
AWS CloudFormation クォータ	20
レジリエンスの計画	20
サポートされている AWS リージョン	21
製品をデプロイする	24
前提条件	24
管理ユーザー AWS アカウント を使用して を作成する	25
Amazon EC2 SSH キーペアを作成する	25
サービスクォータを増やす	25
Cognito ユーザープールを作成する (オプション)	26
カスタムドメインを作成する (オプション)	26
ドメインの作成 (GovCloud のみ)	27
外部リソースを提供する	28
環境で LDAPS を設定する (オプション)	29
Microsoft Active Directory のサービスアカウント	29

プライベート VPC を設定する (オプション) .....	30
外部リソースを作成する .....	43
ステップ 1: 製品を起動する .....	50
ステップ 2: 初めてサインインする .....	58
製品を更新する .....	60
メジャーバージョンの更新 .....	60
マイナーバージョンの更新 .....	61
製品のアンインストール .....	62
の使用 AWS マネジメントコンソール .....	62
の使用 AWS Command Line Interface .....	62
shared-storage-security-group の削除 .....	62
Amazon S3 バケットの削除 .....	63
設定ガイド .....	64
ID 管理 .....	64
Amazon Cognito ID のセットアップ .....	65
Active Directory の同期 .....	72
IAM Identity Center での SSO の設定 .....	81
SSO 用の ID プロバイダーの設定 .....	85
ユーザーのパスワードの設定 .....	95
サブドメインの作成 .....	95
ACM 証明書を作成する .....	96
Amazon CloudWatch Logs .....	97
カスタムアクセス許可の境界の設定 .....	98
RES 対応 AMIs を設定する .....	103
RES 環境にアクセスするための IAM ロールを準備する .....	103
EC2 Image Builder コンポーネントを作成する .....	104
EC2 Image Builder レシピを準備する .....	107
EC2 Image Builder インフラストラクチャを設定する .....	110
Image Builder イメージパイプラインを設定する .....	110
Image Builder イメージパイプラインを実行する .....	112
RES に新しいソフトウェアスタックを登録する .....	112
RES のインストール後にカスタムドメインを設定する .....	112
管理者ガイド .....	115
シークレットの管理 .....	115
コストのモニタリングと制御 .....	118
コストダッシュボード .....	122

前提条件 .....	123
予算割り当てグラフを持つプロジェクト .....	123
経時的なコスト分析グラフ .....	125
CSV をダウンロードする .....	129
セッション管理 .....	129
ダッシュボード .....	131
セッション .....	132
ソフトウェアスタック (AMIs) .....	135
デバッグ .....	147
デスクトップ設定 .....	148
環境管理 .....	150
環境ステータス .....	151
環境設定 .....	152
[ユーザー] .....	152
グループ .....	153
プロジェクト .....	154
アクセス許可ポリシー .....	166
ファイルシステム .....	184
スナップショットの管理 .....	187
Amazon S3 バケット .....	193
製品を使用する .....	210
SSH アクセス .....	210
仮想デスクトップ .....	210
新しいデスクトップを起動する .....	211
デスクトップにアクセスする .....	212
デスクトップの状態を制御する .....	214
仮想デスクトップを変更する .....	216
セッション情報を取得する .....	217
仮想デスクトップをスケジュールする .....	217
VDI 自動停止 .....	221
共有デスクトップ .....	224
デスクトップを共有する .....	224
共有デスクトップにアクセスする .....	226
ファイルブラウザ .....	226
ファイルのアップロード (複数可) .....	227
ファイルの削除 (複数可) .....	227

お気に入りを管理する .....	228
ファイルを編集する .....	228
ファイルの転送 .....	229
トラブルシューティング .....	231
一般的なデバッグとモニタリング .....	235
便利なログおよびイベント情報ソース .....	235
一般的な Amazon EC2 コンソールの外観 .....	240
Windows DCV デバッグ .....	242
Amazon DCV バージョン情報の検索 .....	243
RunBooks の問題 .....	243
インストールの問題 .....	246
ID 管理の問題 .....	252
Storage .....	257
スナップショット .....	262
インフラストラクチャ .....	263
仮想デスクトップの起動 .....	264
仮想デスクトップコンポーネント .....	274
Env 削除 .....	280
デモ環境 .....	287
Active Directory の問題 .....	289
既知の問題 .....	293
既知の問題 2024.x .....	293
Research and Engineering Studio サポートポリシー .....	318
注意 .....	320
改訂 .....	321
アーカイブ .....	329
.....	CCCXXX

## 概要:

### Important

このユーザーガイドでは、での Research and Engineering Studio の現在のリリース (2025.12) について説明します AWS。以前のバージョンについては、「」を参照してください [以前のバージョンのアーカイブ](#)。

Research and Engineering Studio (RES) は、AWS サポートされているオープンソース製品です。IT 管理者は、サイエンティストやエンジニアがテクニカルコンピューティングワークロードを実行できるウェブポータルを提供できます AWS。RES は、ユーザーが安全な仮想デスクトップを起動して、科学研究、製品設計、エンジニアリングシミュレーション、またはデータ分析ワークロードを実行するための単一の画面を提供します。ユーザーは、既存の企業認証情報を使用して RES ポータルに接続し、個々のプロジェクトまたは共同プロジェクトに取り組むことができます。

管理者は、特定のユーザーのセットに対してプロジェクトと呼ばれる仮想コラボレーションスペースを作成し、共有リソースにアクセスしてコラボレーションできます。管理者は、独自のアプリケーションソフトウェアスタックを ([Amazon マシンイメージ](#)または AMIs を使用して) 構築し、RES ユーザーが Windows または Linux 仮想デスクトップを起動できるようにし、共有ファイルシステムを介してプロジェクトデータにアクセスできるようにします。管理者は、ソフトウェアスタックとファイルシステムを割り当て、それらのプロジェクトユーザーのみにアクセスを制限できます。管理者は、組み込みテレメトリを使用して環境の使用状況をモニタリングし、ユーザーの問題をトラブルシューティングできます。また、リソースの過剰消費を防ぐために、個々のプロジェクトの予算を設定することもできます。製品はオープンソースであるため、お客様は自分のニーズに合わせて RES ポータルのユーザーエクスペリエンスをカスタマイズすることもできます。

RES は追加料金なしで利用でき、アプリケーションの実行に必要な AWS リソースに対してのみ料金が発生します。

このガイドでは、での Research and Engineering Studio の概要 AWS、リファレンスアーキテクチャとコンポーネント、デプロイを計画する際の考慮事項、および RES を Amazon Web Services (AWS) クラウドにデプロイするための設定手順について説明します。

## 機能と利点

の Research and Engineering Studio AWS には、次の機能があります。

## ウェブベースのユーザーインターフェイス

RES は、管理者、研究者、エンジニアが研究およびエンジニアリングワークスペースにアクセスして管理するために使用できるウェブベースのポータルを提供します。科学者やエンジニアは、RES を使用するために AWS アカウント やクラウドの専門知識を持っている必要はありません。

## プロジェクトベースの設定

プロジェクトを使用して、アクセス許可の定義、リソースの割り当て、一連のタスクまたはアクティビティの予算の管理を行います。整合性とコンプライアンスのために、特定のソフトウェアスタック (オペレーティングシステムと承認済みアプリケーション) とストレージリソースをプロジェクトに割り当てます。プロジェクトごとに支出を監視および管理します。

## コラボレーションツール

科学者やエンジニアは、プロジェクトの他のメンバーを招待してコラボレーションし、同僚に求めるアクセス許可レベルを設定できます。これらのユーザーは、RES にサインインしてデスクトップに接続できます。

## 既存の ID 管理インフラストラクチャとの統合

既存の ID 管理およびディレクトリサービスインフラストラクチャと統合して、ユーザーの既存の企業 ID を使用して RES ポータルに接続し、既存のユーザーおよびグループメンバーシップを使用してプロジェクトにアクセス許可を割り当てます。

## 永続的ストレージと共有データへのアクセス

仮想デスクトップセッション間で共有データへのアクセスをユーザーに許可するには、RES 内の既存のファイルシステムに接続します。サポートされているストレージサービスには、Linux デスクトップ用の Amazon Elastic File System と、Windows および Linux デスクトップ用の NetApp ONTAP 用の Amazon FSx が含まれます。

## モニタリングとレポート

分析ダッシュボードを使用して、インスタンスタイプ、ソフトウェアスタック、オペレーティングシステムタイプのリソース使用状況をモニタリングします。ダッシュボードには、レポート用のプロジェクト別のリソース使用状況の内訳も表示されます。

## 予算とコストの管理

RES プロジェクト AWS Budgets にリンクして、各プロジェクトのコストをモニタリングします。予算を超えた場合は、VDI セッションの起動を制限できます。

## 概念と定義

このセクションでは、主要な概念について説明し、以下に関する Research and Engineering Studio 固有の用語を定義します AWS。

### ファイルブラウザ

ファイルブラウザは、現在ログインしているユーザーがファイルシステムを表示できる RES ユーザーインターフェイスの一部です。

### ファイルシステム

ファイルシステムは、プロジェクトデータ (データセットと呼ばれることが多い) のコンテナとして機能します。プロジェクトの境界内でストレージソリューションを提供し、コラボレーションとデータアクセスコントロールを向上させます。

### グローバル管理者

RES 環境間で共有される RES リソースにアクセスできる管理者代理。スコープとアクセス許可は複数のプロジェクトにまたがります。プロジェクトを作成または変更し、プロジェクト所有者を割り当てることができます。プロジェクト所有者とプロジェクトメンバーにアクセス許可を委任または割り当てることができます。組織のサイズによっては、同じ人が RES 管理者として機能する場合があります。

### プロジェクト

プロジェクトは、データとコンピューティングリソースの個別の境界として機能するアプリケーション内の論理パーティションです。これにより、データフローのガバナンスが確保され、プロジェクト間でデータと VDI ホストを共有できなくなります。

### プロジェクトベースのアクセス許可

プロジェクトベースのアクセス許可は、複数のプロジェクトが存在するシステム内のデータと VDI ホストの両方の論理パーティションを記述します。プロジェクト内のデータと VDI ホストへのユーザーのアクセスは、関連するロール (複数可) によって決まります。ユーザーには、アクセスが必要なプロジェクトごとにアクセス (またはプロジェクトメンバーシップ) を割り当てる必要があります。それ以外の場合、ユーザーはメンバーシップが付与されていないとプロジェクトデータと VDIs にアクセスできません。

### プロジェクトメンバー

RES リソース (VDI、ストレージなど) のエンドユーザー。スコープとアクセス許可は、割り当てられたプロジェクトに制限されます。アクセス許可を委任または割り当てることはできません。

## プロジェクトの所有者

特定のプロジェクトへのアクセス権と所有権を持つ管理代理人。スコープとアクセス許可は、所有するプロジェクト (複数可) に制限されます。所有するプロジェクトのプロジェクトメンバーにアクセス許可を割り当てることができます。

## ソフトウェアスタック

ソフトウェアスタックは、[ユーザーが VDI ホスト用にプロビジョニングするために選択したオペレーティングシステムに基づく RES 固有のメタデータを持つ Amazon マシンイメージ \(AMIs\)](#) です。

## VDI ホスト

仮想デスクトップインスタンス (VDI) ホストを使用すると、プロジェクトメンバーはプロジェクト固有のデータとコンピューティング環境にアクセスし、安全で隔離されたワークスペースを確保できます。

AWS 用語の一般的なリファレンスについては、[AWS 「用語集」](#) を参照してください。

# アーキテクチャの概要

このセクションでは、この製品でデプロイされたコンポーネントのアーキテクチャ図を示します。

## アーキテクチャ図

デフォルトのパラメータを使用してこの製品をデプロイすると、に次のコンポーネントがデプロイされます AWS アカウント。

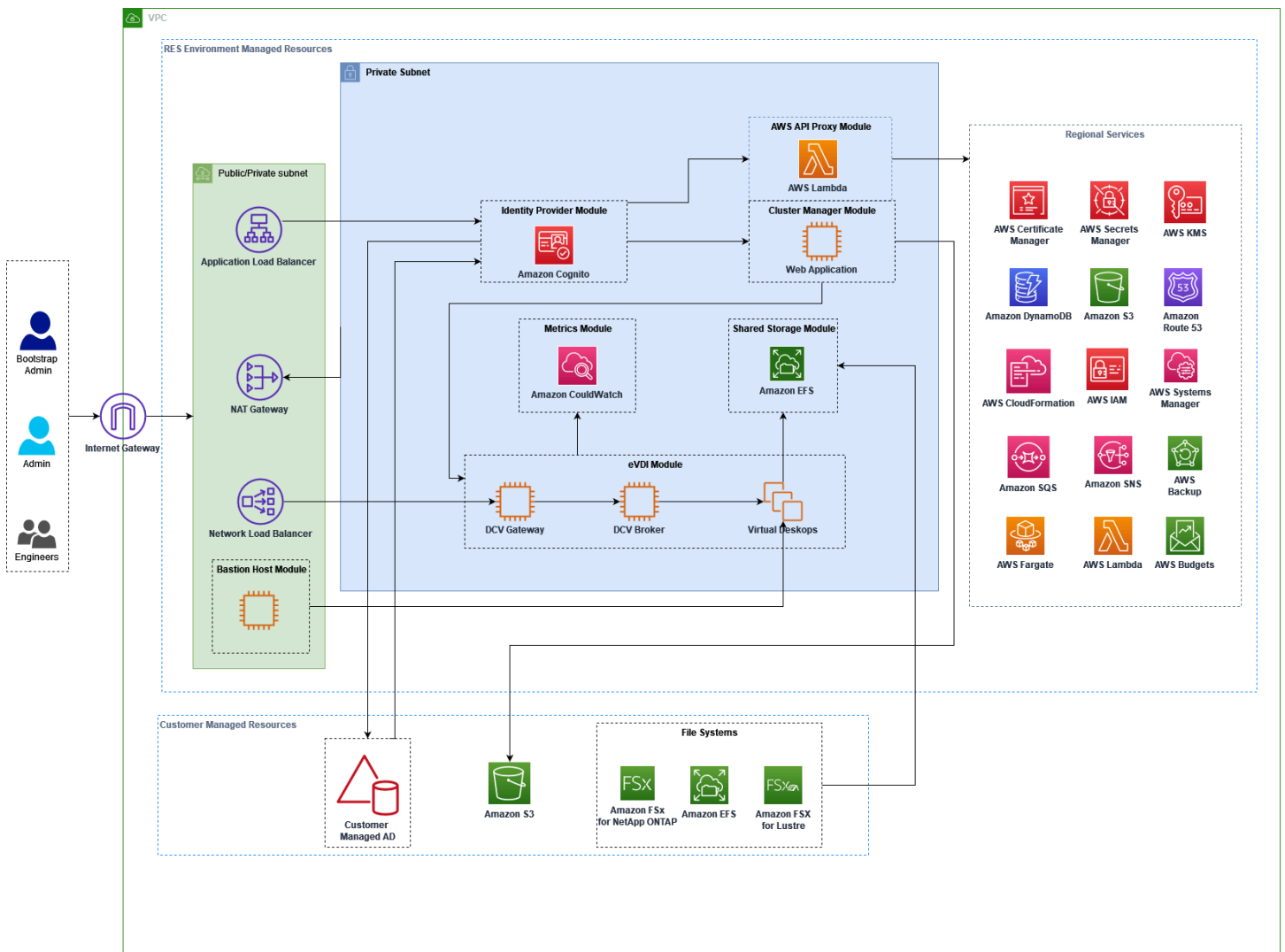


図 1: AWS アーキテクチャに関する Research and Engineering Studio

**Note**

AWS CloudFormation リソースは AWS Cloud Development Kit (AWS CDK) コンストラクトから作成されます。

テンプレートで AWS CloudFormation デプロイされた製品コンポーネントの大まかなプロセスフローは次のとおりです。

1. RES は、ウェブポータルコンポーネントと以下をインストールします。

- a. インタラクティブワークロード用のエンジニアリング仮想デスクトップ (eVDI) コンポーネント
- b. メトリクスコンポーネント

Amazon CloudWatch は eVDI コンポーネントからメトリクスを受け取ります。

c. 踏み台ホストコンポーネント

管理者は SSH を使用して踏み台ホストコンポーネントに接続し、基盤となるインフラストラクチャを管理できます。

2. RES は、NAT ゲートウェイの背後にあるプライベートサブネットにコンポーネントをインストールします。管理者は、Application Load Balancer (ALB) または踏み台ホストコンポーネントを介してプライベートサブネットにアクセスします。

3. Amazon DynamoDB は環境設定を保存します。

4. AWS Certificate Manager (ACM) は、Application Load Balancer (ALB) のパブリック証明書を生成して保存します。

**Note**

を使用して AWS Certificate Manager、ドメインの信頼された証明書を生成することをお勧めします。

5. Amazon Elastic File System (EFS) は、該当するすべてのインフラストラクチャホストと eVDI Linux セッションにマウントされたデフォルトの /home ファイルシステムをホストします。

6. RES は Amazon Cognito を使用して、内に「clusteradmin」という名前の初期ブートストラップユーザーを作成し、インストール時に提供された E メールアドレスに一時的な認証情報を送信します。「clusteradmin」は、初めてログインするときにパスワードを変更する必要があります。

7. Amazon Cognito は、アクセス許可管理のために組織の Active Directory およびユーザー ID と統合します。
8. セキュリティゾーンを使用すると、管理者はアクセス許可に基づいて製品内の特定のコンポーネントへのアクセスを制限できます。

## AWS この製品の サービス

AWS サービス	タイプ	説明
<a href="#">Amazon Elastic Compute Cloud</a>	コア	選択したオペレーティングシステムとソフトウェアスタックで仮想デスクトップを作成するための基盤となるコンピューティングサービスを提供します。
<a href="#">エラスティックロードバランシング</a>	コア	踏み台、クラスターマネージャー、VDI ホストは、ロードバランサーの背後にある Auto Scaling グループに作成されます。ELB は、RES ホスト間でウェブポータルからのトラフィックのバランスを取ります。
<a href="#">Amazon Virtual Private Cloud</a>	コア	すべてのコア製品コンポーネントは VPC 内に作成されます。
<a href="#">Amazon Cognito</a>	コア	ユーザー ID と認証を管理します。Active Directory ユーザーは Amazon Cognito ユーザーとグループにマッピングされ、アクセスレベルを認証します。

AWS サービス	タイプ	説明
<a href="#">Amazon Elastic File System</a>	コア	/home ファイルブラウザと VDI ホスト用のファイルシステム、および共有外部ファイルシステムを提供します。
<a href="#">Amazon DynamoDB</a>	コア	ユーザー、グループ、プロジェクト、ファイルシステム、コンポーネント設定などの設定データを保存します。
<a href="#">AWS Systems Manager</a>	コア	VDI セッション管理のコマンドを実行するためのドキュメントを保存します。
<a href="#">AWS Lambda</a>	コア	DynamoDB テーブル内の設定の更新、Active Directory 同期ワークフローの開始、プレフィックスリストの更新などの製品機能をサポートします。
<a href="#">Amazon CloudWatch</a>	サポート	すべての Amazon EC2 ホストと Lambda 関数のメトリクスとアクティビティログを提供します。
<a href="#">Amazon Simple Storage Service</a>	サポート	ホストブートストラップと設定用のアプリケーションバイナリを保存します。
<a href="#">AWS Key Management Service</a>	サポート	Amazon SQS キュー、DynamoDB テーブル、および Amazon SNS トピックを使用した保管時の暗号化に使用されます。

AWS サービス	タイプ	説明
<a href="#">AWS Secrets Manager</a>	サポート	サービスアカウントの認証情報を Active Directory と VDI の自己署名証明書に保存します。
<a href="#">AWS CloudFormation</a>	サポート	製品のデプロイメカニズムを提供します。
<a href="#">AWS Identity and Access Management</a>	サポート	ホストのアクセスレベルを制限します。
<a href="#">Amazon Route 53</a>	サポート	内部ロードバランサーと踏み台ホスト名を解決するためのプライベートホストゾーンを作成します。
<a href="#">Amazon Simple Queue Service</a>	サポート	非同期実行をサポートするタスクキューを作成します。
<a href="#">Amazon Simple Notification Service</a>	サポート	コントローラーやホストなどの VDI コンポーネント間のパブリケーションサブスクリプションモデルをサポートします。
<a href="#">AWS Fargate</a>	サポート	Fargate タスクを使用して環境をインストール、更新、削除します。
<a href="#">Amazon FSx ファイルゲートウェイ</a>	オプションです。	外部共有ファイルシステムを提供します。
<a href="#">Amazon FSx for NetApp ONTAP</a>	オプションです。	外部共有ファイルシステムを提供します。
<a href="#">AWS Certificate Manager</a>	オプションです。	カスタムドメインの信頼された証明書を生成します。

AWS サービス	タイプ	説明
<a href="#">AWS Backup</a>	オプションです。	Amazon EC2 ホスト、ファイルシステム、DynamoDB のバックアップ機能を提供します。

# デモ環境を作成する

Research and Engineering Studio を試すには、このセクションのステップに従います AWS。このデモでは、[AWS デモ環境スタックテンプレートで Research and Engineering Studio を使用して、最小限のパラメータセットで非本番環境をデプロイします](#)。SSO には Keycloak サーバーを使用します。

スタックをデプロイした後、ログインする前に、[デプロイ後のステップ](#)以下の手順に従って 環境でユーザーを設定する必要があります。

## ワンクリックデモスタックを作成する

この CloudFormation スタックは、Research and Engineering Studio に必要なすべてのコンポーネントを作成します。

デプロイまでの時間: ~90 分

### 前提条件

#### トピック

- [管理ユーザー AWS アカウント を使用して を作成する](#)
- [Amazon EC2 SSH キーペアを作成する](#)
- [サービスクォータを増やす](#)

### 管理ユーザー AWS アカウント を使用して を作成する

管理ユーザー AWS アカウント を持つ が必要です。

1. <https://portal.aws.amazon.com/billing/signup> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

にサインアップすると AWS アカウント、AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があ

ります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、[ルートユーザーアクセスが必要なタスク](#)の実行にはルートユーザーのみを使用するようにしてください。

## Amazon EC2 SSH キーペアを作成する

Amazon EC2 SSH キーペアがない場合は、キーペアを作成する必要があります。詳細については、「[Amazon EC2 ユーザーガイド](#)」の「Amazon EC2 を使用したキーペアの作成」を参照してください。

## サービスクォータを増やす

[以下のサービスクォータを増やす](#)ことをお勧めします。

- [Amazon VPC](#)
  - NAT ゲートウェイあたりの Elastic IP アドレスクォータを 5 から 8 に増やす
  - アベイラビリティーゾーンあたりの NAT ゲートウェイを 5 から 10 に増やす
- [Amazon EC2](#)
  - EC2-VPC Elastic IPs

AWS アカウントには、AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。詳細については、「[the section called “この製品の AWS サービスのクォータ”](#)」を参照してください。

## リソースと入力パラメータを作成する

1. にサインイン AWS マネジメントコンソールし、<https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。

### Note

管理者アカウントにいることを確認します。

2. コンソールで[テンプレートを起動](#)します。
3. パラメータ で、この製品テンプレートのパラメータを確認し、必要に応じて変更します。

パラメータ	デフォルト	説明
EnvironmentName	<res-demo>	res- で始まり、11 文字以下、大文字を含まない RES 環境に与えられる一意の名前。
AdministratorEmail		製品のセットアップを完了したユーザーの E メールアドレス。Active Directory のシングルサインオン統合に障害が発生した場合、このユーザーはさらにブレイクグラスユーザーとして機能します。
KeyPair		インフラストラクチャホストへの接続に使用されるキーペア。
ClientIPCIDR	<0.0.0.0/0>	システムへの接続を制限する IP アドレスフィルター。デプロイ後に ClientIpCidr を更新できます。
InboundPrefixList		(オプション) 踏み台ホストへのウェブ UI と SSH への直接アクセスが許可されている IPs のマネージドプレフィックスリストを指定します。

4. [スタックの作成] を選択してください。

## デプロイ後のステップ

1. clusteradmin ユーザーと、セットアップ時に入力した管理者 E メールに送信された一時パスワードを使用して、デモ環境にログインできるようになりました。最初のログイン時に新しいパスワードを作成するように求められます。

2. 「組織 SSO でサインイン」機能を使用する場合は、まずログインする各ユーザーのパスワードをリセットする必要があります。AWS Directory Service からユーザーパスワードをリセットできます。デモスタックは、admin1、user1、admin2、user2 の 4 人のユーザーをユーザー名で作成します。
  - a. Directory Service コンソールに移動します。
  - b. 環境のディレクトリ ID を選択します。ディレクトリ ID はスタックの出力から取得できません <StackName>\*DirectoryService\*。
  - c. 右上のアクションドロップダウンメニューから、ユーザーのパスワードをリセットを選択します。
  - d. 使用するすべてのユーザーについて、ユーザー名を入力し、新しいパスワードを入力し、パスワードのリセットを選択します。
3. ユーザーパスワードをリセットしたら、シングルサインインのログインページに進み、環境にアクセスします。

これでデプロイの準備ができました。E メールで受け取った EnvironmentUrl を使用して UI にアクセスするか、デプロイされたスタックの出力から同じ URL を取得することもできます。これで、Active Directory で のパスワードをリセットしたユーザーとパスワードを使用して、Research and Engineering Studio 環境にログインできます。

# デプロイを計画する

このセクションでは、での Research and Engineering Studio のデプロイを計画するのに役立つコスト、セキュリティ、サポートされているリージョン、クォータについて説明します AWS。

## Cost

の Research and Engineering Studio AWS は追加料金なしで利用でき、アプリケーションの実行に必要なリソースに対して AWS のみ料金が発生します。詳細については、「[AWS この製品の サービス](#)」を参照してください。

### Note

この製品の実行中に使用される AWS サービスのコストは、お客様の負担となります。コスト管理を容易にするために、[AWS Cost Explorer](#) を使用して [予算](#) を作成することを推奨しています。価格は変更されることがあります。詳細については、この製品で使用される各 AWS サービスの料金ウェブページを参照してください。

## セキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、AWS お客様とお客様の間の責任共有です。責任 [共有モデル](#) では、これをクラウドのセキュリティとクラウド内のセキュリティと定義しています。

- クラウドのセキュリティ – AWS は、で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。AWS は、お客様が安全に使用できるサービスも提供します。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#) コンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。で Research and Engineering Studio に適用されるコンプライアンスプログラムの詳細については AWS、「[コンプライアンス AWS プログラムによる対象範囲内のサービスコンプライアンス](#)」を参照してください。

- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

Research and Engineering Studio で使用される AWS サービスで 責任共有モデルを適用する方法については、「」を参照してください[この製品のサービスに関するセキュリティ上の考慮事項](#)。AWS セキュリティの詳細については、[AWS クラウド「セキュリティ」](#)を参照してください。

## IAM ロール

AWS Identity and Access Management (IAM) ロールを使用すると、 のサービスおよびユーザーにきめ細かなアクセスポリシーとアクセス許可を割り当てることができます AWS クラウド。この製品は、製品の AWS Lambda 関数と Amazon EC2 インスタンスにリージョンリソースを作成するためのアクセス権を付与する IAM ロールを作成します。

RES は IAM 内のアイデンティティベースのポリシーをサポートしています。デプロイすると、RES は管理者のアクセス許可とアクセスを定義するポリシーを作成します。製品を実装する管理者は、RES と統合された既存のカスタマー Active Directory 内でエンドユーザーとプロジェクトリーダーを作成および管理します。詳細については、AWS 「Identity and Access Management ユーザーガイド」の「[IAM ポリシーの作成](#)」を参照してください。

組織の管理者は、アクティブディレクトリを使用してユーザーアクセスを管理できます。エンドユーザーが RES ユーザーインターフェイスにアクセスすると、RES は [Amazon Cognito](#) で認証します。

## セキュリティグループ

この製品で作成されたセキュリティグループは、Lambda 関数、EC2 インスタンス、ファイルシステム CSR インスタンス、リモート VPN エンドポイント間のネットワークトラフィックを制御および分離するように設計されています。セキュリティグループを確認し、製品のデプロイ後に必要に応じてアクセスをさらに制限することをお勧めします。

## データ暗号化

デフォルトでは、AWS (RES) の Research and Engineering Studio は、RES 所有のキーを使用して、保管中および転送中の顧客データを暗号化します。RES をデプロイするときに、 を指定できます AWS KMS key。RES は、認証情報を使用してキーアクセスを付与します。顧客所有および管理の を指定すると AWS KMS key、保管中の顧客データはそのキーを使用して暗号化されます。

RES は、SSL/TLS を使用して転送中の顧客データを暗号化します。TLS 1.2 が必要ですが、TLS 1.3 をお勧めします。

## この製品のサービスに関するセキュリティ上の考慮事項

Research and Engineering Studio で使用されるサービスのセキュリティ上の考慮事項の詳細については、次の表のリンクを参照してください。

AWS サービスセキュリティ情報	サービスタイプ	RES でのサービスの使用方法
<a href="#">Amazon Elastic Compute Cloud</a>	Core	選択したオペレーティングシステムとソフトウェアスタックを使用して仮想デスクトップを作成するための基盤となるコンピューティングサービスを提供します。
<a href="#">エラスティックロードバランシング</a>	Core	踏み台、クラスターマネージャー、VDI ホストは、ロードバランサーの背後にある Auto Scaling グループに作成されます。ELB は、RES ホスト間でウェブポータルからのトラフィックのバランスを取ります。
<a href="#">Amazon Virtual Private Cloud</a>	Core	すべてのコア製品コンポーネントは VPC 内に作成されます。
<a href="#">Amazon Cognito</a>	Core	ユーザー ID と認証を管理します。Active Directory ユーザーは Amazon Cognito ユーザーとグループにマッピングされ、アクセスレベルを認証します。

AWS サービスセキュリティ情報	サービスタイプ	RES でのサービスの使用方法
<a href="#">Amazon Elastic File System</a>	Core	/home ファイルブラウザと VDI ホスト用のファイルシステム、および共有外部ファイルシステムを提供します。
<a href="#">Amazon DynamoDB</a>	Core	ユーザー、グループ、プロジェクト、ファイルシステム、コンポーネント設定などの設定データを保存します。
<a href="#">AWS Systems Manager</a>	Core	VDI セッション管理のコマンドを実行するためのドキュメントを保存します。
<a href="#">AWS Lambda</a>	Core	DynamoDB テーブル内の設定の更新、Active Directory 同期ワークフローの開始、プレフィックスリストの更新などの製品機能をサポートします。
<a href="#">Amazon CloudWatch</a>	サポート	すべての Amazon EC2 ホストと Lambda 関数のメトリクスとアクティビティログを提供します。
<a href="#">Amazon Simple Storage Service</a>	サポート	ホストブートストラップと設定用のアプリケーションバイナリを保存します。
<a href="#">AWS Key Management Service</a>	サポート	Amazon SQS キュー、DynamoDB テーブル、Amazon SNS トピックでの保管時の暗号化に使用されます。

AWS サービスセキュリティ情報	サービスタイプ	RES でのサービスの使用方法
<a href="#">AWS Secrets Manager</a>	サポート	サービスアカウントの認証情報を Active Directory に保存し、VDIs。
<a href="#">AWS CloudFormation</a>	サポート	製品のデプロイメカニズムを提供します。
<a href="#">AWS Identity and Access Management</a>	サポート	ホストのアクセスレベルを制限します。
<a href="#">Amazon Route 53</a>	サポート	内部ロードバランサーと踏み台ホストドメイン名を解決するためのプライベートホストゾーンを作成します。
<a href="#">Amazon Simple Queue Service</a>	サポート	非同期実行をサポートするタスクキューを作成します。
<a href="#">Amazon Simple Notification Service</a>	サポート	コントローラーやホストなどの VDI コンポーネント間のアプリケーションサブスクリバードモデルをサポートします。
<a href="#">AWS Fargate</a>	サポート	Fargate タスクを使用して環境をインストール、更新、削除します。
<a href="#">Amazon FSx ファイルゲートウェイ</a>	オプションです。	外部共有ファイルシステムを提供します。
<a href="#">Amazon FSx for NetApp ONTAP</a>	オプションです。	外部共有ファイルシステムを提供します。
<a href="#">AWS Certificate Manager</a>	オプションです。	カスタムドメインの信頼された証明書を生成します。

AWS サービスセキュリティ情報	サービスタイプ	RES でのサービスの使用方法
<a href="#">AWS Backup</a>	オプションです。	Amazon EC2 ホスト、ファイルシステム、DynamoDB のバックアップ機能を提供します。

## クォータ

Service Quotas (制限とも呼ばれます) は、AWS アカウントのサービスリソースまたはオペレーションの最大数です

### この製品の AWS サービスのクォータ

この製品に実装されている各サービスに十分なクォータがあることを確認してください。詳細については、「[AWS サービスクォータ](#)」を参照してください。

この製品では、次のサービスのクォータを引き上げることをお勧めします。

- Amazon Virtual Private Cloud
- Amazon EC2

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイドの「[クォータ引き上げリクエスト](#)」を参照してください。Service Quotas でクォータがまだ利用できない場合は、[\[上限引き上げ\]](#) フォームを使用してください。

### AWS CloudFormation クォータ

AWS アカウントには、この製品で[スタックを起動](#)するときに注意すべき AWS CloudFormation クォータがあります。これらのクォータを理解することで、この製品を正常にデプロイできないような制限エラーを回避できます。詳細については、「ユーザーガイド」の「[AWS CloudFormation のクォータ](#)」を参照してください。AWS CloudFormation

## レジリエンスの計画

製品は、システムを運用するための Amazon EC2 インスタンスの最小数とサイズを持つデフォルトのインフラストラクチャをデプロイします。大規模な本番環境の耐障害性を向上させるには、イン

フラストラクチャの Auto Scaling グループ (ASG) 内のデフォルトの最小容量設定を増やすことをお勧めします。値を 1 つのインスタンスから 2 つのインスタンスに増やすと、複数のアベイラビリティゾーン (AZ) の利点が得られ、予期しないデータ損失が発生した場合にシステム機能を復元する時間を短縮できます。

ASG 設定は、<https://console.aws.amazon.com/ec2/> の Amazon EC2 コンソール内でカスタマイズできます。製品はデフォルトで 4 つの ASGs を作成し、各名前は `<製品名>-asg` で終わります。最小値と必要な値は、本番環境に適した量に変更できます。変更するグループを選択し、アクションを選択して編集を選択します。ASGs、[「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループのサイズをスケールする」](#)を参照してください。Amazon EC2 Auto Scaling

## サポートされている AWS リージョン

この製品は、現在すべてので利用できないサービスを使用します AWS リージョン。この製品は、すべてのサービス AWS リージョン が利用可能なで起動する必要があります。リージョン別の AWS サービスの最新の可用性については、[「AWS リージョン Services List」](#)を参照してください。

の Research and Engineering Studio AWS は、以下でサポートされています AWS リージョン。

リージョン名	リージョン	以前のバージョン	最新バージョン (2025 年 12 月)
米国東部 (バージニア北部)	us-east-1	はい	はい
米国東部 (オハイオ)	us-east-2	はい	はい
米国西部 (北カリフォルニア)	us-west-1	はい	はい
米国西部 (オレゴン)	us-west-2	はい	はい
アジアパシフィック (東京)	ap-northeast-1	はい	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい	はい

リージョン名	リージョン	以前のバージョン	最新バージョン (2025年 12 月)
アジアパシフィック (大阪)	ap-northeast-3	はい	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい	はい
アジアパシフィック (ジャカルタ)	ap-southeast-3	はい	はい
カナダ (中部)	ca-central-1	はい	はい
欧州 (フランクフルト)	eu-central-1	はい	はい
欧州 (ミラノ)	eu-south-1	はい	はい
欧州 (アイルランド)	eu-west-1	はい	はい
欧州 (ロンドン)	eu-west-2	はい	はい
欧州 (パリ)	eu-west-3	はい	はい
欧州 (ストックホルム)	eu-north-1	はい	はい
イスラエル (テルアビブ)	il-central-1	はい	はい
中東 (UAE)	me-central-1	はい	はい
南米 (サンパウロ)	sa-east-1	はい	はい
AWS GovCloud (米国 東部)	us-gov-east-1	はい	はい

リージョン名	リージョン	以前のバージョン	最新バージョン (2025年 12 月)
AWS GovCloud (米国西部)	us-gov-west-1	はい	はい

# 製品をデプロイする

## Note

この製品は、[AWS CloudFormation テンプレートとスタック](#)を使用してデプロイを自動化します。CloudFormation テンプレートは、この製品に含まれる AWS リソースとそのプロパティを記述します。CloudFormation スタックは、テンプレートに記述されているリソースをプロビジョニングします。

製品を起動する前に、このガイドで前述した[コスト](#)、[アーキテクチャ](#)、[ネットワークセキュリティ](#)、その他の考慮事項を確認してください。

## トピック

- [前提条件](#)
- [外部リソースを作成する](#)
- [ステップ 1: 製品を起動する](#)
- [ステップ 2: 初めてサインインする](#)

## 前提条件

### トピック

- [管理ユーザー AWS アカウント を使用して を作成する](#)
- [Amazon EC2 SSH キーペアを作成する](#)
- [サービスクォータを増やす](#)
- [Cognito ユーザープールを作成する \(オプション\)](#)
- [カスタムドメインを作成する \(オプション\)](#)
- [ドメインの作成 \(GovCloud のみ\)](#)
- [外部リソースを提供する](#)
- [環境で LDAPS を設定する \(オプション\)](#)
- [Microsoft Active Directory のサービスアカウントを設定する](#)
- [プライベート VPC を設定する \(オプション\)](#)

## 管理ユーザー AWS アカウント を使用して を作成する

管理ユーザー AWS アカウント を持つ が必要です。

1. <https://portal.aws.amazon.com/billing/signup> を開きます。
2. オンラインの手順に従います。

サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

にサインアップすると AWS アカウント、AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、[ルートユーザーアクセスが必要なタスク](#)の実行にはルートユーザーのみを使用するようにしてください。

## Amazon EC2 SSH キーペアを作成する

Amazon EC2 SSH キーペアがない場合は、作成する必要があります。詳細については、[「Amazon EC2 ユーザーガイド」](#)の「Amazon EC2 を使用したキーペアの作成」を参照してください。

## サービスクォータを増やす

[以下のサービスクォータを増やす](#)ことをお勧めします。

- [Amazon VPC](#)
  - NAT ゲートウェイあたりの Elastic IP アドレスクォータを 5 から 8 に増やします。
  - アベイラビリティゾーンあたりの NAT ゲートウェイを 5 から 10 に増やします。
- [Amazon EC2](#)
  - EC2-VPC Elastic IPs

AWS アカウントには、AWS サービスごとに、以前は制限と呼ばれていたデフォルトのクォータがあります。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。詳細については、「[この製品の AWS サービスのクォータ](#)」を参照してください。

## Cognito ユーザープールを作成する (オプション)

RES のインストール時に、ユーザー認証とクライアント認証のために既存の Cognito ユーザープールをインポートすることもできます。それ以外の場合、RES は新しい Cognito ユーザープールを自動的に作成します。既存のユーザープールには、次のサインアップカスタム属性が必要です。

名前	型	最小値/長さ	最大値/長さ	Mutable
custom:aws_region	文字列			TRUE
custom:customer_name	文字列			TRUE
custom:password_last_set	数値			TRUE
custom:password_max_age	数値			TRUE
custom:uid	数値	2000200001	4294967294	TRUE

## カスタムドメインを作成する (オプション)

ユーザーフレンドリーな URL を持つには、製品のカスタムドメインを使用することをお勧めします。カスタムドメインを指定し、オプションで証明書を指定できます。

外部リソーススタックには、指定したカスタムドメインの証明書を作成するプロセスがあります。ドメインがあり、外部リソーススタックの証明書生成機能を使用する場合は、ここでステップをスキップできます。

または、以下の手順に従って Amazon Route 53 を使用してドメインを登録し、を使用してドメインの証明書をインポートします AWS Certificate Manager。

1. 指示に従って、Route53 [にドメインを登録](#)します。確認メールが届きます。
2. ドメインのホストゾーンを取得します。これは Route53 によって自動的に作成されます。
  - a. Route53 コンソールを開きます。

- b. 左側のナビゲーションからホストゾーンを選択します。
  - c. ドメイン名用に作成されたホストゾーンを開き、ホストゾーン ID をコピーします。
3. を開き AWS Certificate Manager、以下の手順に従って [ドメイン証明書をリクエスト](#) します。ソリューションをデプロイする予定のリージョンにいることを確認します。
  4. ナビゲーションから証明書を一覧表示を選択し、証明書リクエストを見つけます。リクエストは保留中である必要があります。
  5. 証明書 ID を選択してリクエストを開きます。
  6. ドメインセクションから、Route53 でレコードを作成するを選択します。リクエストの処理には約 10 分かかります。
  7. 証明書が発行されたら、証明書のステータスセクションから ARN をコピーします。

## ドメインの作成 (GovCloud のみ)

AWS GovCloud リージョンにデプロイしていて、Research and Engineering Studio のカスタムドメインを使用している場合は、これらの前提条件のステップを完了する必要があります。

1. パブリックホストドメインが作成された商用パーティション AWS アカウントに [Certificate CloudFormation スタック](#) をデプロイします。
2. 証明書 CloudFormation 出力から、とを見つけCertificateARNでメモしますPrivateKeySecretARN。
3. GovCloud パーティションアカウントで、CertificateARN出力の値を持つシークレットを作成します。がシークレット値vdc-gatewayにアクセスできるように、新しいシークレット ARN を書き留め、シークレットに 2 つのタグを追加します。
  - a. res:ModuleName = virtual-desktop-controller
  - b. res:EnvironmentName = [environment name] (res-demo である可能性があります)
4. GovCloud パーティションアカウントで、PrivateKeySecretArn出力の値を持つシークレットを作成します。がシークレット値vdc-gatewayにアクセスできるように、新しいシークレット ARN を書き留め、シークレットに 2 つのタグを追加します。
  - a. res:ModuleName = virtual-desktop-controller
  - b. res:EnvironmentName = [environment name] (res-demo である可能性があります)

## 外部リソースを提供する

の Research and Engineering Studio では、デプロイ時に次の外部リソースが存在することを AWS 想定しています。

- ネットワーク (VPC、パブリックサブネット、プライベートサブネット)

ここでは、RES 環境、Active Directory (AD)、共有ストレージのホストに使用される EC2 インスタンスを実行します。

- ストレージ (Amazon EFS)

ストレージボリュームには、仮想デスクトップインフラストラクチャ (VDI) に必要なファイルとデータが含まれています。

- ディレクトリサービス (AWS Directory Service for Microsoft Active Directory)

ディレクトリサービスは、RES 環境に対してユーザーを認証します。

- キーと値のペア (ユーザー名、パスワード) としてフォーマットされた Active Directory サービスアカウントのユーザー名とパスワードを含むシークレット

Research and Engineering Studio は、を使用して、サービスアカウントのパスワードなど、指定した[シークレット](#)にアクセスします[AWS Secrets Manager](#)。

### Warning

同期するすべての Active Directory (AD) ユーザーに対して有効な E メールアドレスを指定する必要があります。

### Tip

デモ環境をデプロイしていて、これらの外部リソースを利用できない場合は、AWS ハイパフォーマンスコンピューティングレシピを使用して外部リソースを生成できます。アカウントにリソースをデプロイするには[外部リソースを作成する](#)、次のセクション「」を参照してください。

an AWS GovCloud リージョンでのデモデプロイでは、「」の前提条件ステップを完了する必要があります [ドメインの作成 \(GovCloud のみ\)](#)。

## 環境で LDAPS を設定する (オプション)

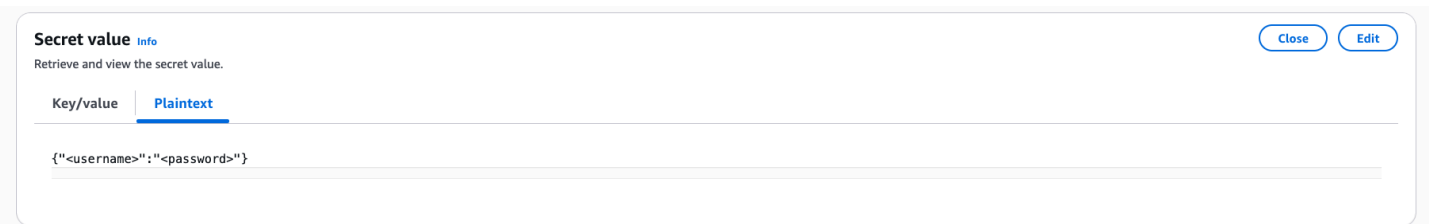
環境で LDAPS 通信を使用する場合は、以下の手順を実行して、証明書を作成して AWS Managed Microsoft AD (AD) ドメインコントローラーにアタッチし、AD と RES 間の通信を提供する必要があります。

1. 「[のサーバー側の LDAPS を有効にする方法 AWS Managed Microsoft AD](#)」に記載されているステップに従います。LDAPS を既に有効にしている場合は、このステップをスキップできます。
2. AD で LDAPS が設定されていることを確認したら、AD 証明書をエクスポートします。
  - a. Active Directory サーバーに移動します。
  - b. 管理者として PowerShell を開きます。
  - c. `certmgr.msc` を実行して証明書リストを開きます。
  - d. 最初に信頼されたルート認証機関を開き、次に証明書を開いて、証明書リストを開きます。
  - e. AD サーバーと同じ名前の証明書を長押し (または右クリック) し、すべてのタスクを選択してからエクスポートします。
  - f. Base-64 でエンコードされた X.509 (.CER) を選択し、次へを選択します。
  - g. ディレクトリを選択し、次へを選択します。
3. シークレットの作成先 AWS Secrets Manager:

シークレットマネージャーでシークレットを作成する場合は、[シークレットのタイプ] で [その他のシークレット] を選択し、[プレーンテキスト] フィールドに PEM エンコードの証明書を貼り付けます。
4. 作成された ARN を書き留めて、の `DomainTLSCertificateSecretARN` パラメータとして入力します [ステップ 1: 製品を起動する](#)。

## Microsoft Active Directory のサービスアカウントを設定する

RES の ID ソースとして Microsoft Active Directory (AD) を選択した場合、AD にプログラムによるアクセスを許可するサービスアカウントがあります。RES のインストールの一環として、サービスアカウントの認証情報を使用してシークレットを渡す必要があります。シークレットは、ここに示す形式である必要があります。



また、usernameフィールドは形式の NT 形式のログオン名をサポートしていないことに注意してくださいDOMAIN\username。

サービスアカウントは次の機能を担当します。

- AD からユーザーを同期する: RES は AD からユーザーを同期して、ユーザーがウェブポータルにログインできるようにする必要があります。同期プロセスは、サービスアカウントを使用して LDAP (複数可) を使用して AD をクエリし、使用可能なユーザーとグループを決定します。
- AD ドメインに参加する: これは、インスタンスが AD ドメインに参加する Linux 仮想デスクトップとインフラストラクチャホストのオプションオペレーションです。RES では、これは DisableADJoin パラメータで制御されます。このパラメータはデフォルトで False に設定されます。つまり、Linux 仮想デスクトップはデフォルト設定で AD ドメインに参加しようとします。
- AD に接続する: Linux 仮想デスクトップとインフラストラクチャホストは、AD ドメインに参加しない場合 (DisableADJoin = True)、AD ドメインに接続します。この機能を使用するには、サービスアカウントで UsersOU および のユーザーとグループの読み取りアクセスも必要です GroupsOU。

サービスアカウントには、次のアクセス許可が必要です。

- ユーザーを同期して AD に接続するには → UsersOU および のユーザーとグループの読み取りアクセス GroupsOU。
- AD ドメインに参加するには → で Computer オブジェクトを作成します ComputersOU。

[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) のスクリプトは、適切なサービスアカウントのアクセス許可を付与する方法の例を示しています。独自の AD に基づいて変更できます。

## プライベート VPC を設定する (オプション)

Research and Engineering Studio を分離された VPC にデプロイすると、組織のコンプライアンスとガバナンス要件を満たすためのセキュリティが強化されます。ただし、標準の RES デプロイは、依

存関係のインストールにインターネットアクセスに依存しています。プライベート VPC に RES をインストールするには、次の前提条件を満たす必要があります。

## トピック

- [Amazon マシンイメージ \(AMIsを準備する\)](#)
- [VPC エンドポイントの設定](#)
- [VPC エンドポイントのない サービスに接続する](#)
- [プライベート VPC デプロイパラメータを設定する](#)

## Amazon マシンイメージ (AMIsを準備する)

1. [で依存関係をダウンロードします https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/latest/res-installation-scripts.tar.gz](https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/latest/res-installation-scripts.tar.gz)。分離された VPC にデプロイするには、RES インフラストラクチャでパブリックインターネットアクセスなしで依存関係を利用できる必要があります。

### Important

RES 環境のバージョンが最新でない場合は、ダウンロード URI **latest**の を正確なバージョン番号 (例: **2025.06**) に置き換えます。

2. Amazon S3 読み取り専用アクセスと Amazon EC2 として信頼できる ID を持つ IAM ロールを作成します。
  - a. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
  - b. ロール から、ロールの作成 を選択します。
  - c. [信頼されたエンティティを選択] ページで以下を行います。
    - 信頼されたエンティティタイプで、 を選択します AWS のサービス。
    - 「サービス」または「ユースケース」で EC2」を選択し、「次へ」を選択します。
  - d. アクセス許可の追加で、次のアクセス許可ポリシーを選択し、次へを選択します。
    - AmazonS3ReadOnlyAccess
    - AmazonSSMManagedInstanceCore
    - EC2InstanceProfileForImageBuilder
  - e. ロール名と説明を追加し、ロールの作成を選択します。

### 3. EC2 Image Builder コンポーネントを作成します。

- a. で EC2 Image Builder コンソールを開きます <https://console.aws.amazon.com/imagebuilder>。
- b. 「保存されたリソース」で、「コンポーネント」を選択し、「コンポーネントの作成」を選択します。
- c. コンポーネントの作成ページで、次の詳細を入力します。
  - コンポーネントタイプで、ビルドを選択します。
  - コンポーネントの詳細については、以下を選択します。

パラメータ	ユーザーエントリ
Image operating system (OS)	Linux
Compatible OS Versions	Amazon Linux 2, Amazon Linux 2023, RHEL8, RHEL 9, or Windows 10 and 11
Component name	Enter a name such as: <i>&lt;research-and-engineering-studio-infrastructure&gt;</i>
Component version	We recommend starting with 1.0.0.
Description	Optional user entry.

- d. コンポーネントの作成ページで、ドキュメントコンテンツの定義を選択します。
  - i. 定義ドキュメントの内容を入力する前に、tar.gz ファイルのファイル URI が必要です。RES が提供する tar.gz ファイルを Amazon S3 バケットにアップロードし、バケットプロパティからファイルの URI をコピーします。
  - ii. 次のように入力します。

#### Note

AddEnvironmentVariables はオプションであり、インフラストラクチャホストにカスタム環境変数が必要ない場合は削除できます。

http\_proxy および https\_proxy 環境変数を設定する場合、インスタンスがプロキシを使用して localhost、インスタンスメタデータ IP アドレス、および

び VPC エンドポイントをサポートするサービスをクエリしないようにするには、no\_proxyパラメータが必要です。

```
# 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:
  - 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-installation-scripts/res-
installation-scripts.tar.gz'
      - name: RunInstallScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
```

```

    commands:
      - 'cd /root/bootstrap/res-installation-scripts'
      - 'tar -xf res-installation-scripts.tar.gz'
      - 'cd scripts/infrastructure-host'
      - '/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 launch template

```

e. [コンポーネントを作成] を選択します。

4. Image Builder イメージレシピを作成します。
- a. レシピの作成ページで、次のように入力します。

セクション	パラメータ	ユーザーエントリ
レシピ詳細	名前	Enter an appropriate name such as res-recipe-linux-x86.
	バージョン	Enter a version, typically starting with 1.0.0.
	説明	Add an optional description.
基本のイメージ	イメージの選択	Select managed images.
	OS	Amazon Linux or Red Hat Enterprise Linux (RHEL)
	イメージオリジン	Quick start (Amazon-managed)
	[イメージ名]	Amazon Linux 2 x86, Amazon Linux 2023 x86, Red Hat Enterprise Linux 8 x86, or Red Hat Enterprise Linux 9 x86
インスタンス設定	自動バージョンニングオプション	Use latest available OS version.
	–	Keep everything in the default settings, and make sure <code>パイプラインの実行後に SSM エージェントを削除する</code> is not selected.

セクション	パラメータ	ユーザーエントリ
作業ディレクトリパス	作業ディレクトリパス	/root/bootstrap/res-installation-scripts
コンポーネント	コンポーネントの構築	<p>以下を検索して選択します。</p> <ul style="list-style-type: none"> <li>• Amazon マネージド: aws-cli-version-2-linux</li> <li>• Amazon マネージド: amazon-cloudwatch-agent-linux</li> <li>• 所有: 以前に作成された Amazon EC2 コンポーネント。現在の AWS リージョンをフィールドに入力します。</li> </ul>
	テストコンポーネント	<p>を検索して選択します。</p> <ul style="list-style-type: none"> <li>• Amazon マネージド: simple-boot-test-linux</li> </ul>

b. [レシピを作成する] を選択します。

5. Image Builder インフラストラクチャ設定を作成します。

a. 保存済みリソースで、インフラストラクチャ設定を選択します。

b. インフラストラクチャー構成の作成 を選択します。

c. インフラストラクチャ設定の作成ページで、次のように入力します。

セクション	パラメータ	ユーザーエントリ
全般	名前	Enter an appropriate name such as res-infra-linux-x86.
	説明	Add an optional description.

セクション	パラメータ	ユーザーエントリ
	IAM ロール	Select the IAM role created previously.
AWS インフラストラクチャ	インスタンスタイプ	Choose t3.medium.
	VPC、サブネット、セキュリティグループ	<p>Amazon S3 バケットへのインターネットアクセスとアクセスを許可するオプションを選択します。セキュリティグループを作成する必要がある場合は、次の入力を使用して Amazon EC2 コンソールから作成できます。</p> <ul style="list-style-type: none"> <li>• VPC: インフラストラクチャ設定に使用されているのと同じ VPC を選択します。この VPC にはインターネットアクセスが必要です。</li> <li>• インバウンドルール: <ul style="list-style-type: none"> <li>• タイプ: SSH</li> <li>• [Source]: Custom</li> <li>• CIDR ブロック: 0.0.0.0/0</li> </ul> </li> </ul>

d. インフラストラクチャ構成の作成 を選択します。

6. 新しい EC2 Image Builder パイプラインを作成します。

a. Image pipelines に移動し、Create image pipeline を選択します。

b. パイプラインの詳細を指定ページで、次のように入力し、次へを選択します。

- パイプライン名とオプションの説明

- ビルドスケジュールで、スケジュールを設定するか、AMI ベーキングプロセスを手動で開始する場合は手動を選択します。
  - c. レシピの選択ページで、既存のレシピを使用を選択し、前に作成したレシピ名を入力します。[次へ] を選択します。
  - d. 画像プロセスの定義ページで、デフォルトのワークフローを選択し、次へを選択します。
  - e. 「インフラストラクチャ設定の定義」ページで、「既存のインフラストラクチャ設定を使用する」を選択し、以前に作成したインフラストラクチャ設定の名前を入力します。[次へ] を選択します。
  - f. デистриビューション設定の定義ページで、選択について次の点を考慮してください。
    - RES がそこからインフラストラクチャホストインスタンスを適切に起動できるように、出カイメージはデプロイされた RES 環境と同じリージョンに存在する必要があります。サービスのデフォルトを使用すると、EC2 Image Builder サービスが使用されているリージョンに出カイメージが作成されます。
    - RES を複数のリージョンにデプロイする場合は、新しいデистриビューション設定を作成し、そこにリージョンを追加できます。
  - g. 選択内容を確認し、パイプラインの作成を選択します。
7. EC2 Image Builder パイプラインを実行します。
- a. イメージパイプラインから、作成したパイプラインを見つけて選択します。
  - b. アクション を選択し、パイプラインの実行 を選択します。

パイプラインは、AMI イメージの作成に約 45 分から 1 時間かかる場合があります。

8. 生成された AMI の AMI ID を書き留め、 の InfrastructureHostAMI パラメータの入力として使用します [the section called “ステップ 1: 製品を起動する”](#)。

## VPC エンドポイントの設定

RES をデプロイして仮想デスクトップを起動するには、プライベートサブネットへのアクセス AWS のサービスが必要です。必要なアクセスを提供するように VPC エンドポイントを設定する必要があります。また、エンドポイントごとにこれらのステップを繰り返す必要があります。

1. エンドポイントが以前に設定されていない場合は、[「インターフェイス VPC エンドポイント AWS のサービスを使用してにアクセスする」](#)に記載されている手順に従ってください。
2. 2 つのアベイラビリティーゾーンのそれぞれで 1 つのプライベートサブネットを選択します。

AWS のサービス	サービス名
<a href="#">アプリケーションの Auto Scaling</a>	com.amazonaws. <i>region</i> .application-autoscaling
<a href="#">AWS CloudFormation</a>	com.amazonaws. <i>region</i> .cloudformation
<a href="#">Amazon CloudWatch</a>	com.amazonaws. <i>region</i> .monitoring
<a href="#">Amazon CloudWatch Logs</a>	com.amazonaws. <i>region</i> .logs
<a href="#">Amazon DynamoDB</a>	com.amazonaws. <i>region</i> .dynamodb (ゲートウェイエンドポイントが必要)
<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> .elasticfilesystem
<a href="#">エラスティックロードバランシング</a>	com.amazonaws. <i>region</i> .elasticloadbalancing
<a href="#">Amazon EventBridge</a>	com.amazonaws. <i>region</i> .events
Amazon FSx	com.amazonaws. <i>region</i> .fsx
<a href="#">AWS Key Management Service</a>	com.amazonaws. <i>region</i> .kms
<a href="#">Amazon Kinesis Data Streams</a>	com.amazonaws. <i>region</i> .kinesis-streams
<a href="#">AWS Lambda</a>	com.amazonaws. <i>region</i> .lambda
<a href="#">Amazon S3</a>	<p>com.amazonaws.<i>region</i>.s3 (RES でデフォルトで作成されるゲートウェイエンドポイントが必要です)。</p> <p>分離された環境でバケットをクロスマウントするには、追加の Amazon S3 インターフェイスエンドポイントが必要です。 <a href="#">「Amazon Simple Storage Service インターフェイスエンドポイントへのアクセス」</a> を参照してください。</p>

AWS のサービス	サービス名
<a href="#">AWS Secrets Manager</a>	com.amazonaws. <i>region</i> .secretsmanager
<a href="#">Amazon Elastic Container Service</a>	com.amazonaws. <i>region</i> .ecs
<a href="#">Amazon SES</a>	com.amazonaws. <i>region</i> .email-smtp (次のアベイラビリティゾーンではサポートされていません: use1-az2、use1-az3、use1-az5、usw1-az2、usw2-az4、apne2-az4、cac1-az3、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> .ec2messages com.amazonaws. <i>region</i> .ssm com.amazonaws. <i>region</i> .ssmmessages

## VPC エンドポイントのない サービスに接続する

VPC エンドポイントをサポートしていないサービスと統合するには、VPC のパブリックサブネットにプロキシサーバーを設定できます。ID プロバイダーとして AWS Identity Center を使用して、Research and Engineering Studio デプロイに必要な最小限のアクセス権を持つプロキシサーバーを作成するには、次の手順に従います。

- RES デプロイに使用する VPC のパブリックサブネットで Linux インスタンスを起動します。
  - Linux ファミリー – Amazon Linux 2 または Amazon Linux 3
  - アーキテクチャ – x86
  - インスタンスタイプ – t2.micro 以上
  - セキュリティグループ – 0.0.0.0/0 からのポート 3128 での TCP
- インスタンスに接続してプロキシサーバーを設定します。
  - http 接続を開きます。

- b. 関連するすべてのサブネットから次のドメインへの接続を許可します。
    - .amazonaws.com (汎用 AWS サービスの場合)
    - .amazoncognito.com (Amazon Cognito の場合)
    - .awsapps.com (アイデンティティセンター用)
    - .signin.aws (アイデンティティセンター用)
    - .amazonaws-us-gov.com ( Gov Cloud の場合)
  - c. 他のすべての接続を拒否します。
  - d. プロキシサーバーをアクティブ化して起動します。
  - e. プロキシサーバーがリッスンする PORT を書き留めます。
3. プロキシサーバーへのアクセスを許可するようにルートテーブルを設定します。
    - a. VPC コンソールに移動し、インフラストラクチャホストと VDI ホストに使用するサブネットのルートテーブルを特定します。
    - b. ルートテーブルを編集して、すべての着信接続が前のステップで作成したプロキシサーバーインスタンスに移動できるようにします。
    - c. これは、インフラストラクチャ/VDIs に使用するすべてのサブネット (インターネットアクセスなし) のルートテーブルに対して行います。
  4. プロキシサーバー EC2 インスタンスのセキュリティグループを変更し、プロキシサーバーがリッスンしている PORT でインバウンド TCP 接続が許可されていることを確認します。

## プライベート VPC デプロイパラメータを設定する

では [the section called “ステップ 1: 製品を起動する”](#)、CloudFormation テンプレートに特定のパラメータを入力することが期待されます。先ほど設定したプライベート VPC に正常にデプロイするには、次のパラメータを必ず設定してください。

パラメータ	Input
InfrastructureHostAMI	Use the infrastructure AMI ID created in <a href="#">the section called “Amazon マシンイメージ (AMIs) を準備する”</a> .
IsLoadBalancerInternetFacing	Set to false.

パラメータ	Input
LoadBalancerSubnets	Choose private subnets without internet access.
InfrastructureHostSubnets	Choose private subnets without internet access.
VdiSubnets	Choose private subnets without internet access.
ClientIP	You can choose your VPC CIDR to allow access for all VPC IP addresses.
HttpProxy	Example: <code>http://10.1.2.3:123</code>
HttpsProxy	Example: <code>http://10.1.2.3:123</code>

## パラメータ

NoProxy

## Input

例:

```
127.0.0.1,169.254.169.254,169.254.170.2,localhost,us-east-1.res,us-east-1.vpce.amazonaws.com,us-east-1.elb.amazonaws.com,s3.us-east-1.amazonaws.com,s3.dualstack.us-east-1.amazonaws.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
```


## 外部リソースを作成する

この CloudFormation スタックは、ネットワーク、ストレージ、アクティブディレクトリ、ドメイン証明書 (PortalDomainName が指定されている場合) を作成します。製品をデプロイするには、これらの外部リソースが必要です。

デプロイ前に [recipes テンプレートをダウンロード](#)できます。

デプロイ時間: 約 40 ~ 90 分

1. にサインイン AWS マネジメントコンソールし、<https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。


 Note

管理者アカウントにいることを確認します。

2. コンソールで[テンプレートを起動](#)します。

AWS GovCloud リージョンにデプロイする場合は、GovCloud パーティションアカウントでテンプレートを起動します ( AWS GovCloud (米国西部) リージョンの[場合](#)など )。

3. テンプレートパラメータを入力します。

 Important

AdminPassword と異なる値を使用してServiceAccountPassword、これらのアカウント間の適切なセキュリティ境界を維持します。

パラメータ	デフォルト	説明
DomainName	corp.res.com	アクティブディレクトリに使用されるドメイン。デフォルト値は、ブートストラップユーザーを設定する LDIF ファイルで提供されます。デフォルトユーザーを使用する場合は、値をデフォルトのままにします。値を変更するには、を更新して別のLDIFファイルを指定します。これは、アクティブディレクトリに使用されるドメイ

パラメータ	デフォルト	説明
		ンと一致する必要はありません。
SubDomain (GovCloud のみ)		<p>このパラメータは商用リージョンではオプションですが、GovCloud リージョンでは必須です。</p> <p>SubDomain を指定すると、パラメータには指定された DomainName のプレフィックスが付けられます。指定された Active Directory ドメイン名はサブドメインになります。</p>

パラメータ	デフォルト	説明
AdminPassword		<p>Active Directory 管理者のパスワード (ユーザー名 Admin)。このユーザーは、最初のブートストラップフェーズのアクティブディレクトリに作成され、その後は使用されません。</p> <p><b>重要:</b> このフィールドの形式は、(1) プレーンテキストのパスワード、または (2) キーと値のペアとしてフォーマットされた AWS シークレットの ARN のいずれかです <code>{"password": "somepassword"}</code>。</p> <p><b>注:</b> このユーザーのパスワードは、<a href="#">Active Directory のパスワードの複雑さの要件</a>を満たしている必要があります。</p>

パラメータ	デフォルト	説明
ServiceAccountPassword		<p>サービスアカウントの作成に使用されるパスワード (ReadOnlyUser )。このアカウントは同期に使用されます。</p> <p><b>重要:</b> このフィールドの形式は、(1) プレーンテキストのパスワード、または (2) キーと値のペアとしてフォーマットされた AWS シークレットの ARN のいずれかです <code>{"password":"somepassword"}</code> 。</p> <p><b>注:</b> このユーザーのパスワードは、<a href="#">Active Directory のパスワードの複雑さの要件</a>を満たしている必要があります。</p>
キーペア		<p>SSH クライアントを使用して管理インスタンスを接続します。</p> <p><b>注:</b> AWS Systems Manager Session Manager を使用してインスタンスに接続することもできます。</p>

パラメータ	デフォルト	説明
LDIFS3Path	aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif	<p>Active Directory セットアップのブートストラップフェーズ中にインポートされた LDIF ファイルへの Amazon S3 パス。詳細については、<a href="#">「LDIF サポート」</a>を参照してください。パラメータには、アクティブディレクトリに多数のユーザーを作成するファイルが事前に入力されています。</p> <p>ファイルを表示するには、GitHub で利用可能な <a href="#">res.ldif ファイル</a>を参照してください。</p>
ClientIpCidr		<p>サイトにアクセスする IP アドレス。例えば、IP アドレスを選択し、[IPADDRESS]/32 を使用してホストからのアクセスのみを許可できます。このデプロイ後に更新できます。</p>
ClientPrefixList		<p>プレフィックスリストを入力して、アクティブディレクトリ管理ノードへのアクセスを提供します。マネージドプレフィックスリストの作成については、<a href="#">「カスタマーマネージドプレフィックスリストの操作」</a>を参照してください。</p>

パラメータ	デフォルト	説明
EnvironmentName	res- <i>[environment name]</i>	PortalDomainName が指定されている場合、このパラメータを使用して生成されたシークレットにタグを追加し、環境内で使用できます。これは、RES スタックの作成時に使用された EnvironmentName パラメータと一致する必要があります。アカウントに複数の環境をデプロイする場合、これは一意である必要があります。
PortalDomainName		GovCloud デプロイの場合、このパラメータを入力しないでください。証明書とシークレットは、前提条件に従って手動で作成されました。 アカウントの Amazon Route 53 のドメイン名。これを指定すると、パブリック証明書とキーファイルが生成され、 にアップロードされます AWS Secrets Manager。独自のドメインと証明書がある場合は、このパラメータと を空白のままに EnvironmentName することができます。

- 機能のすべてのチェックボックスを確認し、スタックの作成を選択します。

## ステップ 1: 製品を起動する

このセクションのstep-by-stepの手順に従って、製品を設定してアカウントにデプロイします。

デプロイ時間: 約 60 分

この製品の [CloudFormation テンプレート](#)は、デプロイする前にダウンロードできます。

AWS GovCloud (米国西部) にデプロイする場合は、この[テンプレート](#)を使用します。

res-stack - このテンプレートを使用して、製品および関連するすべてのコンポーネントを起動します。デフォルト設定では、RES メインスタックと認証、フロントエンド、バックエンドリソースがデプロイされます。

### Note

AWS CloudFormation リソースは AWS Cloud Development Kit (AWS CDK) (AWS CDK) コンストラクトから作成されます。

AWS CloudFormation テンプレートは、の AWS に Research and Engineering Studio をデプロイします AWS クラウド。スタックを起動する前に、[前提条件](#)を満たす必要があります。

1. にサインイン AWS マネジメントコンソール し、<https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。
2. [テンプレート](#) を起動します。

AWS GovCloud (米国西部) にデプロイするには、この[テンプレート](#)を起動します。

3. テンプレートはデフォルトで米国東部 (バージニア北部) リージョンで起動します。別の でソリューションを起動するには AWS リージョン、コンソールナビゲーションバーのリージョンセレクターを使用します。

### Note

この製品では Amazon Cognito サービスを使用していますが、現在すべての で利用できるわけではありません AWS リージョン。この製品は、Amazon Cognito AWS リージョン が利用可能な で起動する必要があります。リージョン別の最新の可用性については、「[al AWS リージョン Services List](#)」を参照してください。

4. パラメータで、この製品テンプレートのパラメータを確認し、必要に応じて変更します。自動外部リソースをデプロイした場合、これらのパラメータは外部リソーススタックの出カタブにあります。

パラメータ	デフォルト	説明
EnvironmentName	<res-demo>	res- で始まり、11 文字以下、大文字を含まない RES 環境に与えられる一意の名前。
AdministratorEmail		製品のセットアップを完了したユーザーの E メールアドレス。さらに、このユーザーは、Active Directory シングルサインオン統合に障害が発生した場合、Break Glass ユーザーとして機能します。
InfrastructureHostAMI	ami-[#####]	(オプション) すべてのインフラストラクチャホストに使用するカスタム AMI ID を指定できます。現在サポートされている Oses は、Amazon Linux 2、Amazon Linux 2023、RHEL8、RHEL9、Windows Server 2019 および 2022 (x86)、Windows 10 および 11 です。詳細については、「 <a href="#">Amazon マシンイメージ (AMIs)を準備する</a> 」を参照してください。
SSHKeyPair		インフラストラクチャホストへの接続に使用されるキーペア。

パラメータ	デフォルト	説明
ClientIP	<code>x.x.x.0/24</code> または <code>x.x.x.0/32</code>	システムへの接続を制限する IP アドレスフィルター。デプロイ後に ClientIpCidr を更新できます。
ClientPrefixList		(オプション) 踏み台ホストへのウェブ UI と SSH への直接アクセスが許可されている IPs のマネージドプレフィックスリストを指定します。
IAMPermissionBoundary		(オプション) RES で作成されたすべてのロールにアクセス許可の境界としてアタッチされる管理ポリシー ARN を指定できます。詳細については、「 <a href="#">カスタムアクセス許可の境界の設定</a> 」を参照してください。
IAMResourcePrefix		(オプション) で終わる RES 環境によってデプロイされた IAM リソースに適用されるプレフィックス。12 文字以下。
IAMResourcePath	/	(オプション) で開始および終了する RES 環境によってデプロイされた IAM リソースに適用されるパス/。
VpcId		インスタンスが起動する VPC の ID。

パラメータ	デフォルト	説明
IsLoadBalancerInternetFacing		インターネット向けロードバランサーをデプロイするには true を選択します (ロードバランサーにはパブリックサブネットが必要です)。制限されたインターネットアクセスを必要とするデプロイの場合は、false を選択します。
LoadBalancerSubnets		ロードバランサーが起動する異なるアベイラビリティーゾーンで、少なくとも2つのサブネットを選択します。制限されたインターネットアクセスを必要とするデプロイの場合は、プライベートサブネットを選択します。インターネットアクセスが必要なデプロイの場合は、パブリックサブネットを選択します。外部ネットワークスタックによって3つ以上作成された場合は、作成されたすべてのサブネットを選択します。
InfrastructureHostSubnets		インフラストラクチャホストが起動する異なるアベイラビリティーゾーンで、少なくとも2つのプライベートサブネットを選択します。外部ネットワークスタックによって3つ以上作成された場合は、作成されたすべてのサブネットを選択します。

パラメータ	デフォルト	説明
VdiSubnets		VDI インスタンスが起動する異なるアベイラビリティーゾーンで、少なくとも2つのプライベートサブネットを選択します。外部ネットワークスタックによって3つ以上作成された場合は、作成されたすべてのを選択します。
ActiveDirectoryName	<i>corp.res.com</i>	アクティブディレクトリのドメイン。ポータルドメイン名と一致する必要はありません。
ADShortName	<i>corp</i>	アクティブディレクトリの短縮名。これは NetBIOS 名とも呼ばれます。
LDAP ベース	<b><i>DC=corp,DC=res,DC=com</i></b>	LDAP 階層内のベースへの LDAP パス。
LDAPConnectionURI		アクティブディレクトリのホストサーバーが到達できる単一の ldap:// パス。デフォルトの AD ドメインで自動外部リソースをデプロイした場合は、ldap://corp.res.com を使用できます。
ServiceAccountCredentialsSecretArn		Active Directory ServiceAccount ユーザーのユーザー名とパスワードを含むシークレット ARN を username: password のキーと値のペアとして指定します。

パラメータ	デフォルト	説明
UsersOU		同期するユーザーの AD 内の組織単位。
GroupsOU		同期するグループの AD 内の組織単位。
SudoersGroupName	RESAdministrators	インストール時にインスタンスへの sudoer アクセスと RES への管理者アクセスを持つすべてのユーザーを含むグループ名。
ComputersOU		インスタンスが参加する AD 内の組織単位。
DomainTLSCertificateSecretARN		(LDAPS に必須) AD への TLS 通信を有効にするためにドメイン TLS 証明書シークレット ARN を指定します。LDAPS を使用しない場合は空のままにします。
EnableLdapIDMapping		UID 番号と GID 番号が SSSD によって生成されるか、AD によって提供される番号を使用するかを決定します。SSSD が生成した UID と GID を使用するには True、AD が提供する UID と GID を使用するには False に設定します。ほとんどの場合、このパラメータは True に設定する必要があります。

パラメータ	デフォルト	説明
DisableADJoin	誤	Linux ホストがディレクトリドメインに参加しないようにするには、を True に変更します。それ以外の場合は、デフォルト設定の False のままにします。
ServiceAccountUserDN		Directory でサービスアカウントユーザーの識別名 (DN) を指定します。
SharedHomeFilesystemID		Linux VDI ホストの共有ホームファイルシステムに使用する EFS ID。
CustomDomainNameforWebApp		(オプション) システムのウェブ部分へのリンクを提供するためにウェブポータルで 사용되는サブドメイン。
CustomDomainNameforVDI		(オプション) システムの VDI 部分へのリンクを提供するためにウェブポータルで 사용되는サブドメイン。

パラメータ	デフォルト	説明
ACMCertificateARNforWebApp		(オプション) デフォルト設定を使用する場合、製品はドメイン amazonaws.com でウェブアプリケーションをホストします。ドメインで製品サービスをホストできます。自動外部リソースをデプロイした場合、これは自動的に生成され、情報は res-bi スタックの出力にあります。ウェブアプリケーションの証明書を生成する必要がある場合は、「」を参照してください <a href="#">設定ガイド</a> 。
CertificateSecretARNforVDI		(オプション) この ARN シークレットは、ウェブポータルパブリック証明書のパブリック証明書を保存します。自動外部リソースにポータルドメイン名を設定すると、res-bi スタックの出力タブにこの値が表示されます。
PrivateKeySecretARNforVDI		(オプション) この ARN シークレットは、ウェブポータルの証明書のプライベートキーを保存します。自動外部リソースにポータルドメイン名を設定すると、res-bi スタックの出力タブにこの値が表示されます。

パラメータ	デフォルト	説明
CognitoUserPoolId		ユーザー認証とクライアント認証用の Cognito ユーザープール。Cognito ユーザープールが指定されていない場合、RES はデフォルトで 1 つを作成します。
CognitoUserPoolDomainUrl		マネージドログイン用の Cognito ユーザープールドメイン。このパラメータ CognitoUserPoolId は、を指定するときに指定する必要があります。

5. スタックオプションの設定 → タグ - オプションで、RES デプロイされたリソースに適用するタグ (キーと値のペア) を追加します。タグキー Name と res:\* は RES によって保持され、タグキーとして使用することはできません。
6. [スタックの作成] を選択してスタックをデプロイします。

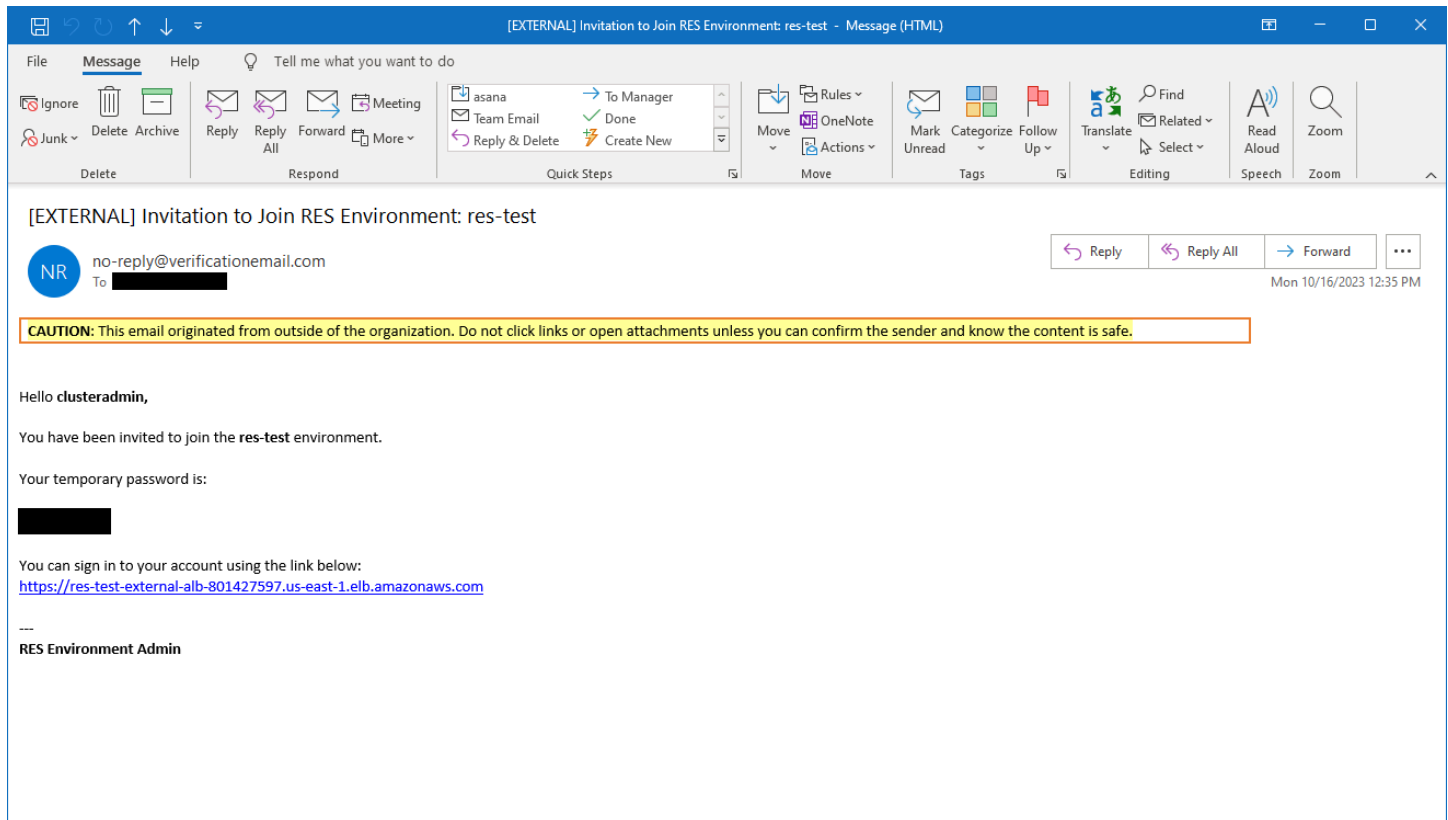
スタックのステータスは、AWS CloudFormation コンソールの Status 列で表示できます。約 60 分で CREATE\_COMPLETE ステータスが表示されます。

### Important

デプロイ後に infra / VDI ホストにパッチを適用するのはお客様の責任です。

## ステップ 2: 初めてサインインする

製品スタックがアカウントにデプロイされると、認証情報が記載された E メールが送信されます。URL を使用してアカウントにサインインし、他のユーザーのワークスペースを設定します。



初めてサインインしたら、ウェブポータルで SSO プロバイダーに接続するように設定することができます。デプロイ後の設定情報については、「 」を参照してください [設定ガイド](#)。clusteradmin はブレイクグラスアカウントです。これを使用してプロジェクトを作成し、それらのプロジェクトにユーザーまたはグループのメンバーシップを割り当てることができます。ソフトウェアスタックを割り当てたり、それ自体にデスクトップをデプロイしたりすることはできません。

# 製品を更新する

Research and Engineering Studio (RES) には、バージョン更新がメジャーかマイナーかに応じて、製品を更新する 2 つの方法があります。

RES は日付ベースのバージョニングスキームを使用します。メジャーリリースでは年と月が使用され、マイナーリリースでは必要に応じてシーケンス番号が追加されます。たとえば、バージョン 2024.01 はメジャーリリースとして 2024 年 1 月にリリースされました。バージョン 2024.01.01 はそのバージョンのマイナーリリース更新でした。

トピック

- [メジャーバージョンの更新](#)
- [マイナーバージョンの更新](#)

## メジャーバージョンの更新

Research and Engineering Studio は、スナップショットを使用して、環境設定を失うことなく、以前の RES 環境から最新の環境への移行をサポートします。このプロセスを使用して、ユーザーをオンボーディングする前に環境の更新をテストおよび検証することもできます。

環境を最新バージョンの RES で更新するには：

1. 現在の環境のスナップショットを作成します。「[the section called “スナップショットを作成する”](#)」を参照してください。
2. 新しいバージョンで RES を再デプロイします。「[the section called “ステップ 1: 製品を起動する”](#)」を参照してください。
3. 更新された環境にスナップショットを適用します。「[the section called “スナップショットを適用する”](#)」を参照してください。
4. 新しい環境に正常に移行されたすべてのデータを検証します。

## マイナーバージョンの更新

### Warning

RES バージョン 2025.06 から 2025.06.01 にアップグレードするには、[メジャーバージョンの更新](#)プロセスを使用する必要があります。

RES のマイナーバージョン更新の場合、新しいインストールは必要ありません。テンプレートを更新することで、既存の RES スタックを更新できます CloudFormation。更新をデプロイ CloudFormation する前に、で現在の RES 環境のバージョンを確認してください。テンプレートの先頭にバージョン番号があります。

例: "Description": "RES\_2024.1"

マイナーバージョンを更新するには：

1. 最新の CloudFormation テンプレートを にダウンロードします [the section called “ステップ 1: 製品を起動する”](#)。
2. <https://console.aws.amazon.com/cloudformation> で CloudFormation コンソールを開きます。
3. スタックから、プライマリスタックを検索して選択します。として表示されます `<stack-name>`。
4. [更新] を選択します。
5. 現在のテンプレートを置き換える を選択します。
6. [テンプレートソース] で、[テンプレートファイルのアップロード] を選択します。
7. ファイルの選択を選択し、ダウンロードしたテンプレートをアップロードします。
8. スタックの詳細を指定する で、次へ を選択します。パラメータを更新する必要はありません。
9. スタックオプションの設定 で、次へ を選択します。
10. レビュー `<stack-name>` で、送信を選択します。

# 製品のアンインストール

AWS 製品上の Research and Engineering Studio は、 から AWS マネジメントコンソール アンインストールするか、 を使用してアンインストールできます AWS Command Line Interface。この製品によって作成された Amazon Simple Storage Service (Amazon S3) バケットを手動で削除する必要があります。この製品は、保持するデータを保存している場合、<EnvironmentName>-shared-storage-security-group を自動的に削除しません。

## の使用 AWS マネジメントコンソール

1. [AWS CloudFormation コンソール](#) にサインインします。
2. スタックページで、この製品のインストールスタックを選択します。
3. [削除] を選択します。

## の使用 AWS Command Line Interface

AWS Command Line Interface ( AWS CLI) がお客様の環境で利用できるかどうかを確認します。インストール手順については、「AWS CLI ユーザーガイド」の「[AWS Command Line Interfaceとは](#)」を参照してください。AWS CLI が使用可能で、製品がデプロイされたリージョンの管理者アカウントに設定されていることを確認したら、次のコマンドを実行します。

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

## shared-storage-security-group の削除

### Warning

製品は、意図しないデータ損失から保護するために、このファイルシステムをデフォルトで保持します。セキュリティグループと関連するファイルシステムを削除すると、それらのシステム内に保持されているデータはすべて完全に削除されます。データをバックアップするか、新しいセキュリティグループにデータを再割り当てすることをお勧めします。

1. にサインイン AWS マネジメントコンソール し、「<https://console.aws.amazon.com/efs/>」で Amazon EFS コンソールを開きます。

2. に関連付けられているすべてのファイルシステムを削除します `<RES-stack-name>-shared-storage-security-group`。または、これらのファイルシステムを別のセキュリティグループに再割り当てして、データを維持することもできます。
3. にサインイン AWS マネジメントコンソールし、<https://console.aws.amazon.com/ec2/>://www.com で Amazon EC2 コンソールを開きます。
4. `<RES-stack-name>-shared-storage-security-group` を削除します。

## Amazon S3 バケットの削除

この製品は、偶発的なデータ損失を防ぐために AWS CloudFormation スタックを削除する場合、製品によって作成された Amazon S3 バケット (オプトインリージョンにデプロイする場合) を保持するように設定されています。製品をアンインストールした後、データを保持する必要がない場合は、この S3 バケットを手動で削除できます。Amazon S3 バケットを削除するには、次の手順に従います。

1. にサインイン AWS マネジメントコンソールし、「<https://console.aws.amazon.com/s3/>.com」で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで [バケット] を選択します。
3. `stack-name` S3 バケットを見つけます。
4. 各 Amazon S3 バケットを選択し、空を選択します。各バケットを空にする必要があります。
5. S3 バケットを選択し、続いて [削除] を選択します。

を使用して S3 バケットを削除するには AWS CLI、次のコマンドを実行します。

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

### Note

--force コマンドは、その内容のバケットを空にします。

# 設定ガイド

この設定ガイドでは、AWS 製品の Research and Engineering Studio をさらにカスタマイズして統合する方法に関するデプロイ後の手順について説明します。

## トピック

- [ID 管理](#)
- [サブドメインの作成](#)
- [ACM 証明書を作成する](#)
- [Amazon CloudWatch Logs](#)
- [カスタムアクセス許可の境界の設定](#)
- [RES 対応 AMIs を設定する](#)
- [RES のインストール後にカスタムドメインを設定する](#)

## ID 管理

Research and Engineering Studio は、SAML 2.0 準拠の任意の ID プロバイダーを使用できます。Amazon Cognito をネイティブユーザーディレクトリとして使用して、ユーザーが Cognito ユーザー ID を使用してウェブポータルと Linux ベースの VDI「」を参照してください[Amazon Cognito ユーザーのセットアップ](#)。外部リソースを使用して RES をデプロイした場合、または IAM アイデンティティセンターを使用する予定の場合は、「」を参照してください[IAM Identity Center でのシングルサインオン \(SSO\) の設定](#)。独自の SAML 2.0 準拠の ID プロバイダーがある場合は、「」を参照してください[シングルサインオン \(SSO\) 用の ID プロバイダーの設定](#)。

## トピック

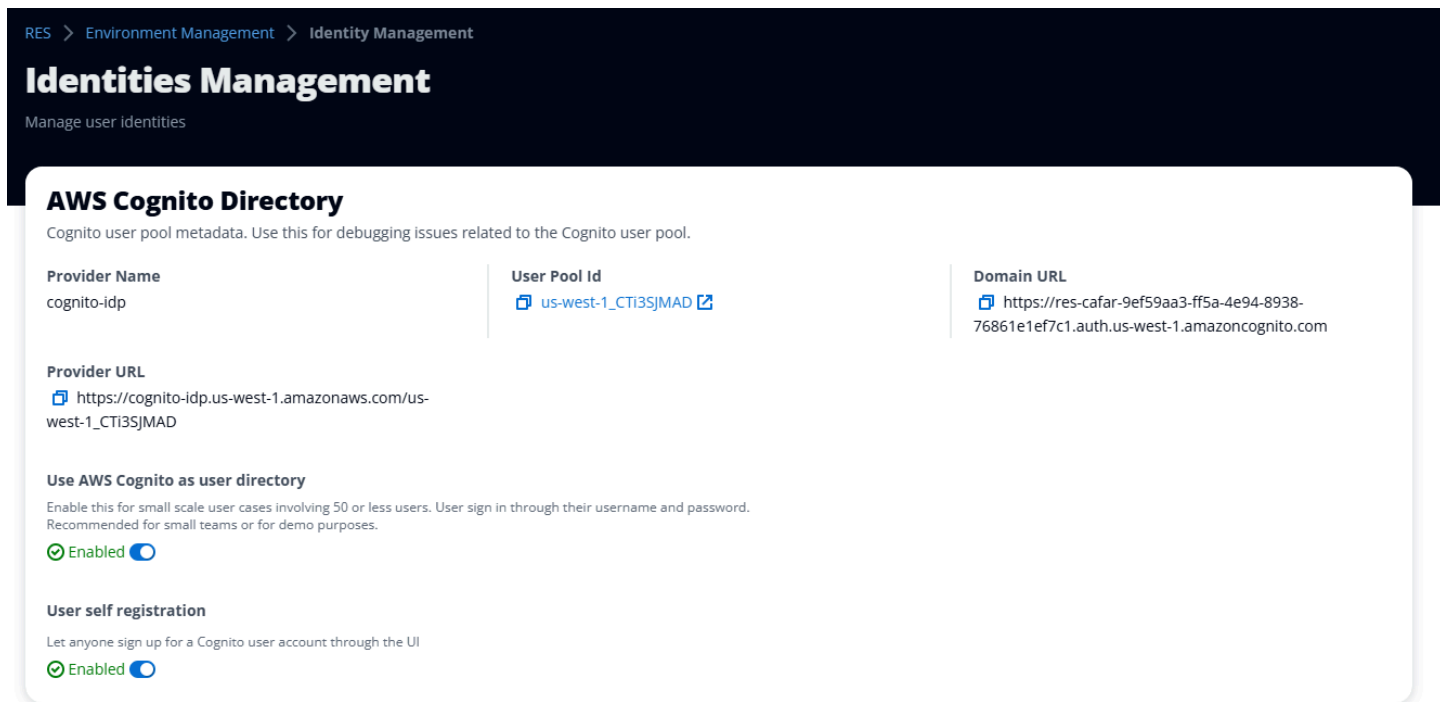
- [Amazon Cognito ユーザーのセットアップ](#)
- [Active Directory の同期](#)
- [IAM Identity Center でのシングルサインオン \(SSO\) の設定](#)
- [シングルサインオン \(SSO\) 用の ID プロバイダーの設定](#)
- [ユーザーのパスワードの設定](#)

## Amazon Cognito ユーザーのセットアップ

Research and Engineering Studio (RES) では、Amazon Cognito をネイティブユーザーディレクトリとして設定できます。これにより、ユーザーは Amazon Cognito ユーザー ID を使用してウェブポータルと Linux ベースの VDI にログインできます。管理者は、AWS コンソールの csv ファイルを使用して、複数のユーザーをユーザープールにインポートできます。一括ユーザーインポートの詳細については、[Amazon Cognito デベロッパーガイド](#)の「[CSV ファイルからユーザープールにユーザーをインポートする](#)」を参照してください。RES は、Amazon Cognito ベースのネイティブユーザーディレクトリと SSO を一緒に使用することをサポートしています。

### 管理の設定

RES 管理者として、Amazon Cognito をユーザーディレクトリとして使用するように RES 環境を設定するには、環境管理ページからアクセスできる ID 管理ページの Amazon Cognito をユーザーディレクトリとして使用するボタンに切り替えます。ユーザーが自己登録できるようにするには、同じページのユーザー自己登録ボタンを切り替えます。



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.

Provider Name cognito-idp	User Pool Id <a href="#">us-west-1_CT135JMAD</a>	Domain URL <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 <a href="https://cognito-idp.us-west-1.amazonaws.com/us-west-1_CT135JMAD">https://cognito-idp.us-west-1.amazonaws.com/us-west-1_CT135JMAD</a>		

**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

### ユーザーサインアップ/サインインフロー

ユーザー自己登録が有効になっている場合は、ウェブアプリケーションの URL をユーザーに付与できます。そこには、まだユーザーではないというオプションがあります。ここでサインアップします。

## 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.

## サインアップフロー

まだユーザーではないを選択するユーザー ここでサインアップすると、Eメールとパスワードを入力してアカウントを作成するように求められます。

## 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.

サインアップフローの一環として、ユーザーは E メールに受信した検証コードを入力してサインアッププロセスを完了するよう求められます。

## 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.

セルフサインアップが無効になっている場合、ユーザーにはサインアップリンクが表示されません。管理者は、RES の外部で Amazon Cognito のユーザーを設定する必要があります。(Amazon Cognito [デベロッパーガイド](#)の「[管理者としてのユーザーアカウントの作成](#)」を参照してください)。

## 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.

## ログインページのオプション

SSO と Amazon Cognito の両方が有効になっている場合、組織 SSO でサインインするオプションが表示されます。ユーザーがそのオプションをクリックすると、SSO ログインページに再ルーティングされます。デフォルトでは、有効になっている場合、ユーザーは Amazon Cognito で認証されます。

## 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.

### 制約

- Amazon Cognito グループ名は最大 6 文字で、小文字のみを使用できます。

- Amazon Cognito サインアップでは、同じユーザー名で異なるドメインアドレスを持つ 2 つの E メールアドレスは許可されません。
- Active Directory と Amazon Cognito の両方が有効で、システムが重複するユーザー名を検出した場合、Active Directory ユーザーのみが認証を許可されます。管理者は、Amazon Cognito と Active Directory の間に重複するユーザー名を設定しない手順を実行する必要があります。
- RES は Windows インスタンスの Amazon Cognito ベースの認証をサポートしていないため、Cognito ユーザーは Windows ベースの VDIs を起動できません。

## Amazon Cognito ユーザーの管理者グループ

デフォルトでは、RES はadminsグループ管理者権限を Cognito ユーザーに付与します。Cognito adminsグループにユーザーを追加するには:

1. [Amazon Cognito コンソール](#)に移動し、RES に使用される既存のユーザープールを選択します。
2. ユーザー管理でグループに移動し、グループの作成を選択します。
3. 「グループの作成」ページの「グループ名」に「」と入力しますadmins。
4. 作成したadminsグループを選択し、Add user to group を選択して Cognito ユーザーを追加します。
5. に従って Cognito 同期を手動で開始します[同期](#)。

Amazon Cognito の同期が成功すると、adminsグループに追加されたユーザーは管理者権限を受け取ります。

## 同期

RES は、データベースを Amazon Cognito のユーザーおよびグループ情報と 1 時間ごとに同期します。グループ「管理者VDIs で sudo 権限が付与されます。

Lambda コンソールから手動で同期を開始することもできます。

同期プロセスを手動で開始します。

1. [Lambda のコンソール](#)を開きます。
2. Cognito 同期 Lambda を検索します。この Lambda は、 という命名規則に従います `{RES_ENVIRONMENT_NAME}_cognito-sync-lambda`。
3. テスト を選択します。

4. テストイベントセクションで、右上のテストボタンを選択します。イベント本文の形式は関係ありません。

## Cognito のセキュリティに関する考慮事項

2024.12 リリース以前は、Amazon Cognito Plus プラン機能の一部である [ユーザーアクティビティのログ](#) 記録がデフォルトで有効になっていました。これをベースラインデプロイから削除して、RES を試したいお客様のコストを削減しました。この機能は、組織のクラウドセキュリティ設定に合わせて必要に応じて再度有効にすることができます。

## Active Directory の同期

### ランタイム設定

Active Directory (AD) に関連するすべての CFN パラメータは、インストール時にオプションです。

**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

実行時に提供されるシークレット ARN (例: ServiceAccountCredentialsSecretArnまたは DomainTLSCertificateSecretArn) については、RES のシークレットに次のタグを追加して、シークレット値を読み取るアクセス許可を取得してください。

- キー: res:EnvironmentName、値: *<your RES environment name>*
- キー: res:ModuleName、値: directoryservice

ウェブポータルでの AD 設定の更新は、次にスケジュールされた AD 同期 (時間単位) 中に自動的に取得されます。AD 設定を変更した後 (別の AD に切り替えた場合など)、ユーザーが SSO を再設定する必要がある場合があります。

初回インストール後、管理者は ID 管理ページの RES ウェブポータルで AD 設定を表示または編集できます。

### 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

<b>Domain Name</b> corp.res.com	<b>Short Name (NETBIOS)</b> CORP	<b>LDAP Base</b> dc=corp,dc=res,dc=com
<b>LDAP Connection URI</b> ldap://corp.res.com	<b>Service Account User DN</b> <a href="#">🔗</a> CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com	<b>Service Account Credentials Secret ARN</b> <a href="#">🔗</a> arn:aws:secretsmanager:us-east-1:905418417732:secret:CredentialsSecret-res-deploy-RESExternal-GZBSYJBLAW4-DirectoryService-1AUMFPSAPKV6E-TVYM7Q
<b>Users OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com	<b>Users Filter</b> -	<b>Groups OU</b> OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
<b>Groups Filter</b> -	<b>Sudoers Group Name</b> RESAdministrators	<b>Computers OU</b> OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
<b>Enable LDAP ID Mapping</b> true	<b>Disable AD Join</b> false	<b>Domain TLS Certificate Secret ARN</b> -

## 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.

### Automatically join Active Directory

Automatically joins Windows and Linux VDIs to your directory domain during launch. Windows instances require domain joining to launch successfully. If you disable this setting, you must implement custom domain-join logic in your Windows instance launch scripts. Linux instances can launch with or without domain joining.

### Organizational Units (OU)

Provide the Organizational Unit within AD that will sync.

#### Users OU

## Active Directory を自動的に結合する

管理者は、VDI の起動中にディレクトリドメインの結合動作を制御するように、Active Directory の自動結合を設定できます。

設定オプション:

- 有効 - 起動時に Windows および Linux VDIs をディレクトリドメインに自動的に結合します。
- 無効 - 自動ドメイン結合をオフにします。Linux インスタンスは、ドメイン結合の有無にかかわらず起動できます。Windows インスタンスが正常に起動するにはドメイン結合が必要なため、管理者はカスタム起動スクリプトにドメイン結合ロジックを含める必要があります。

### Important

この設定を無効にする場合は、Windows インスタンスのカスタム起動スクリプトに必要なドメイン結合ロジックが含まれていることを確認します。

## 詳細設定

### フィルター

管理者は、ユーザーフィルターオプションとグループフィルターオプションを使用して、同期するユーザーまたはグループをフィルタリングできます。フィルターは [LDAP フィルター構文](#) に従う必要があります。フィルターの例は次のとおりです。

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

### カスタム SSSD パラメータ

管理者は、クラスターインスタンスの SSSD 設定ファイルの [domain\_type/DOMAIN\_NAME] セクションに書き込む SSSD パラメータと値を含むキーと値のペアのディクショナリを提供できます。RES は SSSD 更新を自動的に適用します。クラスターインスタンスで SSSD サービスを再起動し、AD 同期プロセスをトリガーします。

一般的なカスタム SSSD 設定は次のとおりです。

- enumerate - ディレクトリサービスからすべてのユーザーエントリとグループエントリをキャッシュするには、「true」に設定します。これを無効にすると、ユーザーの初回ログインに短い遅延が生じる可能性があります。

- `ldap_id_mapping` - LDAP/AD ユーザー ID とグループ IDs にマッピングするには、「true」に設定します。UIDs GIDs これを有効にすると、既存の POSIX スクリプトやアプリケーションとの互換性が向上します。

SSSD 設定ファイルの詳細については、の Linux man ページを参照してくださいSSSD。

### Additional SSSD Configuration - *optional*

Provide additional SSSD configs for your AD domain.

**Key**

`ldap_id_mapping`

**Value**

true ▼

**Key**

`join_active_directory`

**Value**

true ▼

**Add Parameter**

SSSD パラメータと値は、以下に説明するように RES SSSD 設定と互換性がある必要があります。

- `id_provider` は RES によって内部的に設定されるため、変更しないでください。
- `ldap_uri`、`ldap_default_bind_dn` などの AD 関連の設定  
`ldap_default_auth_tok`は`ldap_search_base`、提供されている他の AD 設定に基づいて設定されるため、変更しないでください。

次の例では、SSSD ログのデバッグレベルを有効にします。

## Additional SSSD Configuration - optional

Provide additional SSSD configs for your AD domain.

**Key**

ldap\_id\_mapping

**Value**

true

**Key**

join\_active\_directory

**Value**

true

**Key**

debug\_level

**Value**

0xFFFF0

**Remove**

**Add Parameter**

### 初期 AD 同期後の E メール更新 (リリース 2025 年 9 月以降)

Active Directory ユーザーの E メールアドレスが変更された場合、管理者は手動で AD 同期を開始するか、次にスケジュールされた AD 同期で変更が取得されて RES に同期されるまで待機できます。

### 同期を手動で開始または停止する方法 (リリース 2025.03 以降)

ID 管理ページに移動し、Active Directory ドメインコンテナの「AD 同期の開始」ボタンを選択して、オンデマンドで AD 同期をトリガーします。

## 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-ISylRg

### 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

-

進行中の AD 同期を停止するには、Active Directory ドメインコンテナで AD 同期の停止ボタンを選択します。

## 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-ISylRg

### 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

-

Active Directory ドメインコンテナで AD 同期ステータスと最新の同期時間を確認することもできます。

### 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>		

## 同期を手動で実行する方法 (リリース 2024.12 および 2024.12.01)

Active Directory の同期プロセスは、Cluster Manager インフラストラクチャホストから、バックグラウンドで 1 回限りの Amazon Elastic Container Service (ECS) タスクに移動されました。このプロセスは 1 時間ごとに実行するようにスケジュールされており、クラスターの下で Amazon ECS コンソールで実行中の ECS *<res-environment-name>-ad-sync-cluster* タスクを見つけることができます。

手動で起動するには:

1. [Lambda コンソール](#)に移動し、*という名前の Lambda を検索します <res-environment>-scheduled-ad-sync*。
2. Lambda 関数を開き、テストに進む
3. イベント JSON に次のように入力します。

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

4. [テスト] を選択します。
5. CloudWatch → Log Groups → で実行中の AD Sync タスクのログを確認します/`<environment-name>/ad-sync`。実行中の各 ECS タスクのログが表示されます。ログを表示するには、最新の を選択します。

#### Note

- AD パラメータを変更したり、AD フィルターを追加したりすると、RES は新しく指定されたパラメータを指定して新しいユーザーを追加し、以前に同期され、LDAP 検索スペースに含まれなくなったユーザーを削除します。
- RES は、プロジェクトにアクティブに割り当てられたユーザー/グループを削除することはできません。RES でユーザーを環境から削除するには、プロジェクトからユーザーを削除する必要があります。

## SSO 設定

AD 設定が提供されたら、ユーザーは AD ユーザーとして RES ウェブポータルにログインできるように Single Sign-On (SSO) を設定する必要があります。SSO 設定が全般設定ページから新しい ID 管理ページに移動されました。SSO の設定の詳細については、「」を参照してください [ID 管理](#)。

## IAM Identity Center でのシングルサインオン (SSO) の設定

マネージド Active Directory に接続しているアイデンティティセンターがまだない場合は、 から始めます [ステップ 1: アイデンティティセンターを設定する](#)。マネージド Active Directory に接続されたアイデンティティセンターが既にある場合は、 から始めます [ステップ 2: アイデンティティセンターに接続する](#)。

#### Note

GovCloud リージョンにデプロイする場合は、Research and Engineering Studio を AWS GovCloud (US) デプロイしたパーティションアカウントに SSO を設定します。

## ステップ 1: アイデンティティセンターを設定する

### IAM アイデンティティセンターを有効にする

1. [AWS Identity and Access Management コンソール](#) にサインインします。
2. アイデンティティセンターを開きます。
3. [有効化] を選択します。
4. Enable with AWS Organizations を選択します。
5. [続行] をクリックしてください。

#### Note

マネージド Active Directory があるリージョンと同じリージョンにいることを確認します。

### IAM Identity Center をマネージド Active Directory に接続する

IAM Identity Center を有効にしたら、以下の推奨セットアップステップを完了します。

1. ナビゲーションペインで [設定] を選択します。
2. ID ソースで、アクションを選択し、ID ソースの変更を選択します。
3. 既存のディレクトリで、ディレクトリを選択します。
4. [次へ] を選択します。
5. 変更を確認し、確認ボックスに **ACCEPT** と入力します。
6. [IDソースの変更] を選択します。

### ユーザーとグループの ID センターへの同期

で行われた変更 [IAM Identity Center をマネージド Active Directory に接続する](#) が完了すると、緑色の確認バナーが表示されます。

1. 確認バナーで、ガイド付きセットアップの開始を選択します。
2. 属性マッピングの設定 から、次へ を選択します。
3. ユーザー セクションで、同期するユーザーを入力します。
4. [Add] (追加) を選択します。
5. [次へ] を選択します。

6. 変更を確認し、設定の保存を選択します。
7. 同期プロセスには数分かかる場合があります。同期していないユーザーに関する警告メッセージが表示された場合は、同期を再開を選択します。

## ユーザーの有効化

1. メニューから、ユーザーを選択します。
2. アクセスを有効にするユーザー (複数可) を選択します。
3. ユーザーアクセスを有効にするを選択します。

## ステップ 2: アイデンティティセンターに接続する

### IAM Identity Center でのアプリケーションのセットアップ

1. [IAM Identity Center コンソール](#) を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [アプリケーションの追加] を選択します。
4. セットアップ設定で、セットアップするアプリケーションがあるを選択します。
5. [アプリケーションタイプ] で、[SAML 2.0] を選択します。
6. [次へ] を選択します。
7. 使用する表示名と説明を入力します。
8. IAM Identity Center メタデータで、IAM Identity Center SAML メタデータファイルのリンクをコピーします。これは、RES ポータルで IAM Identity Center を設定するときに必要なになります。
9. アプリケーションプロパティで、アプリケーション開始 URL を入力します。例えば、<your-portal-domain>/sso。
10. Application ACS URL で、RES ポータルからリダイレクト URL を入力します。これを見つけるには:
  - a. 環境管理で、全般設定を選択します。
  - b. ID プロバイダータブを選択します。
  - c. Single Sign-On の下に、SAML リダイレクト URL が表示されます。
11. Application SAML audience で、Amazon Cognito URN を入力します。

URL を作成するには:

- a. RES ポータルから、全般設定を開きます。
- b. ID プロバイダータブで、ユーザープール ID を見つけます。
- c. ユーザープール ID をこの文字列に追加します。

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

12. Amazon Cognito URN を入力したら、送信を選択します。

### アプリケーションの属性マッピングの設定

1. アイデンティティセンターから、作成したアプリケーションの詳細を開きます。
2. アクション を選択し、属性マッピングの編集 を選択します。
3. [件名] に `#{user:email}` と入力します。
4. フォーマット で、emailAddress を選択します。
5. [新規属性マッピングの追加] を選択します。
6. アプリケーションの User 属性に「email」と入力します。
7. 「IAM Identity Center のこの文字列値またはユーザー属性にマップする」に「」と入力します `#{user:email}`。
8. Format に「unspecified」と入力します。
9. [Save changes] (変更の保存) をクリックします。

### IAM Identity Center でのアプリケーションへのユーザーの追加

1. アイデンティティセンターから、作成したアプリケーションの割り当て済みユーザーを開き、ユーザーの割り当てを選択します。
2. アプリケーションアクセスを割り当てるユーザーを選択します。
3. [ユーザーの割り当て] を選択します。

### RES 環境内での IAM Identity Center のセットアップ

1. Research and Engineering Studio 環境から、環境管理で全般設定を開きます。
2. ID プロバイダータブを開きます。
3. シングルサインオンで、編集 (ステータスの横) を選択します。

4. フォームに以下の情報を入力します。
  - a. SAML を選択します。
  - b. プロバイダー名に、わかりやすい名前を入力します。
  - c. Enter metadata document endpoint URL を選択します。
  - d. 中にコピーした URL を入力します [IAM Identity Center でのアプリケーションのセットアップ](#)。
  - e. Provider email 属性に「email」と入力します。
  - f. [Submit] を選択してください。
5. ページを更新し、ステータスが有効と表示されることを確認します。

## シングルサインオン (SSO) 用の ID プロバイダーの設定

Research and Engineering Studio は、任意の SAML 2.0 ID プロバイダーと統合して、RES ポータルへのユーザーアクセスを認証します。これらのステップでは、選択した SAML 2.0 ID プロバイダーと統合する手順を示します。IAM Identity Center を使用する場合は、「」を参照してください [IAM Identity Center でのシングルサインオン \(SSO\) の設定](#)。

### Note

ユーザーの E メールは、IDP SAML アサーションと Active Directory で一致する必要があります。ID プロバイダーを Active Directory に接続し、定期的にユーザーを同期する必要があります。


### トピック

- [ID プロバイダーを設定する](#)
- [ID プロバイダーを使用するように RES を設定する](#)
- [非本番環境での ID プロバイダーの設定](#)
- [SAML IdP の問題のデバッグ](#)

## ID プロバイダーを設定する

このセクションでは、RES Amazon Cognito ユーザープールからの情報を使用して ID プロバイダーを設定する手順について説明します。

1. RES は、RES ポータルとプロジェクトへのアクセスが許可されているユーザー ID を持つ AD (AWS マネージド AD またはセルフプロビジョニング AD) があることを前提としています。AD を ID サービスプロバイダーに接続し、ユーザー ID を同期します。AD を接続し、ユーザー ID を同期する方法については、ID プロバイダーのドキュメントを参照してください。例えば、「AWS IAM アイデンティティセンター ユーザーガイド」の「[ID ソースとしての Active Directory の使用](#)」を参照してください。
2. ID プロバイダー (IdP) で RES の SAML 2.0 アプリケーションを設定します。この設定には、次のパラメータが必要です。
  - SAML リダイレクト URL — IdP が SAML 2.0 レスポンスをサービスプロバイダーに送信するために使用する URL。


 Note

IdP によっては、SAML リダイレクト URL の名前が異なる場合があります。

- アプリケーション URL
- アサーションコンシューマーサービス (ACS) URL
- ACS POST バインディング URL

URL を取得するには

1. 管理者または clusteradmin として RES にサインインします。
  2. 環境管理 ⇒ 一般設定 ⇒ ID プロバイダーに移動します。
  3. SAML リダイレクト URL を選択します。
- SAML オーディエンス URI — サービスプロバイダー側の SAML オーディエンスエンティティの一意的 ID。

 Note

IdP によっては、SAML オーディエンス URI の名前が異なる場合があります。

- ClientID
- アプリケーション SAML 対象者

- SP エンティティ ID

入力を次の形式で指定します。

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

SAML オーディエンス URI を検索するには

1. 管理者または clusteradmin として RES にサインインします。
  2. 環境管理 ⇒ 一般設定 ⇒ ID プロバイダーに移動します。
  3. ユーザープール ID を選択します。
3. RES に投稿される SAML アサーションには、次のフィールド/クレームがユーザーの E メールアドレスに設定されている必要があります。
- SAML Subject または NameID
  - SAML E メール
4. IdP は、設定に基づいて SAML アサーションにフィールド/クレームを追加します。RES にはこれらのフィールドが必要です。ほとんどのプロバイダーは、デフォルトでこれらのフィールドを自動的に入力します。設定する必要がある場合は、次のフィールド入力と値を参照してください。
- AudienceRestriction — を に設定します `urn:amazon:cognito:sp:user-pool-id`。 `user-pool-id` を Amazon Cognito ユーザープールの ID に置き換えます。

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

- レスポンス — InResponseTo を に設定します `https://user-pool-domain/saml2/idpresponse`。 `user-pool-domain` を Amazon Cognito ユーザープールのドメイン名に置き換えます。

```
<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 — Recipient ユーザープールsaml2/idpresponseエンドポイントと元の SAML リクエスト ID InResponseToに設定します。

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

- AuthnStatement — 次のように を設定します。

```
<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. SAML アプリケーションにログアウト URL フィールドがある場合は、 に設定します *<domain-url>/saml2/logout*。

ドメイン URL を取得するには

1. 管理者または clusteradmin として RES にサインインします。
  2. 環境管理 ⇒ 一般設定 ⇒ ID プロバイダーに移動します。
  3. ドメイン URL を選択します。
6. IdP が Amazon Cognito との信頼を確立するために署名証明書を受け入れる場合は、Amazon Cognito 署名証明書をダウンロードし、IdP にアップロードします。

## 署名証明書を取得するには

1. [Amazon Cognito コンソール](#)を開きます。
2. ユーザープールを選択します。ユーザープールは `res-<environment name>-user-pool` である必要があります。
3. サインインエクスペリエンスタブを選択します。
4. フェデレーテッド ID プロバイダーのサインインセクションで、署名証明書の表示を選択します。

The screenshot shows the Amazon Cognito console interface. The top section is titled "Cognito user pool sign-in" and includes a description: "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." Below this, there are two tabs: "Cognito user pool sign-in options" (selected) and "User name requirements". The "Cognito user pool sign-in options" tab shows "User name" and "Email" as options. The "User name requirements" tab shows "User names are not case sensitive".

The bottom section is titled "Federated identity provider sign-in (1)" and includes a description: "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." Below this, there is a search bar "Search identity providers by name" and a table of identity providers. The table has columns for "Identity provider", "Identity provider type", "Created time", and "Last updated time". One provider is listed: "idc" with type "SAML", created "2 weeks ago", and last updated "3 hours ago".

この証明書を使用して、Active Directory IDP をセットアップし、 を追加しrelying party trust、この証明書利用者に対して SAML サポートを有効にできます。

### Note

これは Keycloak と IDC には適用されません。

5. アプリケーションのセットアップが完了したら、SAML 2.0 アプリケーションメタデータ XML または URL をダウンロードします。次のセクションで使用します。

## ID プロバイダーを使用するように RES を設定する

RES のシングルサインオン設定を完了するには

1. 管理者または clusteradmin として RES にサインインします。
2. 環境管理 ⇒ 一般設定 ⇒ ID プロバイダーに移動します。

## 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 Back >

### 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
-------------------	---------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------

- Single Sign-On で、ステータスインジケータの横にある編集アイコンを選択して Single Sign-On Configuration ページを開きます。

## 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)

- ID プロバイダーで、SAML を選択します。
- プロバイダー名には、ID プロバイダーの一意の名前を入力します。

**Note**

次の名前は使用できません。

- Cognito
- IdentityCenter

- c. メタデータドキュメントソースで、適切なオプションを選択し、メタデータ XML ドキュメントをアップロードするか、ID プロバイダーから URL を指定します。
  - d. プロバイダー E メール属性には、テキスト値 を入力します email。
  - e. [Submit] を選択してください。
4. 環境設定ページを再ロードします。設定が正しい場合、シングルサインオンが有効になります。

## 非本番環境での ID プロバイダーの設定

提供された[外部リソース](#)を使用して非本番環境の RES 環境を作成し、IAM Identity Center を ID プロバイダーとして設定した場合は、Okta などの別の ID プロバイダーを設定することをお勧めします。RES SSO 有効化フォームは、次の 3 つの設定パラメータを要求します。

1. プロバイダー名 — 変更できません
2. メタデータドキュメントまたは URL — 変更可能
3. プロバイダー E メール属性 — 変更可能

メタデータドキュメントとプロバイダー E メール属性を変更するには、次の手順を実行します。

1. [Amazon Cognito コンソール](#)に移動します。
2. ナビゲーションから、ユーザープールを選択します。
3. ユーザープールを選択すると、ユーザープールの概要が表示されます。
4. サインインエクスペリエンスタブから、フェデレーテッド ID プロバイダーのサインインに移動し、設定された ID プロバイダーを開きます。
5. 通常、メタデータを変更し、属性マッピングを変更しないだけで済みます。属性マッピングを更新するには、編集 を選択します。メタデータドキュメントを更新するには、メタデータの置き換えを選択します。

**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/MDg4ODM3NTczNjY0X2lucy04M2EyYUzZTFIMDI4</p>
---------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------

6. 属性マッピングを編集した場合は、DynamoDB で<environment name>.cluster-settingsテーブルを更新する必要があります。
  - a. DynamoDB コンソールを開き、ナビゲーションからテーブルを選択します。
  - b. <environment name>.cluster-settings テーブルを検索して選択し、アクションメニューから項目を探索を選択します。
  - c. スキャンまたはクエリ項目で、フィルターに移動し、次のパラメータを入力します。
    - 属性名 — key
    - 値 — identity-provider.cognito.sso\_idp\_provider\_email\_attribute
  - d. [Run] (実行) を選択します。
7. 返された項目 でidentity-provider.cognito.sso\_idp\_provider\_email\_attribute文字列を検索し、編集を選択して、Amazon Cognito の変更と一致するように文字列を変更します。

▼ **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	<b>Remove</b>

**Add filter**

**7**

**Run** **Reset**

Completed. Read capacity units consumed: 13

**Items returned (1)**

<input type="checkbox"/> key (String)
<input type="checkbox"/> <a href="#">identity-provider.cognito.ss</a>

**Edit String** **8**

email

Enter any string value.

**Cancel** **Save**

**Actions** ▼ **Create item**

< 1 > ⚙️ ✖️

▼ | version ▼

1

## SAML IdP の問題のデバッグ

SAML トレーサー — Chrome ブラウザでこの拡張機能を使用して SAML リクエストを追跡し、SAML アサーション値を確認できます。詳細については、Chrome ウェブストアの「[SAML トレーサー](#)」を参照してください。

SAML 開発者ツール — OneLogin には、SAML エンコードされた値をデコードし、SAML アサーションの必須フィールドをチェックするために使用できるツールが用意されています。詳細については、OneLogin ウェブサイトの「[Base 64 Decode + Inflate](#)」を参照してください。

Amazon CloudWatch Logs — CloudWatch Logs で RES ログのエラーや警告を確認できます。ログは、 という名前のロググループにあります `/res-environment-name/cluster-manager`。

Amazon Cognito ドキュメント — Amazon Cognito との SAML 統合の詳細については、「Amazon Amazon Cognito デベロッパーガイド」の [「ユーザープールへの SAML ID プロバイダーの追加」](#) を参照してください。

## ユーザーのパスワードの設定

1. [Directory Service コンソール](#)から、作成したスタックのディレクトリを選択します。
2. アクションメニューで、ユーザーパスワードのリセットを選択します。
3. ユーザーを選択し、新しいパスワードを入力します。
4. パスワードのリセットを選択します。

## サブドメインの作成

カスタムドメインを使用している場合は、ポータルウェブ部分と VDI 部分をサポートするようにサブドメインを設定する必要があります。

### Note

GovCloud リージョンにデプロイする場合は、ドメインパブリックホストゾーンをホストする商用パーティションアカウントでウェブアプリケーションと VDI サブドメインを設定します。

1. [Route 53 コンソール](#)を開きます。
2. 作成したドメインを検索し、レコードの作成を選択します。
3. レコード名として「web」と入力します。
4. レコードタイプとして CNAME を選択します。
5. Value には、最初の E メールで受け取ったリンクを入力します。
6. [レコードを作成] を選択します。
7. " のレコードを作成するには、NLB アドレスを取得します。
  - a. [AWS CloudFormation コンソール](#)を開きます。

- b. <environment-name>-vdc を選択してください。
  - c. リソースを選択し、 を開きます<environmentname>-vdc-external-nlb。
  - d. NLB から DNS 名をコピーします。
8. [Route 53 コンソール](#)を開きます。
  9. ドメインを検索し、レコードの作成を選択します。
  10. レコード名に「」と入力しますvdc。
  11. [レコードタイプ] で、[CNAME] を選択します。
  12. NLB の場合は、DNS を入力します。
  13. [Create record] (レコードを作成) を選択します。

## ACM 証明書を作成する

デフォルトでは、RES はドメイン amazonaws.com を使用してアプリケーションロードバランサーでウェブポータルをホストします。独自のドメインを使用するには、ユーザーが提供する、または AWS Certificate Manager (ACM) からリクエストされたパブリック SSL/TLS 証明書を設定する必要があります。ACM を使用する場合、クライアントとウェブサービスホスト間の SSL/TLS チャンネルを暗号化するためのパラメータとして指定する必要がある AWS リソース名を受け取ります。


### Tip

外部リソースデモパッケージをデプロイする場合は、 に外部リソーススタックをデプロイPortalDomainNameするとき、選択したドメインを に入力する必要があります[外部リソースを作成する](#)。

カスタムドメインの証明書を作成するには:

1. コンソールから [AWS Certificate Manager](#) を開き、パブリック証明書をリクエストします。GovCloud リージョンにデプロイする場合は、GovCloud パーティションアカウントに証明書を作成します。
2. 「パブリック証明書をリクエストする」を選択し、「次へ」を選択します。
3. ドメイン名で、 \*.PortalDomainNameと の両方の証明書をリクエストしますPortalDomainName。
4. 検証メソッドで、DNS 検証を選択します。

5. [リクエスト] を選択します。
6. Certificates リストから、リクエストされた証明書を開きます。各証明書のステータスは、検証保留中になります。

 Note

証明書が表示されない場合は、リストを更新します。

7. 次のいずれかを行います。
  - 商用デプロイ:
 

リクエストされた各証明書の証明書の詳細から、Route 53 でレコードを作成するを選択します。証明書のステータスは発行済みに変わります。
  - GovCloud デプロイ:
 

GovCloud リージョンにデプロイする場合は、CNAME キーと値をコピーします。商用パーティションアカウントから、値を使用してパブリックホストゾーンに新しいレコードを作成します。証明書のステータスは発行済みに変わります。
8. 新しい証明書 ARN をコピーして、 のパラメータとして入力します ACMCertificateARNforWebApp。

## Amazon CloudWatch Logs

Research and Engineering Studio は、インストール中に CloudWatch に次のロググループを作成します。デフォルトの保持については、次の表を参照してください。

CloudWatch Log グループ	Retention
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-endpoints	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-manager-scheduled-ad-sync	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -cluster-settings	有効期限なし

CloudWatch Log グループ	Retention
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -oauth-credentials	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -self-signed-certificate	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -update-cluster-prefix-list	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -vdc-scheduled-event-transformer	有効期限なし
/aws/lambda/ <i>&lt;installation-stack-name&gt;</i> -vdc-update-cluster-manager-client-scope	有効期限なし
<i>&lt;installation-stack-name&gt;</i> / cluster-manager	3 か月間
<i>&lt;installation-stack-name&gt;</i> /vdc/ controller	3 か月間
<i>&lt;installation-stack-name&gt;</i> /vdc/ dcv-broker	3 か月間
<i>&lt;installation-stack-name&gt;</i> /vdc/ dcv-connection-gateway	3 か月間

ロググループのデフォルトの保持を変更する場合は、[CloudWatch コンソール](#)に移動し、[CloudWatch Logs のログデータ保持を変更する](#) 指示に従ってください。

## カスタムアクセス許可の境界の設定

2024 年 4 月現在、オプションでカスタムアクセス許可の境界をアタッチすることで、RES によって作成されたロールを変更できます。カスタムアクセス許可の境界は、アクセス許可の境界の ARN を

IAMPermissionBoundary パラメータの一部として指定することで、RES CloudFormation のインストールの一部として定義できます。このパラメータを空のままにした場合、RES ロールにはアクセス許可の境界は設定されません。以下は、RES ロールが動作するために必要なアクションのリストです。使用する予定のアクセス許可の境界で、次のアクションが明示的に許可されていることを確認します。

```
[
  {
    "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:*",
"quicksight:*",
"rds-data:*",
"rds:*",
"redshift-data:*",
"redshift-serverless:*",
"redshift:*",
"rekognition:*",
"resiliencehub:*",
"resource-groups:*",
```

```
    "route53:*",
    "route53domains:*",
    "route53resolver:*",
    "rum:*",
    "s3:*",
    "sagemaker:*",
    "scheduler:*",
    "schemas:*",
    "sdb:*",
    "secretsmanager:*",
    "securityhub:*",
    "serverlessrepo:*",
    "servicecatalog:*",
    "servicequotas:*",
    "ses:*",
    "signer:*",
    "sns:*",
    "sqs:*",
    "ssm:*",
    "ssmmessages:*",
    "states:*",
    "storagegateway:*",
    "sts:*",
    "support:*",
    "tag:GetResources",
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "textract:*",
    "timestream:*",
    "transcribe:*",
    "transfer:*",
    "translate:*",
    "vpc-lattice:*",
    "waf-regional:*",
    "waf:*",
    "wafv2:*",
    "wellarchitected:*",
    "wisdom:*",
    "xray:*"
  ]
}
]
```

## RES 対応 AMIs を設定する

RES 対応 Amazon マシンイメージ (AMIs) を使用すると、仮想デスクトップインスタンス (VDIs) の RES 依存関係をカスタム AMIs にプリインストールできます。RES 対応 AMIs を使用すると、事前にバイクされたイメージを使用する VDI インスタンスの起動時間が短縮されます。EC2 Image Builder を使用すると、AMIs を構築して新しいソフトウェアスタックとして登録できます。Image Builder の詳細については、「[Image Builder ユーザーガイド](#)」を参照してください。

開始する前に、[最新バージョンの RES をデプロイ](#)する必要があります。

### Important

RES 2025.06.01 より前に作成された RES 対応 AMIs は、RES 2025.06.01 以降のすべてのバージョンと互換性がありません。RES 環境を 2025.06.01 より前のバージョンから最新のバージョンにアップグレードする場合は、すべての RES 対応 AMIs を再構築する必要があります。

### トピック

- [RES 環境にアクセスするための IAM ロールを準備する](#)
- [EC2 Image Builder コンポーネントを作成する](#)
- [EC2 Image Builder レシピを準備する](#)
- [EC2 Image Builder インフラストラクチャを設定する](#)
- [Image Builder イメージパイプラインを設定する](#)
- [Image Builder イメージパイプラインを実行する](#)
- [RES に新しいソフトウェアスタックを登録する](#)

## RES 環境にアクセスするための IAM ロールを準備する

EC2 Image Builder から RES 環境サービスにアクセスするには、RES-EC2InstanceProfileForImageBuilder という IAM ロールを作成または変更する必要があります。Image Builder で使用する IAM ロールの設定については、Image Builder ユーザーガイドの [AWS Identity and Access Management \(IAM\)](#) を参照してください。

ロールには以下が必要です。

- Amazon EC2 サービスを含む信頼された関係。

- AmazonS3ReadOnlyAccess、AmazonSSMManagedInstanceCore、EC2InstanceProfileForImageBuilder ポリシー。

## EC2 Image Builder コンポーネントを作成する

Image [Builder ユーザーガイドの「Image Builder コンソールを使用してコンポーネントを作成する」](#)の指示に従います。

コンポーネントの詳細を入力します。

1. Type で、Build を選択します。
2. イメージオペレーティングシステム (OS) の場合は、Linux または Windows を選択します。
3. コンポーネント名には、などのわかりやすい名前を入力します **research-and-engineering-studio-vdi-*<operating-system>***。
4. コンポーネントのバージョン番号を入力し、オプションで説明を追加します。

key : value

5. 定義ドキュメントには、次の定義ファイルを入力します。エラーが発生した場合、YAML ファイルはスペースに敏感であり、最も可能性の高い原因です。

### Important

定義ファイル **latest** で、RES 環境のバージョンが最新でない場合は、ダウンロード URI (- source: 's3://research-engineering-studio-us-east-1/releases/*latest*/res-installation-scripts.tar.gz') のを正確なバージョン番号 (例: **2025.06**) に置き換えます。

### 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:
  - GPUFamily:
    type: string
    description: GPU family (NONE, NVIDIA, or AMD)
    default: NONE
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://research-engineering-studio-us-east-1/releases/latest/
res-installation-scripts.tar.gz"
            destination: "/root/bootstrap/res-installation-scripts/res-
installation-scripts.tar.gz"
      - name: RunInstallScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - "cd /root/bootstrap/res-installation-scripts"
            - "tar -xf res-installation-scripts.tar.gz"
            - "cd scripts/virtual-desktop-host/linux"
```

```

        - "/bin/bash install.sh -g {{ GPUFamily }}"
    - name: RunInstallPostRebootScript
      action: ExecuteBash
      onFailure: Abort
      maxAttempts: 3
      inputs:
        commands:
          - "cd /root/bootstrap/res-installation-scripts/scripts/virtual-
desktop-host/linux"
          - 'sed -i ''/^export AWS_DEFAULT_PROFILE="bootstrap_profile"$/d''
install_post_reboot.sh'
          - "/bin/bash install_post_reboot.sh -g {{ GPUFamily }}"
    - name: PreventAL2023FromUninstallingCronie
      action: ExecuteBash
      onFailure: Abort
      maxAttempts: 3
      inputs:
        commands:
          - "rm -f /tmp/imagebuilder_service/crontab_installed"

```

## 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

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://research-engineering-studio-us-east-1/releases/
latest/res-installation-scripts.tar.gz'
      destination:
        '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res-installation-
scripts.tar.gz'
    - name: RunInstallScript
      action: ExecutePowerShell
      onFailure: Abort
      maxAttempts: 3
      inputs:
        commands:
          - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
          - 'tar -xf res-installation-scripts.tar.gz'
          - 'Import-Module .\scripts\virtual-desktop-host\windows
\Install.ps1'
          - 'Install-WindowsEC2Instance -PrebakeAMI'
```

6. オプションのタグを作成し、コンポーネントの作成を選択します。

## EC2 Image Builder レシピを準備する

EC2 Image Builder レシピでは、新しいイメージを作成するための開始点として使用するベースイメージと、イメージをカスタマイズしてすべてが期待どおりに動作することを確認するために追加する一連のコンポーネントを定義します。レシピを作成または変更して、必要な RES ソフトウェアの依存関係を持つターゲット AMI を構築する必要があります。レシピの詳細については、[「レシピの管理」](#)を参照してください。

RES は、次のイメージオペレーティングシステムをサポートしています。

- Amazon Linux 2 (x86 および ARM64)

- Amazon Linux 2023 (x86 および ARM64)
- RHEL 8 (x86)、および 9 (x86)
- Rocky Linux 9 (x86)
- Ubuntu 22.04.3 (x86)
- Ubuntu 24.04.3 (x86)
- Windows Server 2019、2022 (x86)
- Windows 10、11 (x86)

### Create a new recipe

1. で EC2 Image Builder コンソールを開きます <https://console.aws.amazon.com/imagebuilder>。
2. 保存済みリソースで、イメージレシピを選択します。
3. [イメージレシピの作成] を選択します。
4. 一意の名前とバージョン番号を入力します。
5. RES でサポートされているベースイメージを選択します。
6. インスタンス設定で、SSM エージェントがプリインストールされていない場合はインストールします。ユーザーデータおよびその他の必要なユーザーデータに情報を入力します。

#### Note

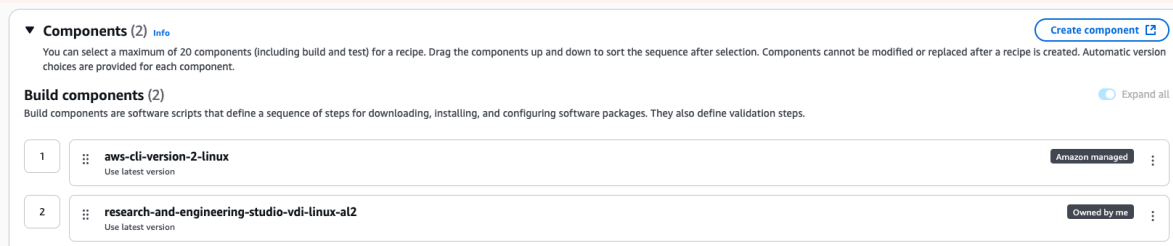
SSM エージェントをインストールする方法については、以下を参照してください。

- [Linux 用 EC2 インスタンスに SSM エージェントを手動でインストールします。](#)
- [Windows Server の EC2 インスタンスに SSM エージェントを手動でインストールおよびアンインストールします。](#)

7. Linux ベースのレシピの場合は、Amazon が管理する `aws-cli-version-2-linux` ビルドコンポーネントをレシピに追加します。Windows ベースのレシピの場合は、Amazon が管理する `aws-cli-version-2-windows` ビルドコンポーネントをレシピに追加します。RES インストールスクリプトはを使用して AWS CLI、DynamoDB クラスター設定の設定値への VDI アクセスを提供します。
8. Linux または Windows 環境用に作成された EC2 Image Builder コンポーネントを追加します。

**⚠ Important**

(Linux の場合) または `aws-cli-version-2-linux` (Windows の場合) ビルドコンポーネントを最初に追加した順序で `aws-cli-version-2-windows`、これらのコンポーネントを追加する必要があります。



- (推奨) Amazon が管理する `simple-boot-test-<linux-or-windows>` テストコンポーネントを追加して、AMI を起動できることを確認します。これは最小限の推奨事項です。要件を満たす他のテストコンポーネントを選択できます。
- 必要に応じてオプションのセクションを完了し、他の必要なコンポーネントを追加して、レシピの作成を選択します。

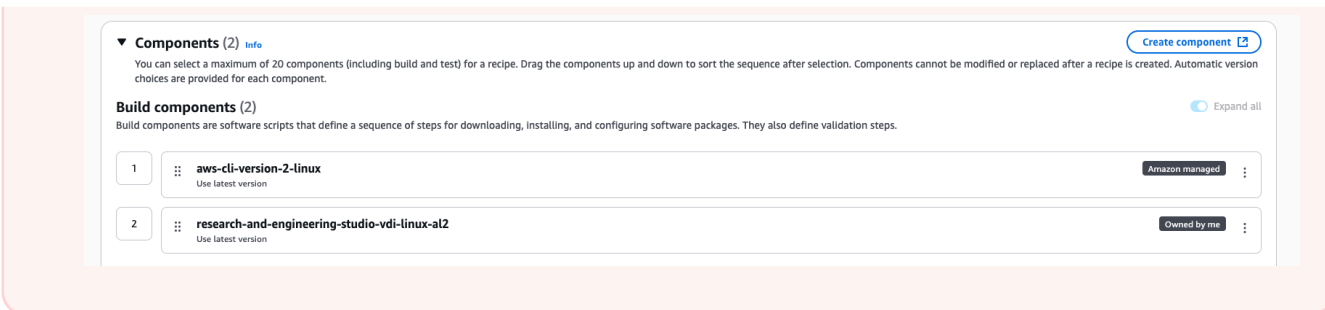
**Modify a recipe**

既存の EC2 Image Builder レシピがある場合は、次のコンポーネントを追加して使用できます。

- Linux ベースのレシピの場合は、Amazon が管理する `aws-cli-version-2-linux` ビルドコンポーネントをレシピに追加します。Windows ベースのレシピの場合は、Amazon が管理する `aws-cli-version-2-windows` ビルドコンポーネントをレシピに追加します。RES インストールスクリプトは を使用して AWS CLI、DynamoDB クラスター設定の設定値への VDI アクセスを提供します。
- Linux または Windows 環境用に作成された EC2 Image Builder コンポーネントを追加します。

**⚠ Important**

(Linux の場合) または `aws-cli-version-2-linux` (Windows の場合) ビルドコンポーネントを最初に追加した順序で `aws-cli-version-2-windows`、これらのコンポーネントを追加する必要があります。



- 必要に応じてオプションのセクションを完了し、他の必要なコンポーネントを追加して、レシピの作成を選択します。

## EC2 Image Builder インフラストラクチャを設定する

インフラストラクチャ設定を使用して、Image Builder が Image Builder イメージの構築とテストに使用する Amazon EC2 インフラストラクチャを指定できます。RES で使用するには、新しいインフラストラクチャ設定を作成するか、既存の設定を使用するかを選択できます。

- 新しいインフラストラクチャ設定を作成するには、[「インフラストラクチャ設定の作成」](#)を参照してください。
- 既存のインフラストラクチャ設定を使用するには、[インフラストラクチャ設定を更新します](#)。

Image Builder インフラストラクチャを設定するには:

- IAM ロールには、で以前に設定したロールを入力します[RES 環境にアクセスするための IAM ロールを準備する](#)。
- インスタンスタイプでは、少なくとも 4 GB のメモリを持つタイプを選択し、選択したベース AMI アーキテクチャをサポートします。[Amazon EC2 インスタンスタイプ](#)」を参照してください。
- VPC、サブネット、およびセキュリティグループの場合、ソフトウェアパッケージをダウンロードするためにインターネットアクセスを許可する必要があります。RES 環境の cluster-settings DynamoDB テーブルと Amazon S3 クラスターバケットへのアクセスも許可する必要があります。

## Image Builder イメージパイプラインを設定する

Image Builder イメージパイプラインは、ベースイメージ、構築とテスト用のコンポーネント、インフラストラクチャ設定、ディストリビューション設定を組み立てます。RES 対応 AMIs 用にイメー

ジパイプラインを設定するには、新しいパイプラインを作成するか、既存のパイプラインを使用するかを選択できます。詳細については、Image Builder ユーザーガイドの「[AMI イメージパイプラインの作成と更新](#)」を参照してください。

### Create a new Image Builder pipeline

1. で Image Builder コンソールを開きます <https://console.aws.amazon.com/imagebuilder>。
2. ナビゲーションペインから、イメージパイプラインを選択します。
3. 「イメージパイプラインの作成」を選択します。
4. 一意の名前、オプションの説明、スケジュール、頻度を入力して、パイプラインの詳細を指定します。
5. 「レシピを選択する」で、「既存のレシピを使用する」を選択し、「」で作成したレシピを選択します [EC2 Image Builder レシピを準備する](#)。レシピの詳細が正しいことを確認します。
6. イメージ作成プロセスを定義する では、ユースケースに応じてデフォルトワークフローまたはカスタムワークフローを選択します。ほとんどの場合、デフォルトのワークフローで十分です。詳細については、[EC2 Image Builder パイプラインのイメージワークフローを設定する](#)」を参照してください。
7. 「インフラストラクチャ設定の定義」で、「既存のインフラストラクチャ設定の選択」を選択し、「」で作成したインフラストラクチャ設定を選択します [EC2 Image Builder インフラストラクチャを設定する](#)。インフラストラクチャの詳細が正しいことを確認します。
8. ディストリビューション設定を定義する で、サービスのデフォルトを使用してディストリビューション設定を作成する を選択します。出カイメージは、RES 環境 AWS リージョンと同じに存在する必要があります。サービスのデフォルトを使用すると、Image Builder が使用されているリージョンにイメージが作成されます。
9. パイプラインの詳細を確認し、パイプラインの作成を選択します。

### Modify an existing Image Builder pipeline

1. 既存のパイプラインを使用するには、で作成されたレシピを使用するように詳細を変更します [EC2 Image Builder レシピを準備する](#)。
2. [Save changes] (変更の保存) をクリックします。

## Image Builder イメージパイプラインを実行する

設定された出カイメージを生成するには、イメージパイプラインを開始する必要があります。イメージレシピのコンポーネント数によっては、構築プロセスに最大 1 時間かかる場合があります。

イメージパイプラインを実行するには:

1. イメージパイプラインから、で作成されたパイプラインを選択します [Image Builder イメージパイプラインを設定する](#)。
2. アクションから、パイプラインの実行を選択します。

## RES に新しいソフトウェアスタックを登録する

1. 「」の指示に従って [the section called “ソフトウェアスタック \(AMIs\)”](#)、ソフトウェアスタックを登録します。
2. AMI ID には、に構築された出カイメージの AMI ID を入力します [Image Builder イメージパイプラインを実行する](#)。

## RES のインストール後にカスタムドメインを設定する

### Note

前提条件: これらのステップを実行する前に、Secrets Manager シークレットに Certificate と PrivateKey のコンテンツを保存する必要があります。

### ウェブクライアントに証明書を追加する

1. external-alb ロードバランサーのリスナーにアタッチされた証明書を更新します。
  - a. ECEC2 Load Balancing > Load Balancer の下の AWS コンソールで RES 外部ロードバランサーに移動します。
  - b. 命名規則に従うロードバランサーを検索します `<env-name>-external-alb`。
  - c. ロードバランサーにアタッチされているリスナーを確認します。
  - d. 新しい証明書の詳細がアタッチされたデフォルトの SSL/TLS 証明書を持つリスナーを更新します。

- e. 変更内容を保存します。
2. クラスター設定テーブルで、次の操作を行います。
    - a. DynamoDB -> Tables -> でクラスター設定テーブルを見つけます `<env-name>.cluster-settings`。
    - b. 属性で項目を検索してフィルタリングする – 名前「key」、タイプ「string」、条件「contains」、値「external\_alb」に移動します。
    - c. `True cluster.load_balancers.external_alb.certificates.provided`に設定します。
    - d. の値を更新します  
`cluster.load_balancers.external_alb.certificates.custom_dns_name`。  
これはウェブユーザーインターフェイスのカスタムドメイン名です。
    - e. の値を更新します  
`cluster.load_balancers.external_alb.certificates.acm_certificate_arn`。  
これは、Amazon Certificate Manager (ACM) に保存されている対応する証明書の Amazon リソースネーム (ARN) です。
  3. ウェブクライアント用に作成した対応する Route53 サブドメインレコードを更新して、外部 Alb ロードバランサーの DNS 名を指定します `<env-name>-external-alb`。
  4. SSO が環境に既に設定されている場合は、RES ウェブポータル環境管理 > ID 管理 > シングルサインオン > ステータス > 編集ボタンから最初に使用したのと同じ入力で SSO を再設定します。

### VDIs に証明書を追加する

1. シークレットに次のタグを追加して、シークレットに対して GetSecret オペレーションを実行するアクセス許可を RES アプリケーションに付与します。
  - `res:EnvironmentName : <env-name>`
  - `res:ModuleName : virtual-desktop-controller`
2. クラスター設定テーブルで、次の操作を行います。
  - a. DynamoDB -> Tables -> でクラスター設定テーブルを見つけます `<env-name>.cluster-settings`。
  - b. 属性で項目を検索してフィルタリングする – 名前「key」、タイプ「string」、条件「contains」、値「dcv\_connection\_gateway」に移動します。

- c. True `vdc.dcv_connection_gateway.certificate.provided`に設定します。
  - d. の値を更新します  
`vdc.dcv_connection_gateway.certificate.custom_dns_name`。これは VDI アクセスのカスタムドメイン名です。
  - e. の値を更新します  
`vdc.dcv_connection_gateway.certificate.certificate_secret_arn`。これは、証明書の内容を保持するシークレットの ARN です。
  - f. の値を更新します  
`vdc.dcv_connection_gateway.certificate.private_key_secret_arn`。これは、プライベートキーの内容を保持するシークレットの ARN です。
3. ゲートウェイインスタンスに使用される起動テンプレートを更新します。
    - a. EC2 > Auto Scaling > Auto Scaling Groups の下の AWS コンソールで Auto Scaling グループを開きます。
    - b. RES 環境に対応するゲートウェイの自動スケーリンググループを選択します。名前は命名規則に従います `<env-name>-vdc-gateway-asg`。
    - c. 詳細セクションで起動テンプレートを見つけて開きます。
    - d. 詳細 > アクション > テンプレートの変更 (新しいバージョンの作成) を選択します。
    - e. 下にスクロールして詳細を表示します。
    - f. 一番下のユーザーデータまでスクロールします。
    - g. `CERTIFICATE_SECRET_ARN` と の単語を探します `PRIVATE_KEY_SECRET_ARN`。これらの値を、証明書 (ステップ 2.c を参照) およびプライベートキー (ステップ 2.d を参照) の内容を保持するシークレットに指定された ARNs で更新します。
    - h. Auto Scaling グループが、(Auto Scaling グループページから) 最近作成されたバージョンの起動テンプレートを使用するように設定されていることを確認します。
  4. 仮想デスクトップ用に作成した対応する Route53 サブドメインレコードを更新して、外部 nlb ロードバランサーの DNS 名を指すようにします `<env-name>-external-nlb`。
  5. 既存の `dcv-gateway` インスタンスを終了 `<env-name>-vdc-gateway` し、新しいインスタンスがスピニングするのを待ちます。

# 管理者ガイド

この管理者ガイドでは、AWS 製品の Research and Engineering Studio をさらにカスタマイズして統合する方法に関する追加の手順を、技術的な対象者に提供します。

## トピック

- [シークレットの管理](#)
- [コストのモニタリングと制御](#)
- [コスト分析ダッシュボード](#)
- [セッション管理](#)
- [環境管理](#)

## シークレットの管理

Research and Engineering Studio は、を使用して次のシークレットを維持します AWS Secrets Manager。RES は、環境の作成時にシークレットを自動的に作成します。環境の作成時に管理者が入力したシークレットはパラメータとして入力されます。

シークレット名	説明	生成された RES	入力された管理者
<code>&lt;envname&gt; -sso-client-secret</code>	環境用のシングルサインオン OAuth2 クライアントシークレット	✓	
<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>	ドメインの自己署名証明書プライベートキー	✓	

シークレット名	説明	生成された RES	入力された管理者
<code>&lt;envname&gt; - vdc-gateway-certificate-certificate</code>	ドメインの自己署名証明書	✓	
<code>&lt;envname&gt; -cluster-manager-client-secret</code>	クラスターマネージャー ClientSecret	✓	
<code>&lt;envname&gt; -cluster-manager-client-id</code>	クラスターマネージャー ClientId	✓	
<code>&lt;envname&gt; -external-private-key</code>	ドメインの自己署名証明書プライベートキー	✓	
<code>&lt;envname&gt; -external-certificate</code>	ドメインの自己署名証明書	✓	
<code>&lt;envname&gt; -internal-private-key</code>	ドメインの自己署名証明書プライベートキー	✓	
<code>&lt;envname&gt; -internal-certificate</code>	ドメインの自己署名証明書	✓	
<code>&lt;envname&gt; -director-service-ServiceAccountUserDN</code>	ServiceAccount ユーザーの識別名 (DN) 属性。	✓	

DynamoDB の `<envname>-cluster-settings` テーブルには、次のシークレット ARN 値が含まれています。

Key	ソース
<code>identity-provider.cognito.sso_client_secret</code>	
<code>vdc.dcv_connection_gateway.certificate.certificate_secret_arn</code>	スタック
<code>vdc.dcv_connection_gateway.certificate.private_key_secret_arn</code>	スタック
<code>cluster.load_balancers.internal_alb.certificates.private_key_secret_arn</code>	スタック
<code>directoryservice.root_username_secret_arn</code>	
<code>vdc.client_secret</code>	スタック
<code>cluster.load_balancers.external_alb.certificates.certificate_secret_arn</code>	スタック
<code>cluster.load_balancers.internal_alb.certificates.certificate_secret_arn</code>	スタック
<code>directoryservice.root_password_secret_arn</code>	
<code>cluster.secretsmanager.kms_key_id</code>	
<code>cluster.load_balancers.external_alb.certificates.private_key_secret_arn</code>	スタック
<code>cluster-manager.client_secret</code>	

## コストのモニタリングと制御

### Note

Research and Engineering Studio プロジェクトの への関連付け AWS Budgets は、ではサポートされていません AWS GovCloud (US)。

Cost [AWS Cost Explorer](#)を使用して**予算**を作成し、コストを管理することをお勧めします。価格は変更されることがあります。詳細については、各の料金ウェブページを参照してください [the section called “AWS この製品の サービス”](#)。

コスト追跡を支援するために、RES プロジェクトを内部で作成された予算に関連付けることができます AWS Budgets。まず、請求コスト配分タグ内で環境タグをアクティブ化する必要があります。

1. AWS マネジメントコンソールにサインインし、[AWS 請求情報とコストマネジメントコンソール](#)を開きます。
2. コスト配分タグを選択します。
3. `res:Project` および `res:EnvironmentName` タグを検索して選択します。
4. [アクティブ化] を選択します。

The screenshot shows the AWS Cost Allocation Tags console. On the left is a navigation menu with 'Billing' selected. The main area is titled 'Cost allocation tags' and shows 'User-defined cost allocation tags (2/47)'. A search bar contains 'res' and shows '11 matches'. Below is a table of tags:

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**

RES タグがデプロイ後に表示されるまでに最大 1 日かかる場合があります。


RES リソースの予算を作成するには:

1. 請求コンソールから、予算を選択します。
2. 予算の作成を選択します。
3. [Budget setup] (予算の設定) で、[Customize (advanced)] (カスタマイズ (高度)) を選択します。
4. Budget types で、Cost budget - Recommended を選択します。
5. [次へ] を選択します。

The screenshot shows the AWS Billing console interface for creating a budget. On the left is a navigation menu with categories: Billing, Cost Management, Preferences, and Permissions. 'Budgets' is highlighted with a red circle and the number 1. The main content area is titled 'Choose budget type' and has a progress indicator on the left with 'Step 1 Choose budget type' selected. The 'Budget setup' section has two options: 'Use a template (simplified)' and 'Customize (advanced)' (3). The 'Budget types' section has four options: 'Cost budget - Recommended' (4), 'Usage budget', 'Savings Plans budget', and 'Reservation budget'. At the bottom right, there is a 'Next' button (5) and a 'Cancel' button.

6. 詳細 に、予算のわかりやすい Budget 名を入力して、アカウントの他の予算と区別します。例えば、`<EnvironmentName>-<ProjectName>-<BudgetName>`。
7. 予算額を設定する に、プロジェクトの予算額を入力します。

8. Budget scope で、Filter specific AWS cost dimensions を選択します。
9. [Add filter] (フィルターを追加) を選択します。
10. デイメンション で、タグ を選択します。
11. タグで、res:Project を選択します。

 Note

タグと値が使用可能になるまでに最大 2 日かかる場合があります。プロジェクト名が使用可能になったら、予算を作成できます。

12. 値 で、プロジェクト名を選択します。
13. フィルターを適用 を選択して、プロジェクトフィルターを予算にアタッチします。
14. [次へ] を選択します。

## 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. (オプション) アラートしきい値を追加します。
16. [次へ] を選択します。
17. (オプション) アラートが設定されている場合は、アタッチアクションを使用して、アラートで目的のアクションを設定します。
18. [次へ] を選択します。
19. 予算設定を確認し、追加の予算パラメータで正しいタグが設定されていることを確認します。
20. [予算を作成] をクリックします。

予算が作成されたら、プロジェクトの予算を有効にできます。プロジェクトの予算を有効にするには、「」を参照してください[the section called “プロジェクトを編集する”](#)。予算を超えると、仮想デスクトップの起動がブロックされます。デスクトップの起動中に予算を超えた場合、デスクトップは引き続き動作します。

Title	Project Code	Status	Budgets	Groups	Updated On
○ project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 <span style="color: red;">⊗</span> <span style="border: 1px solid red; border-radius: 5px; padding: 2px;">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

予算を変更する必要がある場合は、コンソールに戻って予算額を編集します。RES 内で変更が有効になるまでに最大 15 分かかる場合があります。または、プロジェクトを編集して予算を無効にすることもできます。

## コスト分析ダッシュボード

コスト分析ダッシュボードを使用すると、RES 管理者は RES ポータルからプロジェクトの予算とプロジェクトコストを経時的にモニタリングできます。コストはプロジェクトレベルでフィルタリングできます。

### トピック

- [前提条件](#)
- [予算割り当てグラフを持つプロジェクト](#)
- [経時的なコスト分析グラフ](#)

- [CSV をダウンロードする](#)

## 前提条件

Research and Engineering Studio のコストダッシュボードを使用するには、まず以下を行う必要があります。

- [プロジェクトの作成](#).
- [AWS Billing and Cost Management コンソール](#)で**予算**を作成します。
- 予算をプロジェクトにアタッチします (「」を参照[プロジェクトを編集する](#))。
- 新しい RES デプロイを持つアカウントのコスト分析チャートを有効にします。これを実行するには、以下の手順を実行します。
  1. 作成したプロジェクトに [VDI](#) をデプロイします。これにより、[AWS Cost Explorer](#) に `res:Project` タグがプロビジョニングされます。これには最大 24 時間かかる場合があります。
  2. タグが作成されると、タグを有効にするボタンが有効になります。ボタンを選択して、Cost Explorer でタグをアクティブ化します。このプロセスにはさらに 24 時間かかる場合があります。

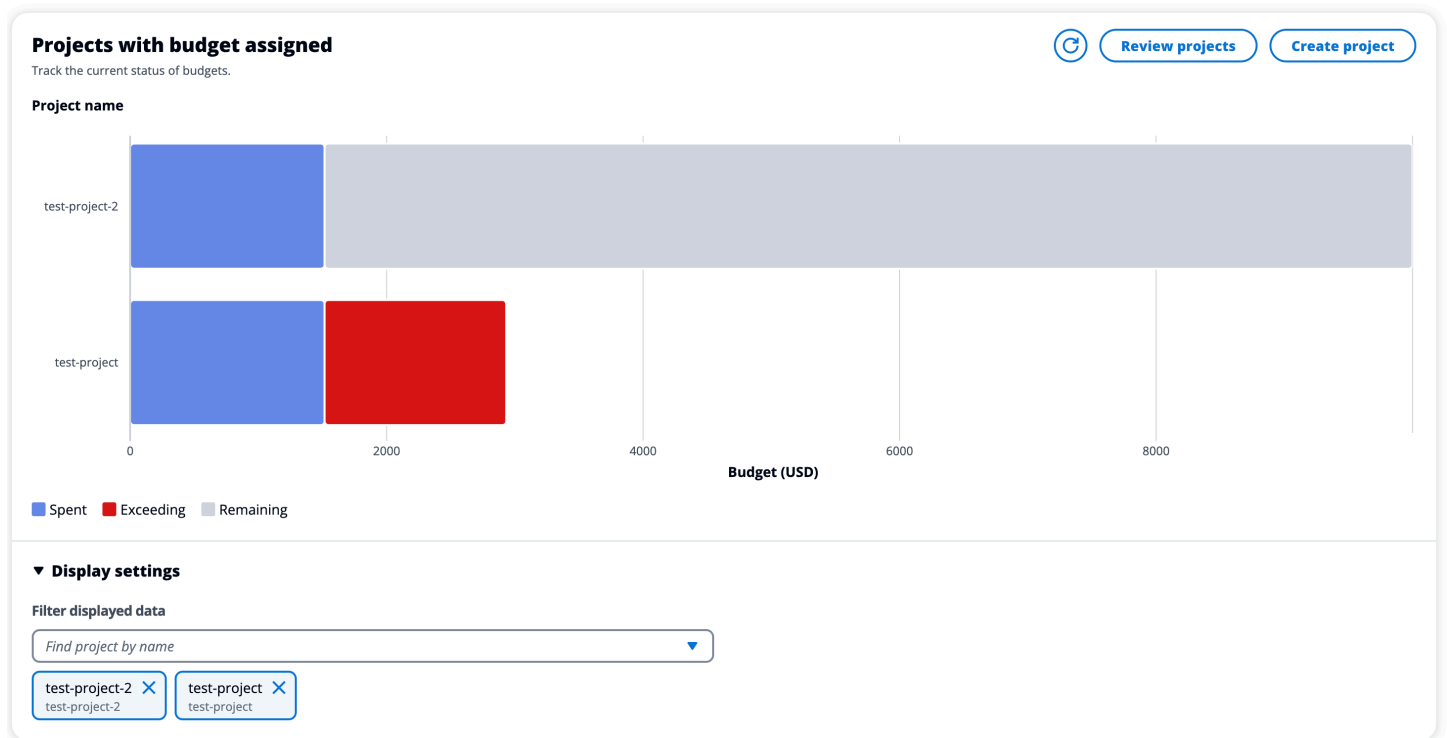
**Cost analysis onboarding** Info

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

<p><b>Step 1 - Launch desktop</b></p> <p>Launch your first desktop within this account and wait up to 24 hours for cost allocation tags to create.</p> <p><a href="#">Launch desktop</a></p>	<p><b>Step 2 - Enable cost tags</b></p> <p>Once tags are created, enable cost allocation tags for the web portal and wait another 24 hours for data to display.</p> <p><a href="#">Enable tags</a></p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 予算割り当てグラフを持つプロジェクト

予算が割り当てられているプロジェクトチャートには、予算が割り当てられている RES 環境のプロジェクトの予算ステータスが表示されます。デフォルトでは、グラフには予算額別に上位 5 つのプロジェクトが表示されます。予算に割り当てられたプロジェクトの完全なリストをロードするフィルター表示データドロップダウンで、特定のプロジェクトを選択できます。

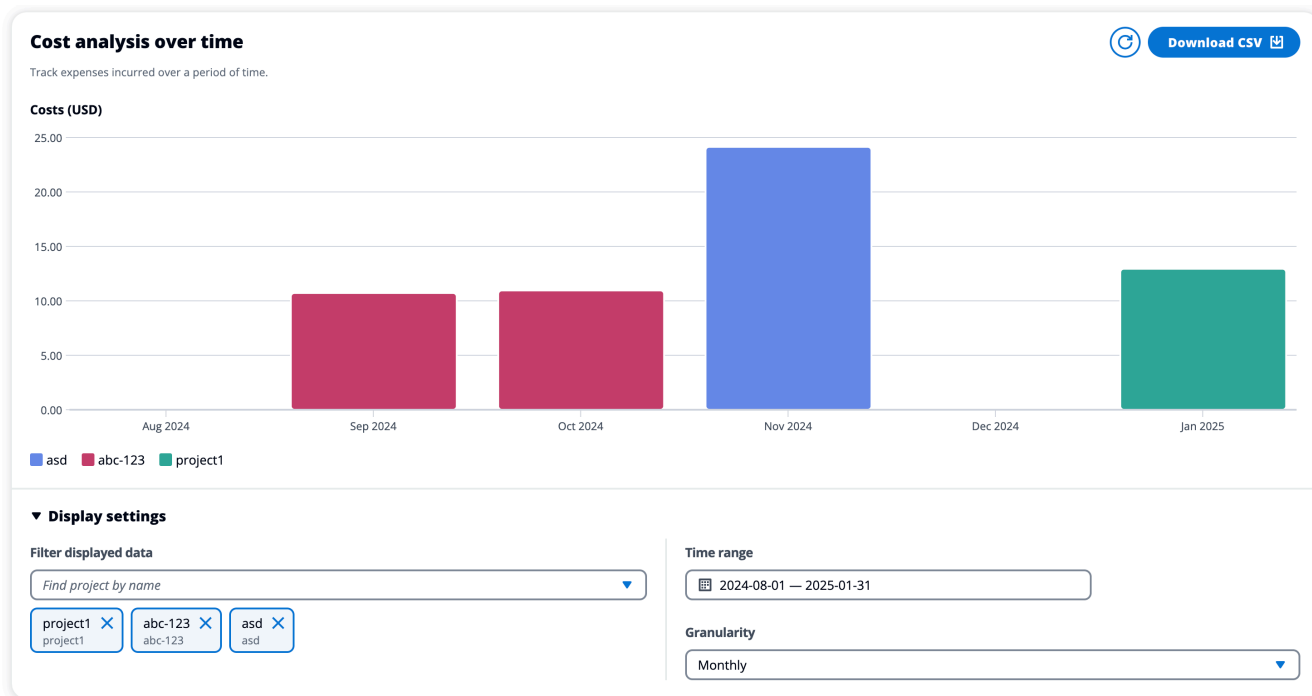


グラフには、各予算の支出額、残り額、超過額が米ドル通貨で表示されます。バーにカーソルを合わせると、各カテゴリの正確な USD 金額が表示されます。右上隅にあるプロジェクトの確認ボタンとプロジェクトの作成ボタンをそれぞれ選択して、プロジェクトページとプロジェクトの作成ページを開くこともできます。



## 経時的なコスト分析グラフ

経時的なコスト分析グラフには、指定した期間におけるプロジェクト別のコスト内訳が表示されます。デフォルトでは、グラフには過去 6 か月間のデータが表示されます。選択した粒度を使用して、選択した時間範囲の合計コストで上位 5 つのプロジェクトが表示されます。上位 5 つのプロジェクト以外の他のすべての選択したプロジェクトは、その他のカテゴリに集約されます。

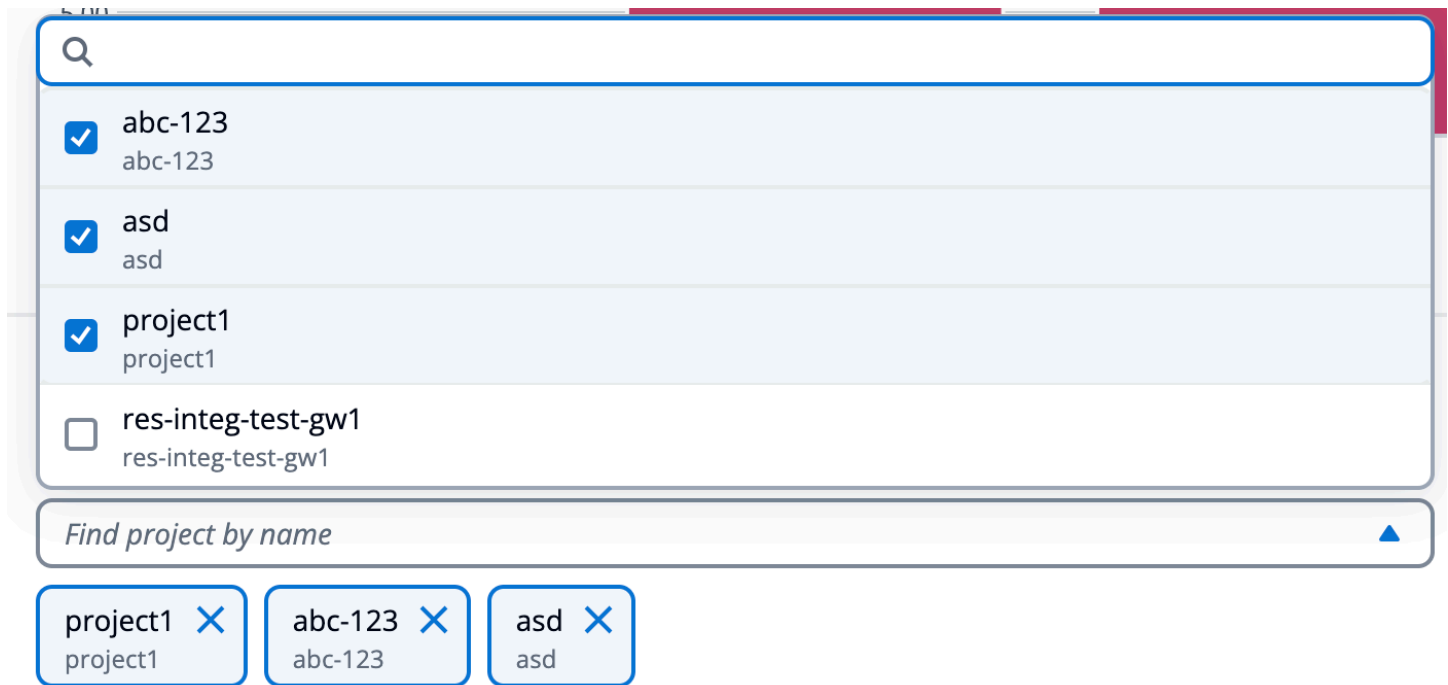


### フィルター

プロジェクト、時間範囲、粒度でフィルタリングして、経時的なコスト分析グラフビューをカスタマイズできます。無効なフィルターの組み合わせが選択されている場合、モーダルウィンドウが表示され、前の設定に戻すか、更新されたフィルターの組み合わせの提案を受け入れるかを選択できます。

### プロジェクト

Filter displayed data ドロップダウンを選択すると、現在の RES 環境のプロジェクトの完全なリストが表示されます。プロジェクト名が表示され、その下にプロジェクトコードが表示されます。



## 時間範囲の指定

日付範囲を指定するときは、絶対範囲または相対範囲を使用できます。相対範囲を選択すると、日付は完全な時間単位を使用して計算されます。たとえば、2025年2月に過去6か月のオプションを選択すると、～ 8/1/25 の時間範囲になります1/31/25。

**Relative range****Absolute range****Choose a range**

- Past 1 day
- Past 7 days
- Past 1 month
- Past 6 months
- Past 12 months
- Custom range  
Set a custom range in the past

**Clear****Cancel****Apply**

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

### 詳細度

月単位、日単位、または時間単位の粒度でデータを表示するように選択できます。時間単位の詳細度は、最大 14 日間の日付範囲のみをサポートします。日単位の詳細度は、最大 14 か月の日付範囲のみをサポートします。

Monthly
✓

Daily

Hourly

Monthly
▲

## CSV をダウンロードする

現在のコスト分析ビューをエクスポートするには、経時的なコスト分析グラフの右上にあるダウンロード CSV を選択します。ダウンロードした CSV には、指定された期間の選択した各プロジェクトのコスト情報と、プロジェクト別および期間別のコスト合計が含まれます。

	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						

## セッション管理

セッション管理は、セッションを開発およびテストするための柔軟でインタラクティブな環境を提供します。管理ユーザーとして、プロジェクト環境内でインタラクティブセッションを作成および管理することをユーザーに許可できます。

トピック

- [ダッシュボード](#)

- [セッション](#)
- [ソフトウェアスタック \(AMIs\)](#)
- [デバッグ](#)
- [デスクトップ設定](#)

# ダッシュボード

**Research and Engineering Studio** RES > Virtual Desktop > Dashboard demoadmin1

## Virtual Desktop Dashboard

7 View Sessions 8

**res-stage (us-west-2)**

- Home
  - Virtual Desktops
  - Shared Desktops
  - File Browser
  - SSH Access
- ADMIN ZONE
- eVDI
  - Dashboard**
  - Sessions
  - Software Stacks (AMIs)
  - Permission Profiles
  - Debug
  - Settings
- Environment Management

### Instance Types 1

Summary of all virtual desktop sessions by instance types.

Instance Type	Count
m6a.large	3

### Session State 2

Summary of all virtual desktop sessions by state.

Session State	Count
STOPPING	3

### Base OS 3

Summary of all virtual desktop sessions by Base OS.

Base OS	Count
Amazon Linux 2	2
Windows	1

### Project 4

Summary of all virtual desktop sessions by Project Code.

Project Code	Count
project1	3

### Availability Zones 5

Summary of all virtual desktop sessions by Availability Zone.

Availability Zone	Count
us-west-2a	3

### Software Stacks 6

Summary of all virtual desktop sessions by Software Stack.

Software Stack	No. of Sessions
Amazon Linux 2 - x86_64	2
Windows - x86_64	1

セッション管理ダッシュボードは、管理者に以下に関するクイックビューを提供します。

1. インスタンスのタイプ
2. セッションの状態
3. ベース OS
4. プロジェクト
5. アベイラビリティゾーン
6. ソフトウェアスタック

さらに、管理者は次のことができます。

7. ダッシュボードを更新して情報を更新します。
8. セッションの表示を選択してセッションに移動します。

## セッション

セッションには、Research and Engineering Studio 内で作成されたすべての仮想デスクトップが表示されます。セッションページから、セッション情報をフィルタリングして表示したり、新しいセッションを作成したりできます。

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 ▾ 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"/>	demoadmin1aml21 5	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. メニューを使用して、指定した期間内に作成または更新されたセッションで結果をフィルタリングします。
2. セッションを選択し、アクションメニューを使用して以下を行います。
  - a. セッションを再開する (複数可)

- b. 停止/休止セッション (複数可)
  - c. 強制停止/休止セッション (複数可)
  - d. セッションの終了 (複数可)
  - e. セッションの強制終了 (複数可)
  - f. セッションの状態 (複数可)
  - g. ソフトウェアスタックの作成
3. セッションの作成 を選択して新しいセッションを作成します。
  4. 名前でセッションを検索し、状態とオペレーティングシステムでフィルタリングします。
  5. セッション名を選択すると、詳細が表示されます。

## セッションを作成する

1. セッションの作成 を選択します。新しい仮想デスクトップの起動モーダルが開きます。
2. 新しいセッションの詳細を入力します。
3. (オプション) Show Advanced Options をオンにして、サブネット ID や DCV セッションタイプなどの追加の詳細を指定します。
4. [Submit] を選択してください。

# 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

## セッションの詳細

セッションリストから、セッション名を選択してセッションの詳細を表示します。

The screenshot shows the 'Session: demoadmin1aml21' details page. At the top, there is a breadcrumb trail: 'RES > Virtual Desktop > Sessions > 8765705b-8919-48ba-901a-19e2c49cf043'. The main title is 'Session: demoadmin1aml21'. Below this is a 'General Information' section with a table:

Session Name	Owner	State
demoadmin1aml21	demoadmin1	Stopped

Below the 'General Information' section is a navigation bar with tabs: 'Details', 'Server', 'Software Stack', 'Project', 'Permissions', 'Schedule', 'Monitoring', and 'Session'. The 'Details' tab is selected. Below the navigation bar is a 'Session Details' section with a table:

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

## ソフトウェアスタック (AMIs)

ソフトウェアスタックページから、Amazon マシンイメージ (AMIs) を設定したり、既存のイメージを管理したりできます。

RES > Virtual Desktops > Software Stacks (AMIs)

## Software Stacks

Manage your Virtual Desktop Software Stacks

Search  All Operating Systems ▼ < 1 2 > ⚙️

	Name	Description	AMI ID / Systems Manager Parameter A...	Base OS	Root Volume Size	Min RA...
<input type="radio"/>	RHEL8 - x86_64	RHEL8 - x86_64	ami-01955109048f9b11d	RedHat Enterprise Linux 8	50GB	4GB
<input type="radio"/>	UBUNTU2204 - x86_64	UBUNTU2204 - x86_64	ami-09ac0b140f63d3458	Ubuntu 22.04	50GB	4GB
<input type="radio"/>	Windows - x86_64	Windows - x86_64	ami-06244562918e090e8	Windows	50GB	4GB
<input type="radio"/>	Windows - AMD	Windows - AMD	ami-0c204e78e7e8c343b	Windows	50GB	4GB
<input type="radio"/>	Windows - NVIDIA	Windows - NVIDIA	ami-06871ff48caabe79e	Windows	50GB	4GB
<input type="radio"/>	RHEL9 - x86_64	RHEL9 - x86_64	ami-0a74a0465cdeea9b3	RedHat Enterprise Linux 9	50GB	4GB
<input type="radio"/>	Amazon Linux 2 - ARM64	Amazon Linux 2 - ARM64	ami-0f27f8ea8f8bd937c	Amazon Linux 2	50GB	4GB
<input type="radio"/>	Amazon Linux 2 - x86_64	Amazon Linux 2 - x86_64	ami-0ad253013fad0a42a	Amazon Linux 2	50GB	4GB
<input type="radio"/>	AL2023 - ARM64	AL2023 - ARM64	ami-0aaf509a1ebd95e61	Amazon Linux 2023	50GB	4GB
<input type="radio"/>	AL2023 - x86_64	AL2023 - x86_64	ami-08a6efd148b1f7504	Amazon Linux 2023	50GB	4GB

< 1 2 >

1. 既存のソフトウェアスタックを検索するには、オペレーティングシステムのドロップダウンを使用して OS でフィルタリングします。
2. ソフトウェアスタックの名前を選択して、スタックの詳細を表示します。
3. ソフトウェアスタックの横にあるラジオボタンを選択し、アクションメニューを使用してスタックを編集し、スタックをプロジェクトに割り当てます。
4. ソフトウェアスタックの登録ボタンを選択して、新しいスタックを作成します。

## 新しいソフトウェアスタックを登録する

ソフトウェアスタックの登録ボタンを使用すると、新しいスタックを作成できます。

### Note

暗号化されていない Systems Manager パラメータをソフトウェアスタック ID のエイリアスとして使用できます。

Systems Manager パラメータにアクセスするには、RES に次のタグが必要です。

- キー: `res:EnvironmentName`、値: `<your RES environment name>`
- キー: `res:ModuleName`、値: `virtual-desktop-controller`

1. ソフトウェアスタックの登録を選択します。
2. 新しいソフトウェアスタックの詳細を入力します。
3. [Submit] を選択してください。

## 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 / Systems Manager Parameter ARN

Enter the AMI ID or Systems Manager Parameter ARN

AMI ID must start with ami-xxx. Systems Manager Parameter ARN must follow the ARN format

### 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

### Tenancy

The type of tenancy

ソフトウェアスタック (AMIs)

## プロジェクトにソフトウェアスタックを割り当てる

新しいソフトウェアスタックを作成するときに、スタックをプロジェクトに割り当てることができます。ただし、最初の作成後にスタックをプロジェクトに追加する必要がある場合は、次の操作を行います。

### Note

ソフトウェアスタックは、自分がメンバーであるプロジェクトにのみ割り当てることができます。

1. ソフトウェアスタックページで、プロジェクトに追加するソフトウェアスタックのラジオボタンを選択します。
2. [アクション] を選択します。
3. [編集] を選択します。
4. プロジェクトドロップダウンを使用してプロジェクトを選択します。

## Update Software Stack: AL2023 - 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

### AMI ID / Systems Manager Parameter ARN

Enter the AMI ID or Systems Manager Parameter ARN

AMI ID must start with ami-xxx. Systems Manager Parameter ARN must follow the ARN format

### 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

### Tenancy

The type of tenancy

ソフトウェアスタック (AMIs)

### Allowed Instance Families and Types

## 5. [Submit] を選択してください。

スタックの詳細ページからソフトウェアスタックを編集することもできます。

### ソフトウェアスタックの VDI インスタンスリストを変更する

登録されたソフトウェアスタックごとに、許可されるインスタンスファミリーとタイプを選択できます。各ソフトウェアスタックのオプションのリストは、デスクトップ設定で定義されたオプションによってフィルタリングされます。グローバルの許可されたインスタンスファミリーとタイプを検索して変更できます。

The screenshot displays the 'Review the virtual desktop settings' page in the Research and Engineering Studio. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation menus for 'Desktops', 'Session management', and 'Environment management'. The main content area shows the configuration for a 'virtual-desktop-controller' module. The 'Server' tab is selected, displaying settings for 'Session' and 'DCV Host'. The 'Session' section includes 'Idle Timeout' (43200 minutes), 'CPU Utilization Threshold' (30%), 'Transition State' (Stop), and 'Enforce Schedule' (Yes). The 'DCV Host' section includes 'Allowed Security Groups' (empty), 'Max Root Volume Size' (1000 GB), 'Allowed Instance Families and Types' (g4ad, g4dn, g5, m6a, t3, m6g), and 'Denied Instance Types' (empty).

ソフトウェアスタックの許可されたインスタンスファミリーとタイプの属性を編集するには:

1. ソフトウェアスタックページで、ソフトウェアスタックのラジオボタンを選択します。
2. アクションを選択し、スタックの編集を選択します。
3. ドロップダウンリストから、許可されたインスタンスファミリーとタイプのドロップダウンリストから目的のインスタンスファミリーとタイプを選択します。

## Update Software Stack: AL2023 - 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

### AMI ID / Systems Manager Parameter ARN

Enter the AMI ID or Systems Manager Parameter ARN

AMI ID must start with ami-xxx. Systems Manager Parameter ARN must follow the ARN format

### 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

### Tenancy

The type of tenancy

ソフトウェアスタック (AMIs)

### Allowed Instance Families and Types

#### 4. [送信] を選択します。

##### Note

許可されたインスタンスファミリーとタイプのグローバルセットにインスタンスファミリーとそのファミリー内のインスタンスタイプ ( t3や などt3.large) が含まれている場合、ソフトウェアスタックの許可されたインスタンスファミリーとタイプの属性で利用できるオプションには、インスタンスファミリーのみが含まれます。

##### Important

- インスタンスタイプ/ファミリーが環境レベルで許可リストから削除されると、すべてのソフトウェアスタックから自動的に削除されます。
- 環境レベルで追加されたインスタンスタイプ/ファミリーは、ソフトウェアスタックに自動的に追加されません。

### ソフトウェアスタックの詳細を表示する

ソフトウェアスタックページから、ソフトウェアスタック名を選択して詳細を表示します。ソフトウェアスタックのラジオボタンを選択し、アクションを選択し、編集を選択してソフトウェアスタックを編集することもできます。

### VDI テナンスのサポート

新しいソフトウェアスタックを登録するとき、または既存のソフトウェアスタックを編集するとき、このソフトウェアスタックから起動された VDI のテナンシーを選択できます。次の 3 つのテナンシーがサポートされています。

- 共有 (デフォルト) - 共有ハードウェアインスタンスで VDI を実行する
- 専用インスタンス - 専用インスタンスを使用して VDI を実行する
- Dedicated Host - 専用ホストを使用して VDI を実行する

## 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 / Systems Manager Parameter ARN

Enter the AMI ID or Systems Manager Parameter ARN

AMI ID must start with ami-xxx. Systems Manager Parameter ARN must follow the ARN format

### 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

### Tenancy

The type of tenancy

ソフトウェアスタック (AMIs)

専用ホストテナンシータイプを選択するときは、テナンシーアフィニティとターゲットホストタイプも選択する必要があります。次のターゲットホストタイプがサポートされています。

- ホストリソースグループ - AWS License Manager で作成されたホストリソースグループ
- ホスト ID - 特定のホスト ID

### 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

専用ホストテナンシーで起動するときに VDI s に必要なセルフマネージドライセンスを指定するには、License AWS Manager ユーザーガイドの[セルフマネージドライセンスと AMI の関連付けに従って、ライセンスを AMIs に関連付け](#)ます。

## Rocky Linux 9 ソフトウェアスタックの追加

RES には Rocky Linux 9 用のデフォルトのソフトウェアスタックがないため、このセクションでは、使用する Rocky AMI とその使用方法に関する推奨事項を提供します。

1. AWS コンソールにログインし、EC2 コンソール内の [AMI Catalog ページ](#) に移動します。
2. Rocky Linux 9 という名前の AWS Marketplace タブで AMIs を検索します。
3. Rocky Linux から Rocky Linux 9 (公式) - x86\_64 という名前の AMI を選択します。

**Rocky Linux 9 (Official) - x86\_64**By [Rocky Linux](#) | Ver 9.5.20241118

★★★★☆ 3 AWS reviews

**Select**

Starting from \$0.00 to \$0.00/hr for software + AWS usage fees

Rocky Linux is a free, open, community enterprise operating system designed to be 100% bug-for-bug compatible with the top upstream enterprise Linux distribution. Built by the community, for the community. With fully open and transparent development, there's plenty of opportunity for anyone to...

4. 選択したら、今すぐサブスクライブを選択します。
5. 上にスクロールし、選択した AMI の AMI ID をコピーします。

**AMI Catalog**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

**AMIs**

Selected AMI: (ami-0a73e96a849c232cc)

[Create Template with AMI](#)[Launch Instance with AMI](#)

Rocky Linux 9

**Quick Start AMIs (0)**  
Commonly used AMIs**My AMIs (176)**  
Created by me**AWS Marketplace AMIs (589)**  
AWS & trusted third-party AMIs**Community AMIs (500)**  
Published by anyone

6. RES ポータルに移動し、この AMI を使用して Software Stacks ページの下に新しい Software Stack を登録します。

## デバッグ

デバッグパネルには、仮想デスクトップに関連付けられたメッセージトラフィックが表示されます。このパネルを使用して、ホスト間のアクティビティを監視できます。VD ホストタブにはインスタンス固有のアクティビティが表示され、VD セッションタブには進行中のセッションアクティビティが表示されます。

## ▼ 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": "aXAtMTAtMy0xNTctMTk0LmNvcnAucmVzLmNvbS0xMC4zLjE1Ny4xOTQ0tNmRmYjJmNWYyYTQ4NDExN2E1MzgwZDU4YjIzM2I2Zjg="
      "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
          
```

## デスクトップ設定

デスクトップ設定ページを使用して、仮想デスクトップに関連付けられたリソースを設定できます。

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 -

## 全般

全般タブでは、次のような設定にアクセスできます。

## QUIC

すべての仮想デスクトップのデフォルトのストリーミングプロトコルとして TCP を優先して QUIC を有効にします。

### デフォルトの DCV セッションタイプ

すべての仮想デスクトップに使用されるデフォルトの DCV セッションタイプ。この設定は、以前に作成したデスクトップには適用されません。これは、インスタンスタイプとオペレーティングシステムが仮想セッションタイプまたはコンソールセッションタイプのいずれかをサポートしている場合にのみ適用されます。

### プロジェクトごとにユーザーごとに許可されるデフォルトのセッション

プロジェクトごとにユーザーごとに許可される VDI セッション数のデフォルト値。

## サーバー

サーバータブでは、次のような設定にアクセスできます。

### DCV セッションアイドルタイムアウト

DCV セッションが自動的に切断されるまでの時間。これにより、デスクトップセッションの状態は変更されず、DCV クライアントまたはウェブブラウザからのみセッションが閉じられます。

### アイドルタイムアウトの警告

アイドル警告がクライアントに提供されるまでの時間。

### CPU 使用率のしきい値

アイドルと見なされる CPU 使用率。

### 最大ルートボリュームサイズ

仮想デスクトップセッションのルートボリュームのデフォルトサイズ。

### 許可されたインスタンスタイプ

この RES 環境で起動できるインスタンスファミリーとサイズのリスト。インスタンスファミリーとインスタンスサイズの組み合わせの両方が受け入れられます。たとえば、「m7a」を指定すると、m7a ファミリーのすべてのサイズが VDI セッションとして起動できるようになります。'm7a.24xlarge' を指定した場合、VDI セッションとして起動できるのは m7a.24xlarge のみです。このリストは、環境内のすべてのプロジェクトに影響します。

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

## 環境管理

Research and Engineering Studio の環境管理セクションから、管理ユーザーは研究およびエンジニアリングプロジェクト用に分離された環境を作成および管理できます。これらの環境には、コンピューティングリソース、ストレージ、その他の必要なコンポーネントを含めることができ、すべて安全な環境内にあります。ユーザーは、プロジェクトの特定の要件を満たすようにこれらの環境を設定およびカスタマイズできるため、他のプロジェクトや環境に影響を与えることなく、ソリューションの実験、テスト、反復が容易になります。

### トピック

- [環境ステータス](#)
- [環境設定](#)
- [\[ユーザー\]](#)
- [グループ](#)
- [プロジェクト](#)
- [アクセス許可ポリシー](#)
- [ファイルシステム](#)

- [スナップショットの管理](#)
- [Amazon S3 バケット](#)

## 環境ステータス

環境ステータスページには、製品内にデプロイされたソフトウェアとホストが表示されます。これには、ソフトウェアバージョン、モジュール名、その他のシステム情報などの情報が含まれます。

**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	-

## 環境設定

環境設定ページには、次のような製品設定の詳細が表示されます。

- General

製品をプロビジョニングしたユーザーの管理者ユーザー名や E メールなどの情報を表示します。ウェブポータルタイトルと著作権テキストを編集できます。

- ID プロバイダー

シングルサインオンステータスなどの情報を表示します。

- Network

アクセス用の VPC ID、プレフィックスリスト IDs を表示します。

- Directory Service

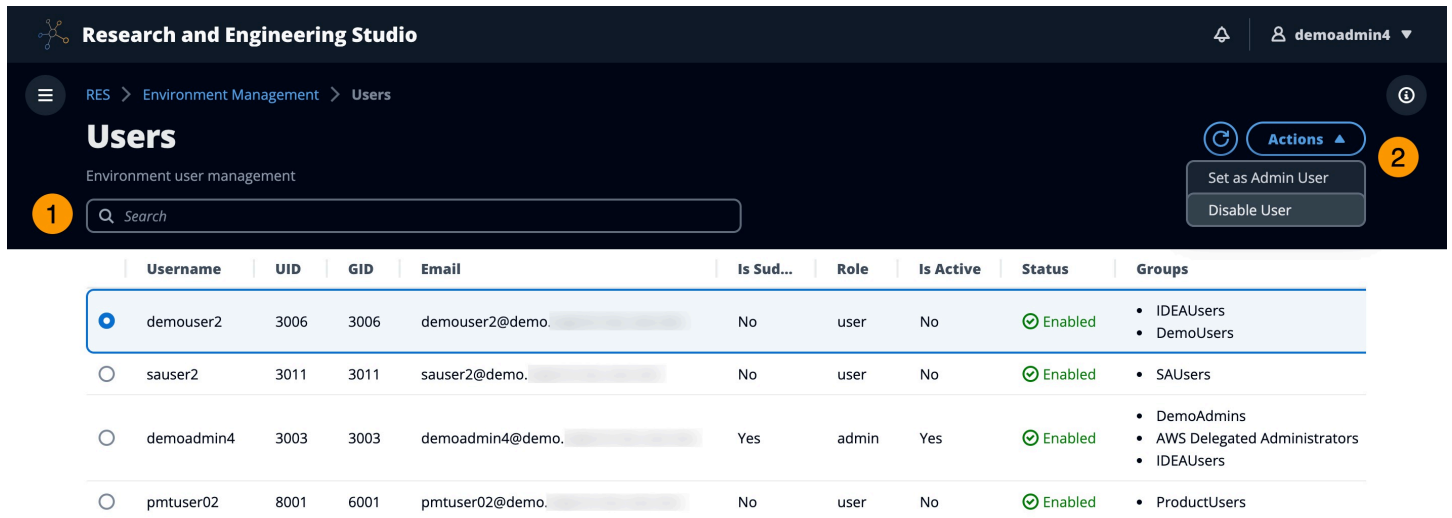
ユーザー名とパスワードのアクティブディレクトリ設定とサービスアカウントのシークレットマネージャー ARN を表示します。

## [ユーザー]

アクティブディレクトリから同期されたすべてのユーザーがユーザーページに表示されます。ユーザーは、製品の設定中に cluster-admin ユーザーによって同期されます。初期ユーザー設定の詳細については、「」を参照してください [設定ガイド](#)。

### Note

管理者は、アクティブなユーザーのセッションのみを作成できます。デフォルトでは、すべてのユーザーは製品環境にサインインするまで非アクティブ状態になります。ユーザーが非アクティブの場合は、セッションを作成する前にサインインするように依頼します。



Research and Engineering Studio

RES > Environment Management > Users

## Users

Environment user management

1 Search

2 Actions

- Set as Admin User
- Disable User

	Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
<input checked="" type="radio"/>	demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"><li>IDEAUsers</li><li>DemoUsers</li></ul>
<input type="radio"/>	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"><li>SAUsers</li></ul>
<input type="radio"/>	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></ul>
<input type="radio"/>	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	<ul style="list-style-type: none"><li>ProductUsers</li></ul>

ユーザーページから、次のことができます。

1. ユーザーを検索します。
2. ユーザー名を選択したら、アクションメニューを使用して次の操作を行います。
  - a. 管理者ユーザーとして設定する
  - b. ユーザーを無効にする

## グループ

アクティブディレクトリから同期されたすべてのグループは、グループページに表示されます。グループの設定と管理の詳細については、「」を参照してください [設定ガイド](#)。

**Research and Engineering Studio**

RES > Environment Management > Groups

**Groups**

Environment user group management

Search

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

**Users in IDEAUsers**

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>SAAAdmins</li> </ul>	10/3

グループページから、次のことができます。

1. ユーザーグループを検索します。
2. ユーザーグループを選択したら、アクションメニューを使用してグループを無効または有効にします。
3. ユーザーグループを選択すると、画面の下部にあるユーザーペインを展開して、グループ内のユーザーを表示できます。

## プロジェクト

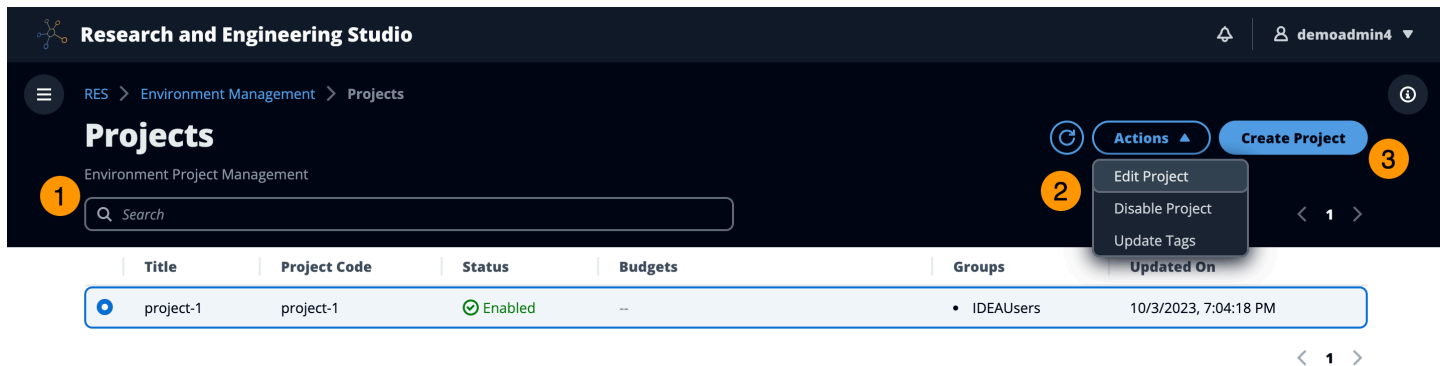
プロジェクトは、仮想デスクトップ、チーム、予算の境界を形成します。プロジェクトを作成するときは、名前、説明、環境設定などの設定を定義します。プロジェクトには通常、コンピューティングリソースのタイプとサイズ、ソフトウェアスタック、ネットワーク設定など、プロジェクトの特定の要件を満たすようにカスタマイズできる1つ以上の環境が含まれます。

### トピック

- [プロジェクトを表示する](#)
- [プロジェクトの作成](#)
- [プロジェクトを編集する](#)

- [プロジェクトを無効にする](#)
- [プロジェクトを削除します。](#)
- [プロジェクトへのタグの追加または削除](#)
- [プロジェクトに関連付けられたファイルシステムを表示する](#)
- [起動テンプレートを追加する](#)

## プロジェクトを表示する



プロジェクトダッシュボードには、利用可能なプロジェクトのリストが表示されます。プロジェクトダッシュボードから、次のことができます。

1. 検索フィールドを使用してプロジェクトを検索できます。
2. プロジェクトを選択すると、アクションメニューを使用して次のことができます。
  - a. プロジェクトを編集する
  - b. プロジェクトの無効化または有効化
  - c. プロジェクトタグを更新する
  - d. プロジェクトを削除します。
3. プロジェクトの作成を選択して、新しいプロジェクトを作成できます。

## プロジェクトの作成

1. [プロジェクトを作成] を選択します。
2. プロジェクトの詳細を入力します。

プロジェクト ID は、でコスト配分を追跡するために使用できるリソースタグです AWS Cost Explorer Service。詳細については、[「ユーザー定義のコスト配分タグのアクティブ化」](#)を参照してください。

**⚠ Important**

作成後にプロジェクト ID を変更することはできません。

詳細オプションの詳細については、「」を参照してください[起動テンプレートを追加する](#)。

3. (オプション) プロジェクトの予算を有効にします。予算の詳細については、「」を参照してください[コストのモニタリングと制御](#)。
4. ホームディレクトリファイルシステムは、共有ホームファイルシステム (デフォルト)、EFS、FSx for Lustre、FSx NetApp ONTAP、または EBS ボリュームストレージのいずれかを使用できます。

共有ホームファイルシステム、EFS、FSx for Lustre、および FSx NetApp ONTAP は、複数のプロジェクトや VDI 間で共有できることに注意してください。ただし、EBS ボリュームストレージオプションでは、そのプロジェクトのすべての VDI に、他の VDI VDI またはプロジェクト間で共有されない独自のホームディレクトリが必要です。

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

5. ユーザーまたはグループに適切なロール（「プロジェクトメンバー」または「プロジェクト所有者」）を割り当てます。各ロールが実行できるアクション [デフォルトのアクセス許可プロファイル](#) については、「」を参照してください。
6. [Submit] を選択してください。

## プロジェクトを編集する

1. プロジェクトリストでプロジェクトを選択します。
2. Actions メニューから、Edit Project を選択します。
3. 更新を入力します。

予算を有効にする場合は、[コストのモニタリングと制御](#)「」を参照してください。プロジェクトの予算を選択すると、予算ドリップダウンオプションがロードされるまでに数秒かかることがあります。先ほど作成した予算が表示されない場合は、ドリップダウンの横にある更新ボタンを選択してください。

詳細オプションの詳細については、「」を参照してください [起動テンプレートを追加する](#)。

#### 4. [Submit] を選択してください。

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

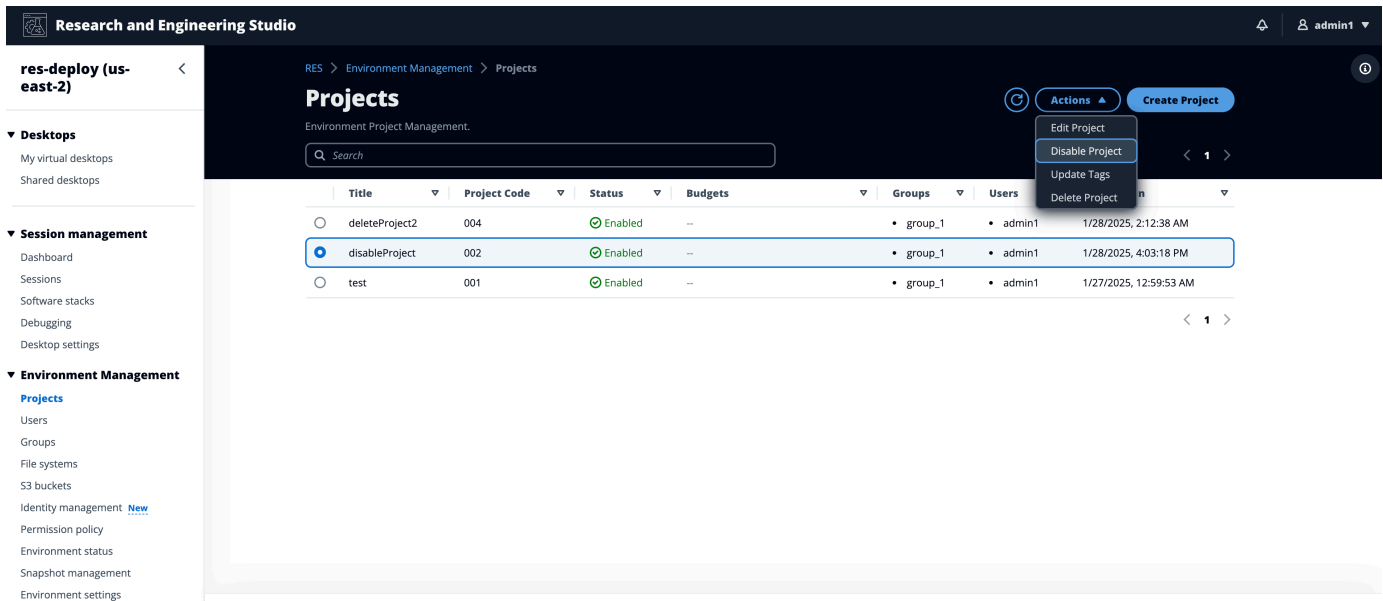
▶ **Linux**

▶ **Windows**

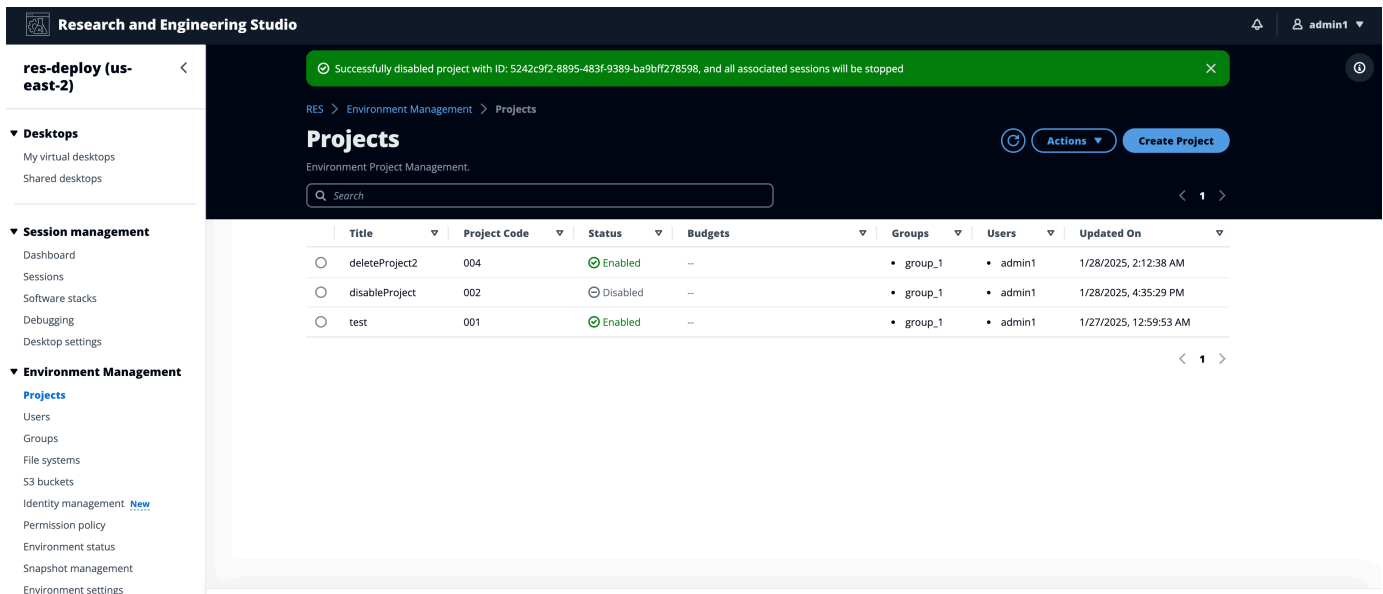
## プロジェクトを無効にする

プロジェクトを無効にするには:

1. プロジェクトリストでプロジェクトを選択します。
2. Actions メニューから、Disable Project を選択します。



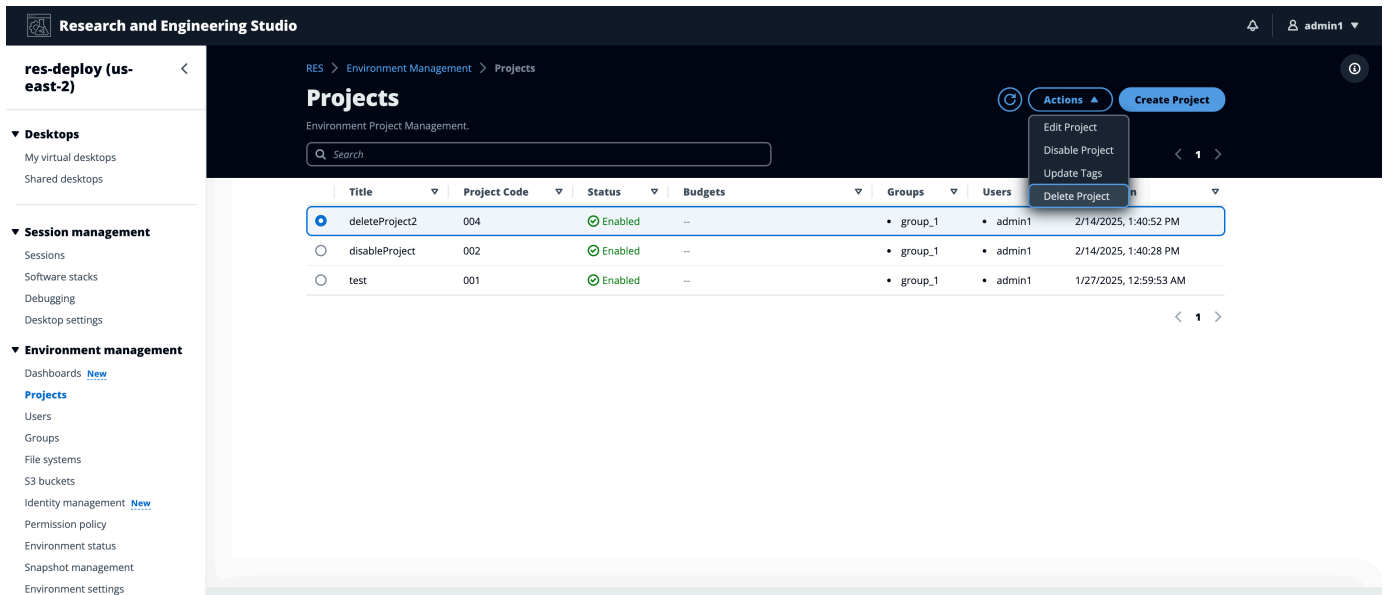
3. プロジェクトが無効になっている場合、そのプロジェクトに関連付けられているすべての VDI セッションが停止します。これらのセッションは、プロジェクトが無効になっている間は再起動できません。



プロジェクトを削除します。

プロジェクトを削除するには:

1. プロジェクトリストでプロジェクトを選択します。
2. アクションメニューから、プロジェクトの削除を選択します。



Title	Project Code	Status	Budgets	Groups	Users	
deleteProject2	004	Enabled	--	• group_1	• admin1	2/14/2025, 1:40:52 PM
disableProject	002	Enabled	--	• group_1	• admin1	2/14/2025, 1:40:28 PM
test	001	Enabled	--	• group_1	• admin1	1/27/2025, 12:59:53 AM

3. 確認ポップアップが表示されます。プロジェクトの名前を入力し、「はい」を選択して削除します。

## 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.

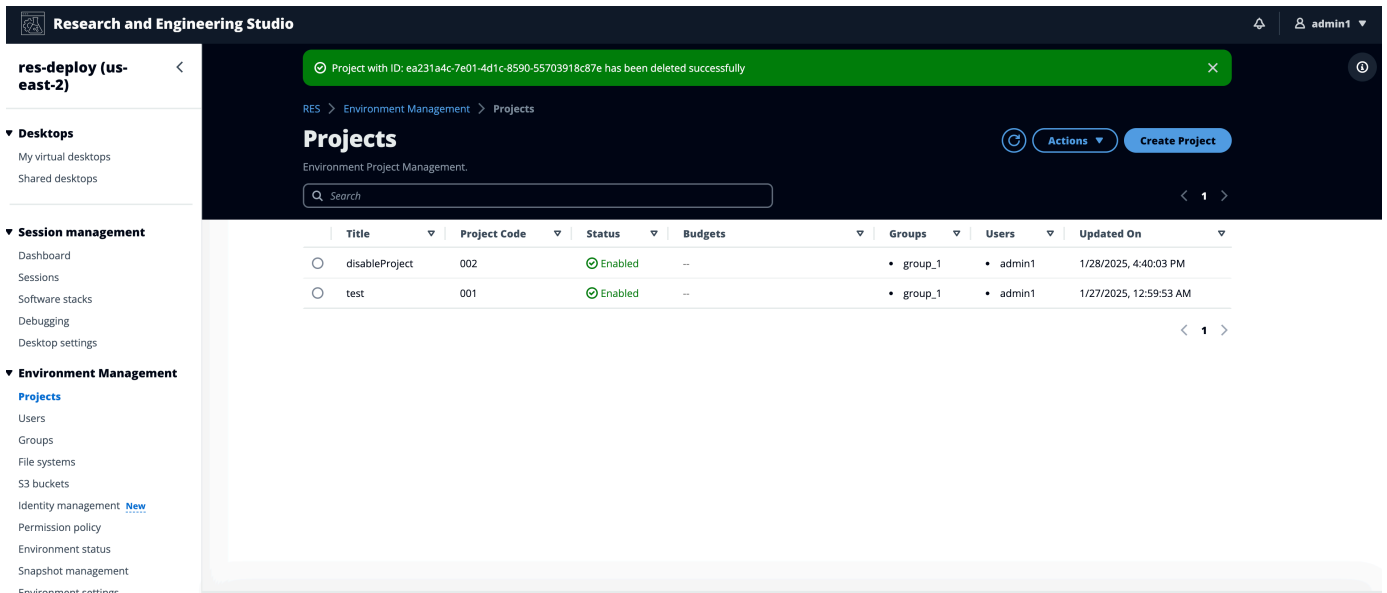
**To confirm deletion, enter the name of the project in the text input field.**

*test-proj-deletion*

Cancel

Yes

4. プロジェクトが削除されると、そのプロジェクトに関連付けられたすべての VDI セッションが終了します。



## プロジェクトへのタグの追加または削除

プロジェクトタグは、そのプロジェクトで作成されたすべてのインスタンスにタグを割り当てます。

1. プロジェクトリストでプロジェクトを選択します。
2. Actions メニューから、Update Tags を選択します。
3. タグの追加を選択し、キーの値を入力します。
4. タグを削除するには、削除するタグの横にある「削除」を選択します。

## プロジェクトに関連付けられたファイルシステムを表示する

プロジェクトを選択すると、画面の下部にあるファイルシステムペインを展開して、プロジェクトに関連付けられたファイルシステムを表示できます。

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUUsers	10/3/2023, 9:06:30 PM

Title	Name	File System ID	Mount Target	Projects	Scope	Provider	Created through RES?
No records							

## 起動テンプレートを追加する

プロジェクトを作成または編集するときは、プロジェクト設定内のアドバンスドオプションを使用して起動テンプレートを追加できます。起動テンプレートは、セキュリティグループ、IAM ポリシー、起動スクリプトなどの追加の設定をプロジェクト内のすべての VDI インスタンスに提供します。

### ポリシーの追加

IAM ポリシーを追加して、プロジェクトの下にデプロイされたすべてのインスタンスの VDI アクセスを制御できます。ポリシーをオンボードするには、ポリシーに次のキーと値のペアをタグ付けします。

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

IAM ロールの詳細については、[「IAM のポリシーとアクセス許可」](#)を参照してください。

### セキュリティグループの追加

セキュリティグループを追加して、プロジェクト内のすべての VDI インスタンスの出力データとイングレスデータを制御できます。セキュリティグループをオンボードするには、セキュリティグループに次のキーと値のペアをタグ付けします。

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

セキュリティグループの詳細については、「[Amazon VPC ユーザーガイドAWS](#)」の「[セキュリティグループを使用してリソースへのトラフィックを制御する](#)」を参照してください。

## 起動スクリプトを追加する

プロジェクト内のすべての VDI セッションで開始する起動スクリプトを追加できます。RES は Linux および Windows のスクリプト開始をサポートしています。スクリプトを開始するには、次のいずれかを選択できます。

### VDI の開始時にスクリプトを実行する

このオプションは、RES 設定またはインストールを実行する前に、VDI インスタンスの先頭でスクリプトを開始します。

### VDI が設定されている場合にスクリプトを実行する

このオプションは、RES 設定の完了後にスクリプトを開始します。

スクリプトは、次のオプションをサポートしています。

スクリプト設定	例
S3 URI	s3://bucketname/script.sh
HTTPS URL	https://sample.samplecontent.com/sample
ローカルファイル	file:///user/scripts/example.sh

S3 バケットでホストされているすべてのカスタムスクリプトは、次のタグでプロビジョニングする必要があります。

```
res:EnvironmentName/<res-environment>
```

引数には、カンマで区切られた引数を指定します。

▼ **Linux**

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

Script | Info Arguments - optional | Info

s3://sample-res-scripts/sample.sh 1,2 Remove Scripts

https://sample.samplecontent.com/sample Remove Scripts

file:///root/bootstrap/latest/launch/script 1,2 Remove Scripts

Add Scripts

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

Script | Info Arguments - optional | Info

s3://sample-res-scripts/sample.sh 1,2 Remove Scripts

Add Scripts

▼ **Windows**

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

Script | Info Arguments - optional | Info

s3://sample-res-scripts/sample.sh 1,2 Remove Scripts

Add Scripts

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

Script | Info Arguments - optional | Info

s3://sample-res-scripts/sample.sh 1,2 Remove Scripts

Add Scripts

## プロジェクト設定の例

起動スクリプトのサンプルテンプレート。

### 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.

#!/bin/bash

echo "start_script.sh running" >> /test_scripts
echo "All arguments: $@" >> /test_scripts
echo "Argument count: $# " >> /test_scripts
echo "Argument 1, $1" >> /test_scripts
echo "Argument 2, $2" >> /test_scripts
echo "end of start_script.sh" >> /test_scripts
```

## 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.

#!pwsh

Write-Output "configure_script.ps1 running" | Out-File -Append -FilePath "/
test_scripts"
Write-Output "All arguments: $args" | Out-File -Append -FilePath "/test_scripts"
Write-Output "Argument count: $($args.Count)" | Out-File -Append -FilePath "/
test_scripts"
Write-Output "Argument 1, $($args[0])" | Out-File -Append -FilePath "/test_scripts"
Write-Output "Argument 2, $($args[1])" | Out-File -Append -FilePath "/test_scripts"
Write-Output "end of configure_script.ps1" | Out-File -Append -FilePath "/
test_scripts"
```

## アクセス許可ポリシー

Research and Engineering Studio (RES) を使用すると、管理者ユーザーは、選択したユーザーに、自分が属するプロジェクトを管理するための追加のアクセス許可を付与するカスタムアクセス許可プロファイルを作成できます。各プロジェクトには、デプロイ後にカスタマイズできる「プロジェクトメンバー」と「プロジェクト所有者」の2つの[デフォルトのアクセス許可プロファイル](#)があります。

現在、管理者はアクセス許可プロファイルを使用して2つのアクセス許可のコレクションを付与できます。

1. 指定されたユーザーがプロジェクトに他のユーザーやグループを追加または削除できるようにする「プロジェクトメンバーシップの更新」と、指定されたユーザーがプロジェクトを有効または無効にできるようにする「プロジェクトステータスの更新」で構成されるプロジェクト管理アクセス許可。
2. 指定されたユーザーがプロジェクト内に VDI セッションを作成できるようにする「セッションの作成」と、指定されたユーザーがプロジェクト内の他のユーザーのセッションを作成または終了できるようにする「別のユーザーのセッションの作成/終了」で構成される VDI セッション管理アクセス許可。

これにより、管理者は環境内の管理者以外のユーザーにプロジェクトベースのアクセス許可を委任できます。

### トピック

- [プロジェクト管理のアクセス許可](#)
- [VDI セッション管理のアクセス許可](#)
- [アクセス許可プロファイルの管理](#)
- [デフォルトのアクセス許可プロファイル](#)
- [環境の境界](#)
- [デスクトップ共有プロファイル](#)

## プロジェクト管理のアクセス許可

### プロジェクトメンバーシップを更新する

このアクセス許可により、付与された管理者以外のユーザーは、プロジェクトからユーザーまたはグループを追加および削除できます。また、アクセス許可プロファイルを設定し、そのプロジェクトの他のすべてのユーザーとグループのアクセスレベルを決定することもできます。

### 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](#)

### プロジェクトのステータスを更新する

このアクセス許可により、付与された管理者以外のユーザーは、プロジェクトページのアクションボタンを使用してプロジェクトを有効または無効にできます。

The screenshot shows the 'Projects' page in the Research and Engineering Studio. The page title is 'Projects' and the subtitle is 'Environment Project Management. These are the projects of which you are a part of.' There is a search bar and a table of projects. The table has columns: Title, Project Code, Status, Budgets, Groups, Users, and Updated On. Two projects are listed: project2 and project3. Project3 is selected, and an 'Actions' menu is open, showing options like Edit Project, Disable Project, and Update Tags.

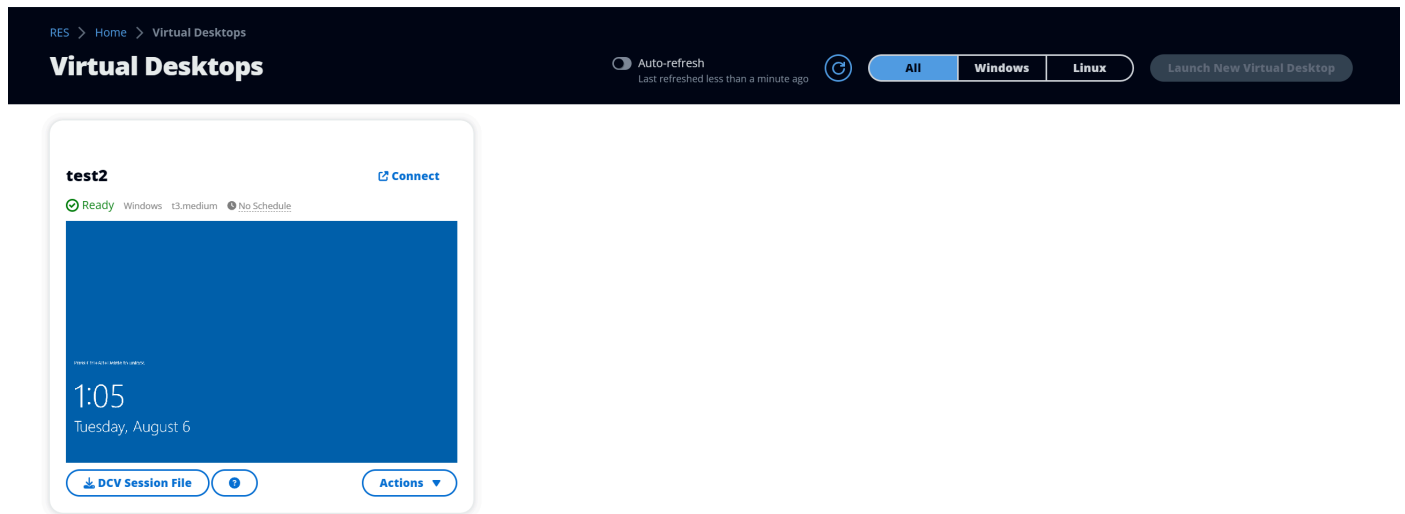
Title	Project Code	Status	Budgets	Groups	Users	Updated On
project2	Project2	Enabled	--	group_2	user1	7/15/2024, 11:45:22 AM
project3	Project3	Enabled	--	group_1, group_2	-	7/15/2024, 8:05:20 AM

## VDI セッション管理のアクセス許可

### セッションを作成する

ユーザーが My Virtual Desktops ページから独自の VDI セッションを起動できるかどうかを制御します。これを無効にして、管理者以外のユーザーが独自の VDI セッションを起動できないようにします。ユーザーはいつでも独自の VDI セッションを停止および終了できます。

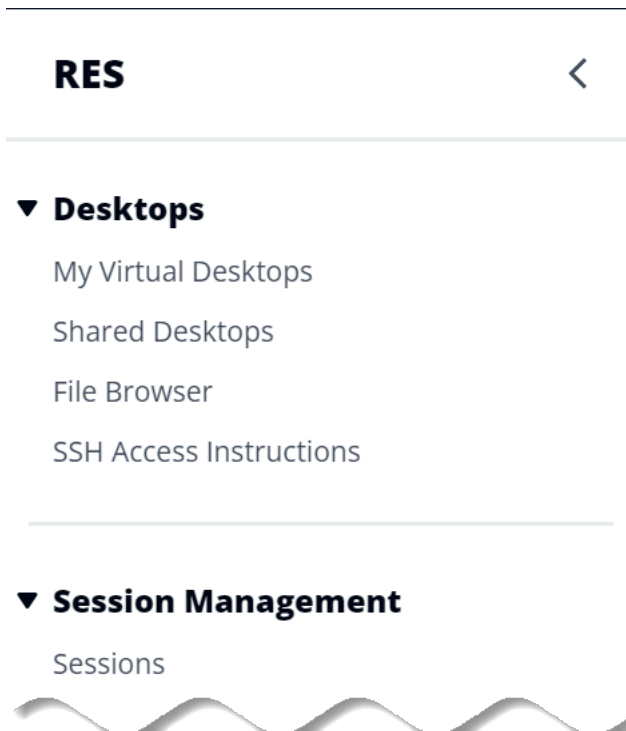
管理者以外のユーザーにセッションを作成するアクセス許可がない場合、新しい仮想デスクトップの起動ボタンは次のように無効になります。



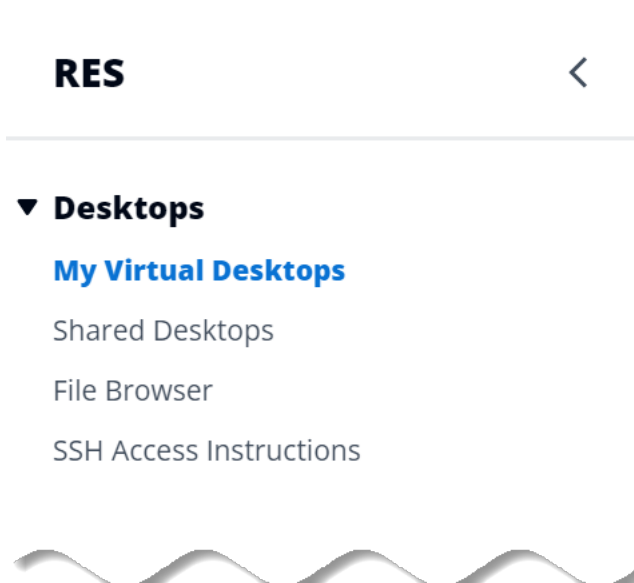
## 他のユーザーのセッションを作成または終了する

管理者以外のユーザーが左側のナビゲーションペインからセッションページにアクセスできるようにします。これらのユーザーは、このアクセス許可が付与されているプロジェクトで他のユーザーの VDI セッションを起動できます。

管理者以外のユーザーが他のユーザーのセッションを起動するアクセス許可を持っている場合、左側のナビゲーションペインには、次に示すようにセッション管理の下のセッションリンクが表示されます。



管理者以外のユーザーに他のユーザーのセッションを作成するアクセス許可がない場合、左側のナビゲーションペインには、次に示すようにセッション管理が表示されません。



## アクセス許可プロファイルの管理

RES 管理者は、次のアクションを実行してアクセス許可プロファイルを管理できます。

## アクセス許可プロファイルを一覧表示する

- Research and Engineering Studio コンソールページで、左側のナビゲーションペインでアクセス許可ポリシーを選択します。このページから、アクセス許可プロファイルを作成、更新、一覧表示、表示、削除できます。

**Project roles (2)**

Find role by ID

Role ID	Role name	Description	Latest update	Affected projects
project_owner	Project Owner	Default Permission Profile for Project Owner	2 weeks ago	0
project_member	Project Member	Default Permission Profile for Project Member	2 weeks ago	10

## アクセス許可プロファイルを表示する

- メインのアクセス許可プロファイルページで、表示するアクセス許可プロファイルの名前を選択します。このページから、選択したアクセス許可プロファイルを編集または削除できます。

RES > Permission Profiles > Project Owner

### Project Owner

Edit Delete

#### General Settings

Profile ID: project\_owner

Description: Default Permission Profile for Project Owner

Creation date: 3 weeks ago

Latest update: 3 weeks ago

#### Permissions

##### Permissions (4)

Permissions granted to this permission profile.

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

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

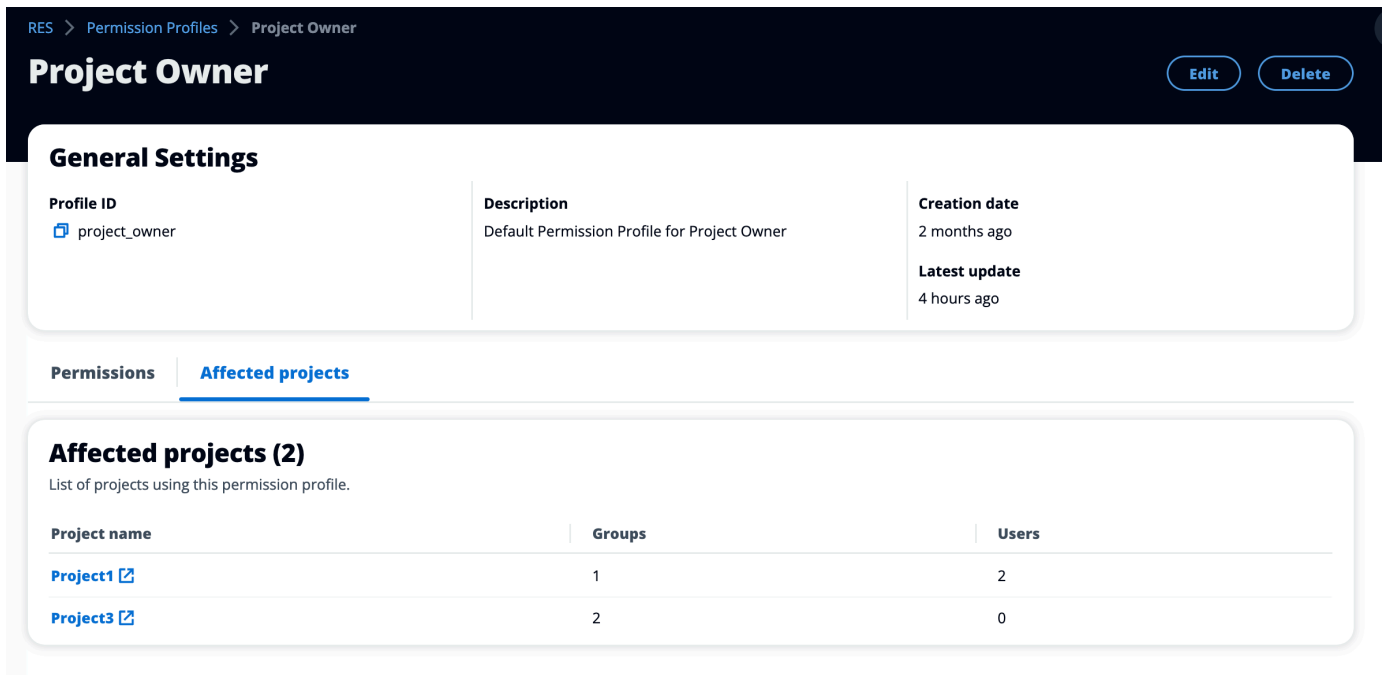
**Update project status**  
Enable or disable a project.  
Enabled

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

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

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

2. アクセス許可プロファイルを現在使用しているプロジェクトを表示するには、影響を受けるプロジェクトタブを選択します。



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

## アクセス許可プロファイルを作成する

1. メインのアクセス許可プロファイルページで、プロファイルの作成を選択してアクセス許可プロファイルを作成します。
2. アクセス許可プロファイルの名前と説明を入力し、このプロファイルに割り当てるユーザーまたはグループに付与するアクセス許可を選択します。

RES > Permission Profiles > Create Profile

## Create permission profile

### 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"/>
-----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------

[Cancel](#) [Create profile](#)

## アクセス許可プロファイルを編集する

- メインのアクセス許可プロファイルページで、プロファイルの横にある円をクリックしてプロファイルを選択し、アクションを選択し、プロファイルの編集を選択してそのアクセス許可プロファイルを更新します。

RES &gt; Permission Profiles &gt; Project Member &gt; 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

## アクセス許可プロファイルを削除する

- メインのアクセス許可プロファイルページで、プロファイルの横にある円をクリックしてプロファイルを選択し、アクションを選択し、プロファイルの削除を選択します。既存のプロジェクトで使用されているアクセス許可プロファイルは削除できません。

RES > Permission Profiles

## Permission Profiles

Create and manage permission profiles.

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

## デフォルトのアクセス許可プロファイル

すべての RES プロジェクトには、グローバル管理者が設定できる 2 つのデフォルトのアクセス許可プロファイルが付属しています。(さらに、グローバル管理者はプロジェクトの新しいアクセス許可プロファイルを作成および変更できます)。次の表は、「プロジェクトメンバー」と「プロジェクト所有者」のデフォルトのアクセス許可プロファイルで許可されるアクセス許可を示しています。アクセス許可プロファイル、およびプロジェクトの特定のユーザーに付与するアクセス許可は、自分が属するプロジェクトにのみ適用されます。グローバル管理者は、すべてのプロジェクトで以下のすべてのアクセス許可を持つスーパーユーザーです。

アクセス許可	説明	プロジェクトメンバー	プロジェクト所有者
セッションの作成	独自のセッションを作成します。ユーザーは、このアクセス許可の有無にかかわらず、いつでも独自のセッションを停	X	X

アクセス許可	説明	プロジェクトメンバー	プロジェクト所有者
	止および終了できません。		
他のユーザーのセッションを作成/終了する	プロジェクト内で別のユーザーのセッションを作成または終了します。		X
プロジェクトメンバーシップの更新	プロジェクトに関連付けられたユーザーとグループを更新します。		X
プロジェクトステータスの更新	プロジェクトを有効または無効にします。		X

## 環境の境界

環境の境界により、Research and Engineering Studio (RES) 管理者は、すべてのユーザーに対してグローバルに有効になるアクセス許可を設定できます。これには、ファイルブラウザと SSH アクセス許可、デスクトップアクセス許可、デスクトップの詳細設定などのアクセス許可が含まれます。

Research and 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](#)

## ファイルブラウザアクセスの設定

RES 管理者は、ファイルブラウザのアクセス許可でアクセスデータのオンとオフを切り替えることができます。アクセスデータがオフになっている場合、ユーザーはウェブポータルにファイルブラウザナビゲーションを表示せず、グローバルファイルシステムにアタッチされたデータをアップロードまたはダウンロードできません。アクセスデータを有効にすると、ユーザーはウェブポータルのファイルブラウザナビゲーションにアクセスして、グローバルファイルシステムにアタッチされたデータをアップロードまたはダウンロードできます。

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, [read the Info](#).

**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 in the environment boundaries can be modified in roles and 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)**

アクセスデータ機能を有効にしてから無効にすると、ウェブポータルに既にログインしているユーザーは、対応するページにある場合でも、ファイルをアップロードまたはダウンロードできなくなります。さらに、ページを更新するとナビゲーションメニューは表示されなくなります。

## SSH アクセスの設定

管理者は、環境境界セクションから RES 環境の SSH を有効または無効にできます。VDIs への SSH アクセスは、踏み台ホストを介して容易になります。このトグルを有効にすると、RES は踏み台ホストをデプロイし、SSH アクセス手順ページがユーザーに表示されます。トグルを無効にすると、RES は SSH アクセスを無効にし、踏み台ホストを終了して、ユーザーの SSH アクセス手順ページを削除します。このトグルはデフォルトで無効になっています。

### Note

RES が踏み台ホストをデプロイすると、AWS アカウントに t3.medium Amazon EC2 インスタンスが追加されます。このインスタンスに関連するすべての料金はお客様の負担となります。詳細については、[Amazon EC2 の料金ページ](#)を参照してください。

## SSH アクセスを有効にするには

1. RES コンソールの左側のナビゲーションペインで、環境管理、アクセス許可ポリシーを選択します。環境の境界で、SSH アクセストグルを選択します。

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, [read the Info](#).

**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 in the environment boundaries can be modified in roles and 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)**

## 2. SSH アクセスが有効になるまで待ちます。

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, [read the Info](#).

**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 in the environment boundaries can be modified in roles and 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)**

## 3. 踏み台ホストが追加されると、SSH アクセスが有効になります。

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 any changes, [read the Info](#).

**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 in the environment boundaries can be modified in roles and 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)**

SSH アクセス手順ページは、左側のナビゲーションペインからユーザーに表示されます。

The screenshot shows the 'SSH Access' page in the Research and Engineering Studio interface. The left sidebar contains navigation options under 'Environment Management', with 'SSH Access Instructions' highlighted. The main content area is divided into two columns:

- Linux / MacOS:**
  - 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_privotekey.pem`
  - Step 3: Connect to the cluster**
    - Run: `ssh -i ~/.ssh/admin1_res-new_privotekey.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_privotekey.pem
```

    - Once updated, you can simply run below to connect to your cluster: `ssh res-new-us-east-1`
- Windows (PuTTY):**
  - Access environment using Windows (PuTTY)**
  - Follow the below steps to connect to the cluster using Terminal on your Windows laptop/workstation:
  - 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 the path of your key `admin1_res-new_privotekey.ppk` 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 after a couple of minutes of inactivity, go to Connection and add "3" as "Seconds between KeepAlives"

SSH アクセスを無効にするには

- RES コンソールの左側のナビゲーションペインで、環境管理を選択し、アクセス許可ポリシーを選択します。環境の境界で、SSH アクセスストグルを選択します。

The screenshot shows the 'Permission policy' page in the Research and Engineering Studio interface. The left sidebar contains navigation options under 'Environment Management', with 'Permission policy' highlighted. The main content area shows:

- Permission policy key concepts** (Info icon): Properly managing a comprehensive permissions policy requires understanding the cascading effects permissions can have across the environment. Before making any changes, [read the Info](#).
- 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 in the environment boundaries can be modified in roles and 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** (Info icon): 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)**

- SSH アクセスが無効になるまで待ちます。

### 3. プロセスが完了すると、SSH アクセスは無効になります。

## デスクトップアクセス許可の設定

管理者はデスクトップのアクセス許可をオンまたはオフに切り替えて、すべてのセッション所有者の VDI 機能をグローバルに管理できます。これらのアクセス許可のすべて、またはサブセットを使用して、デスクトップを共有しているユーザーが実行できるアクションを決定するデスクトップ共有プロファイルを作成できます。デスクトップのアクセス許可が無効になっている場合、デスクトップ共有プロファイルの対応するアクセス許可は自動的に無効になります。これらのアクセス許可には「グローバルに無効」というラベルが付けられます。管理者がこのデスクトップアクセス許可を再度有効にしても、管理者が手動で有効にするまで、デスクトップ共有プロファイルのアクセス許可は無効のままになります。

Research and 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](#)

## デスクトップ共有プロファイル

管理者は新しいプロファイルを作成してカスタマイズできます。これらのプロファイルにはすべてのユーザーがアクセスでき、セッションを他のユーザーと共有するときに使用されます。これらのプロファイル内で付与されるアクセス許可の最大数は、グローバルに許可されるデスクトップアクセス許可を超えることはできません。

### プロファイルの作成

管理者は、プロファイルの作成を選択して新しいプロファイルを作成できます。次に、プロファイル名、プロファイルの説明を入力し、必要なアクセス許可を設定し、変更を保存できます。

## Desktop sharing profiles (3)



Actions ▾

Create profile

Find profile by ID

&lt; 1 &gt; ⚙️

	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)

 Display

Receive visual data from the NICE DCV server

 Pointer

View NICE DCV server mouse position events and pointer shapes

 Mouse

Input from the client mouse to the NICE DCV server

 Audio Out

Receive audio from the NICE DCV server to the client

 Unsupervised Access

Allow a user to connect to session without supervision

 Keyboard

Input from the client keyboard to the NICE DCV server

 Keyboard SAS

Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well

 Screenshot

Save a screenshot of the remote desktop

 Clipboard Copy

Copy data from the NICE DCV server to the client clipboard

 Clipboard Paste

Copy data to the NICE DCV server from the client clipboard

 File Upload

Upload files to the session storage

 File Download

Download files from the session storage

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

Cancel

Save changes

## プロファイルの編集

プロファイルを編集するには:

1. 目的のプロファイルを選択します。
2. アクションを選択し、編集を選択してプロファイルを変更します。

3. 必要に応じてアクセス許可を調整します。
4. [Save changes] (変更の保存) をクリックします。

プロファイルに加えられた変更は、現在のオープンセッションにすぐに適用されます。

Project roles
Desktop sharing profiles

## Desktop sharing profiles

Manage your desktop sharing profiles.

Actions ▲
Create profile
Edit

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 f

### 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.

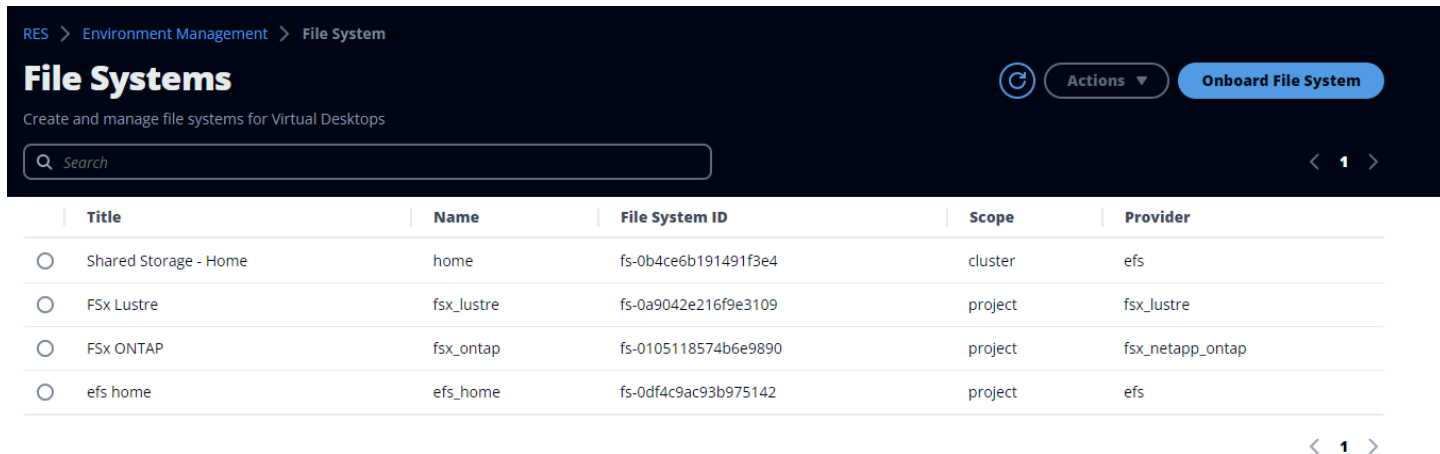
▼ Desktop permissions (enabled 12/12)

<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

# ファイルシステム



RES > Environment Management > File System

## File Systems

Create and manage file systems for Virtual Desktops

Search

	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

ファイルシステムページから、次のことができます。

1. ファイルシステムを検索します。
2. ファイルシステムを選択したら、アクションメニューを使用して次の操作を行います。
  - a. ファイルシステムをプロジェクトに追加します。
  - b. プロジェクトからファイルシステムを削除する
3. 新しいファイルシステムをオンボードします。
4. ファイルシステムを選択すると、画面の下部にあるペインを展開してファイルシステムの詳細を表示できます。

## トピック

- [ファイルシステムのオンボード](#)

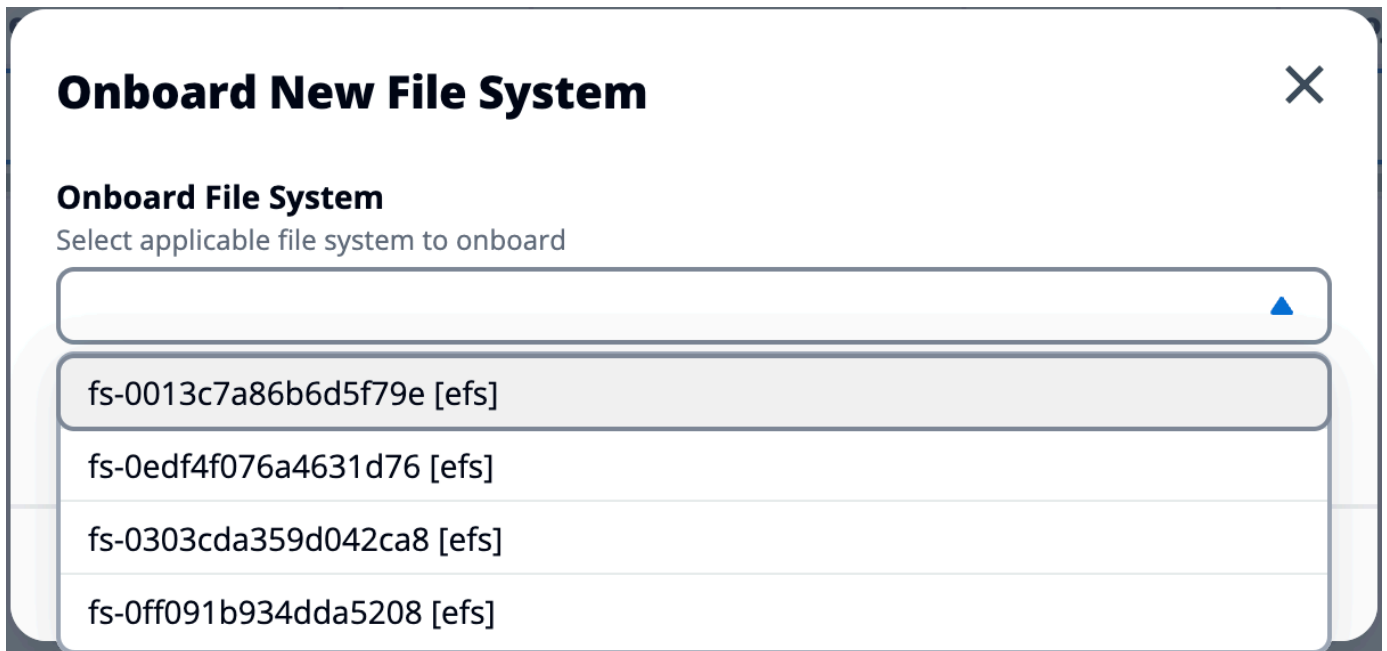
## ファイルシステムのオンボード

### Note

ファイルシステムを正常にオンボードするには、同じ VPC と少なくとも 1 つの RES サブネットを共有する必要があります。また、VDIs がファイルシステムの内容にアクセスできるように、セキュリティグループが適切に設定されていることを確認する必要があります。

1. ファイルシステムのオンボードを選択します。

2. ドロップダウンからファイルシステムを選択します。モーダルは、追加の詳細エントリで展開されます。



3. ファイルシステムの詳細を入力します。

**Note**

デフォルトでは、管理者とプロジェクト所有者は、新しいプロジェクトの作成時にホームファイルシステムを選択できます。これは後で編集することはできません。プロジェクトでホームディレクトリとして使用するファイルシステムは、マウントディレクトリパスを に設定してオンボードする必要があります/home。これにより、オンボードされたファイルシステムがホームディレクトリのファイルシステムのドロップダウンオプションに入力されます。この機能は、プロジェクトに関連付けられたユーザーのみが VDis を介してファイルシステムにアクセスできるため、プロジェクト間でデータを分離するのに役立ちます。VDisは、ファイルシステムのオンボーディング中に選択されたマウントポイントにファイルシステムをマウントします。

4. [Submit] を選択してください。

# 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

## スナップショットの管理

スナップショット管理は、環境間でデータを保存および移行するプロセスを簡素化し、一貫性と正確性を確保します。スナップショットを使用すると、環境の状態を保存し、同じ状態の新しい環境にデータを移行できます。

RES > Environment Management > Snapshot Management

### Snapshot Management

#### Created Snapshots 1

Snapshots created from the environment

Search

< 1 >

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

#### Applied Snapshots 3

Snapshots applied to the environment

Search

< 1 >

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

スナップショット管理ページから、次のことができます。

1. 作成されたすべてのスナップショットとそのステータスを表示します。
2. スナップショットを作成します。スナップショットを作成する前に、適切なアクセス許可を持つバケットを作成する必要があります。
3. 適用されたすべてのスナップショットとそのステータスを表示します。
4. スナップショットを適用します。

### トピック

- [スナップショットを作成する](#)
- [スナップショットを適用する](#)

## スナップショットを作成する

スナップショットを作成する前に、必要なアクセス許可を Amazon S3 バケットに提供する必要があります。バケットの作成については、「[バケットを作成する](#)」を参照してください。バケットのバージョンニングとサーバーアクセスのログ記録を有効にすることをお勧めします。これらの設定は、プロビジョニング後にバケットのプロパティタブから有効にできます。

### Note

この Amazon S3 バケットのライフサイクルは、製品内で管理されません。コンソールからバケットのライフサイクルを管理する必要があります。

バケットにアクセス許可を追加するには:

1. バケットリストから作成したバケットを選択します。
2. [アクセス許可] タブを選択します。
3. [バケットポリシー] で [編集] を選択します。
4. バケットポリシーに次のステートメントを追加します。以下の値を自分の値に置き換えてください。
  - `111122223333` -> AWS アカウント ID
  - `{RES_ENVIRONMENT_NAME}` -> RES 環境名
  - `amzn-s3-demo-bucket` -> S3 バケット名

### Important

でサポートされている限定バージョンの文字列があります AWS。詳細については、「[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)」を参照してください。

## 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": "*"
    }
  ]
}
```

}

スナップショットを作成するには:

1. [スナップショットの作成] を選択します。
2. 作成した Amazon S3 バケットの名前を入力します。
3. バケット内にスナップショットを保存するパスを入力します。例えば、**october2023/23**。
4. [Submit] を選択してください。

## 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 (.), exclamations (!), asterisks (\*), single quotes ('), parentheses (), and hyphens (-).

**Cancel** **Submit**

5. 5~10 分後、スナップショットページで更新を選択してステータスを確認します。スナップショットは、ステータスが IN\_PROGRESS から COMPLETED に変わるまで有効ではありません。

## スナップショットを適用する

環境のスナップショットを作成したら、そのスナップショットを新しい環境に適用してデータを移行できます。環境がスナップショットを読み取れるように、バケットに新しいポリシーを追加する必要があります。

スナップショットを適用すると、ユーザーアクセス許可、プロジェクト、ソフトウェアスタック、アクセス許可プロファイル、ファイルシステムなどのデータが新しい環境に関連付けられてコピーされます。ユーザーセッションはレプリケートされません。スナップショットが適用されると、各リソースレコードの基本情報をチェックして、既に存在するかどうかを確認します。重複レコードの場合、スナップショットは新しい環境でのリソース作成をスキップします。名前やキーを共有するなど、似たようなレコードで、その他の基本的なリソース情報が異なる場合、次の規則を使用して、変更された名前とキーを持つ新しいレコードが作成されます: `RecordName_SnapshotRESVersion_ApplySnapshotID`。はタイムスタンプの `ApplySnapshotID` ように見えるため、スナップショットを適用しようとするたびに識別されません。

スナップショットアプリケーション中に、スナップショットはリソースの可用性をチェックします。新しい環境で使用できないリソースは作成されません。依存リソースを持つリソースの場合、スナップショットは依存リソースの可用性をチェックします。依存リソースが使用できない場合、依存リソースなしでメインリソースが作成されます。

新しい環境が想定どおりにない場合や失敗する場合は、ロググループにある CloudWatch ログで `res-<env-name>/cluster-manager` 詳細を確認できます。各ログには `[apply snapshot]` タグがあります。スナップショットを適用したら、[the section called “スナップショットの管理”](#) ページからそのステータスを確認できます。

バケットにアクセス許可を追加するには:

1. バケットリストから作成したバケットを選択します。
2. [アクセス許可] タブを選択します。
3. [バケットポリシー] で [編集] を選択します。
4. バケットポリシーに次のステートメントを追加します。以下の値を自分の値に置き換えてください。
  - `111122223333` -> AWS アカウント ID
  - `{RES_ENVIRONMENT_NAME}` -> RES 環境名
  - `amzn-s3-demo-bucket` -> S3 バケット名

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": "*"
  }
]
```

スナップショットを適用するには:

1. スナップショットの適用 を選択します。
2. スナップショットを含む Amazon S3 バケットの名前を入力します。
3. バケット内のスナップショットへのファイルパスを入力します。
4. [Submit] を選択してください。

## 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 (.), exclamations (!), asterisks (\*), single quotes ('), parentheses (), and hyphens (-).

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

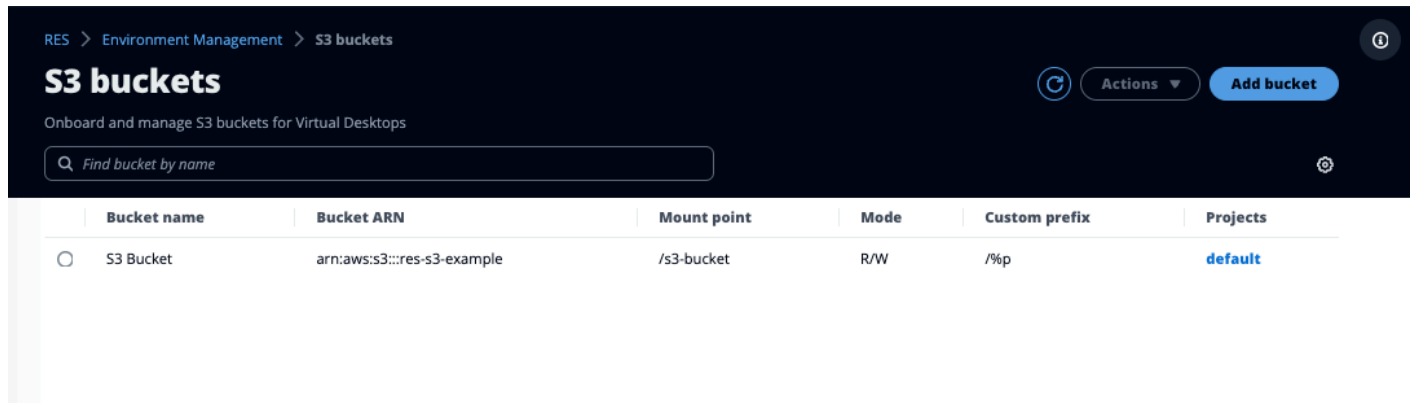
5. 5～10 分後、スナップショット管理ページで更新を選択してステータスを確認します。

## Amazon S3 バケット

Research and Engineering Studio (RES) は、[Linux Virtual Desktop Infrastructure \(VDI\) インスタンスへの Amazon S3 バケット](#)のマウントをサポートしています。RES 管理者は、環境管理の S3 バケットタブで、S3 バケットを RES にオンボードしたり、プロジェクトにアタッチしたり、設定を編集したり、バケットを削除したりできます。

S3 バケットダッシュボードには、利用可能なオンボード S3 バケットのリストが表示されます。S3 バケットダッシュボードから、次のことができます。

1. バケットの追加を使用して、S3 バケットを RES にオンボードします。
2. S3 バケットを選択し、アクションメニューを使用して次の操作を行います。
  - バケットを編集する
  - バケットを削除する
3. 検索フィールドを使用してバケット名で検索し、オンボードされた S3 バケットを検索します。



以下のセクションでは、RES プロジェクトで Amazon S3 バケットを管理する方法について説明します。

## トピック

- [分離された VPC デプロイの Amazon S3 バケットの前提条件](#)
- [Amazon S3 バケットを追加する](#)
- [Amazon S3 バケットを編集する](#)
- [Amazon S3 バケットを削除する](#)
- [データ分離](#)
- [クロスアカウントバケットアクセス](#)
- [プライベート VPC でのデータ流出の防止](#)
- [トラブルシューティング](#)
- [CloudTrail の有効化](#)

## 分離された VPC デプロイの Amazon S3 バケットの前提条件

Research and Engineering Studio を分離された VPC にデプロイする場合は、以下の手順に従って、AWS アカウントに RES をデプロイした後に Lambda 設定パラメータを更新します。

1. Research and Engineering Studio がデプロイされている AWS アカウントの Lambda コンソールにログインします。
2. という名前の Lambda 関数を見つけて移動します `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`。
3. 関数の設定タブを選択します。

The screenshot shows the AWS Lambda console interface. At the top, there's a notification bar and a 'Function overview' section with tabs for 'Diagram' and 'Template'. Below that, there's a 'Configuration' tab with a sidebar on the left containing various settings like 'Triggers', 'Permissions', 'Destinations', 'Function URL', 'Environment variables', 'Tags', 'VPC', 'RDS databases', 'Monitoring and operations tools', 'Concurrency and recursion detection', 'Asynchronous invocation', 'Code signing', 'File systems', and 'State machines'. The 'Environment variables' section is expanded, showing a table of 16 variables. The first row, 'AWS\_STS\_REGIONAL\_ENDPOINTS' with a value of 'regional', is highlighted with a red box. Other variables include 'CLUSTER\_NAME', 'CLUSTER\_SETTINGS\_TABLE\_NAME', 'DCV\_HOST\_DB\_HASH\_KEY', 'DCV\_HOST\_DB\_IDEA\_SESSION\_ID\_KEY', 'DCV\_HOST\_DB\_IDEA\_SESSION\_OWNER\_KEY', 'MODULE\_ID', 'OBJECT\_STORAGE\_CUSTOM\_PROJECT\_NAME\_AND\_USERNAME\_PREFIX', 'OBJECT\_STORAGE\_CUSTOM\_PROJECT\_NAME\_PREFIX', and 'OBJECT\_STORAGE\_NO\_CUSTOM\_PREFIX'.

4. 左側で、環境変数を選択してそのセクションを表示します。
5. 編集を選択し、次の新しい環境変数を関数に追加します。
  - キー: `AWS_STS_REGIONAL_ENDPOINTS`
  - 値: `regional`
6. [保存] を選択します。

## Amazon S3 バケットを追加する

RES 環境に S3 バケットを追加するには:

1. [Add bucket (バケットの追加)] を選択します。
2. バケット名、ARN、マウントポイントなどのバケットの詳細を入力します。

### **⚠ Important**

- 指定されたバケット ARN、マウントポイント、モードは、作成後に変更することはできません。

- バケット ARN には、オンボードされた S3 バケットをそのプレフィックスに分離するプレフィックスを含めることができます。

3. バケットをオンボードするモードを選択します。

 Important

- 特定のモードでのデータ分離に関する詳細については、[データ分離](#)「」を参照してください。

4. 詳細オプションでは、クロスアカウントアクセス用にバケットをマウントするための IAM ロール ARN を指定できます。の手順に従って[クロスアカウントバケットアクセス](#)、クロスアカウントアクセスに必要な IAM ロールを作成します。
5. (オプション) バケットをプロジェクトに関連付けます。プロジェクトは後で変更できます。ただし、S3 バケットをプロジェクトの既存の VDI セッションにマウントすることはできません。プロジェクトがバケットに関連付けられた後に起動されたセッションのみがバケットをマウントします。
6. [Submit] を選択してください。

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

## Amazon S3 バケットを編集する

1. S3 バケットリストで S3 バケットを選択します。
2. アクションメニューから、編集を選択します。
3. 更新を入力します。

### ⚠ Important

- プロジェクトを S3 バケットに関連付けると、そのプロジェクトの既存の仮想デスクトップインフラストラクチャ (VDI) インスタンスにバケットがマウントされません。

バケットは、バケットがそのプロジェクトに関連付けられた後にのみ、プロジェクトで起動された VDI セッションにマウントされます。

- S3 バケットからプロジェクトの関連付けを解除しても、S3 バケット内のデータには影響しませんが、デスクトップユーザーはそのデータにアクセスできなくなります。

#### 4. バケット設定の保存 を選択します。

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 X  
default

Cancel Save bucket setup

## Amazon S3 バケットを削除する

1. S3 バケットリストで S3 バケットを選択します。
2. アクションメニューから、削除を選択します。

### **⚠ Important**

- まず、バケットからすべてのプロジェクトの関連付けを削除する必要があります。
- 削除オペレーションは、S3 バケット内のデータには影響しません。S3 バケットと RES の関連付けのみが削除されます。
- バケットを削除すると、そのセッションの認証情報の有効期限 (約 1 時間) に、既存の VDI セッションがそのバケットの内容にアクセスできなくなります。

## データ分離

RES に S3 バケットを追加すると、バケット内のデータを特定のプロジェクトとユーザーに分離するオプションがあります。バケットの追加ページで、読み取り専用 (R) または読み取りと書き込み (R/W) のモードを選択できます。

### 読み取り専用

Read Only (R) を選択した場合、バケット ARN (Amazon リソースネーム) のプレフィックスに基づいてデータ分離が適用されます。たとえば、管理者が ARN を使用して RES にバケットを追加 `arn:aws:s3:::bucket-name/example-data/` し、このバケットをプロジェクト A とプロジェクト B に関連付けると、プロジェクト A とプロジェクト B 内から VDI を起動するユーザーは、パスの `bucket-name` にあるデータのみを読み取ることができます `/example-data`。そのパス外のデータにはアクセスできません。バケット ARN にプレフィックスが付加されていない場合、バケット全体がそれに関連付けられたプロジェクトで利用可能になります。

### 読み取りと書き込み

Read and Write (R/W) を選択した場合でも、上記のように、バケット ARN のプレフィックスに基づいてデータ分離が適用されます。このモードには、管理者が S3 バケットに変数ベースのプレフィックスを提供できるようにする追加オプションがあります。Read and Write (R/W) を選択すると、カスタムプレフィックスセクションが利用可能になり、次のオプションを含むドロップダウンメニューが表示されます。

- カスタムプレフィックスなし
- `/%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

## カスタムデータ分離なし

カスタムプレフィックスに No custom prefix を選択すると、バケットはカスタムデータ分離なしで追加されます。これにより、バケットに関連付けられたすべてのプロジェクトに読み取りおよび書き込みアクセスが許可されます。たとえば、管理者が `arn:aws:s3:::bucket-name` No custom prefix 選択した ARN を使用して RES にバケットを追加し、このバケットをプロジェクト A とプロジェクト B に関連付けた場合、プロジェクト A とプロジェクト B 内から VDI を起動するユーザーは、バケットへの無制限の読み取りおよび書き込みアクセス権を持ちます。

## プロジェクトレベルごとのデータ分離

カスタムプレフィックスに /%p を選択すると、バケット内のデータは、それに関連付けられた特定のプロジェクトごとに分離されます。%p 変数はプロジェクトコードを表します。たとえば、管理者が `arn:aws:s3:::bucket-name/%p` 選択したと `/bucket` のマウントポイントを使用して RES にバケットを追加し、このバケットをプロジェクト A とプロジェクト B に関連付けると、プロジェクト A のユーザー A は `/bucket` にファイルを書き込むことができます。プロジェクト A のユーザー B は、ユーザー A が `/bucket` で作成したファイルを表示することもできます。

ただし、ユーザー B がプロジェクト B で VDI を起動し、`/bucket` を検索すると、データがプロジェクトによって分離されるため、ユーザー A が作成したファイルが表示されません。ユーザー A が書き込んだファイルは、プレフィックスの S3 バケットにあります `/ProjectA` が、ユーザー B はプロジェクト B から VDI を使用する `/ProjectB` 場合にのみアクセスできます。

## プロジェクトごと、ユーザーごとのデータ分離

カスタムプレフィックスに `/%p/%u` を選択すると、バケット内のデータは、そのプロジェクトに関連付けられた特定のプロジェクトとユーザーに分離されます。`%p` 変数はプロジェクトコードを表し、`%u` はユーザー名 `%u` を表します。たとえば、管理者は `/%p/%u`、選択した `/bucket` のマウントポイント `arn:aws:s3:::bucket-name` を持つ ARN を使用して RES にバケットを追加します。このバケットはプロジェクト A とプロジェクト B に関連付けられています。プロジェクト A のユーザー A は `/bucket` にファイルを書き込むことができます。`%p` 分離のみの以前のシナリオとは異なり、この場合のユーザー B には、`/bucket` のプロジェクト A でユーザー A が書き込んだファイルが表示されません。これは、データがプロジェクトとユーザーの両方によって分離されるためです。ユーザー A が書き込んだファイルは、プレフィックスの S3 バケットにあります `/ProjectA/UserA` が、ユーザー B はプロジェクト A で VDI を使用する `/ProjectA/UserB` 場合にのみアクセスできます。

## クロスアカウントバケットアクセス

RES は、これらのバケットに適切なアクセス許可がある場合、他の AWS アカウントからバケットをマウントできます。次のシナリオでは、アカウント A の RES 環境がアカウント B に S3 バケットをマウントしたいと考えています。

ステップ 1: RES がデプロイされているアカウントに IAM ロールを作成します (これはアカウント A と呼ばれます)。

1. S3 バケット (アカウント A) へのアクセスを必要とする RES アカウントの AWS マネジメントコンソールにサインインします。
2. IAM コンソールを開きます。
  - a. IAM ダッシュボードに移動します。
  - b. ナビゲーションペインで、ポリシー を選択してください。
3. ポリシーを作成する:
  - a. [Create policy] (ポリシーの作成) を選択します。
  - b. [JSON] タブを選択します。

- c. 次の JSON ポリシーを貼り付けます ( をアカウント B にある S3 バケットの名前 *amzn-s3-demo-bucket* に置き換えます )。

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. [次へ] を選択します。
4. ポリシーを確認して作成します。
    - a. ポリシーの名前を指定します (例: "S3AccessPolicy")。
    - b. ポリシーの目的を説明するオプションの説明を追加します。
    - c. ポリシーを確認し、ポリシーの作成を選択します。
  5. IAM コンソールを開きます。
    - a. IAM ダッシュボードに移動します。
    - b. ナビゲーションペインで Roles (ロール) を選択してください。
  6. ロールを作成する:
    - a. [ロールの作成] を選択してください。
    - b. 信頼されたエンティティのタイプとしてカスタム信頼ポリシーを選択します。



- c. 左側のナビゲーションペインで、S3 バケットを選択します。
- d. バケットの追加を選択し、フォームにクロスアカウントの S3 バケット ARN を入力します。
- e. 詳細設定 - オプションのドロップダウンを選択します。
- f. IAM ロール ARN フィールドにロール ARN を入力します。
- g. バケットの追加 を選択します。

## ステップ 2: アカウント B でバケットポリシーを変更する

1. アカウント B の AWS マネジメントコンソールにサインインします。
2. S3 コンソールを開きます。
  - a. S3 ダッシュボードに移動します。
  - b. アクセスを許可するバケットを選択します。
3. バケットポリシーを編集します。
  - a. アクセス許可タブを選択し、バケットポリシーを選択します。
  - b. 次のポリシーを追加して、アカウント A の IAM ロールにバケットへのアクセスを許可します (**111122223333** をアカウント A の実際の実際のアカウント ID に置き換え、**amzn-s3-demo-bucket** を S3 バケットの名前に置き換えます )。

### 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. [保存] を選択します。

## プライベート VPC でのデータ流出の防止

ユーザーが安全な S3 バケットからアカウント内の独自の S3 バケットにデータを流出しないようにするには、VPC エンドポイントをアタッチしてプライベート VPC を保護します。次の手順は、アカウント内の S3 バケットへのアクセスをサポートする S3 サービスの VPC エンドポイントと、クロスアカウントバケットを持つ追加のアカウントを作成する方法を示しています。

1. Amazon VPC コンソールを開きます。
  - a. AWS マネジメントコンソールにサインインします。
  - b. <https://console.aws.amazon.com/vpcconsole/> で Amazon VPC コンソールを開きます。
2. S3 の VPC エンドポイントを作成する:
  - a. 左のナビゲーションペインで [エンドポイント] を選択してください。
  - b. [Create Endpoint] (エンドポイントの作成) を選択します。
  - c. [Service category] (サービスカテゴリ) で、[AWS services] (AWS のサービス) が選択されていることを確認します。
  - d. サービス名フィールドに、「」と入力するか `com.amazonaws.<region>.s3` (AWS リージョン<region>に置き換える)、 「S3」を検索します。
  - e. リストから S3 サービスを選択します。
3. エンドポイント設定の構成:
  - a. [VPC] で、エンドポイントを作成する VPC を選択します。
  - b. サブネットの場合は、デプロイ中に VDI サブネットに使用されるプライベートサブネットの両方を選択します。

- c. DNS 名を有効にする には、オプションがオンになっていることを確認します。これにより、プライベート DNS ホスト名をエンドポイントネットワークインターフェイスに解決できます。
4. アクセスを制限するように ポリシーを設定します。
    - a. Policy で、Custom を選択します。
    - b. ポリシーエディタで、アカウントまたは特定のアカウント内のリソースへのアクセスを制限するポリシーを入力します。ポリシーの例を次に示します (*amzn-s3-demo-bucket* を S3 バケット名に置き換え、*111122223333* と *444455556666* をアクセスする適切な AWS アカウント IDs に置き換えます )。

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. エンドポイントを作成します。
  - a. 設定を確認します。
  - b. エンドポイントの作成 を選択します。

## 6. エンドポイントを検証する:

- a. エンドポイントが作成されたら、VPC コンソールのエンドポイントセクションに移動します。
- b. 新しく作成したエンドポイントを選択します。
- c. 状態が使用可能であることを確認します。

これらのステップに従って、アカウントまたは指定されたアカウント ID 内のリソースに制限された S3 アクセスを許可する VPC エンドポイントを作成します。

## トラブルシューティング

バケットが VDI へのマウントに失敗したかどうかを確認する方法

バケットが VDI へのマウントに失敗した場合、エラーをチェックできる場所がいくつかあります。以下のステップに従います。

1. VDI ログを確認します。
  - a. AWS マネジメントコンソールにログインします。
  - b. EC2 コンソールを開き、インスタンスに移動します。
  - c. 起動した VDI インスタンスを選択します。
  - d. Session Manager を介して VDI に接続します。
  - e. 以下のコマンドを実行します。

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

ここでは、ブートストラップログを確認できます。障害の詳細は `configure.log`. `{time}` ファイルにあります。

さらに、詳細については `/etc/message` ログを確認してください。

2. カスタム認証情報ブローカーの Lambda CloudWatch Logs を確認する:
  - a. AWS マネジメントコンソールにログインします。
  - b. CloudWatch コンソールを開き、ロググループに移動します。

- c. ロググループを検索します `/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`。
  - d. 最初に使用可能なロググループを調べ、ログ内のエラーを見つけます。これらのログには、S3 バケットをマウントするための一時的なカスタム認証情報を提供する潜在的な問題に関する詳細が含まれます。
3. カスタム認証情報ブローカー API Gateway CloudWatch Logs を確認します。
    - a. AWS マネジメントコンソールにログインします。
    - b. CloudWatch コンソールを開き、ロググループに移動します。
    - c. ロググループを検索します `<stack-name>-vdc-custom-credential-broker-lambda-vdc-custom-credential-broker-api-gateway-access-logs<nonce>`。
    - d. 最初に使用可能なロググループを調べ、ログ内のエラーを見つけます。これらのログには、S3 バケットのマウントに必要なカスタム認証情報の API Gateway へのリクエストとレスポンスに関する詳細が含まれます。

#### オンボーディング後にバケットの IAM ロール設定を編集する方法

1. [AWS DynamoDB コンソール](#) にサインインします。
2. テーブルを選択します。
  - a. 左のナビゲーションペインで、[テーブル] を選択します。
  - b. を検索して選択します `<stack-name>.cluster-settings`。
3. テーブルをスキャンします。
  - a. [テーブルアイテムの探索] を選択します。
  - b. スキャンが選択されていることを確認します。
4. フィルターを追加する:
  - a. フィルターを選択してフィルターエントリセクションを開きます。
  - b. キーと一致するようにフィルターを設定します。
    - 属性: キーを入力します。
    - 条件: 「で始まる」を選択します。
    - 値: `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`  
`<filesystem_id>` を変更する必要があるファイルシステムの値に置き換えます。

## 5. スキャンを実行します。

Run を選択して、フィルターを使用してスキャンを実行します。

## 6. 値を確認します。

エントリが存在する場合は、適切な IAM ロール ARN で値が正しく設定されていることを確認します。

エントリが存在しない場合:

a. [項目を作成] を選択します。

b. 項目の詳細を入力します。

- key 属性には、と入力します `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`。
- 正しい IAM ロール ARN を追加します。

c. 保存を選択して項目を追加します。

## 7. VDI インスタンスを再起動します。

インスタンスを再起動して、誤った IAM ロール ARN の影響を受ける VDI が再度マウントされるようにします。

## CloudTrail の有効化

CloudTrail コンソールを使用してアカウントで CloudTrail を有効にするには、「CloudTrail AWS ユーザーガイド CloudTrail」の[CloudTrail コンソールを使用した証跡の作成](#)に記載されている手順に従ってください。CloudTrail は、S3 バケットにアクセスした IAM ロールを記録することで、S3 バケットへのアクセスを記録します。これは、プロジェクトまたはユーザーにリンクされたインスタンス ID にリンクできます。

# 製品を使用する

このセクションでは、仮想デスクトップを使用して他のユーザーとコラボレーションするためのガイドランスをユーザーに提供します。

トピック

- [SSH アクセス](#)
- [仮想デスクトップ](#)
- [共有デスクトップ](#)
- [ファイルブラウザ](#)

## SSH アクセス

SSH を使用して踏み台ホストにアクセスするには:

1. RES メニューから、SSH アクセスを選択します。
2. アクセスに SSH または PuTTY を使用するには、画面の指示に従います。

## 仮想デスクトップ

仮想デスクトップインターフェイス (VDI) モジュールを使用すると、ユーザーは で Windows または Linux 仮想デスクトップを作成および管理できます AWS。ユーザーは、お気に入りのツールとアプリケーションがプリインストールおよび設定された状態で Amazon EC2 インスタンスを起動できます。

サポートされるオペレーティングシステム

RES は現在、次のオペレーティングシステムを使用した仮想デスクトップの起動をサポートしています。

- Amazon Linux 2 (x86 および ARM64)
- Amazon Linux 2023 (x86 および ARM64)
- RHEL 8 (x86)、および 9 (x86)
- Rocky Linux 9 (x86)
- Ubuntu 22.04.03 (x86)

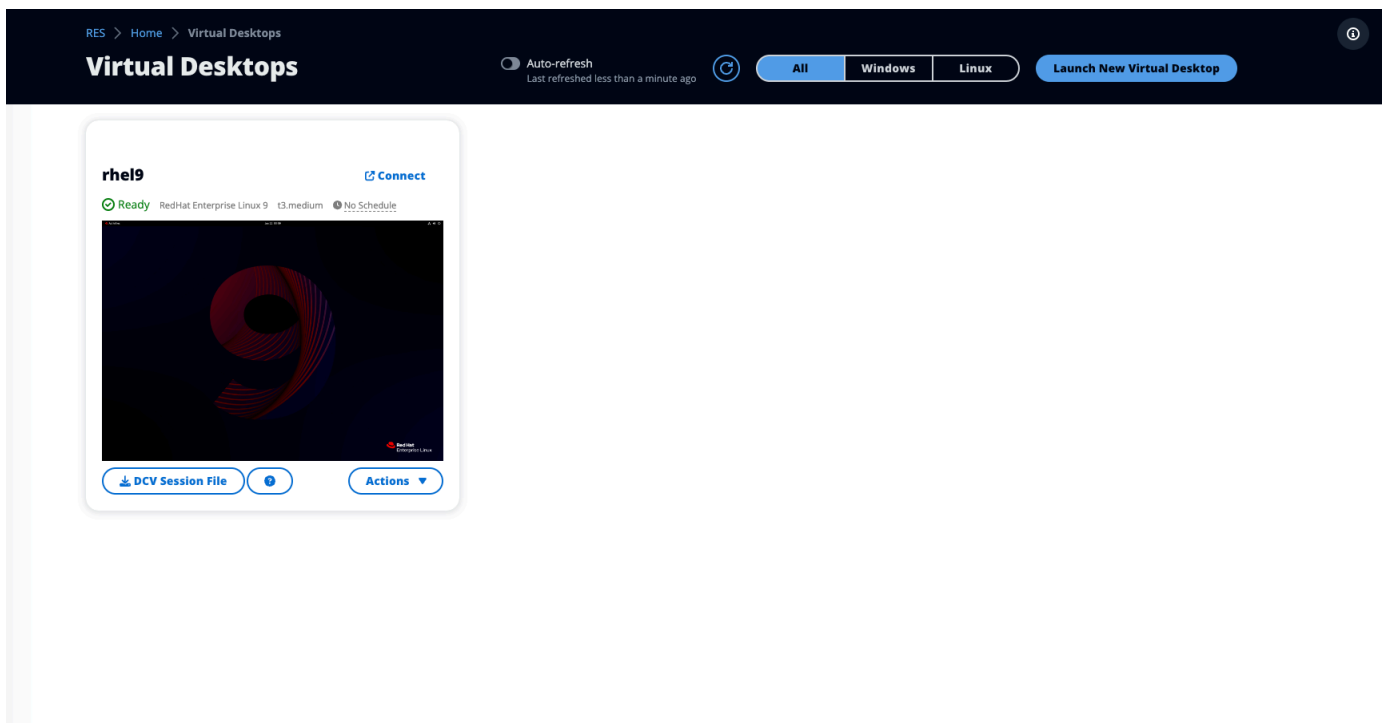
- Windows Server 2019、2022 (x86)
- Windows 10、11 (x86)

## トピック

- [新しいデスクトップを起動する](#)
- [デスクトップにアクセスする](#)
- [デスクトップの状態を制御する](#)
- [仮想デスクトップを変更する](#)
- [セッション情報を取得する](#)
- [仮想デスクトップをスケジュールする](#)
- [仮想デスクトップインターフェ이스の自動停止](#)

## 新しいデスクトップを起動する

1. メニューから、My Virtual Desktops を選択します。
2. 新しい仮想デスクトップを起動を選択します。



3. 新しいデスクトップの詳細を入力します。
4. [Submit] を選択してください。

デスクトップ情報を含む新しいカードがすぐに表示され、デスクトップは 10～15 分以内に使用できるようになります。起動時間は、選択したイメージによって異なります。RES は GPU インスタンスを検出し、関連するドライバーをインストールします。

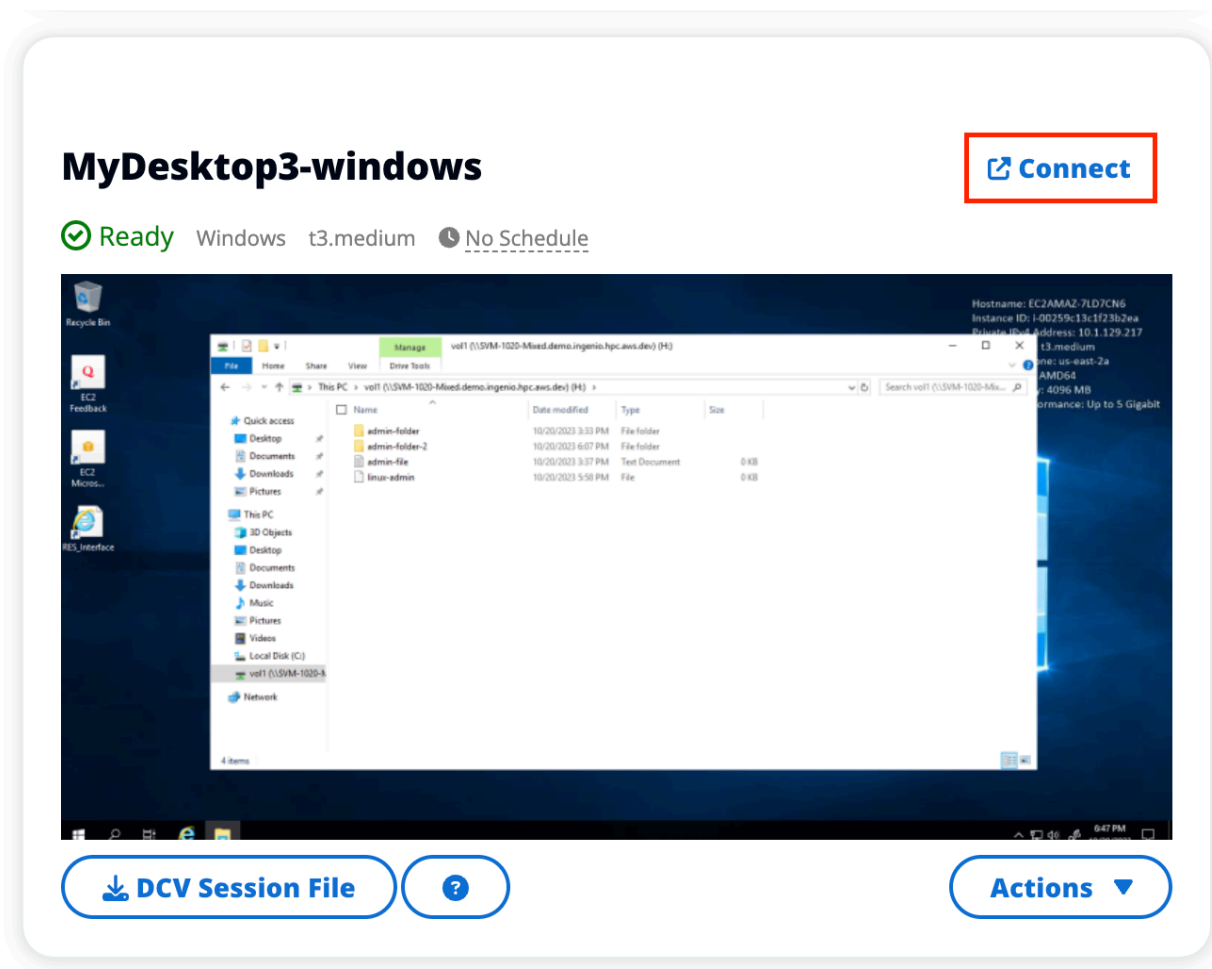
## デスクトップにアクセスする

仮想デスクトップにアクセスするには、デスクトップのカードを選択し、ウェブまたは DCV クライアントを使用して接続します。

### Web connection

ウェブブラウザからデスクトップにアクセスするのが最も簡単な接続方法です。

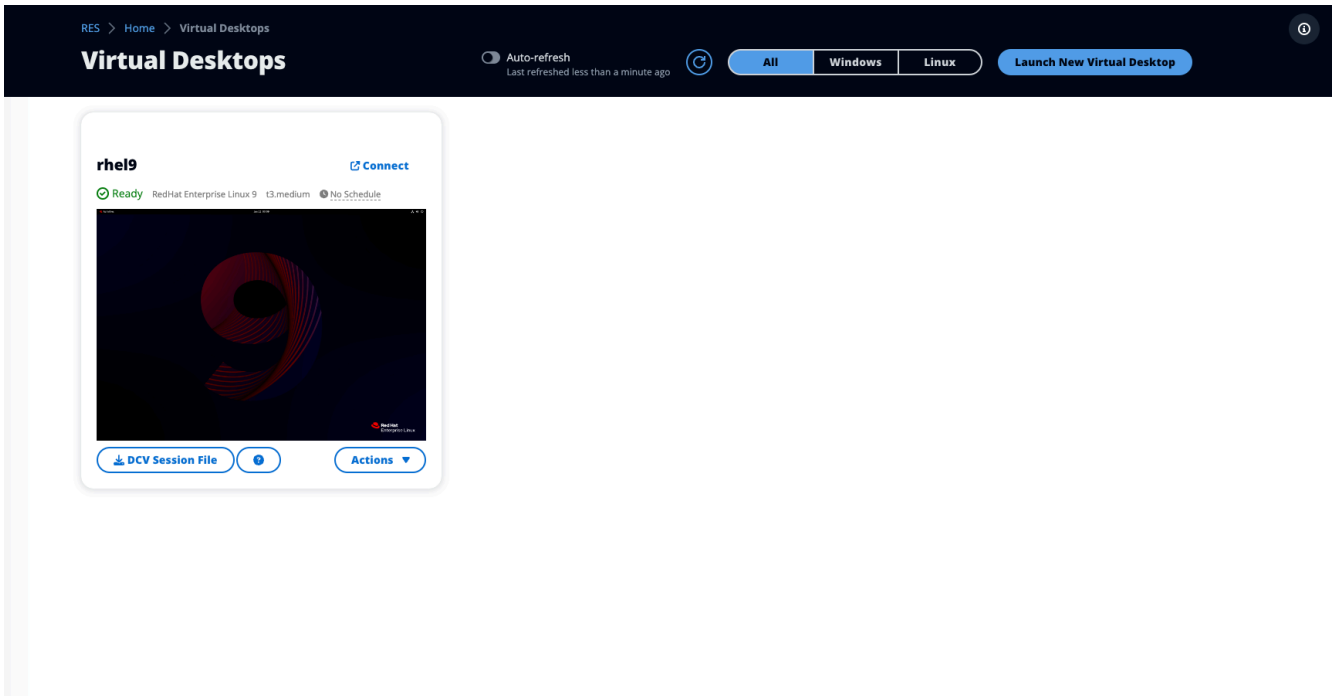
- Connect を選択するか、サムネイルを選択してブラウザから直接デスクトップにアクセスします。



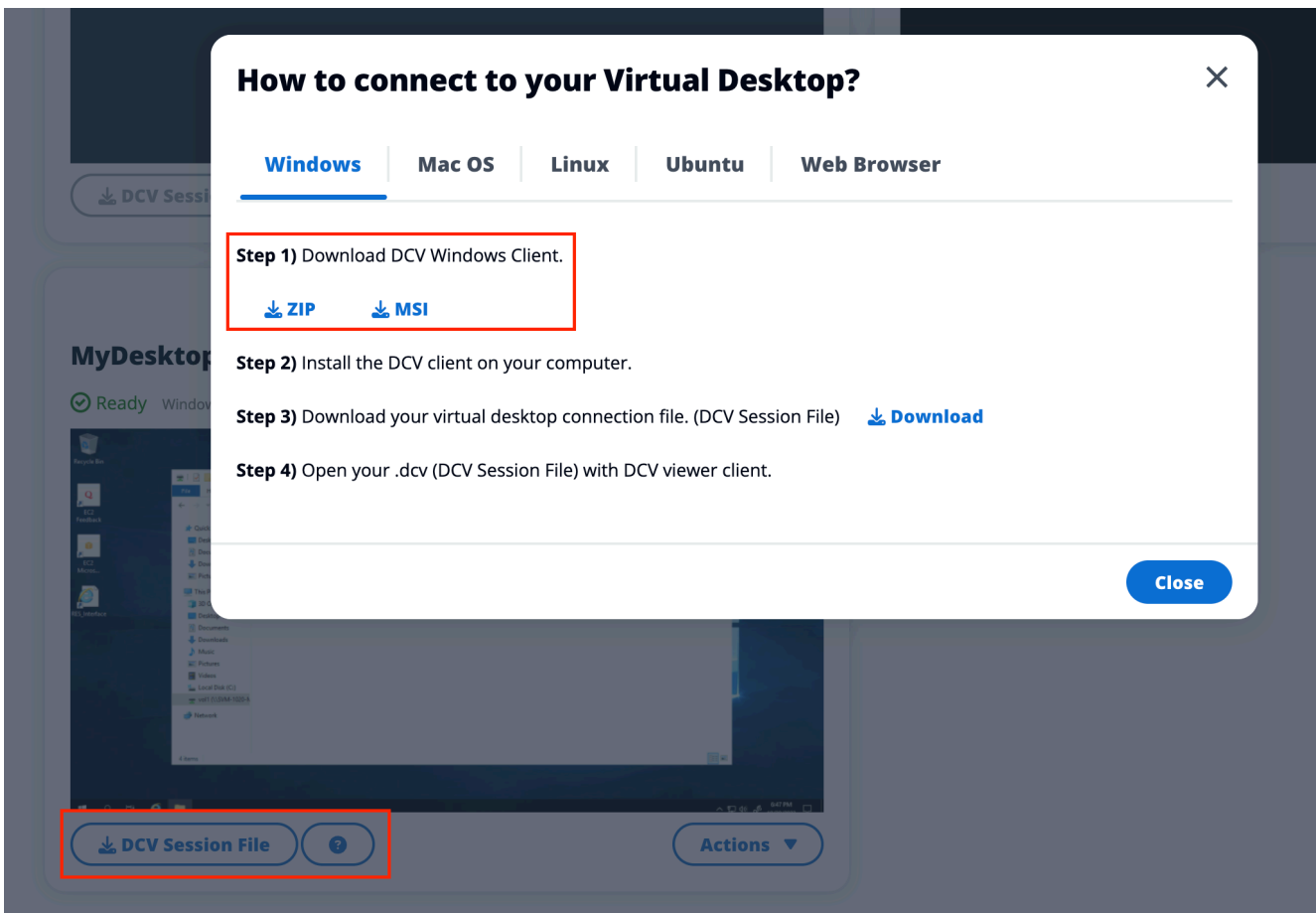
## DCV connection

DCV クライアントを介してデスクトップにアクセスすると、最高のパフォーマンスが得られます。DCV 経由で にアクセスするには:

1. DCV セッションファイルを選択して .dcv ファイルをダウンロードします。DCV クライアントがシステムにインストールされている必要があります。



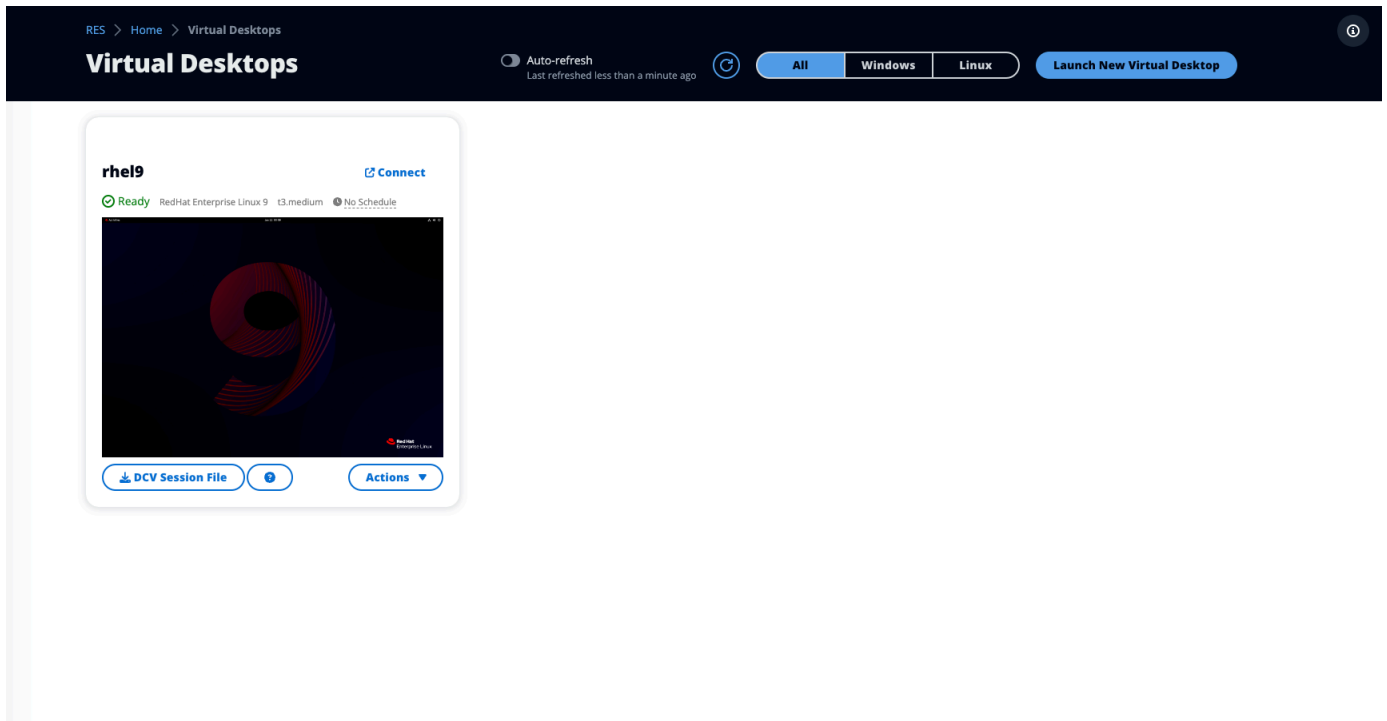
2. インストール手順については、? アイコンを選択します。



## デスクトップの状態を制御する

デスクトップの状態を制御するには:

1. [アクション] を選択します。



2. Virtual Desktop State を選択します。次の 4 つの状態から選択できます。

- 停止

停止したセッションではデータが失われることはなく、停止したセッションはいつでも再開できます。

- 再起動

現在のセッションを再起動します。

- 終了

セッションを完全に終了します。エフェメラルストレージを使用している場合、セッションを終了するとデータが失われる可能性があります。終了する前に、データを RES ファイルシステムにバックアップする必要があります。

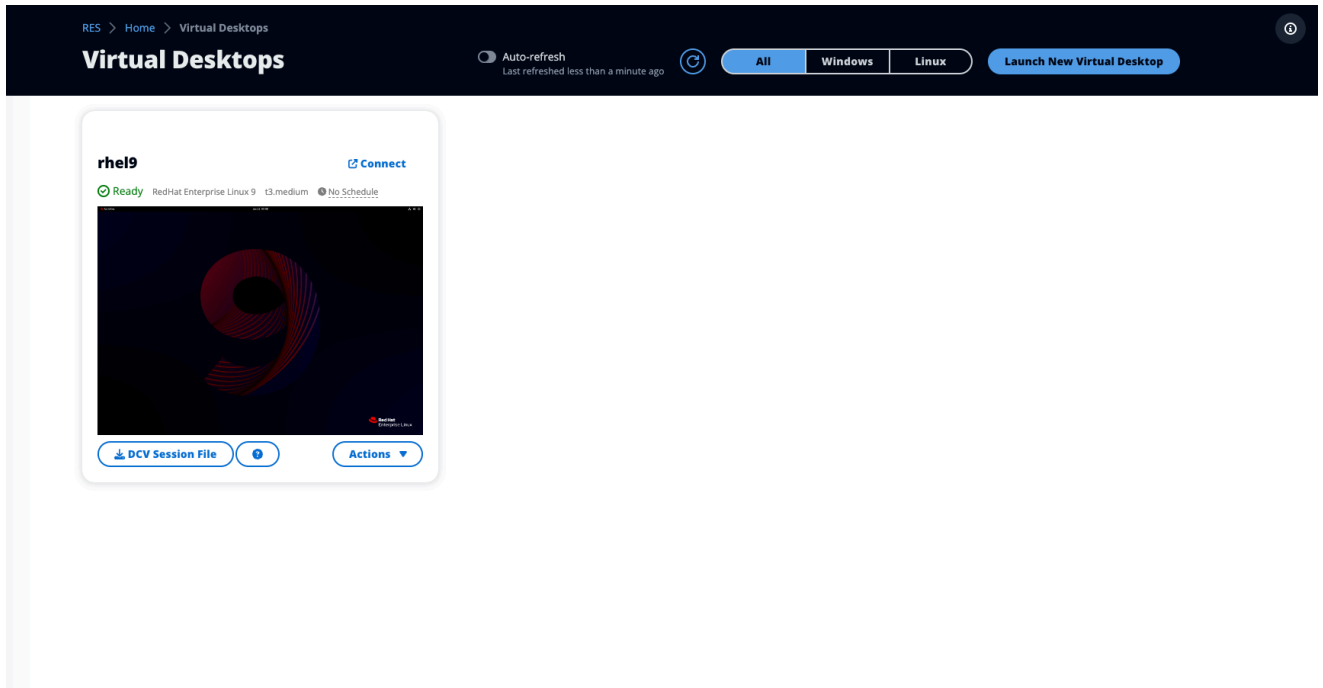
- 休止

デスクトップの状態はメモリに保存されます。デスクトップを再起動すると、アプリケーションは再開されますが、リモート接続が失われる可能性があります。すべてのインスタンスが休止をサポートしているわけではなく、オプションはインスタンスの作成時に有効になっている場合にのみ使用できます。インスタンスがこの状態をサポートしているかどうかを確認するには、[「休止の前提条件」](#)を参照してください。

## 仮想デスクトップを変更する

仮想デスクトップのハードウェアを更新するか、セッション名を変更できます。

1. インスタンスサイズを変更する前に、セッションを停止する必要があります。
  - a. [アクション] を選択します。



- b. Virtual Desktop State を選択します。
- c. [停止] を選択します。

### Note

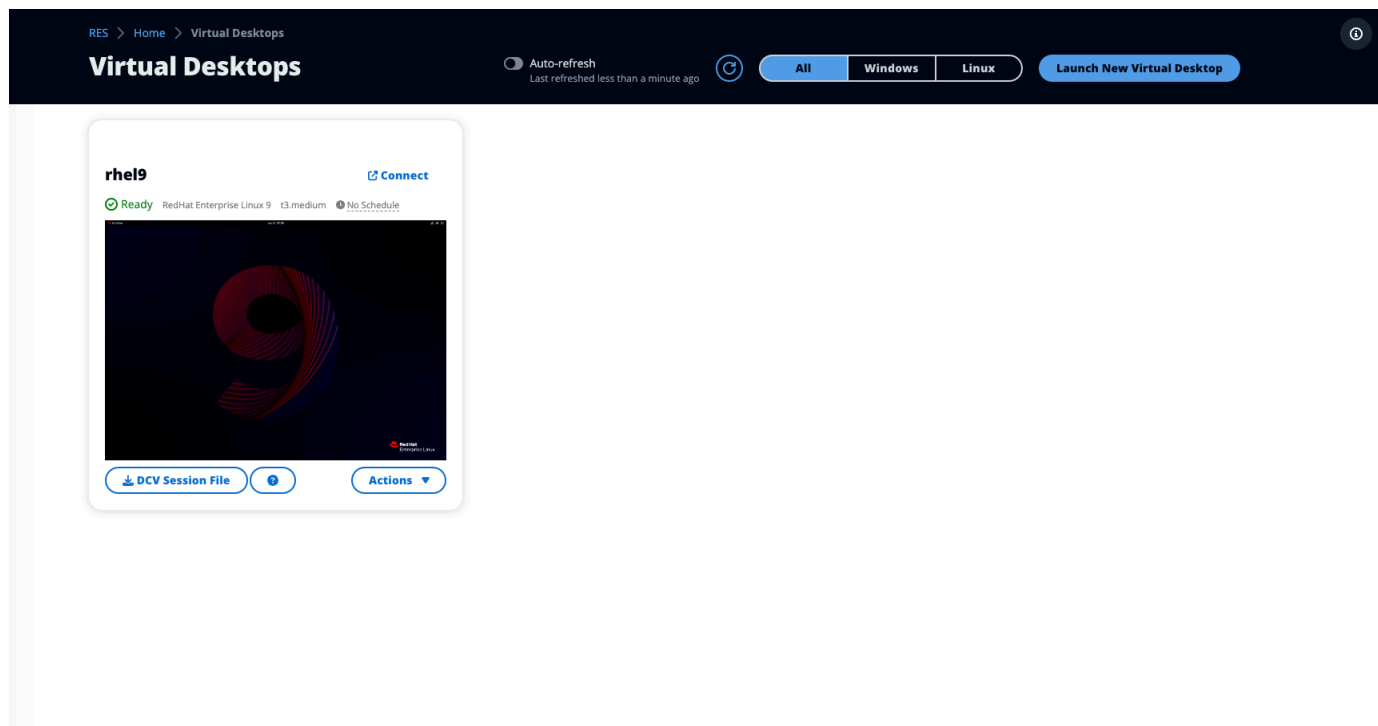
休止したセッションのデスクトップサイズは更新できません。

2. デスクトップが停止したことを確認したら、アクションを選択し、セッションの更新を選択します。
3. セッション名を変更するか、必要なデスクトップサイズを選択します。
4. [Submit] を選択してください。
5. インスタンスが更新されたら、デスクトップを再起動します。
  - a. [アクション] を選択します。

- b. Virtual Desktop State を選択します。
- c. [開始] を選択します。

## セッション情報を取得する

1. [アクション] を選択します。



2. 情報の表示を選択します。

## 仮想デスクトップをスケジュールする

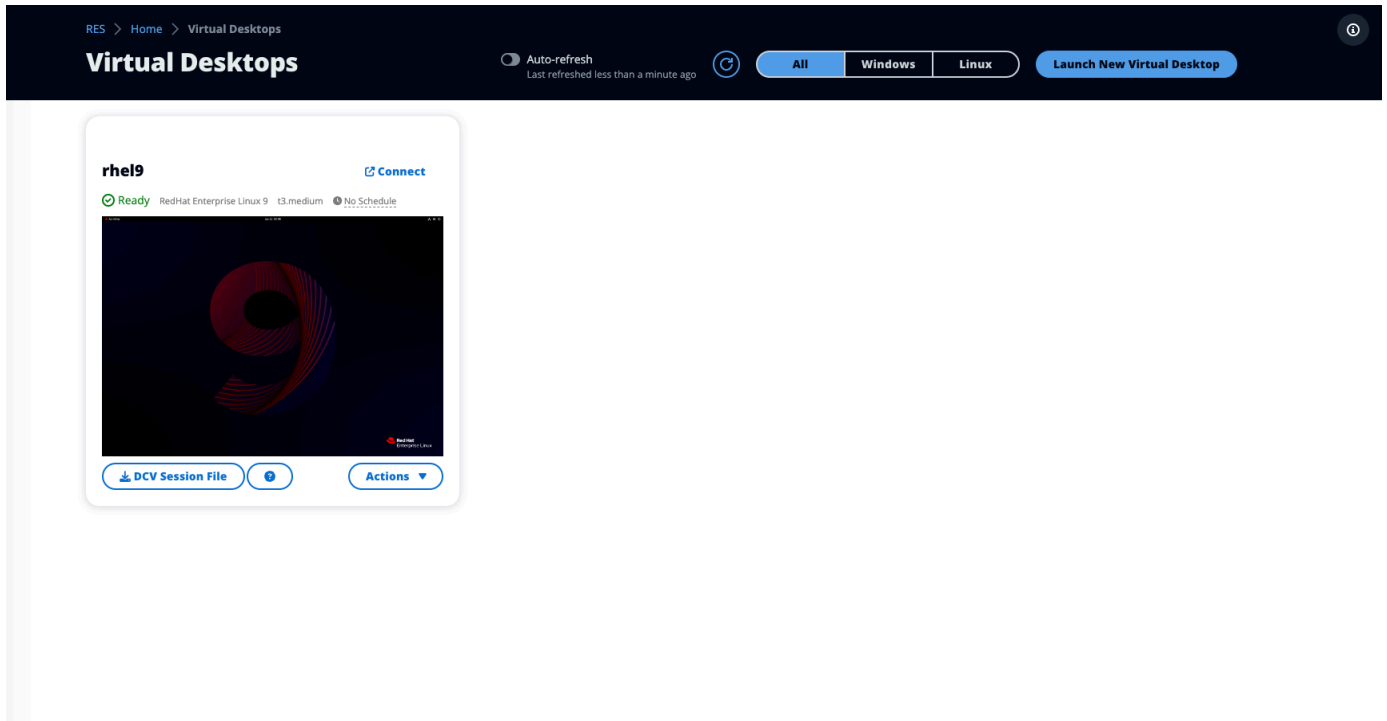
デフォルトでは、仮想デスクトップは土曜日と日曜日に自動的に停止するようにスケジュールされています。個々のデスクトップのスケジュールは、次のセクションに示すように、個々のデスクトップのアクションメニューからアクセスするスケジュールウィンドウを使用して調整できます。詳細については、「」セクション[環境全体でのデフォルトのスケジュールの設定](#)を参照してください。デスクトップは、コストを削減するためにアイドル状態のときに停止することもできます。VDI Autostopの詳細については[仮想デスクトップインターフェイスの自動停止](#)、「」を参照してください。

### トピック

- [個々のデスクトップスケジュールの設定](#)
- [環境全体でのデフォルトのスケジュールの設定](#)

## 個々のデスクトップスケジュールの設定

1. [アクション] を選択します。



2. [スケジュール] を選択します。
3. 各日のスケジュールを設定します。
4. [保存] を選択します。

## 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

## 環境全体でのデフォルトのスケジュールの設定

デフォルトのスケジュールは [DynamoDB](#) で更新できます。

1. 環境のクラスター設定テーブルを検索します: `<env-name>.cluster-settings`。
2. Explore Items を選択します。
3. フィルター に次の 2 つのフィルターを入力します。

### フィルター 1

- 属性名 = **key**
- 条件 = **Contains**
- タイプ = **String**
- 値 = **vdc.dcv\_session.schedule**

### フィルター 2

- 属性名 = **key**
- 条件 = **Contains**
- タイプ = **String**
- 値 = **type**

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

Add filter

Run Reset

これにより、フォーム の各日のデフォルトのスケジュールタイプを表す 7 つのエントリが表示されます `vdc.dcv_session.schedule.<day>.type`。有効な値は以下のとおりです。

- NO\_SCHEDULE
- STOP\_ALL\_DAY
- START\_ALL\_DAY
- WORKING\_HOURS

- CUSTOM\_SCHEDULE
4. が設定されている場合CUSTOM\_SCHEDULEは、カスタマイズされた開始時刻と停止時刻を指定する必要があります。これを行うには、クラスター設定テーブルで次のフィルターを使用します。
    - 属性名 = **key**
    - 条件 = **Contains**
    - タイプ = **String**
    - 値 = **vdc.dcv\_session.schedule**
  5. カスタムスケジュールを設定するそれぞれの  
日vdc.dcv\_session.schedule.<day>.shut\_down\_timeについて、  
vdc.dcv\_session.schedule.<day>.start\_up\_timeおよび の形式の項目を検索します。  
項目内で、次のように Null エントリを削除し、文字列エントリに置き換えます。
    - 属性名 = **value**
    - 値 = **<The time>**
    - タイプ = **String**

時間値は、24 時間制を使用して XX:XX の形式にする必要があります。たとえば、午前 9 時が 09:00、午後 5 時が 17:00 になります。入力された時刻は、常に RES 環境がデプロイされている AWS リージョンの現地時刻に対応します。

## 仮想デスクトップインターフェースの自動停止

管理者は、アイドル状態の VDI を停止または終了できるように設定を構成することができます。設定可能な設定は 4 つあります。

1. アイドルタイムアウト: CPU 使用率がしきい値を下回っているこの時間アイドル状態のセッションはタイムアウトします。
2. CPU 使用率しきい値: インタラクションがなく、このしきい値 (vCPU 使用率) 未満のセッションはアイドル状態と見なされます。これを 0 に設定すると、セッションはアイドル状態と見なされません。

**⚠ Important**

RES は、CPU 使用率をチェックするアイドル検出スクリプトを 1 分ごとに の上部で実行します。このスクリプト自体によって一時的な CPU スパイクが発生し、しきい値の設定が低すぎるとアイドル検出が妨げられる可能性があります。

3. 移行状態: アイドルタイムアウト後、セッションはこの状態に移行します (停止または終了)。
4. スケジュールを適用する: 選択すると、アイドル状態のために停止されたセッションを毎日のスケジュールで再開できます。

## Update Session Settings ✕

**Idle Timeout (minutes)**

Sessions idle for this time with CPU utilization below the threshold will time out

**CPU Utilization Threshold (%)**

Sessions under this threshold are considered idle

**Transition State**

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**

Maximum sessions allowed per user

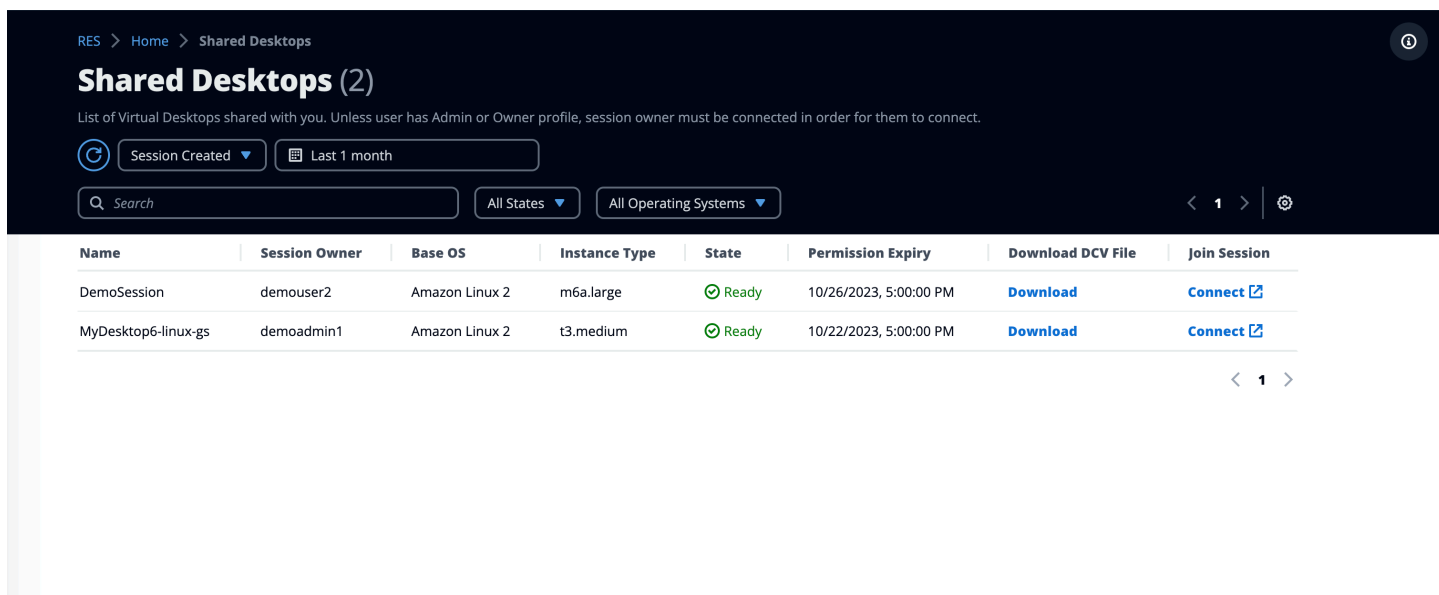
[Cancel](#) [Submit](#)

これらの設定は、サーバータブのデスクトップ設定ページにあります。要件に従って設定を更新したら、送信をクリックして設定を保存します。新しいセッションでは、更新された設定が使用されますが、既存のセッションでは、起動時に使用していた設定が引き続き使用されることに注意してください。

セッションがタイムアウトすると、セッションは設定に基づいて終了するか、STOPPED\_IDLE状態に移行します。ユーザーは UI からSTOPPED\_IDLEセッションを開始できます。

## 共有デスクトップ

共有デスクトップでは、共有されているデスクトップを確認できます。デスクトップに接続するには、管理者または所有者でない限り、セッション所有者も接続されている必要があります。



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 ▾ < 1 > ⚙

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

< 1 >

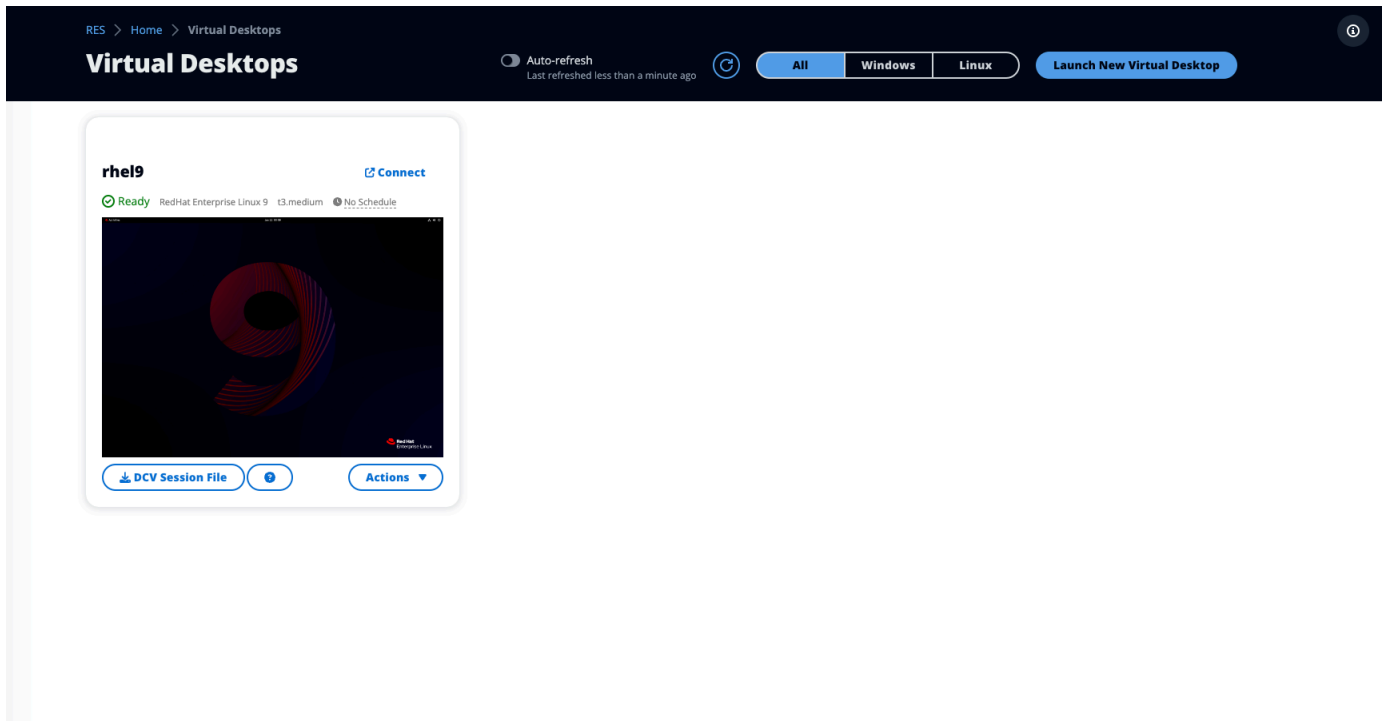
セッションを共有するときに、共同作業者のアクセス許可を設定できます。たとえば、コラボレーションしているチームメイトに読み取り専用アクセス権を付与できます。

### トピック

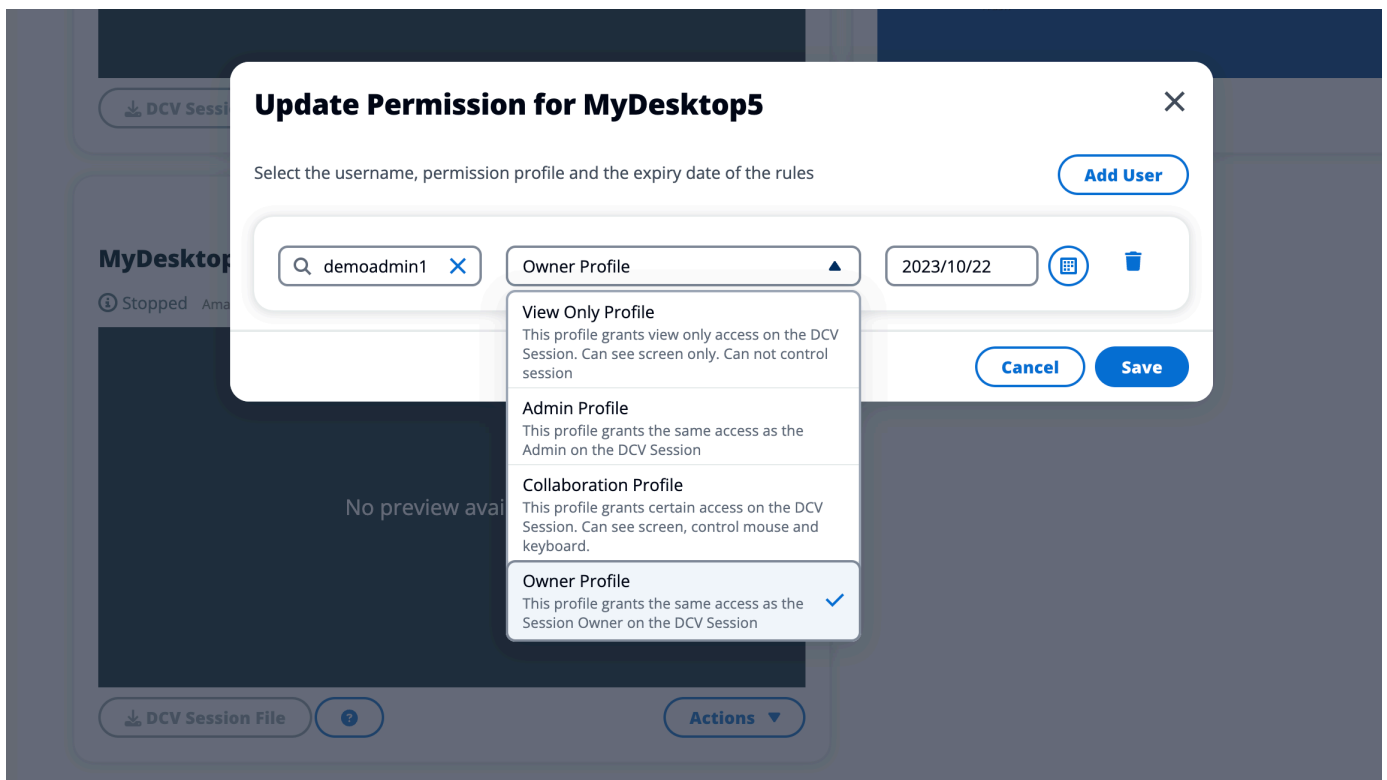
- [デスクトップを共有する](#)
- [共有デスクトップにアクセスする](#)

## デスクトップを共有する

1. デスクトップセッションから、アクションを選択します。



2. セッションのアクセス許可を選択します。
3. ユーザーとアクセス許可レベルを選択します。有効期限を設定することもできます。
4. [保存] を選択します。



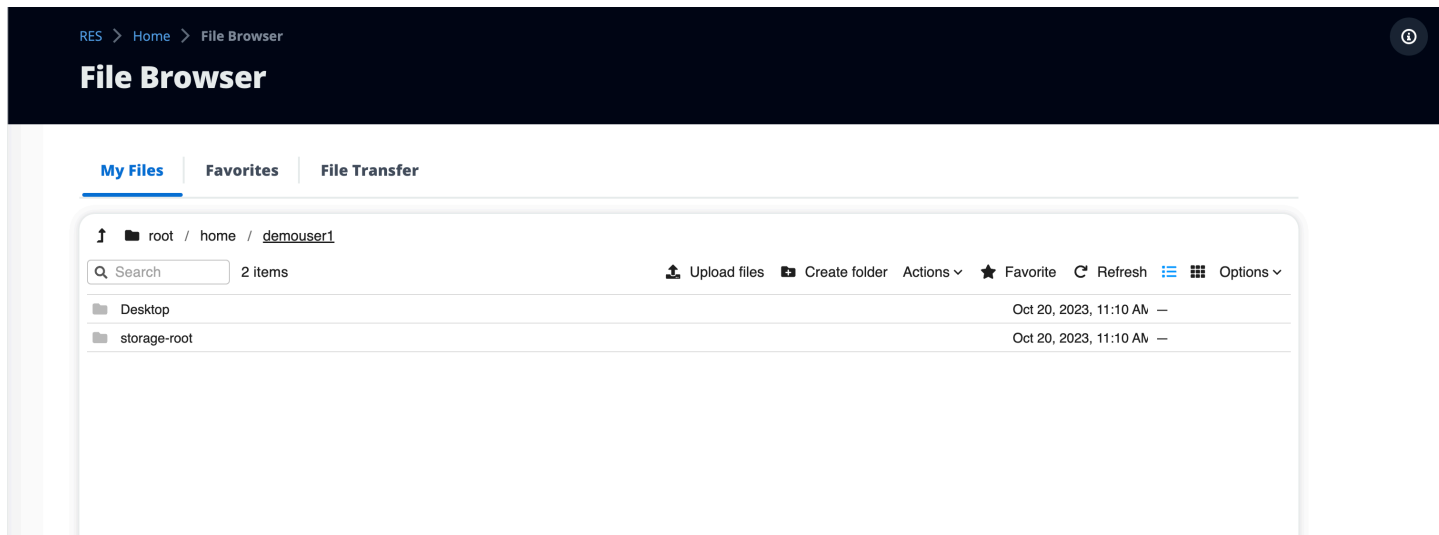
アクセス許可の詳細については、「[the section called “アクセス許可ポリシー”](#)」を参照してください。

## 共有デスクトップにアクセスする

共有デスクトップから、共有されているデスクトップを表示し、インスタンスに接続できます。ウェブブラウザまたは DCV で参加できます。接続するには、「」の指示に従います [デスクトップにアクセスする](#)。

## ファイルブラウザ

ファイルブラウザを使用すると、ウェブポータルからグローバル共有 EFS ファイルシステムにアクセスできます。基盤となるファイルシステムにアクセスするためのアクセス許可を持つ使用可能なすべてのファイルを管理できます。これは、Linux 仮想デスクトップで共有されているのと同じファイルシステムです。仮想デスクトップ上のファイルの更新は、ターミナルまたはウェブベースのファイルブラウザを介したファイルの更新と同じです。

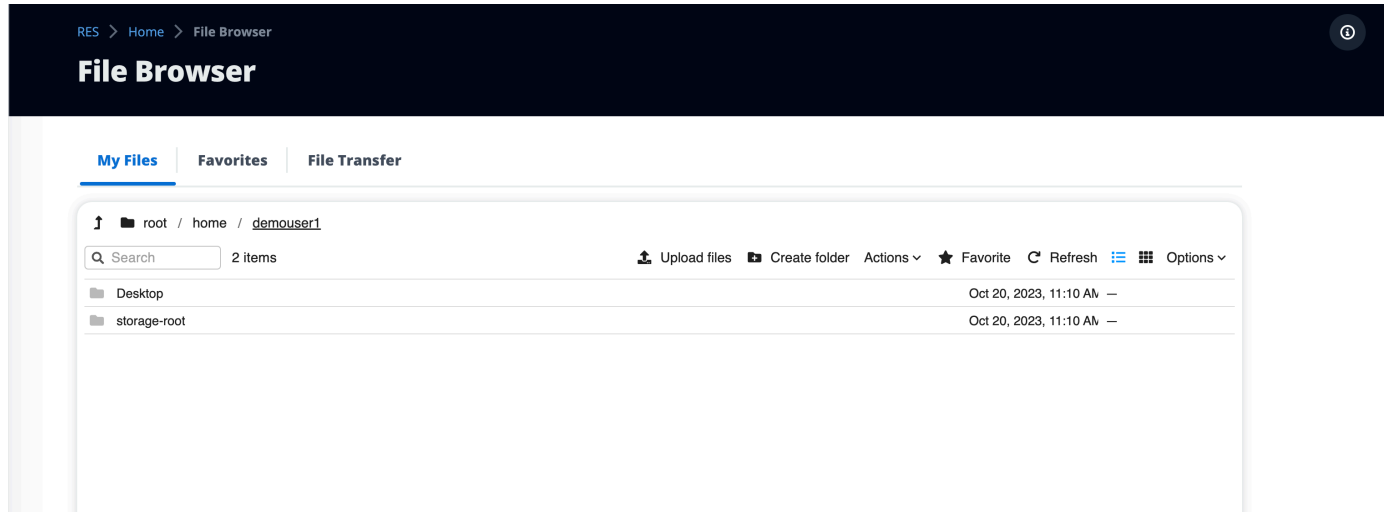


### トピック

- [ファイルのアップロード \(複数可\)](#)
- [ファイルの削除 \(複数可\)](#)
- [お気に入りを管理する](#)
- [ファイルを編集する](#)
- [ファイルの転送](#)

## ファイルのアップロード (複数可)

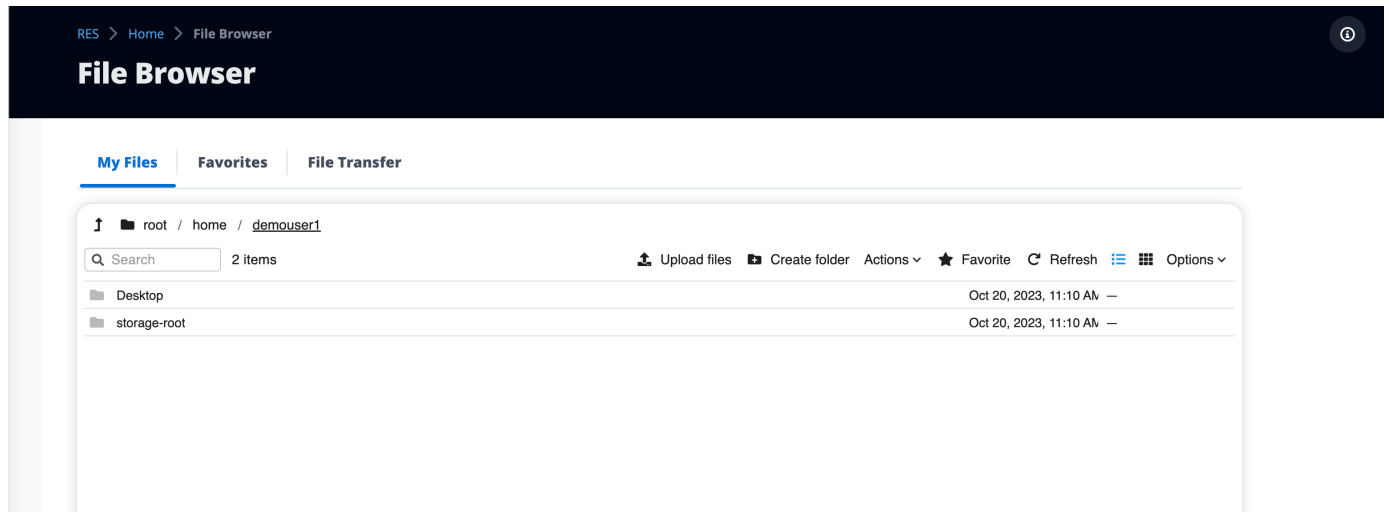
1. ファイルのアップロードを選択します。



2. ファイルを削除するか、アップロードするファイルを参照します。
3. アップロード (n) ファイルを選択します。

## ファイルの削除 (複数可)

1. 削除するファイル (複数可) を選択します。



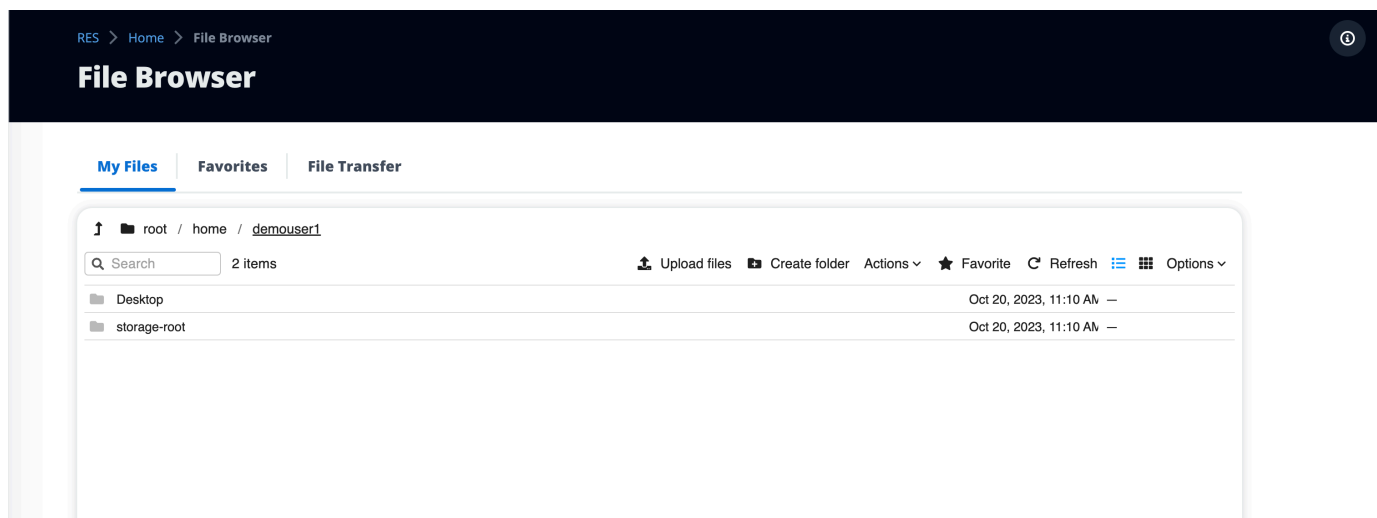
2. [アクション] を選択します。
3. ファイルの削除を選択します。

または、任意のファイルまたはフォルダを右クリックし、ファイルの削除を選択することもできます。

## お気に入りを管理する

重要なファイルやフォルダを固定するには、お気に入りに追加します。

1. ファイルまたはフォルダを選択します。



2. お気に入り を選択します。

または、任意のファイルまたはフォルダを右クリックして、お気に入り を選択することもできます。

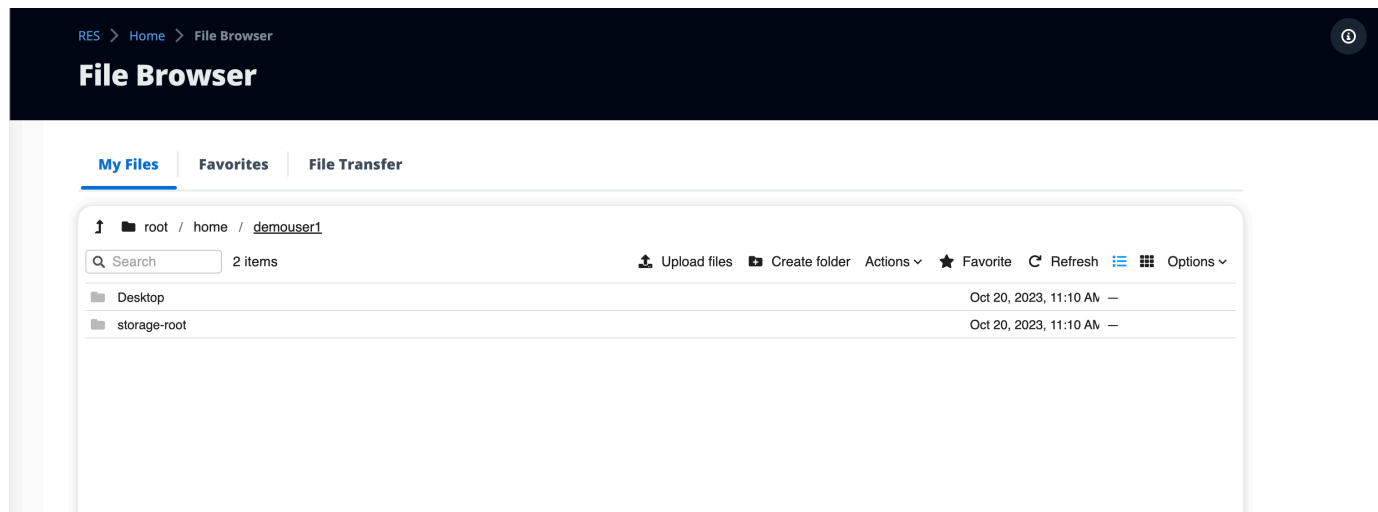
### Note

お気に入りはローカルブラウザに保存されます。ブラウザを変更したり、キャッシュをクリアしたりする場合は、お気に入りを再ピン留めする必要があります。

## ファイルを編集する

ウェブポータル内のテキストベースのファイルのコンテンツを編集できます。

1. 更新するファイルを選択します。モーダルが開き、ファイルの内容が表示されます。



2. 更新を行い、保存を選択します。

## ファイルの転送

ファイル転送を使用して、外部ファイル転送アプリケーションを使用してファイルを転送します。次のアプリケーションから選択し、画面の指示に従ってファイルを転送できます。

- 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:

<b>Host</b> [Redacted]	<b>Port</b> [Redacted]
<b>Protocol</b> SFTP	<b>Logon Type</b> Key File
<b>User</b> demouser3	<b>Key File</b> /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 [Redacted]. Check "Always Trust this Host" and Click "Ok".

Once connected, simply drag & drop to upload/download files.

# トラブルシューティング

このセクションでは、システムをモニタリングする方法と、発生する可能性のある特定の問題のトラブルシューティング方法について説明します。

## トピック

- [一般的なデバッグとモニタリング](#)
- [RunBooks の問題](#)
- [既知の問題](#)

## 詳細内容 :

- [一般的なデバッグとモニタリング](#)
  - [便利なログおよびイベント情報ソース](#)
    - [環境変数の場所](#)
    - [環境 Amazon EC2 インスタンスのログファイル](#)
    - [CloudFormation スタック](#)
    - [問題によるシステム障害が発生し、Amazon EC2 Auto Scaling グループアクティビティに反映される](#)
  - [一般的な Amazon EC2 コンソールの外観](#)
    - [インフラストラクチャホスト](#)
    - [インフラストラクチャホストと仮想デスクトップ](#)
    - [終了状態のホスト](#)
    - [参照に便利な Active Directory \(AD\) 関連のコマンド](#)
  - [Windows DCV デバッグ](#)
  - [Amazon DCV バージョン情報の検索](#)
- [RunBooks の問題](#)
  - [インストールの問題](#)
    - [CloudFormation スタックはWaitCondition received failed message」というメッセージで作成に失敗します。エラー:States.TaskFailed"](#)
    - [CloudFormation スタックが正常に作成された後に E メール通知が受信されない](#)
    - [インスタンスサイクルまたは vdc-controller が失敗状態](#)

- 環境 CloudFormation スタックが依存オブジェクトエラーにより削除に失敗する
- 環境の作成中に CIDR ブロックパラメータでエラーが発生しました
- 環境作成中の CloudFormation スタック作成の失敗
- AdDomainAdminNode CREATE\_FAILED で外部リソース (デモ) スタックの作成が失敗する
- ID 管理の問題
  - iam:PassRole を実行する権限がありません
  - 自分の AWS アカウント以外のユーザーに AWS リソースの Research and Engineering Studio へのアクセスを許可したい
  - 環境にログインすると、すぐにログインページに戻ります。
  - ログイン試行時の「ユーザーが見つかりません」エラー
  - Active Directory に追加されたが、RES に欠落しているユーザー
  - セッションの作成時に使用できないユーザー
  - CloudWatch クラスタマネージャーログのサイズ制限超過エラー
- Storage
  - RES を使用してファイルシステムを作成しましたが、VDI ホストにマウントされません
  - RES を介してファイルシステムをオンボードしたが、VDI ホストにマウントされない
  - VDI ホストから読み書きできない
    - アクセス許可処理のユースケースの例
  - RES から Amazon FSx for NetApp ONTAP を作成しましたが、ドメインに参加していません
- スナップショット
  - スナップショットのステータスが Failed である
  - スナップショットは、テーブルをインポートできなかったことを示すログとともに適用されません。
- インフラストラクチャ
  - 正常なインスタスがないロードバランサーターゲットグループ
- 仮想デスクトップの起動
  - RES ウェブポータルで多数の VDIs を起動/再開する必要がある
  - Windows Virtual Desktop のログインアカウントが管理者に設定されています
  - 外部リソース CertificateRenewalNode の使用時に証明書の有効期限が切れる
- 以前に機能していた仮想デスクトップが正常に接続できなくなりました
- 5 つの仮想デスクトップしか起動できない

- デスクトップ Windows の接続試行は「接続が閉じられました。トランスポートエラー」
- VDIsプロビジョニング状態でスタックする
- 起動後に VDI がエラー状態になる
- ログイン後、VDI セッションは空白の画面に移動します
- 仮想デスクトップコンポーネント
  - Amazon EC2 インスタンスがコンソールで終了を繰り返し表示
  - AD / eVDI モジュールに参加できなかったために vdc-controller インスタンスがサイクルしていますが、API ヘルスチェックが失敗しています
  - プロジェクトは、ソフトウェアスタックを編集して追加するときにプルダウンに表示されません
  - cluster-manager Amazon CloudWatch ログには、「<user-home-init> アカウントはまだ利用できません。ユーザーの同期を待っています」と表示されます (アカウントはユーザー名です)。
  - ログイン試行時の Windows デスクトップに「アカウントが無効になっています。管理者にお問い合わせください」
  - 外部/顧客の AD 設定に関する DHCP オプションの問題
  - Firefox エラー MOZILLA\_PKIX\_ERROR\_REQUIRED\_TLS\_FEATURE\_MISSING
- Env 削除
  - res-xxx-cluster スタックが「DELETE\_FAILED」状態で、「Role is invalid or cannot be assumed」エラーのため手動で削除できない
- ログの収集
  - VDI ログのダウンロード
  - Linux EC2 インスタンスからのログのダウンロード
  - Windows EC2 インスタンスからのログのダウンロード
  - WaitCondition エラーの ECS ログの収集
- デモ環境
  - ID プロバイダーへの認証リクエストを処理する際のデモ環境ログインエラー
  - デモスタックのキークロックが機能しない
- Active Directory の問題
  - VDI がプロビジョニング状態で長時間スタックしているか、VDI の準備が整った後に VDI を AD ユーザーとしてログインできない

- [SSO の設定後に RES ウェブポータルにログインできない](#)
- [AD ユーザーは、Linux VDIs を正常に起動した後でも、ファイルブラウザを使用してホームディレクトリにアクセスできません](#)
- [SSH アクセスが有効になっていると、AD 管理者ユーザーは踏み台ホストにアクセスできません](#)
- [RES 外部リソーススタックによってデプロイされた Active Directory の表示と管理](#)
- [既知の問題 2024.x](#)
  - [既知の問題 2024.x](#)
    - [\(2024.12 および 2024.12.01\) 新しい Cognito ユーザーを登録する際の正規表現の失敗](#)
    - [\(2024.12.01 以前\) カスタムドメインを使用して VDI に接続するときに無効な不正な証明書エラーが発生する](#)
    - [\(2024.12 および 2024.12.01\) Active Directory ユーザーは踏み台ホストに SSH できません](#)
    - [\(2024.10\) 隔離された VPCs](#)
    - [\(2024.10 以前\) Graphic 拡張インスタンスタイプの VDI の起動に失敗しました](#)
    - [\(2024 年 8 月\) インフラストラクチャ AMI 障害の準備](#)
    - [\(2024.08\) 仮想デスクトップがルートバケット ARN とカスタムプレフィックスを使用して Amazon S3 バケットの読み取り/書き込みをマウントできない](#)
    - [\(2024.06\) AD グループ名にスペースが含まれている場合、スナップショットの適用は失敗する](#)
    - [\(2024.06 以前\) AD 同期中に RES に同期されていないグループメンバー](#)
    - [\(2024.06 以前\) CVE-2024-6387、RegreSSHion、RHEL9 および Ubuntu VDIs のセキュリティ脆弱性](#)
    - [\(2024.04-2024.04.02\) VDI インスタンスのロールにアタッチされていない IAM アクセス許可境界が提供されました](#)
    - [\(2024.04.02 以前\) ap-southeast-2 \(シドニー\) の Windows NVIDIA インスタンスが起動に失敗する](#)
    - [\(2024.04 および 2024.04.01\) GovCloud での RES 削除の失敗](#)
    - [\(2024.04 - 2024.04.02\) Linux 仮想デスクトップは再起動時に「RESUMING」ステータスのままになる可能性があります](#)
    - [\(2024.04.02 以前\) SAMAccountName 属性に大文字または特殊文字が含まれている AD ユーザーの同期に失敗しました](#)
  - [\(2024.04.02 以前\) 踏み台ホストにアクセスするためのプライベートキーが無効です](#)

## 一般的なデバッグとモニタリング

このセクションでは、RES 内の情報がどこにあるかについて説明します。

- [便利なログおよびイベント情報ソース](#)
  - [環境変数の場所](#)
  - [環境 Amazon EC2 インスタンスのログファイル](#)
  - [CloudFormation スタック](#)
  - [問題によるシステム障害が発生し、Amazon EC2 Auto Scaling グループアクティビティに反映される](#)
- [一般的な Amazon EC2 コンソールの外観](#)
  - [インフラストラクチャホスト](#)
  - [インフラストラクチャホストと仮想デスクトップ](#)
  - [終了状態のホスト](#)
  - [参照に便利な Active Directory \(AD\) 関連のコマンド](#)
- [Windows DCV デバッグ](#)
- [Amazon DCV バージョン情報の検索](#)

### 便利なログおよびイベント情報ソース

保持される情報のさまざまなソースは、トラブルシューティングやモニタリングの用途で参照できます。

#### 環境変数の場所

デフォルトでは、セッション所有者のユーザー名などの環境変数は、次の場所にあります。

- Linux: /etc/environment
- Windows: C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\environment\_variables.json

## 環境 Amazon EC2 インスタンスのログファイル

ログファイルは、RES で使用されている Amazon EC2 インスタンスに存在します。SSM セッションマネージャーを使用して、これらのファイルを調べるためにインスタンスへのセッションを開くことができます。

cluster-manager や vdc-controller などのインフラストラクチャインスタンスでは、アプリケーションやその他のログは次の場所にあります。

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

Linux 仮想デスクトップでは、以下には便利なログファイルが含まれています。

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages
- /opt/idea/app/logs/
- /opt/res/logs/vdi\_idle\_check.log

Windows 仮想デスクトップインスタンスのログについては、「」を参照してください。

- PS C:\ProgramData\nice\dcv\log
- PS C:\ProgramData\nice\DCVSessionManagerAgent\log
- PS C:\IDEA\Logs\RESIdleCheckVDI\
- C:\Program Files\RES\app\

Windows では、一部のアプリケーションのログ記録は次の場所にあります。

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

Windows では、NICE DCV 証明書ファイルは以下にあります。

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

### Amazon CloudWatch ロググループ

Amazon EC2 と AWS Lambda コンピューティングリソースのログ情報は Amazon CloudWatch Log Groups に記録されます。ログエントリ内のログエントリは、潜在的な問題のトラブルシューティングや一般的な情報の役に立つ情報を提供します。

これらのグループの名前は次のとおりです。

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

ロググループを調べるときは、次のような大文字と小文字の文字列を使用してフィルタリングすると便利です。これにより、メモされた文字列を含むメッセージのみが出力されます。

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

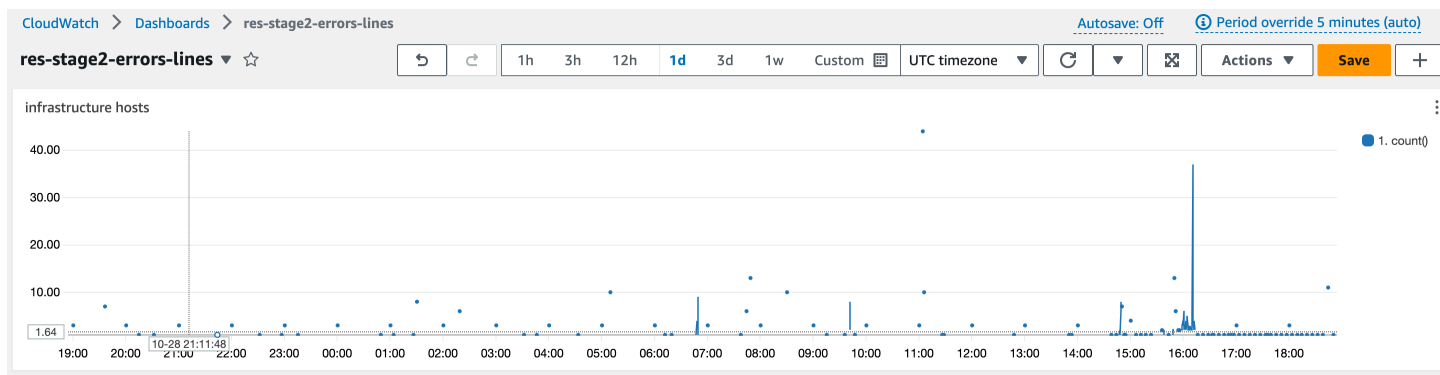
問題をモニタリングするもう 1 つの方法は、対象のデータを表示するウィジェットを含む Amazon CloudWatch Dashboards を作成することです。

たとえば、文字列エラーと ERROR の発生をカウントするウィジェットを作成し、線としてグラフ化します。この方法により、パターン変更が発生したことを示す潜在的な問題や傾向の出現を簡単に検出できます。

インフラストラクチャホストの の例を次に示します。これを使用するには、クエリ行を連結し、`<envname>` および `<region>` 属性を適切な値に置き換えます。

```
{
  "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
      }
    }
  ]
}
```

ダッシュボードの例を次に示します。



## CloudFormation スタック

環境の作成時に作成された CloudFormation スタックには、環境の設定に関連するリソース、イベント、出力情報が含まれます。

スタックごとに、イベント、リソース、出力タブを参照して、スタックに関する情報を確認できます。

RES スタック:

- <envname>-bootstrap
- <envname>-cluster
- <envname>-metrics
- <envname>-directoryservice
- <envname>-identity-provider
- <envname>-shared-storage
- <envname>-cluster-manager
- <envname>-vdc
- <envname>-踏み台ホスト

デモ環境スタック (デモ環境をデプロイしていて、これらの外部リソースを利用できない場合は、AWS ハイパフォーマンスコンピューティングレシピを使用してデモ環境のリソースを生成できます)。

- <envname>
- <envname>-Networking
- <envname>-DirectoryService
- <envname>-Storage
- <envname>-WindowsManagementHost

問題によるシステム障害が発生し、Amazon EC2 Auto Scaling グループアクティビティに反映される

RES UIs がサーバーエラーを示している場合、原因はアプリケーションソフトウェアやその他の問題である可能性があります。

各インフラストラクチャの Amazon EC2 インスタンスの自動スケーリンググループ (ASGs) には、インスタンスのスケーリングアクティビティを検出するのに役立つアクティビティタブが含まれています。UI ページにエラーがある場合やアクセスできない場合は、Amazon EC2 コンソールで複数の終了したインスタンスをチェックし、関連する ASG の Auto Scaling グループアクティビティタブをチェックして、Amazon EC2 インスタンスが循環しているかどうかを確認します。

その場合は、インスタンスの関連する Amazon CloudWatch ロググループを使用して、問題の原因を示す可能性のあるエラーがログに記録されているかどうかを確認します。SSM セッションコンソールを使用して、そのタイプの実行中のインスタンスへのセッションを開き、インスタンスが異常とマークされて ASG によって終了される前に、インスタンスのログファイルを調べて原因を特定することもできます。

この問題が発生した場合、ASG コンソールには次のようなアクティビティが表示されることがあります。

The screenshot shows the Amazon EC2 console interface for a Target Group named 'res-bicfn3-web-portal-e2958adc'. The breadcrumb navigation at the top is 'EC2 > Target groups > res-bicfn3-web-portal-e2958adc'. The 'Load Balancing' menu item in the left sidebar is circled in red. The 'Details' section shows the following information:

- Target type: Instance
- Protocol: Port: HTTPS: 8443
- Protocol version: HTTP1
- VPC: vpc-011d10e23ad10cb8e
- IP address type: IPv4
- Load balancer: res-bicfn3-external-alb

The 'Summary' section shows the following counts:

- Total targets: 1
- Healthy: 1
- Unhealthy: 0
- Unused: 0
- Initial: 0
- Draining: 0

The 'Registered targets' table shows one target:

Instance ID	Name	Port	Zone	Health status	Health status details
i-0ba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1-c	healthy	

## 一般的な Amazon EC2 コンソールの外観

このセクションには、さまざまな状態で動作しているシステムのスクリーンショットが含まれています。

## インフラストラクチャホスト

Amazon EC2 コンソールでは、デスクトップが実行されていない場合、通常、次のようになります。表示されるインスタンスは、RES インフラストラクチャの Amazon EC2 ホストです。インスタンス名のプレフィックスは RES 環境名です。

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

**Instances (5) Info**

Find Instance by attribute or tag (case-sensitive)

res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▲	Instance type ▼
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	🟢 Running	m5.large

## インフラストラクチャホストと仮想デスクトップ

Amazon EC2 コンソールでは、仮想デスクトップが実行されていると、次のように表示されます。この場合、仮想デスクトップは赤で表示されます。インスタンス名のサフィックスは、デスクトップを作成したユーザーです。中央の名前は起動時に設定されたセッション名であり、デフォルトの「MyDesktop」またはユーザーが設定した名前です。

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

**Instances (7) Info**

Find Instance by attribute or tag (case-sensitive)

res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▼	Instance type ▼
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	🟢 Running	m6a.large
<input type="checkbox"/>	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	🟢 Running	m6a.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	🟢 Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	🟢 Running	m5.large

## 終了状態のホスト

Amazon EC2 コンソールに終了したインスタンスが表示されると、通常は終了したデスクトップホストになります。コンソールに終了した状態のインフラストラクチャホストが含まれている場合、特に同じタイプのが複数ある場合は、システムの問題が進行中である可能性があります。

次の図は、終了したデスクトップインスタンスを示しています。

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-windows1-demoadmin4	i-092cdf6a7e52e9b9a	Terminated	m6a.large
res-stage2-rhel91-demoadmin4	i-0b3d134f606a53636	Terminated	m6a.large
res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
res-stage2-aml21-demoadmin4	i-023844b29c12b9393	Terminated	m6a.large
res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

## 参照に便利な Active Directory (AD) 関連のコマンド

以下は、AD 設定関連情報を表示するためにインフラストラクチャホストに入力できる ldap 関連のコマンドの例です。使用するドメインやその他のパラメータには、環境の作成時に入力されたパラメータを反映する必要があります。

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

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

## Windows DCV デバッグ

Windows デスクトップでは、以下を使用して関連するセッションを一覧表示できます。

```
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)
```

## Amazon DCV バージョン情報の検索

Amazon DCV は仮想デスクトップセッションに使用されます。[AWS Amazon DCV](#)。次の例は、インストールされている DCV ソフトウェアのバージョンを確認する方法を示しています。

### 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.
```

### Server

```
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.
```

## RunBooks の問題

次のセクションには、発生する可能性のある問題、それらを検出する方法、問題の解決方法に関する提案が含まれています。

- [インストールの問題](#)

- [CloudFormation スタックはWaitCondition received failed message」というメッセージで作成に失敗します。エラー:States.TaskFailed"](#)
- [CloudFormation スタックが正常に作成された後に E メール通知が受信されない](#)
- [インスタンスサイクルまたは vdc-controller が失敗状態](#)
- [環境 CloudFormation スタックが依存オブジェクトエラーにより削除に失敗する](#)
- [環境の作成中に CIDR ブロックパラメータでエラーが発生しました](#)
- [環境作成中の CloudFormation スタック作成の失敗](#)
- [AdDomainAdminNode CREATE\\_FAILED で外部リソース \(デモ\) スタックの作成が失敗する](#)
- [ID 管理の問題](#)
  - [iam:PassRole を実行する権限がありません](#)
  - [自分の AWS アカウント以外のユーザーに AWS リソースの Research and Engineering Studio へのアクセスを許可したい](#)
  - [環境にログインすると、すぐにログインページに戻ります。](#)
  - [ログイン試行時の「ユーザーが見つかりません」エラー](#)
  - [Active Directory に追加されたが、RES に欠落しているユーザー](#)
  - [セッションの作成時に使用できないユーザー](#)
  - [CloudWatch クラスタマネージャーログのサイズ制限超過エラー](#)
- [Storage](#)
  - [RES を使用してファイルシステムを作成しましたが、VDI ホストにマウントされません](#)
  - [RES を介してファイルシステムをオンボードしたが、VDI ホストにマウントされない](#)
  - [VDI ホストから読み書きできない](#)
    - [アクセス許可処理のユースケースの例](#)
  - [RES から Amazon FSx for NetApp ONTAP を作成しましたが、ドメインに参加していません](#)
- [スナップショット](#)
  - [スナップショットのステータスが Failed である](#)
  - [スナップショットは、テーブルをインポートできなかったことを示すログとともに適用されません。](#)
- [インフラストラクチャ](#)
  - [正常なインスタスがないロードバランサーターゲットグループ](#)
- [仮想デスクトップの起動](#)
  - [RES ウェブポータルで多数の VDI を起動/再開する必要がある](#)

- [Windows Virtual Desktop のログインアカウントが管理者に設定されています](#)
- [外部リソース CertificateRenewalNode の使用時に証明書の有効期限が切れる](#)
- [以前に機能していた仮想デスクトップが正常に接続できなくなりました](#)
- [5 つの仮想デスクトップしか起動できない](#)
- [デスクトップ Windows の接続試行は「接続が閉じられました。トランスポートエラー」](#)
- [VDIsプロビジョニング状態でスタックする](#)
- [起動後に VDI がエラー状態になる](#)
- [ログイン後、VDI セッションは空白の画面に移動します](#)
- [仮想デスクトップコンポーネント](#)
  - [Amazon EC2 インスタンスがコンソールで終了を繰り返し表示](#)
  - [AD / eVDI モジュールに参加できなかったために vdc-controller インスタンスがサイクルしていますが、API ヘルスチェックが失敗しています](#)
  - [プロジェクトは、ソフトウェアスタックを編集して追加するときにプルダウンに表示されません](#)
  - [cluster-manager Amazon CloudWatch ログには、「<user-home-init> アカウントはまだ利用できません。ユーザーの同期を待っています」と表示されます \(アカウントはユーザー名です\)。](#)
  - [ログイン試行時の Windows デスクトップに「アカウントが無効になっています。管理者にお問い合わせください」](#)
  - [外部/顧客の AD 設定に関する DHCP オプションの問題](#)
  - [Firefox エラー MOZILLA\\_PKIX\\_ERROR\\_REQUIRED\\_TLS\\_FEATURE\\_MISSING](#)
- [Env 削除](#)
  - [res-xxx-cluster スタックが「DELETE\\_FAILED」状態で、「Role is invalid or cannot be assumed」エラーのため手動で削除できない](#)
  - [ログの収集](#)
  - [VDI ログのダウンロード](#)
  - [Linux EC2 インスタンスからのログのダウンロード](#)
  - [Windows EC2 インスタンスからのログのダウンロード](#)
  - [WaitCondition エラーの ECS ログの収集](#)
- [デモ環境](#)
  - [ID プロバイダーへの認証リクエストを処理する際のデモ環境ログインエラー](#)
  - [デモスタックのキークロークが機能しない](#)

- [VDI がプロビジョニング状態で長時間スタックしているか、VDI の準備が整った後に VDI を AD ユーザーとしてログインできない](#)
- [SSO の設定後に RES ウェブポータルにログインできない](#)
- [AD ユーザーは、Linux VDI を正常に起動した後でも、ファイルブラウザを使用してホームディレクトリにアクセスできません](#)
- [SSH アクセスが有効になっていると、AD 管理者ユーザーは踏み台ホストにアクセスできません](#)
- [RES 外部リソーススタックによってデプロイされた Active Directory の表示と管理](#)

## インストールの問題

### トピック

- [CloudFormation スタックはWaitCondition received failed message」というメッセージで作成に失敗します。エラー:States.TaskFailed"](#)
- [CloudFormation スタックが正常に作成された後に E メール通知が受信されない](#)
- [インスタンスサイクルまたは vdc-controller が失敗状態](#)
- [環境 CloudFormation スタックが依存オブジェクトエラーにより削除に失敗する](#)
- [環境の作成中に CIDR ブロックパラメータでエラーが発生しました](#)
- [環境作成中の CloudFormation スタック作成の失敗](#)
- [AdDomainAdminNode CREATE\\_FAILED で外部リソース \(デモ\) スタックの作成が失敗する](#)

.....

CloudFormation スタックはWaitCondition received failed message」というメッセージで作成に失敗します。エラー:States.TaskFailed"

問題を特定するには、 という名前の Amazon CloudWatch ロググループを調べます <stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>。同じ名前のロググループが複数ある場合は、最初に使用可能なロググループを調べます。ログ内のエラーメッセージには、問題に関する詳細情報が表示されます。

#### Note

パラメータ値にスペースがないことを確認します。

## CloudFormation スタックが正常に作成された後に E メール通知が受信されない

CloudFormation スタックが正常に作成された後に Eメールの招待を受信しなかった場合は、以下を確認します。

1. E メールアドレスパラメータが正しく入力されたことを確認します。

E メールアドレスが正しくないか、アクセスできない場合は、Research and Engineering Studio 環境を削除して再デプロイします。

2. インスタンスのサイクルの証拠については、Amazon EC2 コンソールを確認してください。

<envname> プレフィックスが の Amazon EC2 インスタンスが終了済みとして表示され、新しいインスタンスに置き換えられる場合、ネットワークまたは Active Directory の設定に問題がある可能性があります。

3. High AWS Performance Compute レシピをデプロイして外部リソースを作成した場合は、VPC、プライベートサブネットとパブリックサブネット、およびその他の選択したパラメータがスタックによって作成されたことを確認します。

パラメータのいずれかが正しくない場合は、RES 環境を削除して再デプロイする必要がある場合があります。詳細については、「[製品のアンインストール](#)」を参照してください。

4. 独自の外部リソースを使用して製品をデプロイした場合は、ネットワークと Active Directory が予想される設定と一致していることを確認します。

インフラストラクチャインスタンスが Active Directory に正常に参加したことを確認することが重要です。このステップを試す [the section called “インスタンスサイクルまたは vdc-controller が失敗状態”](#)して問題を解決します。

## インスタンスサイクルまたは vdc-controller が失敗状態

この問題の最も可能性の高い原因は、リソース (複数可) が Active Directory に接続または参加できないことです。

問題を検証するには:

1. コマンドラインから、vdc-controller の実行中のインスタンスで SSM とのセッションを開始します。
2. `sudo su -` を実行します。
3. `systemctl status sssd` を実行します。

ステータスが非アクティブ、失敗、またはログにエラーが表示される場合、インスタンスは Active Directory に参加できませんでした。

```
[root@ip-10-3-144-194 ~]# 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)
     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

## SSM エラーログ

問題を解決するには:

- 同じコマンドラインインスタンスから、`cat /root/bootstrap/logs/userdata.log` を実行してログを調査します。

この問題には、3つの根本原因のいずれかが考えられます。

根本原因 1: 不正な Idap 接続の詳細が入力されました

ログを見直します。以下が複数回繰り返される場合、インスタンスは Active Directory に参加できませんでした。

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

```
+ [[ 0 -1e 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. RES スタックの作成中に以下のパラメータ値が正しく入力されたことを確認します。
  - directoryservice.ldap\_connection\_uri
  - directoryservice.ldap\_base
  - directoryservice.users.ou
  - directoryservice.groups.ou
  - directoryservice.sudoers.ou
  - directoryservice.computers.ou
  - directoryservice.name
2. DynamoDB テーブルの誤った値を更新します。テーブルは、テーブルの下の DynamoDB コンソールにあります。テーブル名は `<stack name>.cluster-settings`。
3. テーブルを更新したら、現在環境インスタンスを実行している cluster-manager と vdc-controller を削除します。Auto Scaling は、DynamoDB テーブルの最新の値を使用して新しいインスタンスを開始します。

根本原因 2: ServiceAccount ユーザー名が正しく入力されていない

ログが を返す場合 Insufficient permissions to modify computer account、スタックの作成時に入力した ServiceAccount 名が正しくない可能性があります。

1. AWS コンソールから Secrets Manager を開きます。
2. directoryserviceServiceAccountUsername を検索します。シークレットは `<stack name>-directoryservice-ServiceAccountUsername`。
3. シークレットを開いて詳細ページを表示します。シークレット値 で、シークレット値の取得 を選択し、プレーンテキスト を選択します。

4. 値が更新された場合は、環境の現在実行中の cluster-manager インスタンスと vdc-controller インスタンスを削除します。自動スケーリングは、Secrets Manager の最新値を使用して新しいインスタンスを起動します。

### 根本原因 3: ServiceAccount パスワードが正しくない

ログにと表示される場合 Invalid credentials、スタックの作成時に入力した ServiceAccount パスワードが正しくない可能性があります。

1. AWS コンソールから Secrets Manager を開きます。
2. `directoryserviceServiceAccountPassword` を検索します。シークレットは `directoryservice-ServiceAccountPassword` である必要があります `<stack name>-directoryservice-ServiceAccountPassword`。
3. シークレットを開いて詳細ページを表示します。シークレット値 で、シークレット値の取得 を選択し、プレーンテキスト を選択します。
4. パスワードを忘れた場合、または入力したパスワードが正しいかどうかわからない場合は、Active Directory と Secrets Manager でパスワードをリセットできます。
  - a. でパスワードをリセットするには AWS Managed Microsoft AD:
    - i. AWS コンソールを開き、 に移動します Directory Service。
    - ii. RES ディレクトリのディレクトリ ID を選択し、アクションを選択します。
    - iii. ユーザーパスワードのリセットを選択します。
    - iv. ServiceAccount ユーザー名を入力します。
    - v. 新しいパスワードを入力し、パスワードのリセットを選択します。
  - b. Secrets Manager でパスワードをリセットするには:
    - i. AWS コンソールを開き、Secrets Manager に移動します。
    - ii. `directoryserviceServiceAccountPassword` を検索します。シークレットは `directoryservice-ServiceAccountPassword` である必要があります `<stack name>-directoryservice-ServiceAccountPassword`。
    - iii. シークレットを開いて詳細ページを表示します。シークレット値 で、シークレット値の取得 を選択し、プレーンテキスト を選択します。
    - iv. [編集] を選択します。
    - v. ServiceAccount ユーザーの新しいパスワードを設定し、保存を選択します。

5. 値を更新した場合は、環境の現在実行中の cluster-manager インスタンスと vdc-controller インスタンスを削除します。Auto Scaling は、最新の値を使用して新しいインスタンスを開始します。

## 環境 CloudFormation スタックが依存オブジェクトエラーにより削除に失敗する

などの依存オブジェクトエラーが原因で `<env-name>-vdc` CloudFormation スタックの削除が失敗した場合 `vdcvhostsecuritygroup`、コンソールを使用して AWS RES が作成したサブネットまたはセキュリティグループに起動された Amazon EC2 インスタンスが原因である可能性があります。

この問題を解決するには、この方法で起動されたすべての Amazon EC2 インスタンスを検索して終了します。その後、環境の削除を再開できます。

## 環境の作成中に CIDR ブロックパラメータでエラーが発生しました

環境を作成すると、レスポンスステータスが [FAILED] の CIDR ブロックパラメータにエラーが表示されます。

エラーの例:

```
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.
```

この問題を解決するために想定される形式は `x.x.x.0/24` または `x.x.x.0/32` です。

## 環境作成中の CloudFormation スタック作成の失敗

環境の作成には、一連のリソース作成オペレーションが含まれます。一部のリージョンでは、容量の問題が発生し、CloudFormation スタックの作成が失敗する可能性があります。

この場合、環境を削除し、作成を再試行します。または、別のリージョンで作成を再試行することもできます。

## AdDomainAdminNode CREATE\_FAILED で外部リソース (デモ) スタックの作成が失敗する

デモ環境スタックの作成が次のエラーで失敗した場合、インスタンスの起動後のプロビジョニング中に Amazon EC2 パッチ適用が予期せず発生した可能性があります。

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

失敗の原因を特定するには:

1. SSM ステートマネージャーで、パッチ適用が設定されているかどうか、およびすべてのインスタンスに対して設定されているかどうかを確認します。
2. SSM RunCommand/Automation の実行履歴で、パッチ適用関連の SSM ドキュメントの実行がインスタンスの起動と一致するかどうかを確認します。
3. 環境の Amazon EC2 インスタンスのログファイルで、ローカルインスタンスのログ記録を確認して、プロビジョニング中にインスタンスが再起動したかどうかを確認します。

パッチ適用が原因で問題が発生した場合は、起動から少なくとも 15 分後に RES インスタンスのパッチ適用を遅らせます。

## ID 管理の問題

シングルサインオン (SSO) と ID 管理のほとんどの問題は、設定ミスが原因で発生します。SSO 設定の設定については、以下を参照してください。

- [the section called “IAM Identity Center での SSO の設定”](#)
- [the section called “SSO 用の ID プロバイダーの設定”](#)

ID 管理に関連するその他の問題をトラブルシューティングするには、以下のトラブルシューティングトピックを参照してください。

トピック

- [iam:PassRole を実行する権限がありません](#)

- [自分の AWS アカウント以外のユーザーに AWS リソースの Research and Engineering Studio へのアクセスを許可したい](#)
- [環境にログインすると、すぐにログインページに戻ります。](#)
- [ログイン試行時の「ユーザーが見つかりません」エラー](#)
- [Active Directory に追加されたが、RES に欠落しているユーザー](#)
- [セッションの作成時に使用できないユーザー](#)
- [CloudWatch クラスターマネージャーログのサイズ制限超過エラー](#)

## iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して RES にロールを渡すことができるようにする必要があります。

一部の AWS サービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

次の例のエラーは、marymajor という名前の IAM ユーザーがコンソールを使用して RES でアクションを実行しようとするときに発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。サポートが必要な場合は、AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

## 自分の AWS アカウント以外のユーザーに AWS リソースの Research and Engineering Studio へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用し、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- 所有している AWS アカウント間でリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「[所有している別の AWS アカウントの IAM ユーザーへのアクセスを提供する](#)」を参照してください。
- サードパーティー AWS アカウントにリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「[サードパーティーが所有する AWS アカウントへのアクセスを提供する](#)」を参照してください。
- ID フェデレーションを通じてアクセスを提供する方法については、IAM ユーザーガイドの「[外部で認証されたユーザー \(ID フェデレーション\) へのアクセスを提供する](#)」を参照してください。
- クロスアカウントアクセスにロールとリソースベースのポリシーを使用する方法の違いについては、[IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーの違い」](#)を参照してください。

.....

環境にログインすると、すぐにログインページに戻ります。

この問題は、SSO 統合の設定が間違っている場合に発生します。問題を特定するには、コントローラーインスタンスログをチェックし、エラーがないか設定を確認します。

ログを確認するには:

1. [CloudWatch コンソール](#)を開きます。
2. ロググループから、という名前のグループを見つけます/`<environment-name>/cluster-manager`。
3. ロググループを開いて、ログストリームのエラーを検索します。

設定を確認するには:

1. [DynamoDB コンソール](#)を開く
2. テーブルから、という名前のテーブルを見つけます `<environment-name>.cluster-settings`。
3. テーブルを開き、Explore table items を選択します。

4. フィルターセクションを展開し、次の変数を入力します。
  - 属性名 – キー
  - 条件 – を含む
  - 値 – sso
5. [Run] (実行) を選択します。
6. 返された文字列で、SSO 設定値が正しいことを確認します。正しくない場合は、sso\_enabled キーの値を False に変更します。

### 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](#)

The screenshot shows a configuration interface for attributes. It has a table with two columns: 'Attribute name' and 'Value'. The first row has 'key - Partition key' in the first column and 'identity-provider.cognito.sso\_enabled' in the second. Below this, there is a 'value' field with two radio buttons: 'True' and 'False'. The 'False' radio button is selected, and an orange arrow points to it from the right.

7. RES ユーザーインターフェイスに戻り、SSO を再設定します。

.....

## ログイン試行時の「ユーザーが見つかりません」エラー

ユーザーが RES インターフェイスにログインしようとしたときに「ユーザーが見つかりません」というエラーが表示され、そのユーザーが Active Directory に存在する場合:

- ユーザーが RES に存在せず、最近 AD にユーザーを追加した場合
  - ユーザーがまだ RES に同期されていない可能性があります。RES は 1 時間ごとに同期するため、次の同期後にユーザーが追加されたことを待機して確認する必要がある場合があります。すぐに同期するには、「」の手順に従います [Active Directory に追加されたが、RES に欠落しているユーザー](#)。
- ユーザーが RES に存在する場合:
  1. 属性マッピングが正しく設定されていることを確認します。詳細については、「[シングルサインオン \(SSO\) 用の ID プロバイダーの設定](#)」を参照してください。

2. SAML 件名と SAML E メール の両方がユーザーの E メールアドレスにマッピングされていることを確認します。

.....

## Active Directory に追加されたが、RES に欠落しているユーザー

### Note

このセクションは RES 2024.10 以前に適用されます。RES 2024.12 以降については、「」を参照してください[同期を手動で実行する方法 \(リリース 2024.12 および 2024.12.01\)](#)。RES 2025.03 以降については、「」を参照してください[同期を手動で開始または停止する方法 \(リリース 2025.03 以降\)](#)。

ユーザーを Active Directory に追加しても RES がない場合は、AD 同期をトリガーする必要があります。AD 同期は、AD エントリを RES 環境にインポートする Lambda 関数によって 1 時間ごとに実行されます。場合によっては、新しいユーザーまたはグループを追加した後、次の同期プロセスが実行されるまで遅延することがあります。Amazon Simple Queue Service から手動で同期を開始できます。

同期プロセスを手動で開始します。

1. [Amazon SQS コンソール](#)を開きます。
2. キューから、 を選択します <environment-name>-cluster-manager-tasks.fifo。
3. [メッセージの送信と受信] を選択します。
4. メッセージ本文には、次のように入力します。

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

5. メッセージグループ ID には、次のように入力します。 **adsync.sync-from-ad**
6. メッセージ重複排除 ID には、ランダムな英数字文字列を入力します。このエントリは、過去 5 分以内に行われたすべての呼び出しとは異なる必要があります。そうしないと、リクエストは無視されます。

## セッションの作成時に使用できないユーザー

セッションを作成する管理者が、セッションの作成時に Active Directory に属しているユーザーが利用できない場合、ユーザーは初めてログインする必要がある場合があります。セッションはアクティブなユーザーに対してのみ作成できます。アクティブなユーザーは、少なくとも 1 回環境にログインする必要があります。

.....

## CloudWatch クラスタマネージャーログのサイズ制限超過エラー

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

CloudWatch クラスタマネージャーログにこのエラーが表示された場合、ldap 検索が返したユーザーレコードが多すぎる可能性があります。この問題を修正するには、IDP の ldap 検索結果の制限を引き上げます。

.....

## Storage

### トピック

- [RES を使用してファイルシステムを作成しましたが、VDI ホストにマウントされません](#)
  - [RES を介してファイルシステムをオンボードしたが、VDI ホストにマウントされない](#)
  - [VDI ホストから読み書きできない](#)
  - [RES から Amazon FSx for NetApp ONTAP を作成しましたが、ドメインに参加していません](#)
- .....

## RES を使用してファイルシステムを作成しましたが、VDI ホストにマウントされません

ファイルシステムは、VDI ホストでマウントする前に「使用可能」状態である必要があります。以下のステップに従って、ファイルシステムが必須状態であることを確認します。

### Amazon EFS

1. [Amazon EFS コンソール](#)に移動します。
2. ファイルシステムの状態が使用可能であることを確認します。
3. ファイルシステムの状態が使用可能でない場合は、VDI ホストを起動する前に待ちます。

## Amazon FSx ONTAP

1. [Amazon FSx コンソール](#)に移動します。
2. ステータスが使用可能であることを確認します。
3. Status が使用可能でない場合は、VDI ホストを起動するまで待ちます。

## RES を介してファイルシステムをオンボードしたが、VDI ホストにマウントされない

RES にオンボードされるファイルシステムには、VDI ホストがファイルシステムをマウントできるように、必要なセキュリティグループルールが設定されている必要があります。これらのファイルシステムは RES の外部で作成されるため、RES は関連するセキュリティグループルールを管理しません。

オンボードされたファイルシステムに関連付けられたセキュリティグループは、次のインバウンドトラフィックを許可する必要があります。

- Linux " ホストからの NFS トラフィック (ポート: 2049)
- Windows " ホストからの SMB トラフィック (ポート: 445)

## VDI ホストから読み書きできない

ONTAP は、ボリュームの UNIX、NTFS、MIXED セキュリティスタイルをサポートしています。セキュリティスタイルは、ONTAP がデータアクセスを制御するために使用するアクセス許可のタイプと、これらのアクセス許可を変更できるクライアントタイプを決定します。

たとえば、ボリュームが UNIX セキュリティスタイルを使用している場合でも、ONTAP のマルチプロトコル特性により、SMB クライアントは引き続きデータにアクセスできます (ただし、適切に認証および認可される場合に限り)。ただし、ONTAP は UNIX クライアントのみがネイティブツールを使用して変更できる UNIX アクセス許可を使用します。

## アクセス許可処理のユースケースの例

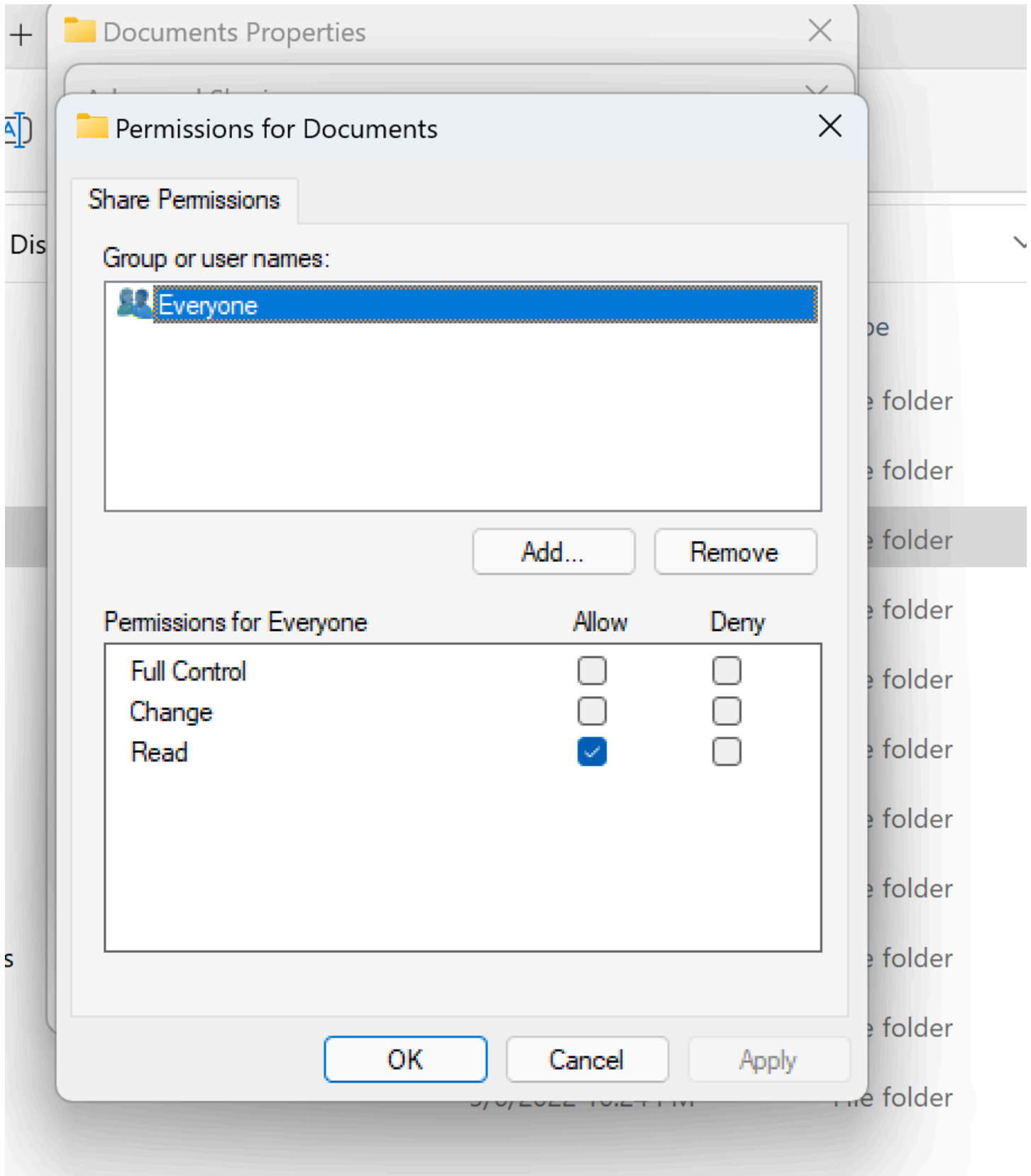
### Linux ワークロードでの UNIX スタイルのボリュームの使用

アクセス許可は、他のユーザーの sudoer で設定できます。たとえば、次の例では、 /<project-name> ディレクトリに対する <group-ID> 完全な読み取り/書き込みアクセス許可のすべてのメンバーに付与します。

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

### Linux および Windows ワークロードでの NTFS スタイルのボリュームの使用

共有アクセス許可は、特定のフォルダの共有プロパティを使用して設定できます。たとえば、ユーザー user\_01 とフォルダ がある場合 myfolder、Full Control、Change または のアクセス許可 Read を Allow または に設定できます Deny。



ボリュームを Linux クライアントと Windows クライアントの両方で使用する場合は、Linux ユーザー名を同じユーザー名に domain\username の NetBIOS ドメイン名形式に関連付ける名前マッピングを SVM に設定する必要があります。これは、Linux ユーザーと Windows ユーザーの間で変換するために必要です。リファレンスについては、[「Amazon FSx for NetApp ONTAP によるマルチプロトコルワークロードの有効化」](#)を参照してください。

.....

RES から Amazon FSx for NetApp ONTAP を作成しましたが、ドメインに参加していません

現在、RES コンソールから Amazon FSx for NetApp ONTAP を作成すると、ファイルシステムはプロビジョニングされますが、ドメインには参加しません。作成した ONTAP ファイルシステム SVM をドメインに結合するには、[「Microsoft Active Directory SVMs の結合」](#)を参照して、[Amazon FSx コンソール](#)の手順に従ってください。必要な[アクセス許可が AD の Amazon FSx サービスアカウントに委任](#)されていることを確認します。SVM がドメインに正常に参加したら、SVM 概要 > エンドポイント > SMB DNS 名に移動し、後で必要になるため DNS 名をコピーします。

ドメインに結合したら、クラスター設定 DynamoDB テーブルの SMB DNS 設定キーを編集します。

1. [Amazon DynamoDB コンソール](#)に移動します。
2. テーブルを選択し、`<stack-name>-cluster-settings` を選択します。
3. 「Explore table items」で、フィルターを展開し、次のフィルターを入力します。
  - 属性名 - キー
  - 条件 - に等しい
  - 値 - shared-storage.<file-system-name>.fsx\_netapp\_ontap.svm.smb\_dns
4. 返された項目を選択し、次にアクション、編集項目を選択します。
5. 以前にコピーした SMB DNS 名で値を更新します。
6. [保存して閉じる] を選択します。

さらに、ファイルシステムに関連付けられたセキュリティグループが、[Amazon VPC によるファイルシステムアクセスコントロール](#)で推奨されているトラフィックを許可していることを確認します。ファイルシステムを使用する新しい VDI ホストは、ドメインに参加している SVM とファイルシステムをマウントできるようになりました。

または、RES Onboard File System 機能を使用してドメインに既に参加している既存のファイルシステムをオンボードすることもできます。環境管理からファイルシステム、オンボードファイルシステムを選択します。

## スナップショット

### トピック

- [スナップショットのステータスが Failed である](#)
- [スナップショットは、テーブルをインポートできなかったことを示すログとともに適用されません。](#)

### スナップショットのステータスが Failed である

RES スナップショットページで、スナップショットのステータスが Failed の場合、エラーが発生した時間、クラスターマネージャーの Amazon CloudWatch ロググループに移動することで原因を特定できます。

```
[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
```

スナップショットは、テーブルをインポートできなかったことを示すログとともに適用されません。

以前の env から取得したスナップショットが新しい env に適用されない場合は、クラスターマネージャーの CloudWatch ログを調べて問題を特定します。必要なテーブルクラウドがインポートされないことが問題で言及されている場合は、スナップショットが有効な状態であることを確認します。

1. metadata.json ファイルをダウンロードし、さまざまなテーブルの ExportStatus のステータスが COMPLETED であることを確認します。さまざまなテーブルに ExportManifest フィールドが

設定されていることを確認します。上記のフィールドが設定されていない場合、スナップショットは無効な状態であり、スナップショットの適用機能では使用できません。

- スナップショットの作成を開始したら、RES でスナップショットのステータスが COMPLETED になっていることを確認します。スナップショットの作成プロセスには最大 5~10 分かかります。スナップショット管理ページを再ロードまたは再アクセスして、スナップショットが正常に作成されたことを確認します。これにより、作成されたスナップショットが有効な状態になります。

## インフラストラクチャ

### トピック

- [正常なインスタスがないロードバランサーターゲットグループ](#)

### 正常なインスタスがないロードバランサーターゲットグループ

サーバーエラーメッセージなどの問題が UI に表示されるか、デスクトップセッションが接続できない場合、インフラストラクチャの Amazon EC2 インスタンスに問題がある可能性があります。

問題の原因を特定する方法は、まず Amazon EC2 コンソールで、繰り返し終了し、新しいインスタンスに置き換えられていると思われる Amazon EC2 インスタスがないかを確認することです。その場合は、Amazon CloudWatch logsを確認することで原因が判断される場合があります。

もう 1 つの方法は、システム内のロードバランサーを確認することです。システムに問題がある可能性があることを示すのは、Amazon EC2 コンソールで見つかったロードバランサーに、登録された正常なインスタスが表示されない場合です。

通常の外観の例を以下に示します。

The screenshot shows the AWS Management Console interface for a target group. The breadcrumb navigation is 'EC2 > Target groups > res-bicfn3-web-portal-e2958adc'. The main heading is 'res-bicfn3-web-portal-e2958adc'. Below this, there are tabs for 'Details', 'Monitoring', 'Health checks', 'Attributes', and 'Tags'. The 'Details' tab is active, showing a summary of the target group's configuration and health status. The health status section shows 'Total targets: 1', 'Healthy: 1', and 'Unhealthy: 0'. Below this, there is a section for 'Distribution of targets by Availability Zone (AZ)'. The 'Registered targets' section is also visible, showing a table with one entry: 'I-Oba5d508631f20043' with name 'res-bicfn3-cluster-manager', port '8443', zone 'eu-central-1c', and health status 'healthy'.

Healthy エントリが 0 の場合、リクエストを処理できる Amazon EC2 インスタンスがないことを示します。

Unhealthy エントリが 0 以外の場合は、Amazon EC2 インスタンスが循環している可能性があります。これは、インストールされているアプリケーションソフトウェアがヘルスチェックに合格していないことが原因である可能性があります。

Healthy エントリと Unhealthy エントリの両方が 0 の場合、ネットワークの設定ミスの可能性を示します。たとえば、パブリックサブネットとプライベートサブネットには、対応する AZs がない場合があります。この状態が発生すると、ネットワーク状態が存在することを示す追加のテキストがコンソールに表示される場合があります。

## 仮想デスクトップの起動

### トピック

- [RES ウェブポータルで多数の VDI を起動/再開する必要がある](#)
- [Windows Virtual Desktop のログインアカウントが管理者に設定されています](#)
- [外部リソース CertificateRenewalNode の使用時に証明書の有効期限が切れる](#)
- [以前に機能していた仮想デスクトップが正常に接続できなくなりました](#)
- [5 つの仮想デスクトップしか起動できない](#)

- デスクトップ Windows の接続試行は「接続が閉じられました。トランスポートエラー」
- VDIsプロビジョニング状態でスタックする
- 起動後に VDI がエラー状態になる
- ログイン後、VDI セッションは空白の画面に移動します

.....

## RES ウェブポータルで多数の VDI s を起動/再開する必要がある

多数の VDI s をバッチで起動または再開すると、DynamoDB テーブルのプロビジョニングされたスループット (5 ~ 20) *environment-name*.vdc.dcv-broker.dcvServer が設定されているため、エラー状態になる可能性があります。

この問題を回避するには、次に示すように、AWS DynamoDB コンソールの *environment-name*.vdc.dcv-broker.dcvServer テーブルの最大読み取り/書き込みキャパシティーユニットを、過去のキャパシティー使用状況データに基づいて変更できます。

### Edit read/write capacity

#### Capacity mode [Info](#)

On-demand

Simplify billing by paying for the actual reads and writes your application performs.

Provisioned

Manage and optimize your costs by allocating read/write capacity in advance.

#### ► Capacity calculator [Info](#)

#### Table capacity

##### Read capacity

###### Auto scaling [Info](#)

Dynamically adjusts provisioned throughput capacity on your behalf in response to actual traffic patterns.

On

Off

Minimum capacity units

Maximum capacity units

Target utilization (%)

##### Write capacity

###### Auto scaling [Info](#)

Dynamically adjusts provisioned throughput capacity on your behalf in response to actual traffic patterns.

On

Off

Minimum capacity units

Maximum capacity units

Target utilization (%)

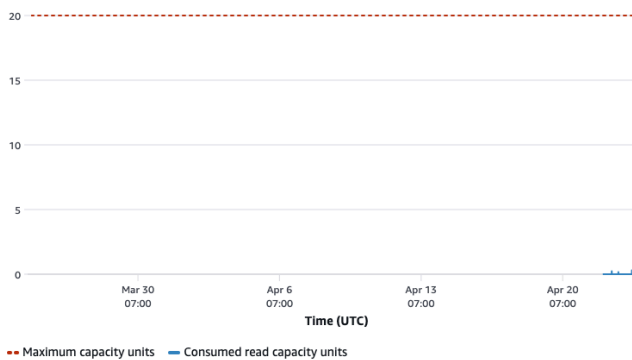
#### ▼ Historical capacity usage vs current selection

To see detailed historical read and write usage data for your table, go to [Cloudwatch](#)

##### Read usage vs current unit selection

The number of read capacity units consumed over the last month. [Learn more](#)

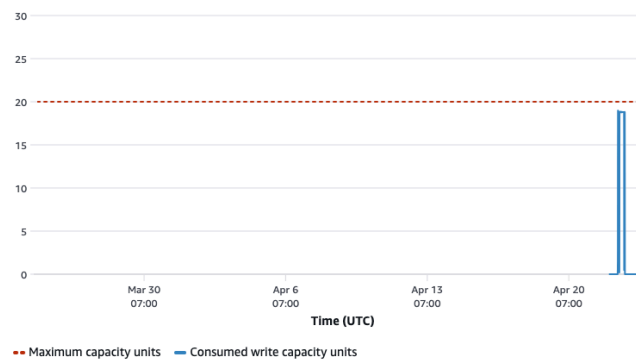
Filter displayed data



##### Write usage vs current unit selection

The number of write capacity units consumed over the last month. [Learn more](#)

Filter displayed data



5つのVDIsを起動するには、約1WCUの書き込みオペレーションが必要であり、読み取り/書き込みキャパシティーユニットを変更すると、RESのコストに影響する可能性があることに注意してください。詳細については、Amazon DynamoDB [の料金ページでプロビジョンドキャパシティーの料金を確認してください](#)。DynamoDB

.....

## Windows Virtual Desktop のログインアカウントが管理者に設定されています

RES ウェブポータルで Windows Virtual Desktop を起動できるが、接続時にログインアカウントが管理者に設定されている場合、Windows VDI が Active Directory に正常に参加していない可能性があります。

確認するには、Amazon EC2 コンソールから Windows インスタンスに接続し、のブートストラップログを確認します `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\`。で始まるエラーメッセージ `[Join AD] authorization failed:` は、インスタンスが AD に参加できなかったことを示します。障害の詳細については、ロググループ名で CloudWatch の Cluster Manager ログ / `<res-environment-name>/cluster-manager` を確認してください。

- Insufficient permissions to modify computer account
  - このエラーは、サービスアカウントに AD にコンピュータを追加する適切なアクセス許可がないことを示します。[Microsoft Active Directory のサービスアカウントを設定する](#) 「」セクションで、サービスアカウントに必要なアクセス許可を確認してください。
- Invalid Credentials
  - AD のサービスアカウントの認証情報の有効期限が切れているか、誤った認証情報が指定されています。サービスアカウントの認証情報を確認または更新するには、[Secrets Manager コンソールにパスワードを保存するシークレット](#) にアクセスします。RES 環境の Identity Management ページの Active Directory Domain の Service Account Credentials Secret ARN フィールドで、このシークレットの ARN が正しいことを確認します。

## 外部リソース CertificateRenewalNode の使用時に証明書の有効期限が切れる

[外部リソースレシピ](#) をデプロイし、Linux VDIs への接続 "The connection has been closed. Transport error" 中に というエラーが発生した場合、最も可能性の高い原因は、Linux での pip インストールパスが正しくないために自動的に更新されない期限切れの証明書です。証明書の有効期限は 3 か月です。

Amazon CloudWatch ロググループは、次のようなメッセージで接続試行エラーをログに記録する `<envname>/vdc/dcv-connection-gateway` 場合があります。

```
| 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
|
```

問題を解決するには:

1. AWS アカウントで、[EC2](#) に移動します。という名前のインスタスがある場合は\*-CertificateRenewalNode-\*、インスタスを終了します。
2. [Lambda](#) に移動します。という名前の Lambda 関数が表示されます。Lambda コードに次のようなものがないか\*-CertificateRenewalLambda-\*確認してください。

```
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. 最新の外部リソース Certs スタックテンプレートについては、[こちらを参照してください](#)。テンプレートで Lambda コードを見つけます: リソース → CertificateRenewalLambda → プロパティ → コード。次のようなものがあります。

```
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. \*-CertificateRenewalLambda-\* Lambda 関数のステップ 2 の セクションをステップ 3 のコードに置き換えます。デプロイを選択し、コード変更が有効になるまで待ちます。
5. Lambda 関数を手動でトリガーするには、テストタブに移動し、テストを選択します。追加の入力は必要ありません。これにより、Secret Manager で Certificate シークレットと PrivateKey シークレットを更新する証明書 EC2 インスタンスが作成されます。
6. 既存の dcv-gateway インスタンスを終了 *<env-name>*-vdc-gatewayし、自動スケーリンググループが新しいインスタンスを自動的にデプロイするのを待ちます。

## 以前に機能していた仮想デスクトップが正常に接続できなくなりました

デスクトップ接続が閉じられたり、接続できなくなったりすると、基盤となる Amazon EC2 インスタンスが失敗するか、Amazon EC2 インスタンスが RES 環境の外部で終了または停止されたことが原因である可能性があります。管理者 UI のステータスは、準備完了状態を引き続き表示する場合がありますが、接続の試行は失敗します。

Amazon EC2 コンソールを使用して、インスタンスが終了または停止されたかどうかを判断する必要があります。停止した場合は、もう一度開始してみてください。状態が終了した場合は、別のデスクトップを作成する必要があります。ユーザーのホームディレクトリに保存されたデータは、新しいインスタンスの起動時に引き続き使用できます。

以前に失敗したインスタンスが管理者 UI にまだ表示されている場合は、管理者 UI を使用して終了する必要がある場合があります。

## 5 つの仮想デスクトップしか起動できない

ユーザーが起動できる仮想デスクトップの数のデフォルトの制限は 5 です。これは、次のように管理者 UI を使用して管理者が変更できます。

- デスクトップ設定に移動します。
- [一般] タブを選択します。
- プロジェクトごとのユーザーあたりのデフォルトの許可されたセッションの右側にある編集アイコンを選択し、値を目的の新しい値に変更します。
- [Submit] を選択してください。
- ページを更新して、新しい設定が設定されていることを確認します。

## デスクトップ Windows の接続試行は「接続が閉じられました。トランスポートエラー」

Windows デスクトップ接続が UI エラー「接続が閉じられました。トランスポートエラー」。Windows インスタンスでの証明書の作成に関連する DCV サーバーソフトウェアの問題が原因である可能性があります。

Amazon CloudWatch ロググループは、次のようなメッセージで接続試行エラーをログに記録する <envname>/vdc/dcv-connection-gateway 場合があります。

```
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)
```

この場合、SSM セッションマネージャーを使用して Windows インスタンスへの接続を開き、次の 2 つの証明書関連ファイルを削除することが解決される場合があります。

```
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
```

ファイルは自動的に再作成され、それ以降の接続試行が成功する可能性があります。

この方法で問題を解決し、Windows デスクトップの新しい起動で同じエラーが発生した場合は、ソフトウェアスタックの作成 関数を使用して、再生成された証明書ファイルを含む固定インスタンスの新しい Windows ソフトウェアスタックを作成します。これにより、正常な起動と接続に使用できる Windows ソフトウェアスタックが生成されます。

.....

## VDIsプロビジョニング状態でスタックする

デスクトップ起動が管理者 UI のプロビジョニング状態のままである場合は、いくつかの理由が考えられます。

原因を特定するには、デスクトップインスタンスのログファイルを調べ、問題の原因となっている可能性のあるエラーを探します。このドキュメントには、ログファイルと Amazon CloudWatch ロググループのリストが含まれており、有用なログおよびイベント情報ソースというラベルが付いたセクションに関連情報が含まれています。

この問題の潜在的な原因は次のとおりです。

- 使用されている AMI ID は software-stack として登録されていますが、RES ではサポートされていません。

Amazon マシンイメージ (AMI) に必要な設定またはツールがないため、ブートストラッププロビジョニングスクリプトを完了できませんでした。Linux インスタンスなど、インスタンス/root/bootstrap/logs/のログファイルには、これに関する有用な情報が含まれている場合があります。AWS Marketplace から取得した AMIs ID は、RES デスクトップインスタンスでは機能しない場合があります。サポートされているかどうかを確認するには、テストが必要です。

- ユーザーデータスクリプトは、Windows 仮想デスクトップインスタンスがカスタム AMI から起動されたときに実行されません。

デフォルトでは、ユーザーデータスクリプトは Amazon EC2 インスタンスの起動時に 1 回実行されます。既存の仮想デスクトップインスタンスから AMI を作成し、その AMI にソフトウェアスタックを登録して、このソフトウェアスタックで別の仮想デスクトップを起動しようとする、ユーザーデータスクリプトは新しい仮想デスクトップインスタンスでは実行されません。

この問題を解決するには、AMI の作成に使用した元の仮想デスクトップインスタンスで管理者として PowerShell コマンドウィンドウを開き、次のコマンドを実行します。

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

次に、インスタンスから新しい AMI を作成します。新しい AMI を使用してソフトウェアスタックを登録し、後で新しい仮想デスクトップを起動できます。プロビジョニング状態のままのインスタンスで同じコマンドを実行し、インスタンスを再起動して仮想デスクトップセッションを修正することもできますが、設定ミスのある AMI から別の仮想デスクトップを起動すると、同じ問題が再度発生することに注意してください。

## 起動後に VDI がエラー状態になる

考えられる問題 1: ホームファイルシステムに、異なる POSIX アクセス許可を持つユーザーのディレクトリがあります。

これは、次のシナリオが当てはまる場合に直面する問題である可能性があります。

1. デプロイされた RES バージョンは 2024.01 以降です。

2. RES スタックのデプロイ中に、 の属性が に設定EnableLdapIDMappingされましたTrue。
3. RES スタックのデプロイ中に指定されたホームファイルシステムは、 RES 2024.01 より前のバージョンで使用されたか、 を EnableLdapIDMappingに設定して以前の環境で使用されましたFalse。

解決手順: ファイルシステム内のユーザーディレクトリを削除します。

1. クラスタマネージャーホストへの SSM。
2. `cd /home.`
3. `ls -` は、 admin1、 などのユーザー名に一致するディレクトリ名を持つディレクトリを一覧表示する必要がありますadmin2。
4. ディレクトリ を削除しますsudo `rm -r 'dir_name'`。 ssm-user ディレクトリと ec2-user ディレクトリを削除しないでください。
5. ユーザーが新しい env に既に同期されている場合は、 ユーザーの DDB テーブルからユーザーの を削除します (clusteradmin を除く)。
6. AD 同期の開始 - クラスタマネージャー Amazon EC2 sudo `/opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad`で実行します。
7. RES ウェブページから Error状態の VDI インスタンスを再起動します。 VDI が約 20 分で Ready状態に移行することを確認します。

.....

## ログイン後、VDI セッションは空白の画面に移動します

ログイン後にコンソールセッションタイプの VDI セッションが空白で応答しない場合、X サーバーが壊れていることを意味します。これは、DCV がデスクトップをストリーミングしようとしているが、ストリーミングする OS の問題が原因である可能性があります。この最も可能性の高い原因は、Xorg 設定の問題です。次のコマンドを実行して、デフォルトの Xorg 設定にあまり依存しないようにできます。

Debian ベースの Linux:

```
dpkg-divert --package nice-xdvc --divert /usr/bin/Xorg.orig --rename /usr/bin/Xorg ln -sf /usr/bin/Xdvc-console /usr/bin/Xorg
```

Red Hat ベースの Linux:

```
rpm -q --whatprovides /usr/bin/Xorg && \
```

```
cp /usr/bin/Xorg /usr/bin/Xorg.orig && \  
ln -sf /usr/bin/Xdcv-console /usr/bin/Xorg
```

## 仮想デスクトップコンポーネント

### トピック

- [Amazon EC2 インスタンスがコンソールで終了を繰り返し表示](#)
- [AD / eVDI モジュールに参加できなかったために vdc-controller インスタンスがサイクルしていますが、API ヘルスチェックが失敗しています](#)
- [プロジェクトは、ソフトウェアスタックを編集して追加するときにプルダウンに表示されません](#)
- [cluster-manager Amazon CloudWatch ログには、「<user-home-init> アカウントはまだ利用できません。ユーザーの同期を待っています」と表示されます \(アカウントはユーザー名です\)。](#)
- [ログイン試行時の Windows デスクトップに「アカウントが無効になっています。管理者にお問い合わせください」](#)
- [外部/顧客の AD 設定に関する DHCP オプションの問題](#)
- [Firefox エラー MOZILLA\\_PKIX\\_ERROR\\_REQUIRED\\_TLS\\_FEATURE\\_MISSING](#)

## Amazon EC2 インスタンスがコンソールで終了を繰り返し表示

インフラストラクチャインスタンスが Amazon EC2 コンソールで終了済みとして繰り返し表示される場合、原因はその設定に関連している可能性があり、インフラストラクチャインスタンスタイプによって異なります。以下に、原因を特定する方法を示します。

Amazon EC2 コンソールで vdc-controller インスタンスが終了状態が繰り返し表示される場合は、シークレットタグが正しくない可能性があります。RES によって維持されるシークレットには、インフラストラクチャの Amazon EC2 インスタンスにアタッチされた IAM アクセスコントロールポリシーの一部として使用されるタグがあります。vdc-controller がサイクルしていて、CloudWatch ロググループに次のエラーが表示された場合、シークレットが正しくタグ付けされていない可能性があります。シークレットには、次のタグを付ける必要があることに注意してください。

```
{  
  "res:EnvironmentName": "<envname>" # e.g. "res-demo"
```

```
"res:ModuleName": "virtual-desktop-controller"
}
```

このエラーの Amazon CloudWatch ログメッセージは、次のように表示されます。

```
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
```

Amazon EC2 インスタンスのタグをチェックし、上記のリストと一致することを確認します。

AD / eVDI モジュールに参加できなかったために vdc-controller インスタンスがサイクルしていますが、API ヘルスチェックが失敗しています

eVDI モジュールがヘルスチェックに失敗した場合、環境ステータスセクションに以下が表示されます。

## 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

この場合、デバッグの一般的なパスは、クラスターマネージャーの [CloudWatch](#) ログを調べることで、(という名前のロググループを探します <env-name>/cluster-manager。)

考えられる問題:

- ログにテキストが含まれている場合は Insufficient permissions、res スタックの作成時に指定された ServiceAccount ユーザー名のスペルが正しいことを確認してください。

ログ行の例:

```
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
```

- [SecretsManager コンソール](#) から、RES デプロイ中に提供される ServiceAccount ユーザー名にアクセスできます。Secrets Manager で対応するシークレットを検索し、プレーンテキストの取得を選択します。ユーザー名が正しくない場合は、編集を選択してシークレット値を更新します。現在の cluster-manager インスタンスと vdc-controller インスタンスを終了します。新しいインスタンスは安定した状態になります。
- 提供された [外部リソーススタック](#) によって作成されたリソースを使用している場合、ユーザー名は「ServiceAccount」である必要があります。RES のデプロイ中に DisableADJoin パラメータが False に設定されている場合は、「ServiceAccount」ユーザーに AD でコンピュータオブジェクトを作成するアクセス許可があることを確認します。
- 使用したユーザー名が正しいが、ログにテキストが含まれている場合 Invalid credentials、入力したパスワードが間違っているか、有効期限が切れている可能性があります。

ログ行の例:

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

- 環境の作成時に入力したパスワードは、[Secrets Manager コンソールにパスワードを保存するシークレット](#) にアクセスして読み取ることができます。シークレット ( など <env\_name>directoryserviceServiceAccountPassword) を選択し、プレーンテキストの取得を選択します。

- シークレットのパスワードが正しくない場合は、編集を選択してシークレットの値を更新します。現在の cluster-manager インスタンスと vdc-controller インスタンスを終了します。新しいインスタンスは更新されたパスワードを使用し、安定した状態になります。
- パスワードが正しい場合、接続された Active Directory でパスワードの有効期限が切れている可能性があります。まず Active Directory でパスワードをリセットしてから、シークレットを更新する必要があります。[Directory Service コンソール](#)から Active Directory でユーザーのパスワードをリセットできます。
  1. 適切なディレクトリ ID を選択する
  2. アクション、ユーザーパスワードのリセットを選択し、ユーザー名 (ServiceAccount など) と新しいパスワードをフォームに入力します。
  3. 新しく設定したパスワードが以前のパスワードと異なる場合は、対応する Secret Manager シークレットのパスワードを更新します (例: <env\_name>directoryserviceServiceAccountPassword)。
  4. 現在の cluster-manager インスタンスと vdc-controller インスタンスを終了します。新しいインスタンスは安定した状態になります。

.....

プロジェクトは、ソフトウェアスタックを編集して追加するときにプルダウンに表示されません

この問題は、ユーザーアカウントと AD の同期に関連する次の問題に関連している可能性があります。この問題が発生した場合は、クラスターマネージャーの Amazon CloudWatch ロググループでエラー<user-home-init> account not available yet. waiting for user to be synced 「」をチェックして、原因が同じか関連しているかを判断します。

.....

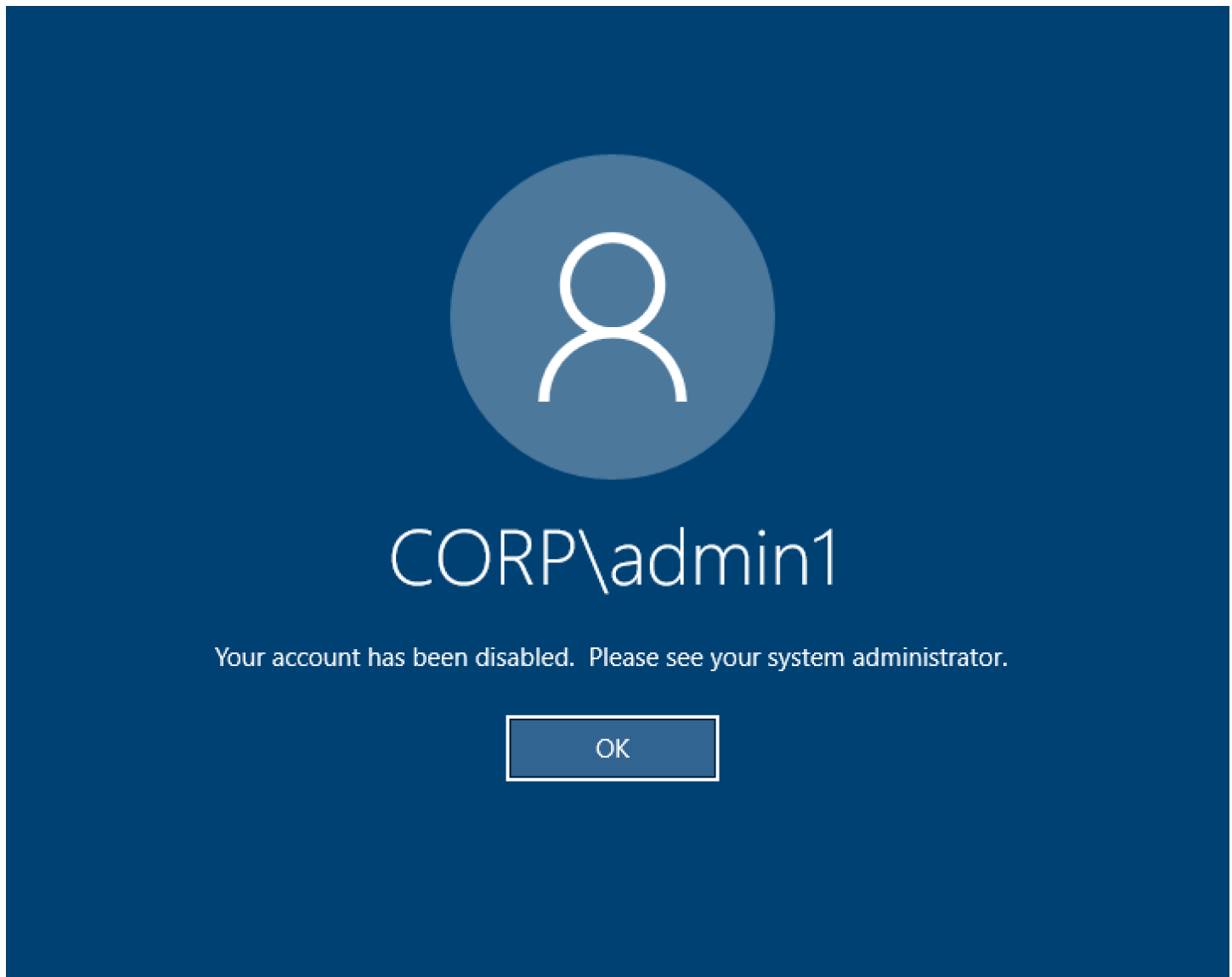
cluster-manager Amazon CloudWatch ログには、「<user-home-init> アカウントはまだ利用できません。ユーザーの同期を待っています」と表示されます (アカウントはユーザー名です)。

SQS サブスクライバーは、ユーザーアカウントにアクセスできないため、ビジー状態で無限ループに陥っています。このコードは、ユーザーの同期中にユーザーのホームファイルシステムを作成しようとしたときにトリガーされます。

ユーザーアカウントにアクセスできない理由は、使用中の AD に対して RES が正しく設定されていない可能性があります。たとえば、BI/RES 環境の作成時に使用された ServiceAccountCredentialsSecretArn パラメータの値が正しくない可能性があります。

.....

ログイン試行時の Windows デスクトップに「アカウントが無効になっています。管理者にお問い合わせください」



ユーザーがロックされた画面に再度ログインできない場合は、SSO 経由で正常にサインオンした後、RES 用に設定された AD でユーザーが無効になっている可能性があります。

AD でユーザーアカウントが無効になっている場合、SSO ログインは失敗します。

## 外部/顧客の AD 設定に関する DHCP オプションの問題

独自の Active Directory "The connection has been closed. Transport error"で RES を使用するとき Windows 仮想デスクトップでというエラーが発生した場合は、dcv-connection-gateway Amazon CloudWatch ログで次のような点を確認してください。

```
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
```

独自の VPC の DHCP オプションに AD ドメインコントローラーを使用している場合は、以下を行う必要があります。


1. AmazonProvidedDNS を 2 つのドメインコントローラー IPs。
2. ドメイン名を ec2.internal に設定します。

以下に例を示します。この設定がない場合、RES/DCV は ip-10-0-x-xx.ec2.internal ホスト名を検索するため、Windows デスクトップはトランスポートエラーを返します。

### Domain name

 ec2.internal

### Domain name servers

 10.0.2.168, 10.0.3.228,  
AmazonProvidedDNS

## Firefox エラー MOZILLA\_PKIX\_ERROR\_REQUIRED\_TLS\_FEATURE\_MISSING

Firefox ウェブブラウザを使用すると、仮想デスクトップに接続しようとする  
と、MOZILLA\_PKIX\_ERROR\_REQUIRED\_TLS\_FEATURE\_MISSING というエラーメッセージが表示されることがあります。

原因は、RES ウェブサーバーが TLS + Stapling On でセットアップされているが、Stapling Validation で応答していないことです (<https://support.mozilla.org/en-US/questions/1372483>)。

これは、[https://really-simple-ssl.com/mozilla\\_pkix\\_error\\_required\\_tls\\_feature\\_missing](https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing) の指示に従って修正できます。

## Env 削除

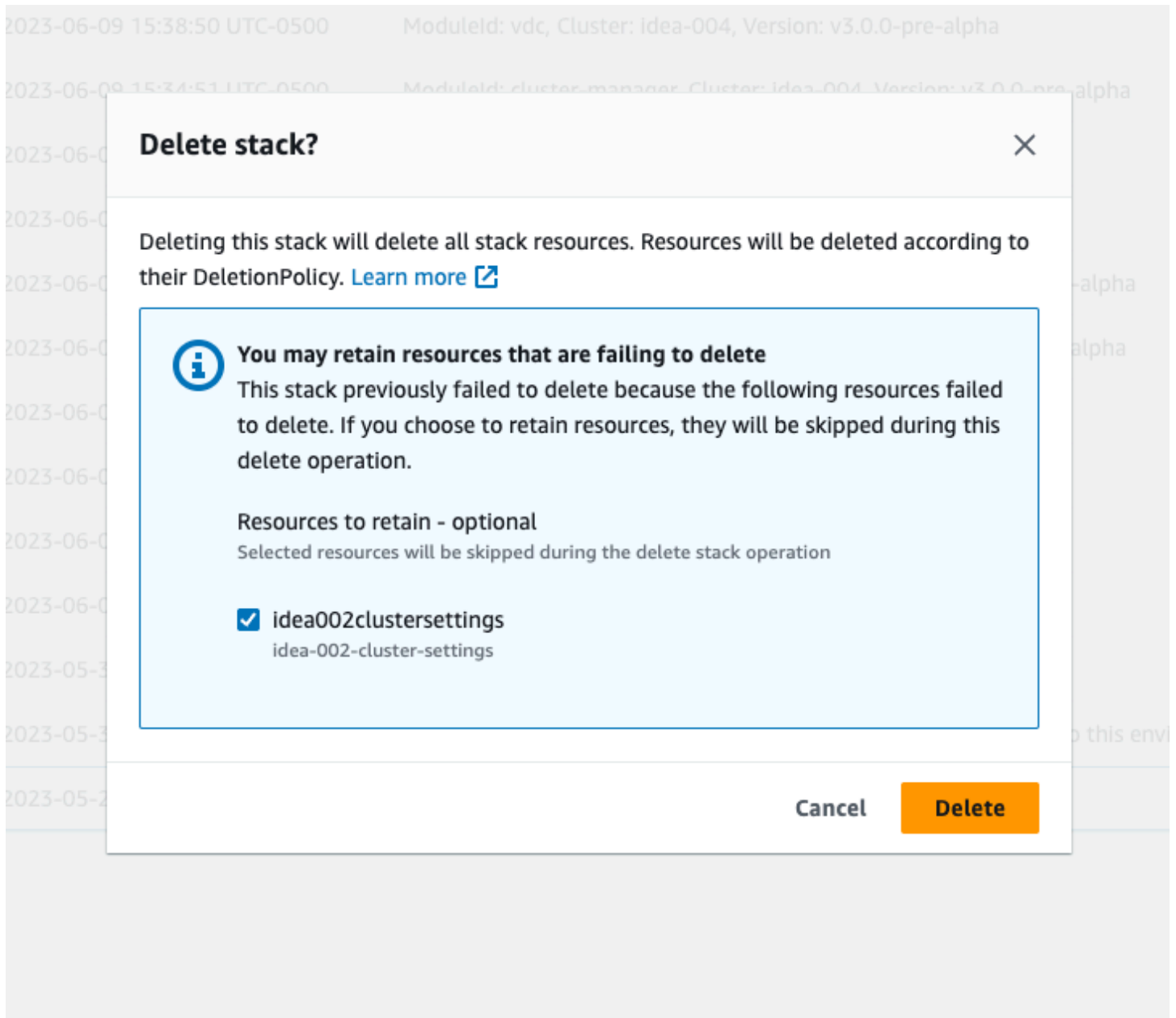
### トピック

- [res-xxx-cluster スタックが「DELETE\\_FAILED」状態で、「Role is invalid or cannot be assumed」エラーのため手動で削除できない](#)
- [ログの収集](#)
- [VDI ログのダウンロード](#)
- [Linux EC2 インスタンスからのログのダウンロード](#)
- [Windows EC2 インスタンスからのログのダウンロード](#)
- [WaitCondition エラーの ECS ログの収集](#)

res-xxx-cluster スタックが「DELETE\_FAILED」状態で、「Role is invalid or cannot be assumed」エラーのため手動で削除できない

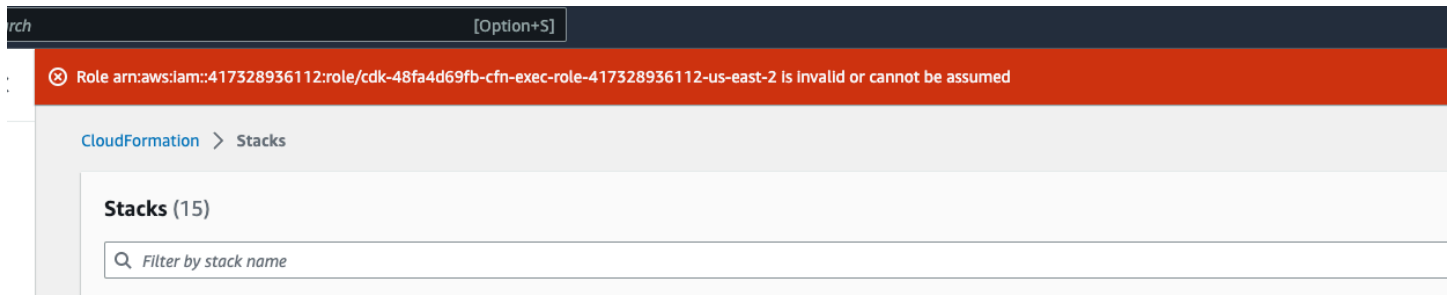
「res-xxx-cluster」スタックが「DELETE\_FAILED」状態で、手動で削除できない場合は、次の手順を実行して削除できます。

スタックが「DELETE\_FAILED」状態にある場合は、まずスタックを手動で削除してみてください。スタックの削除を確認するダイアログが表示される場合があります。[削除] を選択します。



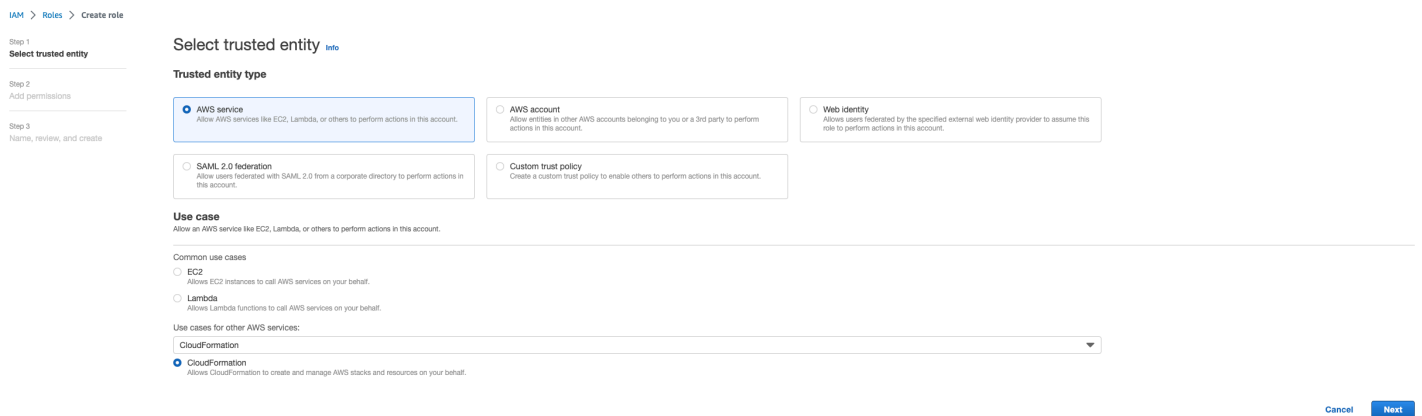
必要なスタックリソースをすべて削除しても、保持するリソースを選択するメッセージが表示されることがあります。その場合は、「保持するリソース」としてすべてのリソースを選択し、「削除」を選択します。

次のようなエラーが表示される場合があります。 `Role: arn:aws:iam::... is Invalid or cannot be assumed`



これは、スタックの削除に必要なロールが、スタックの前に最初に削除されたことを意味します。これを回避するには、ロールの名前をコピーします。IAM コンソールに移動し、次に示すパラメータを使用して、その名前のロールを作成します。

- 信頼されたエンティティタイプでAWS サービスを選択します。
- ユースケースで、Use cases for other AWS servicesを選択しますCloudFormation。



[次へ] を選択します。ロールにAWSCloudFormationFullAccess「」およびAdministratorAccess「」のアクセス許可を付与してください。レビューページは次のようになります。

## 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

次に、CloudFormation コンソールに戻り、スタックを削除します。これで、ロールを作成した後で削除できるようになります。最後に、IAM コンソールに移動し、作成したロールを削除します。

## ログの収集

### EC2 コンソールから EC2 インスタンスにログインする

- Linux EC2 インスタンスにログインするには、[次の手順に従います](#)。
- Windows EC2 インスタンスにログインするには、[次の手順に従います](#)。次に、Windows PowerShell を開いてコマンドを実行します。

### インフラストラクチャホストログの収集

- Cluster-manager: 次の場所からクラスターマネージャーのログを取得し、チケットにアタッチします。
  - CloudWatch ロググループ からのすべてのログ <env-name>/cluster-manager。
  - <env-name>-cluster-manager EC2 インスタンスの /root/bootstrap/logs ディレクトリにあるすべてのログ。このセクションの冒頭にある EC2 コンソールから EC2 インスタンスにログインする」から リンクされた手順に従って、インスタンスにログインします。

2. Vdc-controller: 次の場所から vdc-controller のログを取得し、チケットにアタッチします。
  - a. CloudWatch ロググループ からのすべてのログ<env-name>/vdc-controller。
  - b. <env-name>-vdc-controller EC2 インスタンスの /root/bootstrap/logs ディレクトリにあるすべてのログ。このセクションの冒頭にあるEC2 コンソールから EC2 インスタンスにログインする」から にリンクされた手順に従って、インスタンスにログインします。

ログを簡単に取得する方法の 1 つは、[Linux EC2 インスタンスからのログのダウンロード](#)セクションの指示に従うことです。モジュール名はインスタンス名になります。

## VDI ログの収集

### 対応する Amazon EC2 インスタンスを特定する

ユーザーがセッション名 で VDI を起動した場合VDI1、Amazon EC2 コンソールのインスタンスの対応する名前は になります<env-name>-VDI1-<user name>。

### Linux VDI ログの収集

このセクションの冒頭にあるAmazon EC2 コンソールから EC2 インスタンスにログインする」の「」にリンクされた手順に従って、Amazon EC2 コンソールから対応する Amazon EC2 インスタンスにログインします。VDI Amazon EC2 インスタンスの /root/bootstrap/logsおよび /var/log/dcv/ ディレクトリにあるすべてのログを取得します。

ログを取得する方法の 1 つは、ログを s3 にアップロードし、そこからダウンロードすることです。そのためには、次のステップに従って 1 つのディレクトリからすべてのログを取得し、アップロードします。

1. /root/bootstrap/logs ディレクトリの下に dcv ログをコピーするには、次の手順に従います。

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

2. 次に、次のセクション「」に記載されている手順に従って[VDI ログのダウンロード](#)ログをダウンロードします。

## Windows VDI ログの収集

このセクションの冒頭にあるAmazon EC2 コンソールから EC2 インスタンスにログインする」の「」にリンクされた手順に従って、Amazon EC2 コンソールから対応する Amazon

EC2 インスタンスにログインします。VDI EC2 インスタンスの `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log` ディレクトリですべてのログを取得します。

ログを取得する方法の 1 つは、ログを S3 にアップロードし、そこからダウンロードすることです。これを行うには、次のセクション「」に記載されているステップに従います [VDI ログのダウンロード](#)。

## VDI ログのダウンロード

1. VDI EC2 インスタンスの IAM ロールを更新して S3 アクセスを許可します。
2. EC2 コンソールに移動し、VDI インスタンスを選択します。
3. 使用している IAM ロールを選択します。
4. アクセス許可の追加ドロップダウンメニューのアクセス許可ポリシーセクションで、ポリシーの アタッチを選択し、AmazonS3FullAccess ポリシーを選択します。
5. アクセス許可を追加 を選択して、そのポリシーをアタッチします。
6. その後、VDI タイプに基づいて以下の手順に従ってログをダウンロードします。モジュール名はインスタンス名になります。
  - a. [Linux EC2 インスタンスからのログのダウンロード](#) Linux 用。
  - b. [Windows EC2 インスタンスからのログのダウンロード](#) Windows 用。
7. 最後に、ロールを編集してAmazonS3FullAccessポリシーを削除します。

### Note

すべての VDI、と同じ IAM ロールを使用します。 `<env-name>-vdc-host-role-<region>`

## Linux EC2 インスタンスからのログのダウンロード

ログをダウンロードする EC2 インスタンスにログインし、次のコマンドを実行してすべてのログを s3 バケットにアップロードします。

```

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

```

その後、S3 コンソールに移動<environment\_name>-cluster-<region>-<aws\_account\_number>し、名前が のバケットを選択し、以前にアップロードした<module\_name>\_logs.tar.gzファイルをダウンロードします。

.....

## Windows EC2 インスタンスからのログのダウンロード

ログをダウンロードする EC2 インスタンスにログインし、次のコマンドを実行してすべてのログを S3 バケットにアップロードします。

```

$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

```

その後、S3 コンソールに移動<environment\_name>-cluster-<region>-<aws\_account\_number>し、名前が のバケットを選択し、以前にアップロードした<module\_name>\_logs.zipファイルをダウンロードします。

.....

## WaitCondition エラーの ECS ログの収集

1. デプロイされたスタックに移動し、リソースタブを選択します。
2. Deploy → ResearchAndEngineeringStudio → Installer → Tasks → CreateTaskDef → CreateContainer → LogGroup を展開し、CloudWatch ログを開くロググループを選択します。
3. このロググループから最新のログを取得します。

## デモ環境

### トピック

- [ID プロバイダーへの認証リクエストを処理する際のデモ環境ログインエラー](#)
- [デモスタックのキークロックが機能しない](#)

## ID プロバイダーへの認証リクエストを処理する際のデモ環境ログインエラー

### 問題

ログインしようとして、ID プロバイダーへの認証リクエストを処理するときに「予期しないエラー」が発生した場合、パスワードの有効期限が切れている可能性があります。これは、ログインしようとしているユーザーのパスワードまたは Active Directory サービスアカウントのいずれかです。

### 緩和策

1. [Directory サービスコンソール](#)でユーザーとサービスアカウントのパスワードをリセットします。
2. [Secrets Manager](#) のサービスアカウントのパスワードを、上記で入力した新しいパスワードと一致するように更新します。
  - Keycloak スタックの : PasswordSecret-...-RESExternal-...-DirectoryService-... with Description: Password for Microsoft Active Directory
  - for RES: res-ServiceAccountPassword-... with 説明: Active Directory サービスアカウントのパスワード

3. [EC2 コンソール](#)に移動し、クラスターマネージャーインスタンスを終了します。Auto Scaling ルールは、新しいインスタンスのデプロイを自動的にトリガーします。

## デモスタックのキークロークが機能しない

### 問題

キークロークサーバーがクラッシュし、サーバーを再起動したときにインスタンスの IP が変更された場合、キークロークが壊れた可能性があります。RES ポータルのログインページがロードに失敗するか、ロード状態でスタックし、解決されません。

### 緩和策

Keycloak を正常な状態に復元するには、既存のインフラストラクチャを削除し、Keycloak スタックを再デプロイする必要があります。以下の手順に従ってください。

1. Cloudformation に移動します。そこに 2 つのキークローク関連スタックが表示されます。
  - `<env-name>-RESSsoKeycloak-<random characters>` (Stack1)
  - `<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-*` (スタック 2)
2. Stack1 を削除します。ネストされたスタックを削除するように求められたら、はいを選択してネストされたスタックを削除します。

スタックが完全に削除されていることを確認します。
3. ここで RES SSO Keycloak スタックテンプレートをダウンロード[します](#)。
4. 削除されたスタックとまったく同じパラメータ値を使用して、このスタックを手動でデプロイします。CloudFormation コンソールからデプロイするには、スタックの作成 → 新しいリソース (標準) を使用 → 既存のテンプレートを選択する → テンプレートファイルをアップロードします。削除されたスタックと同じ入力を使用して、必要なパラメータを入力します。これらの入力は、CloudFormation コンソールでフィルターを変更し、Parameters タブに移動することで、削除されたスタックで確認できます。環境名、キーペア、およびその他のパラメータが元のスタックパラメータと一致していることを確認します。
5. スタックがデプロイされると、環境を再度使用する準備が整います。ApplicationUrl は、デプロイされたスタックの出力タブにあります。

## Active Directory の問題

### トピック

- [VDI がプロビジョニング状態で長時間スタックしているか、VDI の準備が整った後に VDI を AD ユーザーとしてログインできない](#)
- [SSO の設定後に RES ウェブポータルにログインできない](#)
- [AD ユーザーは、Linux VDI を正常に起動した後でも、ファイルブラウザを使用してホームディレクトリにアクセスできません](#)
- [SSH アクセスが有効になっていると、AD 管理者ユーザーは踏み台ホストにアクセスできません](#)
- [RES 外部リソーススタックによってデプロイされた Active Directory の表示と管理](#)

VDI がプロビジョニング状態で長時間スタックしているか、VDI の準備が整った後に VDI を AD ユーザーとしてログインできない

最初に VDI のインストールログと設定ログ (/root/bootstrap/logs/Linux の場合は および /opt/idea/app/logs/ ディレクトリ、Windows の場合は C:\Users\Administrator\RES\Bootstrap\Log\および C:\Program Files\RES\app\logs\ ディレクトリ) で、インストールエラーまたは設定エラーを確認します。

インスタンスが Active Directory に参加できなかったというエラーメッセージが表示された場合は、通常、Cluster Manager が AD のインスタンスのコンピュータアカウントをプリセットできないためです。/*environment-name*/cluster-manager CloudWatch ロググループの Cluster Manager ログを確認し、を含むエラーメッセージをフィルタリングします[preset-computer]。一般的な問題は次のとおりです。

- AD サービスアカウントの認証情報が無効です。
  - RES に提供したサービスアカウントのシークレットを確認します。ユーザー名とパスワードがキーと値のペアとして提供され{*username*: *password*}、認証情報が有効であることを確認します。既存のインスタンスを終了し、サービスアカウントのシークレットを変更した後に自動スケジューリンググループが新しいインスタンスを自動的に起動できるようにして、クラスターマネージャーインスタンスをサイクルする必要があります。次に、新しい VDI を起動して変更を適用します。
- サービスアカウントには、AD でコンピュータアカウントを作成するアクセス許可がありません。

- サービスアカウントに、「」に記載されているすべての必要なアクセス許可があることを確認します [Microsoft Active Directory のサービスアカウントを設定する](#)。AD でサービスアカウントのアクセス許可を修正した後、新しい VDI を起動する必要があります。
- LDAP サーバーに接続できません。
- AWS マネージド AD を使用している場合は [AWS](#)、[Managed Microsoft AD の DHCP オプションセットを作成または変更した後、AD 設定で VPC 内の LDAP/LDAPS 接続が許可され、VPC の DHCP オプションが正しく設定されていることを確認](#) します。
- LDAPS 接続の場合、DomainTLSCertificateSecretArn パラメータが必要であり、接続を保護するために有効な CA 証明書を指定する必要があります。既存のインスタンスを終了し、TLS 証明書シークレットを変更した後に自動スケーリンググループが新しいインスタンスを自動的に起動できるようにして、Cluster Manager インスタンスをサイクルする必要があります。次に、新しい VDI を起動して変更を適用します。
- RES と AD 間の接続をテストするには、Cluster Manager インスタンスで次の ldapsearch コマンドを実行します (ユーザー OU、LDAP 接続 URI、サービスアカウントのユーザー名とパスワードを置き換えます)。AD が接続を許可するように適切に設定されている場合、このコマンドは指定された OU のすべてのユーザーを返します。

```
ldapsearch -x -b "OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com" -D
"ServiceAccount@corp.res.com" -H ldap://corp.res.com -w service-account-password
"(objectClass=group)"
```

RES のインストール true 時に DisableADJoin を に設定した場合、Linux VDI sssd サービスを介して接続するのではなく、Active Directory にのみ接続します。EC2 コンソールから VDI インスタンスに接続し、コマンドを実行します `id username`。コマンドが対応する AD ユーザーの UID / GID を返すことができない場合は、VDI インスタンス `sudo systemctl status sssd` のコマンドと `/var/log/sss/` ディレクトリの SSSD サービスログを使用して SSSD サービスのステータスを確認します。

AD に接続するように SSSD 設定をカスタマイズする必要がある場合は、SSSD 設定ファイル (`/etc/sss/sss.conf`) を手動で編集し、`infra / VDI host (2024.12.01 release 以前)` `sudo systemctl restart sssd` でコマンドを使用して SSSD サービスを再起動するか、RES ウェブポータルから追加の SSSD 設定を提供できます。 [Active Directory の同期](#) これは、既存または新しい VDI に自動的に適用されます (2025.03 release 以降)。

.....

## SSO の設定後に RES ウェブポータルにログインできない

`environment-name.accounts.users` と `environment-name.accounts.groups` DynamoDB テーブルをチェックして、ユーザーとグループが Active Directory から同期されているかどうかを確認します。テーブルが空であるか、ログインしているユーザーが見つからない場合は、`/environment-name/cluster-managerCloudWatch` ロググループ (2024.12 リリース以前) または `/environment-name/ad-sync CloudWatch` ロググループ (2024.12 リリース以降) の AD 同期ログを確認します。

に記載されている一般的な AD 設定の問題に加えて [VDI がプロビジョニング状態で長時間スタックしているか、VDI の準備が整った後に VDI を AD ユーザーとしてログインできない](#)、他のエラーには次のようなものがあります。

- サービスアカウントには、AD のユーザーとグループをクエリするアクセス許可がありません。
  - サービスアカウントに、「」に記載されているすべての必要なアクセス許可があることを確認します [Microsoft Active Directory のサービスアカウントを設定する](#)。
- Active Directory のユーザー/グループに E メールアドレスなどの必須属性がありません。
  - ユーザー/グループの属性を更新して問題を解決します。

AD 同期の問題を修正したら、次にスケジュールされた AD 同期が 1 時間ごとに発生するのを待つか、[同期を手動で実行する方法 \(リリース 2024.12 および 2024.12.01\)](#) (2024.12 および 2024.12.01 リリース) または [同期を手動で開始または停止する方法 \(リリース 2025.03 以降\)](#) (リリース 2025.03 以降) の指示に従って手動でトリガーできます。

AD ユーザーは、Linux VDIs を正常に起動した後でも、ファイルブラウザを使用してホームディレクトリにアクセスできません

Cluster Manager インスタンス id `username` で コマンドを実行して、AD ユーザーが Cluster Manager に表示されるかどうかを確認します。コマンドが対応する AD ユーザーの UID / GID を返すことができない場合は、`/environment-name/cluster-managerCloudWatch` ロググループの Cluster Manager ログを確認し、SSSD サービスの開始に関するエラーを検索します。Cluster Manager ログにエラーがない場合は、Cluster Manager インスタンス `sudo systemctl status sssd` のコマンドと `/var/log/sss/` ディレクトリの SSSD サービスログを使用して、SSSD サービスのステータスを確認します。

AD ユーザーが Cluster Manager に表示されている場合は、コマンドを実行して、ユーザーのホームディレクトリ (`/home/username`) の UID / GID を確認します `ls -n /home`。ユーザーのホームディレクトリの UID/GID を、 `id username` コマンドによって返された UID/GID と比較します。UID / GID が一致しない場合、ユーザーのホームディレクトリが RES の外部または以前の RES デプロイから作成される可能性があります。重要なユーザーデータをバックアップし、ホームディレクトリを削除して、ユーザーとともに新しい Linux VDI を起動します。新しい VDI が正常にプロビジョニングされると、ホームディレクトリは適切な UID/GID で再作成されます。

.....

SSH アクセスが有効になっていると、AD 管理者ユーザーは踏み台ホストにアクセスできません

踏み台ホストインスタンス `id username` で コマンドを実行して、AD ユーザーが踏み台ホストに表示されるかどうかを確認します。コマンドが対応する AD ユーザーの UID / GID を返すことができない場合は、`/environment-name/bastion-hostCloudWatch` ロググループの踏み台ホストログをチェックし、SSSD サービスの開始に関するエラーを検索します。踏み台ホストログにエラーがない場合は、踏み台ホストインスタンス `sudo systemctl status sssd` のコマンドと `/var/log/sss/` ディレクトリの SSSD サービスログを使用して、SSSD サービスのステータスを確認します。

.....

## RES 外部リソーススタックによってデプロイされた Active Directory の表示と管理

AWS マネージド Active Directory が RES 外部リソーススタックによってデプロイされている場合、Active Directory へのアクセスと管理に使用できる AWS、アカウントの下に `AdDomainWindowsNode-external-resource-stack-name-WindowsManagementHost` デプロイされた で始まる名前のインスタンスが必要です。次の認証情報を使用して、EC2 コンソールの Fleet Manager を介してインスタンスにログインできます。

- username: 管理者
- password: 外部リソーススタックをデプロイするときに提供される AdminPassword パラメータ

AWS マネージド Active Directory を管理するには、AWS 「[Directory Service 管理ガイド](#)」の [Amazon EC2 インスタンスを使用してユーザーとグループを管理する](#)」を確認してください。

## 既知の問題

### • [既知の問題 2024.x](#)

- [\(2024.12 および 2024.12.01\) 新しい Cognito ユーザーを登録する際の正規表現の失敗](#)
- [\(2024.12.01 以前\) カスタムドメインを使用して VDI に接続するときに無効な不正な証明書エラーが発生する](#)
- [\(2024.12 および 2024.12.01\) Active Directory ユーザーは踏み台ホストに SSH できません](#)
- [\(2024.10\) 隔離された VPCs](#)
- [\(2024.10 以前\) Graphic 拡張インスタンスタイプの VDI の起動に失敗しました](#)
- [\(2024 年 8 月\) インフラストラクチャ AMI 障害の準備](#)
- [\(2024.08\) 仮想デスクトップがルートバケット ARN とカスタムプレフィックスを使用して Amazon S3 バケットの読み取り/書き込みをマウントできない](#)
- [\(2024.06\) AD グループ名にスペースが含まれている場合、スナップショットの適用は失敗する](#)
- [\(2024.06 以前\) AD 同期中に RES に同期されていないグループメンバー](#)
- [\(2024.06 以前\) CVE-2024-6387、RegreSSHion、RHEL9 および Ubuntu VDIs のセキュリティ脆弱性](#)
- [\(2024.04-2024.04.02\) VDI インスタンスのロールにアタッチされていない IAM アクセス許可境界が提供されました](#)
- [\(2024.04.02 以前\) ap-southeast-2 \(シドニー\) の Windows NVIDIA インスタンスが起動に失敗する](#)
- [\(2024.04 および 2024.04.01\) GovCloud での RES 削除の失敗](#)
- [\(2024.04 - 2024.04.02\) Linux 仮想デスクトップは再起動時に「RESUMING」ステータスのままになる可能性があります](#)
- [\(2024.04.02 以前\) SAMAccountName 属性に大文字または特殊文字が含まれている AD ユーザーの同期に失敗しました](#)
- [\(2024.04.02 以前\) 踏み台ホストにアクセスするためのプライベートキーが無効です](#)

### 既知の問題 2024.x

.....  
(2024.12 および 2024.12.01) 新しい Cognito ユーザーを登録する際の正規表現の失敗

バグの説明

などの「.」を含む E メールプレフィックスを持つウェブポータルを介して AWS Cognito ユーザーを登録しようとする <firstname>.<lastname>@<company>.com、Cognito ユーザー名が定義された正規表現パターンと一致しないことを示すエラーが発生します。

❌ 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.

このエラーは、ユーザーの E メールプレフィックスから RES 自動生成ユーザー名が原因で発生します。ただし、「.VDIs」では有効なユーザーではありません。この修正により、ユーザー名の生成時に E メールプレフィックスの「.VDIs」でユーザー名が有効になります。

### 影響を受けるバージョン

RES バージョン 2024.12 および 2024.12.01

### 緩和策

1. 次のコマンドを実行して、バージョン 2024.12 `cognito_sign_up_email_fix.patch` の場合は `patch.py` と、バージョン 2024.12.01 `cognito_sign_up_email_fix.patch` の場合は `をダウンロードします。` <output-directory> をパッチスクリプトとパッチファイルをダウンロードするディレクトリに、`を RES 環境の名前<environment-name>に置き換えます。`
  - a. パッチは RES 2024.12 および 2024.12.01 に適用されます。
  - b. パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
  - c. RES AWS がデプロイされているアカウントとリージョンの CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされたディレクトリに移動します。次のパッチコマンドを実行します。

```
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. 環境の Cluster Manager インスタンスを再起動します。Amazon EC2 マネジメントコンソールからインスタンスを終了することもできます。

```
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. 名前 で始まる Auto Scaling グループのアクティビティを確認して、Cluster Manager インスタンスのステータスを確認します <RES-EnvironmentName>-cluster-manager-asg。新しいインスタンスが正常に起動されるまで待ちます。

.....

(2024.12.01 以前) カスタムドメインを使用して VDI に接続するときは無効な不正な証明書エラーが発生する

#### バグの説明

[外部リソースレシピ](#)と RES をカスタムポータルドメイン名でデプロイすると、CertificateRenewalNode は VDI 接続の TLS 証明書の更新に失敗し、で次のエラーが発生します / 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
}
```

その結果、RES ウェブポータルで VDI に接続すると、`net::ERR_CERT_DATE_INVALID` (Chrome) または `Error code: SSL_ERROR_BAD_CERT_DOMAIN` (Firefox) というエラーが発生します。

## 影響を受けるバージョン

2024.12.01 以前

## 緩和策

1. EC2 コンソールに移動します。という名前のインスタスがある場合は `CertificateRenewalNode-`、インスタスを終了します。
2. Lambda コンソールに移動します。という名前の Lambda 関数のソースコードを開きます - `CertificateRenewalLambda-`。で見つめている行を特定し `./acme.sh --issue --dns dns_aws --ocsp-must-staple --keylength 4096`、引 `--ocsp-must-staple` 数を削除します。
3. `デプロイ` を選択し、コード変更が有効になるまで待ちます。
4. Lambda 関数を手動でトリガーするには、テストタブに移動し、テストを選択します。追加の入力は必要ありません。これにより、Secret Manager で Certificate シークレットと PrivateKey シークレットを更新する証明書 EC2 インスタスが作成されます。シークレットが更新されると、インスタスは自動的に終了します。
5. 既存の `dvc-gateway` インスタスを終了する: `<env-name>-vdc-gateway` とは、自動スケーリンググループが新しいインスタスを自動的にデプロイするのを待ちます。

## エラーの詳細

Let's Encrypt は 2025 年に OCSP サポートを終了します。2025 年 1 月 30 日以降、OCSP Must-Staple リクエストは、リクエスト元のアカウントが OCSP Must Staple 拡張機能を含む証明書を以前に発行していない限り失敗します。詳細については、<https://letsencrypt.org/2024/12/05/ending-ocsp/> を参照してください。

.....

## (2024.12 および 2024.12.01) Active Directory ユーザーは踏み台ホストに SSH できません

### バグの説明

Active Directory ユーザーは、RES ウェブポータル の指示に従って踏み台ホストに接続すると、アクセス許可拒否エラーを受け取ります。

踏み台ホストで実行される Python アプリケーションは、環境変数がないため、SSSD サービスを起動できません。その結果、AD ユーザーはオペレーティングシステムに対して不明であり、ログインできません。

### 影響を受けるバージョン

2024 年 12 月 2024.12.01

### 緩和策

1. EC2 コンソールから踏み台ホストインスタンスに接続します。
2. IDEA\_CLUSTER\_NAME で編集/etc/environmentして新しい行environment\_name=<res-environment-name>として追加します。
3. インスタンスで次のコマンドを実行します。

```
source /etc/environment
sudo service supervisord restart
sudo systemctl restart supervisord
```

4. RES ウェブポータル の指示に従って、踏み台ホストに再度接続してみてください。

.....

## (2024.10) 隔離された VPCs

### バグの説明

2024.10 RES リリースでは、一定期間アイドル状態の VDI に VDI s 自動停止が追加されました。この設定は、デスクトップ設定 → サーバー → セッションで設定できます。

VDI 自動停止は現在、分離された VPCs にデプロイされた RES 環境ではサポートされていません。

### 影響を受けるバージョン

2024 年 10 月

## 緩和策

現在、今後のリリースに含まれる修正に取り組んでいます。ただし、隔離された VPCs VDI を手動で停止することは可能です。

### (2024.10 以前) Graphic 拡張インスタンスタイプの VDI の起動に失敗しました

#### バグの説明

Amazon Linux 2 - x86\_64、RHEL 8 - x86\_64、または RHEL 9 x86\_64 VDI がグラフィック拡張インスタンスタイプ (g4、g5) で起動されると、インスタンスはプロビジョニング状態でスタックします。つまり、インスタンスが「準備完了」状態になり、接続可能になることはありません。

これは、X Server がインスタンスで適切にインスタンス化されないために発生します。このパッチを適用したら、グラフィックインスタンスのソフトウェアスタックのルートボリュームサイズを 50 GB に増やして、すべての依存関係をインストールするための十分なスペースを確保することをお勧めします。

#### 影響を受けるバージョン

すべての RES バージョン 2024.10 以前。

## 緩和策

1. をパッチスクリプトとパッチファイルをダウンロードするディレクトリ<output-directory>に、を以下のコマンドで RES 環境の名前<environment-name>に置き換えて、[patch.py](#) と [graphic\\_enhanced\\_instance\\_types\\_fix.patch](#) をダウンロードします。
  - a. パッチは RES 2024.10 にのみ適用されます。
  - b. パッチスクリプトには、AWS CLI v2、Python 3.9.16 以降、および Boto3 が必要です。
  - c. RES AWS がデプロイされているアカウントとリージョンの CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされたディレクトリに移動します。次のパッチコマンドを実行します。

```
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. 環境の Virtual Desktop Controller (vdc-controller) インスタンスを終了するには、次のコマンドを実行し、表示されている RES 環境の名前を置き換えます。

```
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. 名前が始まるターゲットグループが正常<RES-EnvironmentName>-vdc-extになったら、新しいインスタンスを起動します。グラフィックインスタンスに登録する新しいソフトウェアスタックには、少なくとも 50GB のストレージがあることをお勧めします。

## .....

## (2024 年 8 月) インフラストラクチャ AMI 障害の準備

### バグの説明

[前提条件ドキュメント](#)に記載されている指示に従って EC2 Image Builder を使用して AMIs を準備すると、ビルドプロセスが失敗し、次のエラーメッセージが表示されます。

```
CmdExecution: [ERROR] Command execution has resulted in an error
```

これは、ドキュメントで提供されている依存関係ファイルのエラーが原因です。

## 影響を受けるバージョン

2024 年 8 月

### 緩和策

新しい EC2 Image Builder リソースを作成します。

(RES インスタンス用に AMIs を準備したことがない場合は、以下の手順に従います)

1. 更新された [res-installation-scripts.tar.gz](#) ファイルをダウンロードします。
2. AMIs) の準備「[???](#)」に記載されているステップに従います。

以前の EC2 Image Builder リソースの再利用:

(RES インスタンス用に AMIs を準備している場合は、以下の手順に従います)

1. 更新された [res-installation-scripts.tar.gz](#) ファイルをダウンロードします。
2. EC2 Image Builder → コンポーネント → RES AMIs の準備用に作成されたコンポーネントをクリックします。
3. Content → DownloadRESInstallScripts ステップ → input → source にリストされている S3 の場所を書き留めます。
4. 上記の S3 の場所には、以前に使用された依存関係ファイルが含まれています。このファイルを最初のステップでダウンロードしたファイルに置き換えます。

.....

(2024.08) 仮想デスクトップがルートバケット ARN とカスタムプレフィックスを使用して Amazon S3 バケットの読み取り/書き込みをマウントできない

### バグの説明

Research and Engineering Studio 2024.08 は、ルートバケット ARN (つまり、) とカスタムプレフィックス (プロジェクト名またはプロジェクト名とユーザー名) を使用する場合、仮想デスクトップインフラストラクチャ (VDIarn:aws:s3:::example-bucket) インスタンスへの読み取り/書き込み S3 バケットのマウントに失敗します。

この問題の影響を受けないバケット設定は次のとおりです。

- 読み取り専用バケット

- バケット ARN (つまり、arn:aws:s3:::example-bucket/example-folder-prefix) およびカスタムプレフィックス (プロジェクト名またはプロジェクト名とユーザー名) の一部としてプレフィックスを持つバケットの読み取り/書き込み
- ルートバケット ARN を持つが、カスタムプレフィックスがないバケットの読み取り/書き込み

VDI インスタンスをプロビジョニングした後、その S3 バケットに指定されたマウントディレクトリにはバケットがマウントされません。VDI のマウントディレクトリは存在しますが、ディレクトリは空になり、バケットの現在のコンテンツは含まれません。ターミナルを使用してディレクトリにファイルを書き込むと、エラー Permission denied, unable to write a file がスローされ、ファイルの内容は対応する S3 バケットにアップロードされません。

## 影響を受けるバージョン

2024 年 8 月

## 緩和策

1. パッチスクリプトとパッチファイル (patch.py および s3\_mount\_custom\_prefix\_fix.patch) をダウンロードするには、次のコマンドを実行し、 をパッチスクリプトとパッチファイルをダウンロードするディレクトリ <output-directory> に、 を RES 環境の名前 <environment-name> に置き換えます。
  - a. パッチは RES 2024.08 にのみ適用されます。
  - b. パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
  - c. RES がデプロイされているアカウントとリージョンの AWS CLI を設定し、RES によって作成されたバケットに書き込むための Amazon S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行します。

```
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. 環境の Virtual Desktop Controller (vdc-controller) インスタンスを終了するには、次のコマンドを実行します。(最初のステップで ENVIRONMENT\_NAME 変数を RES 環境の名前に設定済みです)。

```
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

プライベート VPC セットアップの場合、まだ行っていない場合は、<RES-EnvironmentName>-vdc-custom-credential-broker-lambda 関数に名前 AWS\_STS\_REGIONAL\_ENDPOINTS と値が Environment variable の を追加してください regional。詳細については「[分離された VPC デプロイの Amazon S3 バケットの前提条件](#)」を参照してください。

4. 名前で始まるターゲットグループが正常 <RES-EnvironmentName>-vdc-ext になったら、ルートバケット ARN とカスタムプレフィックスが正しくマウントされた読み取り/書き込み S3 バケットを持つ新しい VDI s を起動する必要があります。

.....  
(2024.06) AD グループ名にスペースが含まれている場合、スナップショットの適用は失敗する

#### 問題

AD グループに名前にスペースが含まれている場合、RES 2024.06 は以前のバージョンのスナップショットを適用できません。

クラスターマネージャーの CloudWatch ログ (`/<environment-name>/cluster-manager` ロググループの下) には、AD 同期中に次のエラーが含まれます。

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

このエラーは、以下の要件を満たすグループ名のみを RES が受け入れることが原因です。

- 小文字と大文字の ASCII 文字、数字、ダッシュ (-)、ピリオド (.)、アンダースコア (\_) のみを含めることができます。
- ダッシュ (-) は最初の文字として使用できません
- スペースを含めることはできません。

## 影響を受けるバージョン

2024 年 6 月

## 緩和策

1. パッチスクリプトとパッチファイル ([patch.py](#) および [groupname\\_regex.patch](#)) をダウンロードするには、次のコマンドを実行し、をファイルを配置するディレクトリ `<output-directory>` に、を RES 環境の名前 `<environment-name>` に置き換えます。
  - a. パッチは RES 2024.06 にのみ適用されます
  - b. パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
  - c. RES AWS がデプロイされているアカウントとリージョンの CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行します。

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

3. 環境の Cluster Manager インスタンスを再起動するには、次のコマンドを実行します。Amazon EC2 マネジメントコンソールからインスタンスを終了することもできます。

```
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

このパッチでは、AD グループ名に小文字と大文字の ASCII 文字、数字、ダッシュ (-)、ピリオド (.)、アンダースコア (\_)、および合計長が 1~30 のスペースを含めることができます。

## .....

### (2024.06 以前) AD 同期中に RES に同期されていないグループメンバー

#### バグの説明

GroupOU が UserOU と異なる場合、グループメンバーは RES に正しく同期されません。UserOU

RES は、AD グループからユーザーを同期しようとする、ldapsearch フィルターを作成します。現在のフィルターは、GroupOU パラメータの代わりに UserOU GroupOU パラメータを誤って使用します。その結果、検索はユーザーを返すことができません。この動作は UsersOU と GroupOU が異なるインスタンスでのみ発生します。

#### 影響を受けるバージョン

すべての RES バージョン 2024.06 以前

## 緩和策

問題を解決するには、次の手順に従います。

1. patch.py スクリプトと group\_member\_sync\_bug\_fix.patch ファイルをダウンロードするには、次のコマンドを実行し、 をファイルをダウンロードするローカルディレクトリ<output-directory>に置き換え、 をパッチを適用する RES のバージョン<res\_version>に置き換えます。

### Note

- パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
- RES がデプロイされているアカウントとリージョンの AWS CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。
- パッチは RES バージョン 2024.04.02 と 2024.06 のみをサポートしています。2024.04 または 2024.04.01 を使用している場合は、「」に記載されている手順に従って[マイナーバージョンの更新](#)、パッチを適用する前に環境を 2024.04.02 に更新できます。

- RES バージョン: RES 2024.04.02

パッチダウンロードリンク: [2024.04.02\\_group\\_member\\_sync\\_bug\\_fix.patch](#)

- RES バージョン: RES 2024.06

パッチダウンロードリンク: [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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行し、 を RES 環境の名前<environment-name>に置き換えます。

```
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. 環境の cluster-manager インスタンスを再起動するには、次のコマンドを実行します。

```
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 以前) CVE-2024-6387、RegreSSHion、RHEL9 および Ubuntu VDIs のセキュリティ脆弱性

### バグの説明

regreSSHion と呼ばれる [CVE-2024-6387](#) は、OpenSSH サーバーで識別されています。この脆弱性により、リモートの認証されていない攻撃者はターゲットサーバーで任意のコードを実行し、安全な通信に OpenSSH を利用するシステムに重大なリスクをもたらします。

RES の場合、標準設定は踏み台ホストを経由し、仮想デスクトップに SSH されます。踏み台ホストはこの脆弱性の影響を受けません。ただし、すべての RES バージョンで RHEL9 および Ubuntu2024 VDIs (仮想デスクトップインフラストラクチャ) に提供するデフォルトの AMI (Amazon マシンイメージ) は、セキュリティの脅威に対して脆弱な OpenSSH バージョンを使用します。

つまり、既存の RHEL9 および Ubuntu2024 VDIs は悪用される可能性があります。攻撃者は踏み台ホストへのアクセスが必要になります。

問題の詳細については、[こちら](#)を参照してください。

## 影響を受けるバージョン

すべての RES バージョン 2024.06 以前。

## 緩和策

RHEL9 と Ubuntu の両方が OpenSSH のパッチをリリースし、セキュリティの脆弱性を修正しました。これらは、プラットフォームのそれぞれのパッケージマネージャーを使用してプルできます。

既存の RHEL9 または Ubuntu VDI がある場合は、以下の PATCH EXISTING VDI の手順に従うことをお勧めします。今後の VDI パッチを適用するには、PATCH FUTURE VDI の手順に従うことをお勧めします。以下の手順では、スクリプトを実行してプラットフォームの更新を VDI に適用する方法について説明します。

### 既存の VDI

1. 既存のすべての Ubuntu および RHEL9 VDI にパッチを適用する次のコマンドを実行します。
  - a. パッチスクリプトには [AWS CLI v2](#) が必要です。
  - b. RES がデプロイされているアカウントとリージョンの AWS CLI を設定し、AWS Systems Manager Run Command を送信するための Systems Manager アクセス許可があることを確認します。

```
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. Run [Command ページ](#) でスクリプトが正常に実行されたことを確認できます。コマンド履歴タブをクリックし、最新のコマンド ID を選択し、すべてのインスタンス ID に SUCCESS メッセージがあることを確認します。

### 将来の VDI パッチを適用する

1. パッチスクリプトとパッチファイル ([patch.py](#) と [update\\_openssh.patch](#)) をダウンロードするには、`をファイルをダウンロードするディレクトリ<output-directory>`に、`を RES 環境の名前<environment-name>`に置き換えて、次のコマンドを実行します。

**Note**

- パッチは RES 2024.06 にのみ適用されます。
- パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
- RES がデプロイされているアカウントとリージョンに AWS CLI のコピーを設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. 次のパッチコマンドを実行します。**

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

**3. 次のコマンドを使用して、環境の " Controller インスタンスを再起動します。**

```
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

将来の VDI へのパッチ適用は、RES バージョン 2024.06 以降でのみサポートされています。2024.06 より前のバージョンの RES 環境の将来の VDI にパッチを適用するには、まずの順序を使用して RES 環境を 2024.06 にアップグレードします [メジャーバージョンの更新](#)。

## (2024.04-2024.04.02) VDI インスタンスのロールにアタッチされていない IAM アクセス許可境界が提供されました

### 問題

仮想デスクトップセッションがプロジェクトのアクセス許可の境界設定を適切に継承していない。これは、IAMPermissionBoundary パラメータで定義されたアクセス許可の境界が、そのプロジェクトの作成中にプロジェクトに適切に割り当てられていないためです。

### 影響を受けるバージョン

2024 年 4 月 - 2024.04.02

### 緩和策

VDI がプロジェクトに割り当てられたアクセス許可の境界を適切に継承できるようにするには、次の手順に従います。

1. パッチスクリプトとパッチファイル ([patch.py](#) および [vdi\\_host\\_role\\_permission\\_boundary.patch](#)) をダウンロードするには、次のコマンドを実行し、ファイルを配置するローカルディレクトリ<output-directory>に置き換えます。
  - a. パッチは RES 2024.04.02 にのみ適用されます。バージョン 2024.04 または 2024.04.01 を使用している場合は、[マイナーバージョンの更新についてパブリックドキュメントに記載されている手順に従って](#)、環境を 2024.04.02 に更新できます。
  - b. パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
  - c. RES がデプロイされているアカウントとリージョンの AWS CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行し、を RES 環境の名前<environment-name>に置き換えます。

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

3. を RES 環境の名前<environment-name>に置き換えて、このコマンドを実行して環境内の cluster-manager インスタンスを再起動します。Amazon EC2 マネジメントコンソールからインスタンスを終了することもできます。

```
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 以前) ap-southeast-2 (シドニー) の Windows NVIDIA インスタンスが起動に失敗する

## 問題

Amazon マシンイメージ (AMIs) は、特定の設定で RES で仮想デスクトップ (VDIs) をスピンアップするために使用されます。各 AMI には、リージョンごとに異なる ID が関連付けられています。RES

で ap-southeast-2 (シドニー) で Windows Nvidia インスタンスを起動するように設定された AMI ID は現在正しくありません。

このタイプのインスタンス設定 ami-0e190f8939a996caf の AMI-ID は、ap-southeast-2 (シドニー) に誤ってリストされています。代わりに AMI ID ami-027cf6e71e2e442f4 を使用する必要があります。

デフォルトの AMI ami-0e190f8939a996caf でインスタンスを起動しようとする、次のエラーが発生します。

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

設定ファイルの例を含む、バグを再現する手順:

- ap-southeast-2 リージョンに RES をデプロイします。
- Windows-NVIDIA のデフォルトソフトウェアスタック (AMI ID) を使用してインスタンスを起動します ami-0e190f8939a996caf。

### 影響を受けるバージョン

すべての RES バージョン 2024.04.02 以前が影響を受けます

### 緩和策

以下の緩和策は RES バージョン 2024.01.01 でテストされています。

- 次の設定で新しいソフトウェアスタックを登録する
  - AMI ID: ami-027cf6e71e2e442f4
  - オペレーティングシステム: Windows
  - GPU 製造元: NVIDIA
  - 最小ストレージサイズ (GB): 30
  - 最小 RAM (GB): 4
- このソフトウェアスタックを使用して Windows-NVIDIA インスタンスを起動する

.....

## (2024.04 および 2024.04.01) GovCloud での RES 削除の失敗

### 問題

RES 削除ワークフロー中に、UnprotectCognitoUserPoolLambda は後で削除される Cognito ユーザープールの削除保護を無効にします。Lambda の実行は、によって開始されず InstallerStateMachine。

商用リージョンと GovCloud リージョンでデフォルトの AWS CLI バージョンが異なるため、Lambda の update\_user\_pool 呼び出しは GovCloud リージョンで失敗します。

GovCloud リージョンで RES を削除しようとする、次のエラーが表示されます。

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection\n\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,\nSmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,\nVerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,\nDeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,\nAdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

バグを再現する手順:

- GovCloud リージョンに RES をデプロイする
- RES スタックを削除する

影響を受けるバージョン

RES バージョン 2024.04 および 2024.04.01

緩和策

RES バージョン 2024.04 では、次の緩和策がテストされています。

- UnprotectCognitoUserPool Lambda を開く
  - 命名規則: `<env-name>-InstallerTasksUnprotectCognitoUserPool-...`
- ランタイム設定 -> 編集 -> ランタイム -> 保存 Python 3.11 を選択します。
- CloudFormation を開きます。
- RES スタックの削除 -> Retain Installer Resource UNCHECKED -> Delete のままにします。

.....

(2024.04 - 2024.04.02) Linux 仮想デスクトップは再起動時に「RESUMING」ステータスのままになる可能性があります

## 問題

Linux 仮想デスクトップは、手動またはスケジュールされた停止後に再起動すると、「RESUMING」ステータスのままになることがあります。

インスタンスを再起動した後、AWS Systems Manager は新しい DCV セッションを作成するためのリモートコマンドを実行せず、次のログメッセージが vdc-controller CloudWatch ログ (/<environment-name>/vdc/controllerCloudWatch ロググループの下) に欠落しています。

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

## 影響を受けるバージョン

2024 年 4 月 - 2024.04.02

## 緩和策

「RESUMING」状態でスタックしている仮想デスクトップを復旧するには:

1. EC2 コンソールから問題インスタンスに SSH 接続します。
2. インスタンスで次のコマンドを実行します。

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

3. インスタンスが再起動するのを待ちます。

新しい仮想デスクトップが同じ問題に陥らないようにするには:

1. パッチスクリプトとパッチファイル ([patch.py](#) および [vdi\\_stuck\\_in\\_resuming\\_status.patch](#)) をダウンロードするには、次のコマンドを実行し、をファイルを配置するディレクトリ<output-directory>に置き換えます。

**Note**

- パッチは RES 2024.04.02 にのみ適用されます。
- パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。
- RES AWS がデプロイされているアカウントとリージョンの CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行し、を RES 環境の名前<environment-name>に、を RES がデプロイされているリージョン<aws-region>に置き換えます。

```
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. 環境の " Controller インスタンスを再起動するには、次のコマンドを実行し、を RES 環境の名前<environment-name>に置き換えます。

```
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 以前) SAMAccountName 属性に大文字または特殊文字が含まれている AD ユーザーの同期に失敗しました

### 問題

SSO が少なくとも 2 時間 (2 つの AD 同期サイクル) セットアップされると、RES は AD ユーザーの同期に失敗します。クラスターマネージャーの CloudWatch ログ (/<environment-name>/cluster-manager ロググループの下) には、AD 同期中に次のエラーが含まれます。

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

エラーは、以下の要件を満たす SAMAccount ユーザー名のみを RES が受け入れることが原因です。

- 小文字の ASCII 文字、数字、ピリオド (.)、アンダースコア (\_) のみを含めることができます。
- ピリオドまたはアンダースコアは、最初または最後の文字として使用できません。
- 2 つの連続したピリオドまたはアンダースコア (...、\_\_、\_.、\_ など) を含めることはできません。

### 影響を受けるバージョン

2024.04.02 以前

### 緩和策

1. パッチスクリプトとパッチファイル ([patch.py](#) と [samaccountname\\_regex.patch](#)) をダウンロードするには、次のコマンドを実行し、 をファイルを配置するディレクトリ<output-directory>に置き換えます。

#### Note

- パッチは RES 2024.04.02 にのみ適用されます。
- パッチスクリプトには、[AWS CLI v2](#)、Python 3.9.16 以降、および [Boto3](#) が必要です。

- RES AWS がデプロイされているアカウントとリージョンの CLI を設定し、RES によって作成されたバケットに書き込む S3 アクセス許可があることを確認します。

```
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. パッチスクリプトとパッチファイルがダウンロードされるディレクトリに移動します。次のパッチコマンドを実行し、 を RES 環境の名前<environment-name>に置き換えます。

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

3. 環境の Cluster Manager インスタンスを再起動するには、次のコマンドを実行し、 を RES 環境の名前<environment-name>に置き換えます。Amazon EC2 マネジメントコンソールからインスタンスを終了することもできます。

```
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 以前) 踏み台ホストにアクセスするためのプライベートキーが無効です

問題

ユーザーがプライベートキーをダウンロードして RES ウェブポータルから踏み台ホストにアクセスすると、キーの形式が正しくありません。複数の行が 1 行としてダウンロードされ、キーが無効になります。ダウンロードしたキーを使用して踏み台ホストにアクセスしようとする、次のエラーが表示されます。

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

## 影響を受けるバージョン

2024.04.02 以前

## 緩和策

このブラウザは影響を受けないため、Chrome を使用してキーをダウンロードすることをお勧めします。

または、 の後に新しい行を作成し、 の直前に別の行を作成して-----BEGIN PRIVATE KEY-----、キーファイルを再フォーマットすることもできます-----END PRIVATE KEY-----。

.....

# Research and Engineering Studio サポートポリシー

Research and Engineering Studio (RES) は、複数のリリースを同時にサポートします。RES は YYYY.mm.patch バージョンスキームを使用します。 はメジャーリリース YYYY.mm を表します。 YYYY は年を表し、 はリリース月 mm を表し、 は増分リリース patch を示します。各 RES リリースには、 +YYYY1 年の mm 月の最終日であるサポート終了 (EOSL) 日がスケジュールされています。たとえば、2025 年 9 月の EOSL 日付は 2026 年 9 月 30 日です。EOSL の日付を過ぎると、そのリリースに対するサポートやメンテナンスは提供されません。

新機能、パフォーマンスの向上、セキュリティ更新、バグ修正は、新しいメジャーバージョンリリース () に含まれています。重大な問題の場合、 はパッチリリースを通じて修正 AWS を提供しますが、EOSL に達していないリリースに対してのみ修正を提供します。

インプレース更新は、同じメジャーリリース ( から 2024.04.01 など) 内のパッチリリース間でのみサポートされます。新しいメジャー RES バージョンから更新を使用するには、そのバージョンの新しいインストールを実行する必要があります。最新の機能とセキュリティ更新プログラムにアクセスできるように、RES のインストールを最新のリリース up-to-date に更新することをお勧めします。

サポート終了日 (EOSL) が近づいているバージョンを実行している場合は、サポートを維持し、最新の改善点にアクセスできるように、新しいバージョンにアップグレードする計画を立ててください。RES のアップグレードの詳細な手順については、 [ドキュメントを参照してください](#)。アップグレードに関するご質問やサポートが必要な場合は、 AWS サポートにお問い合わせください。

Research and Engineering Studio バージョン	サポート終了 (EOSL) 日
2023 年 11 月 x 日	11/30/2024
2024 年 1 月 x 日	1/31/2025
2024 年 4 月 x 日	4/30/2025
2024 年 6 月 x 日	6/30/2025
2024 年 8 月 x 日	8/31/2025
2024 年 10 月 x 日	10/31/2025
2024 年 12 月 x 日	12/31/2025

Research and Engineering Studio バージョン	サポート終了 (EOSL) 日
2025 年 3 月x 日	3/30/2026
2025 年 6 月x 日	6/30/2026
2025 年 9 月x 日	9/30/2026

 Important

デプロイ後に infra / VDI ホストにパッチを適用するのはお客様の責任です。

## 注意

各 Amazon EC2 インスタンスには、管理目的で 2 つのリモートデスクトップサービス (ターミナルサービス) ライセンスが付属しています。この[情報は](#)、これらのライセンスを管理者にプロビジョニングするのに役立ちます。また、[を使用することもできます](#)。これにより[AWS Systems Manager Session Manager](#)、RDP を使用せずに、RDP ライセンスを必要とせずに Amazon EC2 インスタンスにリモートでログインできます。追加のリモートデスクトップサービスライセンスが必要な場合は、Microsoft または Microsoft ライセンスリセラーからリモートデスクトップユーザー CALs を購入する必要があります。アクティブなソフトウェアアシュアランスを持つリモートデスクトップユーザー CALs にはライセンスモビリティの利点があり、デフォルト (共有) テナント環境に移行 AWS できます。ソフトウェアアシュアランスまたはライセンスモビリティのメリットなしでライセンスを持ち込む方法については、FAQ の[このセクション](#)を参照してください。

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。このドキュメント：(a) は情報提供のみを目的としています。(b) 現在の製品の提供とプラクティスを表す AWS 予告なしに変更される可能性がある場合 および (c) は、AWS およびその関連会社からのいかなるコミットメントまたは保証も作成しません。サプライヤーまたは licensors. AWS products またはサービスは、保証なしで「現状有姿」で提供されます。表現、またはあらゆる種類の条件、明示的か暗示的かにかかわらず、顧客に対する AWS 責任と責任は AWS 契約によって管理されます。このドキュメントは の一部ではありません。 も変更されません。AWS とその顧客との間の契約。

の Research and Engineering Studio AWS は、Apache [Software Foundation で利用可能な Apache License Version 2.0](#) の条項に基づいてライセンスされています。

# リビジョン

詳細については、GitHub リポジトリの [CHANGELOG.md](#) ファイルを参照してください。

Date	変更
2025 年 12 月	<ul style="list-style-type: none"><li>• リリースバージョン 2025.12</li></ul> <p>機能強化</p> <ul style="list-style-type: none"><li>• デプロイ中のすべての RES コンポーネントへのカスタム CloudFormation タグの伝播。</li><li>• 管理者が Windows ホストの Active Directory 結合を無効にすることを許可します。</li><li>• 管理者が VDI デスクトップインスタンスのデフォルトスケジュールを設定できるようにします。</li><li>• コンプライアンスと監査の要件に対して S3 バケットアクセスのログ記録が有効になっています。</li><li>• すべての S3 バケット通信に必要な SSL/TLS 暗号化。</li><li>• RES マネージド DynamoDB テーブルの point-in-timeリカバリを有効にしました。</li><li>• /opt/cognito_auth ディレクトリのアクセス許可をルートのみアクセスに更新しました。</li></ul> <p>変更</p> <ul style="list-style-type: none"><li>• " EC2 ホストからバックエンド Lambda に " 関連の APIs を移行しました。</li></ul> <p>バグ修正</p>

Date	変更
	<ul style="list-style-type: none"><li>• 新しい VDI の起動時に許可されたインスタンスタイプの更新。</li><li>• efs_utils の欠落している依存関係を修正しました。</li><li>• RES ポータルのコストダッシュボードのセッションの合計数を修正しました。</li><li>• ユーザーが許可されたインスタンスタイプを手動でバイパスできる問題を修正しました。</li><li>• Linux VDIs。</li><li>• Software Stack ページの OS ドロップダウンメニューから欠落しているオペレーティングシステムを追加しました。</li><li>• Chrome でカスタムドメインを使用する場合の頻繁なログアウトの問題を修正しました。</li><li>• AD 結合を無効にした後にランタイム SSSD 設定が適用されない問題を修正しました。</li><li>• VDI ロールの残りによる RES 環境の削除エラーを修正しました。</li></ul>
2025 年 9 月	<ul style="list-style-type: none"><li>• リリースバージョン 2025.09</li></ul> <p>機能強化</p> <ul style="list-style-type: none"><li>•</li></ul> <p>変更</p> <ul style="list-style-type: none"><li>•</li></ul> <p>バグ修正</p> <ul style="list-style-type: none"><li>•</li></ul>

Date	変更
2025 年 7 月	<ul style="list-style-type: none"><li>リリースバージョン 2025.06.01</li></ul> <p>機能強化</p> <ul style="list-style-type: none"><li>システムのデフォルト Python を使用して、インフラストラクチャホストとデフォルトの VDI の起動時間を改善しました。</li><li>Ubuntu 24.04 VDI のサポートが追加されました。</li></ul> <p>変更</p> <ul style="list-style-type: none"><li>Infra ホストと VDI、システムデフォルト Python が利用可能で、RES 要件 (バージョン 3.9.16 以上) を満たしている場合、システムデフォルト Python を使用するようになりました。</li></ul> <p>バグ修正</p> <ul style="list-style-type: none"><li>disable_ad_join が true の場合の Windows および Linux VDI ログインの問題を解決しました。</li><li>カスタム IAM ポリシーがプロジェクト固有のロールにアタッチされない問題を解決しました。</li></ul>

Date	変更
2025 年 6 月	<ul style="list-style-type: none"><li>• リリースバージョン 2025.06</li></ul> <p>機能強化</p> <ul style="list-style-type: none"><li>• AWS GovCloud (米国東部) リージョンのサポートが追加されました。</li><li>• g6e インスタンスタイプのサポートが追加されました。</li><li>• Amazon Linux 2023 で仮想デスクトップセッションを起動するサポートが追加されました。</li><li>• Rocky Linux 9 で仮想デスクトップセッションを起動するサポートが追加されました。</li><li>• IAM リソースプレフィックスとパスのカスタマイズのサポートが追加されました。</li><li>• RES UI からマウントされたファイルシステムを削除する機能を追加しました。</li><li>• Amazon CloudWatch から VDI ブートストラップログを取得する機能を追加しました。</li><li>• RedHat 8 および RedHat 9 VDIs。</li></ul> <p>変更</p> <ul style="list-style-type: none"><li>• インフラストラクチャホストと VDI ホストの IAM アクセス許可の範囲を絞り込みます。</li><li>• インフラストラクチャホストと VDI ホストのブートストラッププロセスが改善されました。</li><li>• DCV ブローカーの DynamoDB テーブル WCU を 20 から 100 に増やしました。</li></ul> <p>バグ修正</p>

Date	変更
	<ul style="list-style-type: none"><li>• RES がオンボーディングのために Elastic Filesystem を一覧表示できない問題を解決しました。</li><li>• Elastic Filesystem のリストが原因で RES がスナップショットの適用に失敗する問題を解決しました。</li><li>• DCV コンソールセッションの解決を調整できない問題を解決しました。</li><li>• スケジュールを変更せずに再保存するときにカスタム VDI スケジュールを削除できる問題を解決しました。</li><li>• AD の多数のユーザーやグループに対してファイルブラウザが応答しなくなる問題を解決しました。</li><li>• セッション管理で VDI セッションが欠落する問題を解決しました。</li><li>• My Virtual Desktop ページで VDI セッションが欠落する問題を解決しました。</li><li>• 休止が有効になっていVDIs でアイドルタイムアウトが機能しない問題を解決しました。</li><li>• ソフトウェアスタック AMIs が古い RES バージョンより前の問題を解決しました。</li></ul>

Date	変更
2025 年 3 月	<ul style="list-style-type: none"><li>• リリースバージョン 2025.03</li></ul> <p>追加されたセクション —</p> <ul style="list-style-type: none"><li>• <a href="#">プロジェクトを無効にする.</a></li><li>• <a href="#">プロジェクトを削除します。</a></li><li>• <a href="#">コスト分析ダッシュボード.</a></li></ul> <p>変更されたセクション —</p> <ul style="list-style-type: none"><li>• <a href="#">仮想デスクトップ.</a></li><li>• <a href="#">ソフトウェアスタック (AMIs).</a></li><li>• <a href="#">RES 対応 AMIs を設定する.</a></li><li>• <a href="#">デスクトップ設定.</a></li><li>• <a href="#">SSH アクセスの設定.</a></li><li>• <a href="#">Active Directory の同期.</a></li></ul>
2024 年 12 月	<ul style="list-style-type: none"><li>• リリースバージョン 2024.12</li></ul> <p>追加されたセクション —</p> <ul style="list-style-type: none"><li>• <a href="#">Active Directory の同期.</a></li><li>• <a href="#">デスクトップアクセス許可の設定.</a></li><li>• <a href="#">ファイルブラウザアクセスの設定.</a></li><li>• <a href="#">SSH アクセスの設定.</a></li><li>• <a href="#">Amazon Cognito ユーザーのセットアップ.</a></li></ul> <p>変更されたセクション —</p> <ul style="list-style-type: none"><li>• <a href="#">環境の境界.</a></li><li>• <a href="#">プライベート VPC を設定する (オプション).</a></li></ul>

Date	変更
2024 年 10 月	<ul style="list-style-type: none"><li>リリースバージョン 2024.10: のサポートを追加 —<ul style="list-style-type: none"><li><a href="#">環境の境界</a>.</li><li><a href="#">デスクトップ共有プロファイル</a>.</li><li><a href="#">仮想デスクトップインターフェイスの自動停止</a>.</li></ul></li></ul>
2024 年 8 月	<ul style="list-style-type: none"><li>リリースバージョン 2024.08: のサポートを追加 —<ul style="list-style-type: none"><li>Amazon S3 バケットを Linux Virtual Desktop Infrastructure (VDI) インスタンスにマウントする。「<a href="#">Amazon S3 バケット</a>」を参照してください。</li><li>カスタムプロジェクトアクセス許可、既存のロールのカスタマイズとカスタムロールの追加を可能にする拡張アクセス許可モデル。「<a href="#">アクセス許可ポリシー</a>」を参照してください。</li></ul></li><li>ユーザーガイド: <a href="#">トラブルシューティングセクション</a>を展開しました。</li></ul>
2024 年 6 月	<ul style="list-style-type: none"><li>リリースバージョン 2024.06 — Ubuntu サポート、プロジェクト所有者のアクセス許可。</li><li>ユーザーガイド: を追加 <a href="#">デモ環境を作成する</a></li></ul>
2024 年 4 月	リリースバージョン 2024.04 — RES 対応 AMIsとプロジェクト起動テンプレート
2024 年 3 月	その他のトラブルシューティングトピック、CloudWatch Logs の保持、マイナーバージョンのアンインストール

Date	変更
2024 年 2 月	リリースバージョン 2024.01.01 — デプロイテンプレートを更新
2024 年 1 月	リリースバージョン 2024.01
2023 年 12 月	GovCloud の指示とテンプレートを追加
2023 年 11 月	初回リリース

## 以前のバージョンのアーカイブ

このユーザーガイドでは、次のアーカイブバージョンを使用できます。

- [Research and Engineering Studio ユーザーガイド 2025.09 リリース](#)
- [Research and Engineering Studio ユーザーガイド 2025.06 リリース](#)
- [Research and Engineering Studio ユーザーガイド 2025.03 リリース](#)
- [Research and Engineering Studio ユーザーガイド 2024.12 リリース](#)

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。