aws

ユーザーガイド

Research and Engineering Studio

Research and Engineering Studio: ユーザーガイド

Table of Contents

概要

Research and Engineering Studio (RES) は、IT 管理者が科学者やエンジニアが でテクニカルコンピューティングワークロードを実行するためのウェブポータルを提供できるようにする、 AWS サポートされているオープンソース製品です 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、データ分析ワークロードを実行するための単一画面を提供します。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構築し (Amazon マシンイメージまたは を使用AMIs)、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へのアクセスを可能にします。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、お客様はポータルのユーザーエクスペリエンスRESを独自のニーズに合わせて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、 の Research and Engineering Studio の概要 AWS、その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、Amazon Web Services (AWS) クラウドRESにデプロイするための設定ステップについて説明します。

特徴と利点

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、を使用するために AWS アカウント または クラウドの専門知識を持つ必要はありませんRES。

プロジェクトベースの設定

プロジェクトを使用して、一連のタスクまたはアクティビティのアクセス許可の定義、リソースの割り当て、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、同僚に付与させたい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、 にサインインRES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ポータルへの接続を有効にし、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。

永続的な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、既存のファイルシステムに接続するか、 内に新しいファイルシステムを作成しますRES。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FSx用の NetApp ONTAP Amazon for Linux 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、 の主要な概念について説明し、 の Research and Engineering Studio に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 (多くの場合、データセットと呼ばれます) のコンテナとして機能します。プロジェクトの境界内に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の委任者。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権限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、同じ人物が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、データリソースとコンピューティングリソースの明確な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、データフローをガバナンスし、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VDIs場合、ユーザーは、メンバーシップが付与されていない場合、プロジェクトデータ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にアクセスし、そのプロジェクトに対する所有権を持つ管理委任者。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内のプロジェクトメンバーに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いてRES、 固有のメタデータを持つ Amazon マシンイメージ (AMI) 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でき、安全で分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 全般のリファレンス の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、次のコンポーネントが にデプロイされます AWS アカウント。

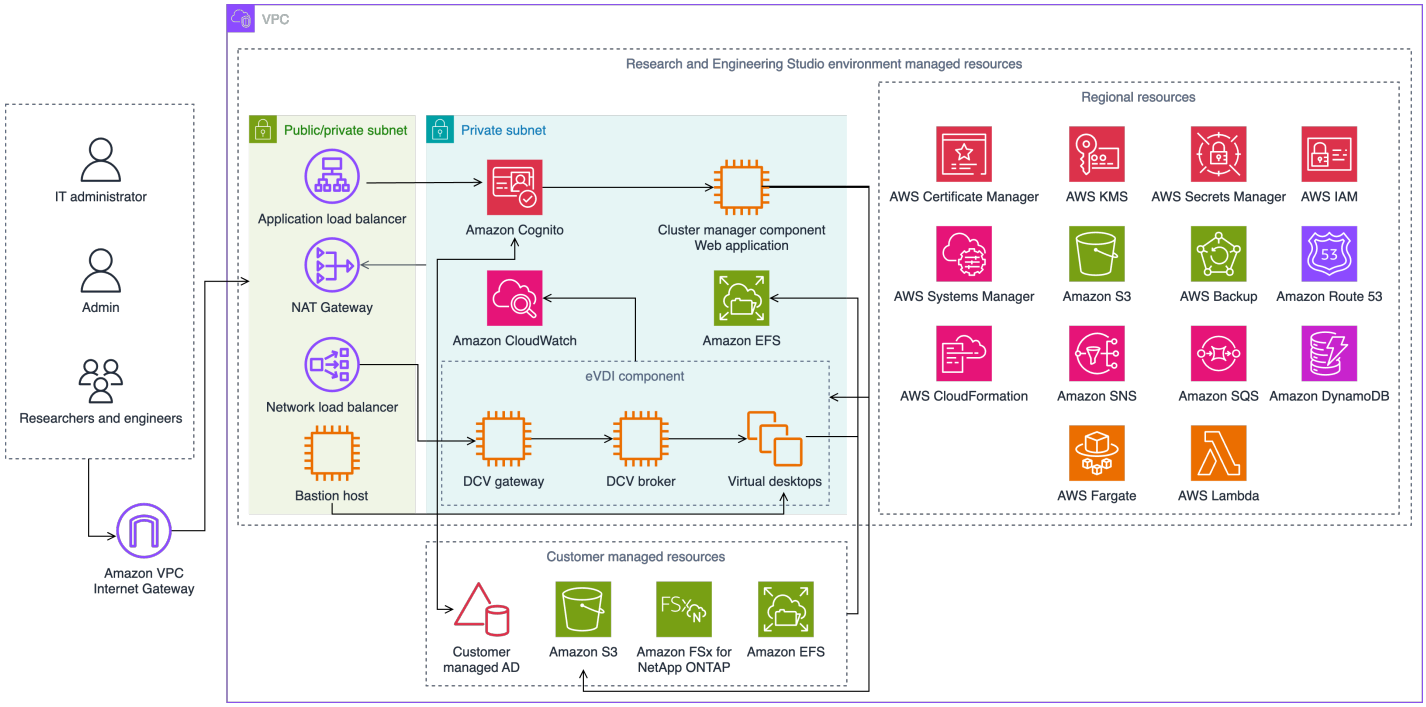


図 1: AWS アーキテクチャに関する Research and Engineering Studio

> **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、ウェブポータルの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 (e VDI) コンポーネント

b. メトリクスコンポーネント

   Amazon は eVDI コンポーネントからメトリクス CloudWatch 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 Bastion Host 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 () のパブリック証明書を生成して保存しますALB。

> **Note**
>
> AWS Certificate Manager を使用して、ドメインの信頼できる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、インストール中に提供された 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 とユーザー 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	型	説明
Amazon Elastic Compute Cloud	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。
Elastic Load Balancing	コア	Bastion、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調整します。
Amazon Virtual Private Cloud	コア	すべてのコア製品コンポーネントは、 内に作成されますVPC。
Amazon Cognito	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。
Amazon Elastic File System	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。
Amazon DynamoDB	コア	ユーザー、グループ、プロジェクト、ファイルシステ

AWS サービス	型	説明
		ム、コンポーネント設定などの設定データを保存します。
AWS Systems Manager	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。
AWS Lambda	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。
Amazon CloudWatch	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。
Amazon Simple Storage Service	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。
AWS Key Management Service	サポート	Amazon SQSキュー、DynamoDB テーブル、Amazon SNSトピックで保管中の暗号化に使用されます。
AWS Secrets Manager	サポート	のサービスアカウントの認証情報を Active Directory と の自己署名証明書に保存します VDIs。
AWS CloudFormation	サポート	製品のデプロイメカニズムを提供します。

AWS サービス	型	説明
AWS Identity and Access Management	サポート	ホストのアクセスレベルを制限します。
Amazon Route 53	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。
Amazon Simple Queue Service	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。
Amazon Simple Notification Service	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ライブモデルをサポートします。
AWS Fargate	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。
Amazon FSx File Gateway	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。
Amazon FSx for NetApp ONTAP	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。
AWS Certificate Manager	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 Backup	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

このセクションの手順に従って、 で Research and Engineering Studio を試してください AWS。このデモでは、AWS デモ環境スタックテンプレートの 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。には Keycloak サーバーを使用しますSSO。

スタックをデプロイした後は、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 AWS 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: 約 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 EC2SSH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/サインアップ 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、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   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。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

Amazon EC2SSHキーペアを作成する

Amazon EC2SSH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 ユーザーガイド」の「Amazon を使用してキーペアを作成するEC2EC2」を参照してください。

サービスクォータを増やす

次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 を 5 IPsから 10 に増やす

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 Management Console し、https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。

   > **Note**
   >
   > 管理者アカウントに登録して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 res-、11 文字以内、大文字を含まない環境で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。このユーザーは、Active Directory のシングルサインオン統合に障害が発生した場合、さらにブレー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 ClientIpCidr 後に を更新できます。
InboundPrefixList		（オプション）ウェブ UI と踏み台ホストSSHへの直接アクセスIPsを許可する のマネージドプレフィックスリストを提供します。

4. [スタックの作成] を選択します。

デプロイ後のステップ

1. でのユーザーパスワードのリセット AWS Directory Service– デモスタックは、、admin1、user1、 の 4 つのユーザーをユーザー名で作成admin2しますuser2。

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`<StackName>*DirectoryService*`スタックの出力から取得できます。
c. 右上のアクションドロップダウンメニューから、ユーザーパスワードのリセット 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、使用する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。

2. ユーザーパスワードをリセットしたら、Research and Engineering Studio が環境内のユーザーを同期するまで待つ必要があります。Research and Engineering Studio は、xx.00 に 1 時間ごとにユーザーを同期します。これが発生するのを待つか、「」に記載されている手順に従ってユーザーをすぐにActive Directory に追加されたが、 から欠落しているユーザー RES同期できます。

これでデプロイの準備が整いました。E メールで EnvironmentUrl 受け取った 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URLから同じもの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るようになりました。

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。

コスト

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AWS Cost Explorerに役立つ予算を作成することをお勧めします。料金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 、最もセキュリティに敏感な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 とユーザーの間で責任を共有します。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して説明しています。

- クラウドのセキュリティ – AWS 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があります AWS クラウド。 AWS は、安全に使用できる の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。 の Research and Engineering Studio に適用されるコンプライアンスプログラムについては AWS、AWS「コンプライアンス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、お客様は、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 が使用する AWS サービスと 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の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、お客様は 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を許可するIAMロールを作成します。

RES は、 内のアイデンティティベースのポリシーをサポートしますIAM。デプロイされると、 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RESを作成します。製品を実装する管理者は、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RES。詳細については、「 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。 AWS

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、 は Amazon CognitoでRES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。をデプロイするときはRES、 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。カスタマー所有および管理の を指定すると AWS KMS key、保管中のカスタマーデータはそのキーを使用して暗号化されます。

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

この製品のサービスの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	での サービスの使用方法 RES
Amazon Elastic Compute Cloud	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。
Elastic Load Balancing	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。
Amazon Virtual Private Cloud	コア	すべてのコア製品コンポーネントは、 内に作成されますVPC。
Amazon Cognito	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。
Amazon Elastic File System	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

AWS サービスセキュリティ情報	サービスタイプ	での サービスの使用方法 RES
		ム、および共有外部ファイルシステムを提供します。
Amazon DynamoDB	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。
AWS Systems Manager	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。
AWS Lambda	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。
Amazon CloudWatch	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。
Amazon Simple Storage Service	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。
AWS Key Management Service	サポート	Amazon SQSキュー、DynamoDB テーブル、Amazon SNSトピックで保管中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	での サービスの使用方法 RES
AWS Secrets Manager	サポート	のサービスアカウントの認証情報を Active Directory と の自己署名証明書に保存しますVDIs。
AWS CloudFormation	サポート	製品のデプロイメカニズムを提供します。
AWS Identity and Access Management	サポート	ホストのアクセスレベルを制限します。
Amazon Route 53	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。
Amazon Simple Queue Service	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。
Amazon Simple Notification Service	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ライブモデルをサポートします。
AWS Fargate	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。
Amazon FSx File Gateway	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。
Amazon FSx for NetApp ONTAP	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。
AWS Certificate Manager	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	での サービスの使用方法 RES
AWS Backup	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

サービスクォータ (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 のサービスクォータ」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、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て、システムを運用します。大規模な本番環境の回復力を向上させるには、インフラス

トラクチャの Auto Scaling グループ () 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ASG。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ーゾーン (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が短縮されます。

ASG 設定は、 の Amazon EC2コンソール内でカスタマイズできますhttps://console.aws.amazon.com/ec2/。製品はASGsデフォルトで 4 つの名前を作成し、各名前は で終わります-asg。最小値と希望の値は、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。の詳細についてはASGs、「Amazon 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。 EC2 Auto Scaling

サポートされる 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「al Services List」を参照してください。

の Research and Engineering Studio AWS は、次の 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 (2024.10)
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 (2024.10)
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
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	いいえ	はい
イスラエル (テルアビブ)	il-central-1	はい	はい
AWS GovCloud （米国西部）	us-gov-west-1	はい	はい

製品のデプロイ

> **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 テンプレートには、この製品に含まれる AWS リソースとそのプロパティが記載されています。 CloudFormation スタックは、 テンプレートで説明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、コスト、アーキテクチャ、ネットワークセキュリティ、およびこのガイドで前述した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

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

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/サインアップ 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、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   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。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

Amazon EC2SSHキーペアを作成する

Amazon EC2SSH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 ユーザーガイド」の「Amazon を使用してキーペアを作成するEC2EC2」を参照してください。

サービスクォータを増やす

次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。
  - アベイラビリティーゾーンあたりのNATゲートウェイを 5 から 10 に増やします。
- Amazon EC2
  - EC2-VPC Elastic を 5 IPsから 10 に増やす

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。

パブリックドメインを作成する (オプション)

ユーザーフレンドリな 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 URL。Amazon Route 53 または他のプロバイダー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する必要があります AWS Certificate Manager。パブリックドメインと証明書が既にある場合は、このステップをスキップできます。

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検索します。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、証明書ステータスセクションARNから をコピーします。

ドメインの作成 (GovCloud のみ)

AWS GovCloud （ 米国西部) リージョンにデプロイしていて、Research and Engineering Studio に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 アカウントに証明書 AWS CloudFormation スタックをデプロイします。
2. Certificate CloudFormation Outputs から、 と を見つけ`CertificateARN`てメモします`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ARN、新しいシークレットを書き留め、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 = [環境名] (これは 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ARN、新しいシークレットを書き留め、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 = [環境名] (これは res-demo である可能性があります)

外部リソースの提供

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が AWS 期待されます。

- ネットワーキング (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 () に必要なファイルとデータが含まれますVDI。

- 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。

- サービスアカウントの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。

> **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 High Performance Compute 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、次のセクションの外部リソースを作成する「」を参照してください。

AWS GovCloud （ 米国西部) リージョンでのデモデプロイでは、 の前提条件の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 ）。

LDAPS 環境で 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 間の通信を提供する必要がありますRES。

1. のサーバー側を有効にする方法に記載されているステップに従いますLDAPS AWS Managed Microsoft AD。既に を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LDAPS。
2. LDAPS が AD に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 PowerShell として 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. まず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選択および保持 (または右クリック) し、すべてのタスクを選択し、 をエクスポートします。
   f. Base-64 エンコード X.509 (.CER ） を選択し、Next 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. でシークレットを作成します AWS Secrets Manager。

   Secrets Manager でシークレットを作成するときは、シークレットタイプで他のタイプのシークレットを選択し、エンPEMコードされた証明書をプレーンテキストフィールドに貼り付けます。
4. ARN が作成したことを書き留め、 の `DomainTLSCertificateSecretARN`パラメータとして入力しますステップ 1: 製品の起動。

プライベートを設定する VPC (オプション)

Research and Engineering Studio を にデプロイするとVPC、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RESデプロイでは、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 RESに をインストールするにはVPC、次の前提条件を満たす必要があります。

トピック

Amazon マシンイメージを準備する (AMIs)

1. 依存関係 をダウンロードします。分離された にデプロイするにはVPC、RESインフラストラクチャに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。
2. Amazon S3 読み取り専用アクセスと Amazon として信頼された ID を持つIAMロールを作成しますEC2。

   a. でIAMコンソールを開きますhttps://console.aws.amazon.com/iam/。
   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の選択ページで、次の操作を行います。

      - 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 のユースケースまたはユースケース で、 EC2を選択して次へ 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
イメージオペレーティングシステム (OS)	Linux
互換性のある OS バージョン	Amazon Linux 2
コンポーネント名	次のような名前を入力します。*<research-and-engineering-studio-infrastructure>*
コンポーネントのバージョン	1.0.0 から始めることをお勧めします。
説明	オプションのユーザーエントリ。

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URI用の ファイルが必要です。から提供された tar.gz ファイルを RES Amazon S3 バケットにアップロードし、バケットプロパティURIからファイルをコピーします。

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 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:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd /root/bootstrap/res_dependencies'
                - 'tar -xf res_dependencies.tar.gz'
                - 'cd all_dependencies'
                - '/bin/bash install.sh'
       - name: AddEnvironmentVariables
         action: ExecuteBash
         onFailure: Abort
```

```
          maxAttempts: 3
          inputs:
             commands:
                 - |
                   echo -e "
                   http_proxy=http://<ip>:<port>
                   https_proxy=http://<ip>:<port>

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

e. [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
レシピの詳細	名前	res-recipe-linux-x86 などの適切な名前を入力します。
	バージョン	バージョンを入力します。通常は 1.0.0 で始まります。
	説明	オプションの説明を追加します。
ベースイメージ	イメージの選択	マネージドイメージを選択します。
	OS	Amazon Linux
	イメージオリジン	クイックスタート (Amazon マネージド)
	[イメージ名]	Amazon Linux 2 x86
	自動バージョニングオプション	利用可能な最新の OS バージョンを使用します。
インスタンス設定	–	すべてをデフォルト設定のままにし、パイプライン実行が選択されていない後にSSMエージェントを削除してください。
作業ディレクトリ	作業ディレクトリパス	/root/bootstrap/res_ 依存関係

セクション	パラメータ	ユーザーエントリ
コンポーネント	コンポーネントの構築	以下を検索して選択します。 • Amazon マネージド: aws-cli-version-2-linux • Amazon マネージド: amazon-cloudwatch-agent-linux • 所有: 以前に作成された Amazon EC2コンポーネント。ID AWS アカウント と最新を フィールドに AWS リージョン 入力します。
	テストコンポーネント	を検索して選択します。 • Amazon マネージド: simple-boot-test-linux

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. 「保存されたリソース」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	res-infra-linux-x86 などの適切な名前を入力します。
	説明	オプションの説明を追加します。

セクション	パラメータ	ユーザーエントリ
	IAM ロール	前に作成したIAMロールを選択します。
AWS インフラストラクチャ	インスタンスタイプ	t3.medium を選択します。

	VPC、サブネット、およびセキュリティグループ	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。
		• VPC: インフラストラクチャ設定でVPC使用されているものと同じものを選択します。これにはインターネットアクセスVPCが必要です。
		• インバウンドルール：
		  • タイプ: SSH
		  • [Source]: Custom
		  • CIDR ブロック: 0.0.0.0/0

d. インフラストラクチャー構成の作成 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 では、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、以前に作成したレシピ名を入力します。[Next (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の使用を選択し、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。[Next (次へ)] を選択します。

f. ディストリ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。

- がインフラストラクチャホストインスタンスRESを適切に起動できるように、出力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、Image Builder サービスが使用されているリージョンに出力EC2イメージが作成されます。
- 複数のリージョンRESにデプロイする場合は、新しいディストリビューション設定を作成し、そこにリージョンを追加することができます。

g. 選択を確認し、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. Image pipelines から、作成したパイプラインを検索して選択します。

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 の AMI ID を書き留めAMI、 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: 製品の起動”。

VPC エンドポイントの設定

仮想デスクトップをデプロイRESして起動するには、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
Application Auto Scaling	com.amazonaws。*region*.application-autoscaling
AWS CloudFormation	com.amazonaws。*region*cloudformation.
Amazon CloudWatch	com.amazonaws。*region*.モニタリング
Amazon CloudWatch Logs	com.amazonaws。*region*.logs
Amazon DynamoDB	com.amazonaws。*region*.dynamodb (ゲートウェイエンドポイントが必要)
Amazon EC2	com.amazonaws。*region*ec2.
Amazon ECR	com.amazonaws。*region*.ecr.api
	com.amazonaws。*region*.ecr.dkr
Amazon Elastic File System	com.amazonaws。*region*elasticfilesystem。
Elastic Load Balancing	com.amazonaws。*region*.elasticloadbalancing
Amazon EventBridge	com.amazonaws。*region*.events
Amazon FSx	com.amazonaws。*region*.fsx
AWS Key Management Service	com.amazonaws。*region*kms.
Amazon Kinesis Data Streams	com.amazonaws。*region*.kinesis-streams
AWS Lambda	com.amazonaws。*region*lambda。
Amazon S3	com.amazonaws。*region*.s3 (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) RES。 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。 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を参照してください。

AWS のサービス	サービス名
AWS Secrets Manager	com.amazonaws。*region*secretsmanager。
Amazon SES	com.amazonaws。*region*.email-smtp (次のアベイラビリティーゾーンではサポートされていません: use-1-az2、use1-az3、use1-az5、usw1-az2、usw2-az4、apne2-az4、cac1-az3、cac1-az4)
AWS Security Token Service	com.amazonaws。*region*.sts
Amazon SNS	com.amazonaws。*region*.sns
Amazon SQS	com.amazonaws。*region*sqs。
AWS Systems Manager	com.amazonaws。*region*.ec2 メッセージ
	com.amazonaws。*region*ssm。
	com.amazonaws。*region*.ssmmessages

VPC エンドポイントなしで 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、 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VPC。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。

1. RES デプロイVPCに使用する 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 以降
   - セキュリティグループ — 0.0.0.0/0 からのポート 3128 TCP上
2. 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。
   a. 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 用)

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PORTがリッスンする に注意してください。

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、Infrastructure/ 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VDIs。

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: 製品の起動”、 AWS 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。設定したプライベートに正常にデプロイするには、次のパラメータを必ず設定VPCしてください。

パラメータ	入力
InfrastructureHostAMI	で作成されたインフラストラクチャ AMI ID を使用しますthe section called “Amazon マシンイメージを準備する (AMIs) ”。
IsLoadBalancerInternetFacing	false に設定します。

パラメータ	入力
LoadBalancerSubnets	インターネットアクセスのないプライベートサブネットを選択します。
InfrastructureHostSubnets	インターネットアクセスのないプライベートサブネットを選択します。
VdiSubnets	インターネットアクセスのないプライベートサブネットを選択します。
ClientIP	を選択してVPCCIDR、すべての VPC IP アドレスへのアクセスを許可できます。

外部リソースを作成する

この CloudFormation スタックは、ネットワーク証明書、ストレージ証明書、アクティブディレクトリ証明書、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を使用できる必要があります。

デプロイ前にレシピテンプレートをダウンロードできます。

デプロイまでの時間： 約 40～90 分

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。

   > **Note**
   >
   > 管理者アカウントに登録して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 （ 米国西部) 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。

3. テンプレートパラメータを入力します。

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ンと一致する必要はありません。
SubDomain (GovCloud のみ)		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。 を指定すると SubDomain、パラメータは DomainName 指定された に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。

パラメータ	デフォルト	説明
AdminPassword		Active Directory 管理者 (ユーザー名 Admin) のパスワード。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。 重要： このフィールドの形式は、(1) プレーンテキストパスワード、または (2) キーと値のペアとしてフォーマットされたARN AWS シークレットの形式のいずれかです`{"password":"somepassword"}` 。 注： このユーザーのパスワードは、アクティブディレクトリ のパスワードの複雑さの要件を満たしている必要があります。

パラメータ	デフォルト	説明
ServiceAccountPassword		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。 重要： このフィールドの形式は、(1) プレーンテキストパスワード、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ARNの形式のいずれかです`{"password":"somepassword"}` 。 注： このユーザーのパスワードは、アクティブディレクトリ のパスワードの複雑さの要件を満たしている必要があります。
キーペア		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。 注: AWS Systems Manager Session Manager はインスタンスへの接続にも使用できます。

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`	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、LDIF「 サポート」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入力されます。 ファイルを表示するには、で利用可能な res.ldif ファイルを参照してください GitHub。
ClientIpCidr		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。このデプロイ後を更新できます。
ClientPrefixList		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、「カスタマーマネージドプレフィックスリストの操作」を参照してください。

パラメータ	デフォルト	説明
EnvironmentName	`res-[environment name]`	`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する`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は、一意である必要があります。
PortalDomainName		GovCloud デプロイの場合は、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、前提条件中に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 は空白のまま`EnvironmentName` にできます。

4. Capabilities のすべてのチェックボックスを確認し、Create stack を選択します。

ステップ 1: 製品の起動

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

デプロイまでの時間： 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 Research and Engineering Studio を AWS にデプロイします 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 Management Console し、https://console.aws.amazon.com/cloudformation で AWS 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を使用します。

   > **Note**
   >
   > この製品は 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、AWS リージョン「al 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力タブにあります。

パラメータ	デフォルト	説明
EnvironmentName	*<res-demo>*	RES res-、11 文字以内、大文字を含まない環境で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。このユーザーは、Active Directory のシングルサインオン統合に障害が発生した場合、ブレークグラスユーザーとしても機能します。
InfrastructureHostAMI	ami-*[numbers or letters only]*	（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 ID AMI を指定できます。現在サポートされているベース OS は Amazon Linux 2 です。詳細については、「RES-ready を設定する AMIs」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。
ClientIP	*x.x.x*.0/24 または *x.x.x*.0/32	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 ClientIpCidr 後に を更新できます。

パラメータ	デフォルト	説明
ClientPrefixList		（オプション）がウェブ UIとSSH踏み台ホストに直接アクセスIPsすることを許可するマネージドプレフィックスリストを提供します。
IAMPermissionBoundary		（オプション）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ARNされる管理ポリシーを指定できますRES。詳細については、「カスタムアクセス許可の境界を設定する」を参照してください。
VpcId		インスタンスが起動VPCするの ID。
IsLoadBalancerInternetFacing		true を選択して、インターネット向けロードバランサーをデプロイします (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。

パラメータ	デフォルト	説明
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 を選択します。
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。

パラメータ	デフォルト	説明
ActiveDirectoryName	*corp.res.com*	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	*corp*	Active Directory の短縮名。これはネットBIOS名とも呼ばれます。
LDAP ベース	***DC=corp,DC=res,DC=com***	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ARNを含むシークレットを、username:password キーと値のペアとしてフォーマットして指定します。
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。

パラメータ	デフォルト	説明
SudoersGroupName	RESAdministrators	インストール時のインスタンスに sudoer アクセスを持つすべてのユーザーと、 に管理者アクセスを含むグループ名RES。
ComputersOU		インスタンスが参加する AD 内の組織単位。
D omainTLSCertificateシークレットARN		（オプション）AD へのTLS通信を有効にするARNドメインTLS証明書シークレットを指定します。
EnableLdapIDMapping		UID と のGID数値が によって生成されるかSSSD、AD によって提供される数値が使用されるかを決定します。SSSD 生成された UID と を使用するには True に設定しGID、AD によって使用UIDおよびGID提供されるには 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。
DisableADJoin	False	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。

パラメータ	デフォルト	説明
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。
CustomDomainNamefo rWebApp		（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使用されるサブドメイン。
CustomDomainNameforVDI		（オプション）システムVDIの一部へのリンクを提供するためにウェブポータルで使用されるサブドメイン。
ACMCertificateARNf orWebApp		（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。お客様は、お客様の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、これはユーザーのために生成され、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設定ガイド。

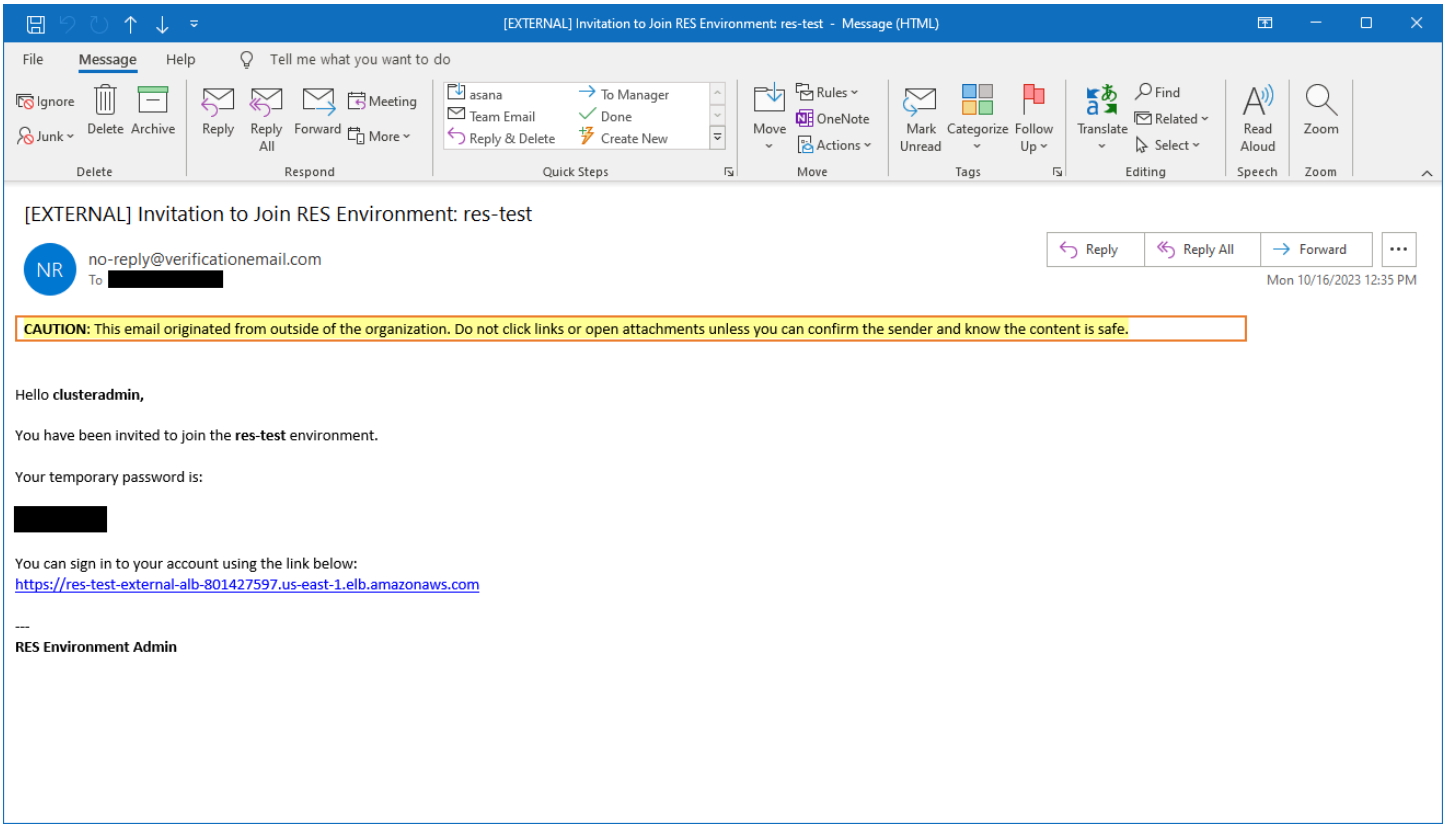
パラメータ	デフォルト	説明
CertificateSecretARNforVDI		（オプション）このARNシークレットは、ウェブポータルのパブリック証明書のパブリック証明書を保存します。自動外部リソースにポータルドメイン名を設定する場合、この値は res-bi スタックの Outputs タブにあります。
PrivateKeySecretARNforVDI		（オプション）このARNシークレットは、ウェブポータルの証明書のプライベートキーを保存します。自動外部リソースにポータルドメイン名を設定する場合、この値は res-bi スタックの Outputs タブにあります。

5. [Create stack] (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 コンソールのステータス列で確認できます。約 60 分後に CREATE_COMPLETE ステータスが表示されます。

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はブレー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、ユーザーまたはグループのメンバーシップをそれらのプロジェクトに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、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依存する 2 つの更新方法があります。

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。例えば、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

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。

の最新バージョンで環境を更新するにはRES :

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RESで再デプロイします。「the section called “ステップ 1: 製品の起動”」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. すべてのデータが新しい環境に正常に移行されたことを確認します。

マイナーバージョンの更新

へのマイナーバージョンの更新ではRES、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 AWS CloudFormation 。更新をデプロイ AWS 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表示されます。

例: `"Description": "RES_2024.1"`

マイナーバージョンを更新するには：

1. で最新の AWS CloudFormation テンプレートをダウンロードしますthe section called “ステップ 1: 製品の起動”。
2. AWS CloudFormation コンソールを https://console.aws.amazon.com/cloudformation で開きます。
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. [Update] (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を設定する 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

Research and Engineering Studio は、 または AWS Management Console を使用して、 AWS 製品で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shared-storage-security-group 、 <EnvironmentName>- を自動的に削除しません。

の使用 AWS Management Console

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 環境で使用可能かどうかを決定します。インストール手順については、AWS CLI 「 ユーザーガイド」の「 とは AWS Command Line Interface」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>
```

の削除 shared-storage-security-group

> **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 Management Console し、 で Amazon https://console.aws.amazon.com/efs/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 Management Console し、 で Amazon EC2コンソールを開きますhttps://console.aws.amazon.com/ec2/。
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ことを決定した場合、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 Management Console し、 で Amazon S3 コンソールを開きますhttps://console.aws.amazon.com/s3/。
2. ナビゲーションペインからバケットを選択します。
3. S3 バケットを見つけ`stack-name`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、コンテンツ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 製品で 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

ユーザーとグループの管理

Research and Engineering Studio は、任意の SAML 2.0 準拠の ID プロバイダーを使用できます。外部リソースRESを使用してデプロイした場合、または IAM Identity Center 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) のセットアップ。独自の SAML2.0 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用の ID プロバイダーの設定 (SSO) 。

トピック

IAM Identity Center でのシングルサインオン (SSO) のセットアップ

マネージド Active Directory に接続している ID 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 に接続している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**
>
> AWS GovCloud （ 米国西部) リージョンにデプロイする場合は、Research and Engineering Studio SSO を AWS GovCloud (US) デプロイしたパーティションアカウントに 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 Identity Center の有効化

1. AWS Identity and Access Management コンソール にサインインします。
2. Identity Center を開きます。
3. [Enable (有効化)] を選択します。
4. で有効化 AWS Organizationsを選択します。
5. [Continue] (続行 ） を選択します。

> **Note**
>
> マネージド Active Directory があるの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. Identity source で、Actions を選択し、Change identity source 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. [Next (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. [Change identity source] (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. [追加] を選択します。
5. [Next (次へ)] を選択します。
6. 変更を確認してから、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、 を設定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、SAML2.0 を選択します。
6. [Next (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、IAMIdentity 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です。

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` と指定します。
10. アプリケーション ACS URLで、RESポータルURLからリダイレクトを入力します。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. シングルサインオン には、SAMLリダイレクト URLがあります。
11. アプリケーションSAMLオーディエンス で、Amazon Cognito を入力しますURN。

    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 を入力したらURN、「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. Identity Center 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 **`${user:email}`** と入力します。
4. フォーマット で、 を選択しますemailAddress。
5. [新規属性マッピングの追加] を選択します。
6. アプリケーション の User 属性に「Email」と入力します。
7. Identity IAM Center のこの文字列値またはユーザー属性へのマップで、 を入力します**`${user:email}`**。
8. 書式 に「未指定」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 のアプリケーションへのユーザーの追加

1. Identity Center 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. Identity Provider 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 の隣) を選択します。
4. 以下の情報を使用してフォームに入力します。
    a. を選択しますSAML。
    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URLした 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. プロバイダー E メール属性 に「E メール」と入力します。
    f. [送信] を選択します。
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用の ID プロバイダーの設定 (SSO)

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 2.0 ID SAML 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) のセットアップ。

> **Note**
>
> ユーザーの E メールは、IDPSAML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

このセクションでは、RESAmazon 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 Identity Center 「 ユーザーガイド」の「ID ソースとして Active Directory を使用する」を参照してください。
2. ID プロバイダー (IdP) RESで SAML の 2.0 アプリケーションを設定します。 IdP 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 URLが 2.0 SAML 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 。

     > **Note**
     >
     > IdP によっては、SAMLリダイレクトの名前URL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

     を取得するには URL

     1. 管理者または clusteradmin RESとして にサインインします。
     2. 環境管理 ⇒ 全般の設定 ⇒ Identity Provider 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の ID。

  > **Note**
  >
  > IdP によっては、SAMLオーディエンスの名前URIが異なる場合があります。
  >
  > - ClientID
  > - アプリケーションSAMLオーディエンス
  > - 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 オーディエンスを検索するには URI

  1. 管理者または clusteradmin RESとして にサインインします。
  2. 環境管理 ⇒ 全般の設定 ⇒ Identity Provider に移動します。
  3. ユーザープール ID を選択します。

3. に投稿された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RES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*。置換 *user-pool-id* Amazon Cognito ユーザープールの ID。

     ```
     <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。置換 *user-pool-domain* Amazon Cognito ユーザープールのドメイン名。

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

```
<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。

ドメインを取得するには URL

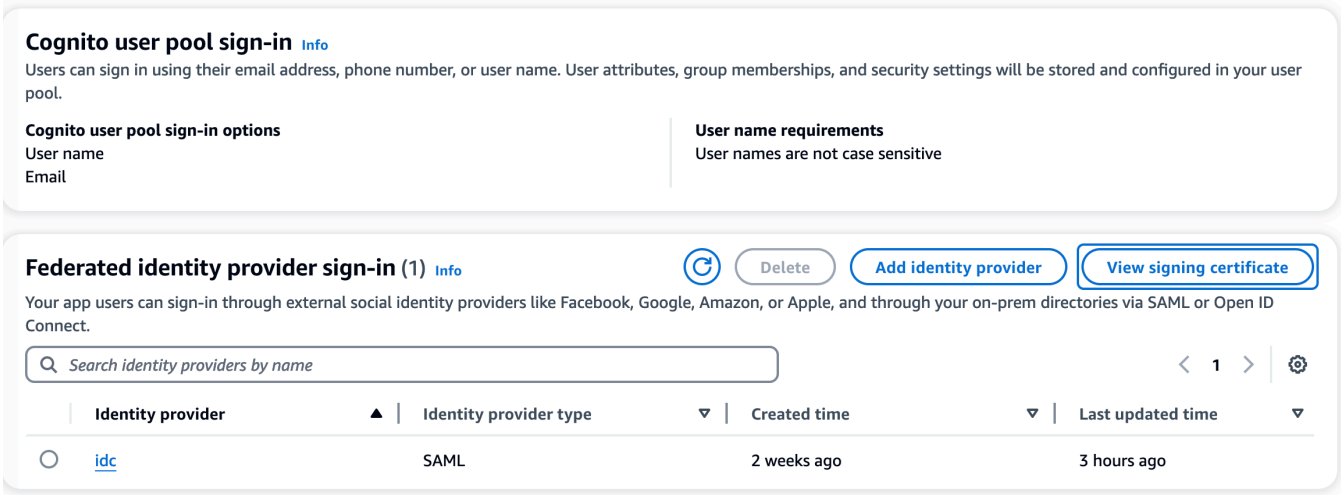
1. 管理者または clusteradmin RESとして にサインインします。

2. 環境管理 ⇒ 全般の設定 ⇒ Identity Provider 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. の開始方法 で Amazon Cognito コンソールを開きます。 AWS Management Console
2. ユーザープールを選択します。ユーザープールは である必要がありますres-*<environment name>*-user-pool。
3. サインインエクスペリエンスタブを選択します。
4. フェデレーティッド 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。



この証明書を使用して、Active Directory をセットアップしIDP、 を追加しrelying party trust、この依存当事者SAMLに対するサポートを有効にすることができます。

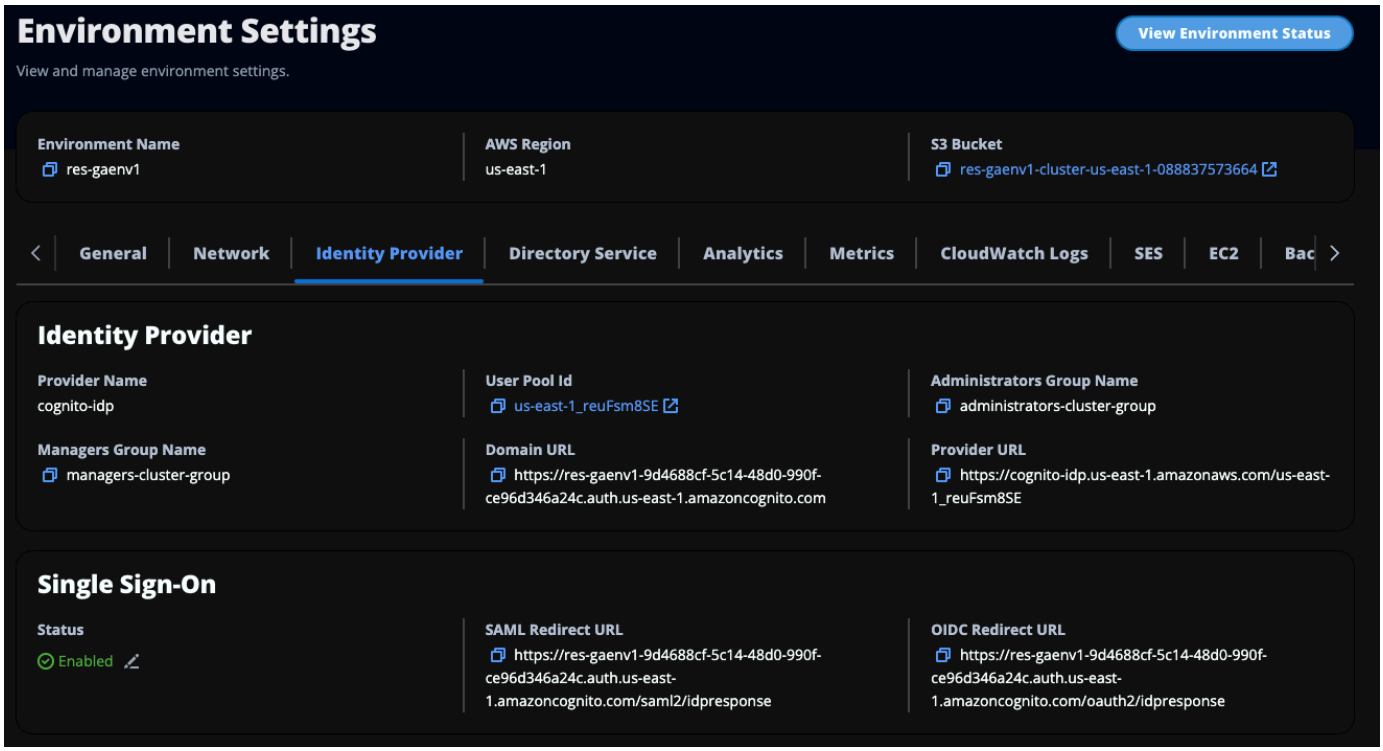
> **Note**
>
> これは Keycloak と には適用されませんIDC。

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

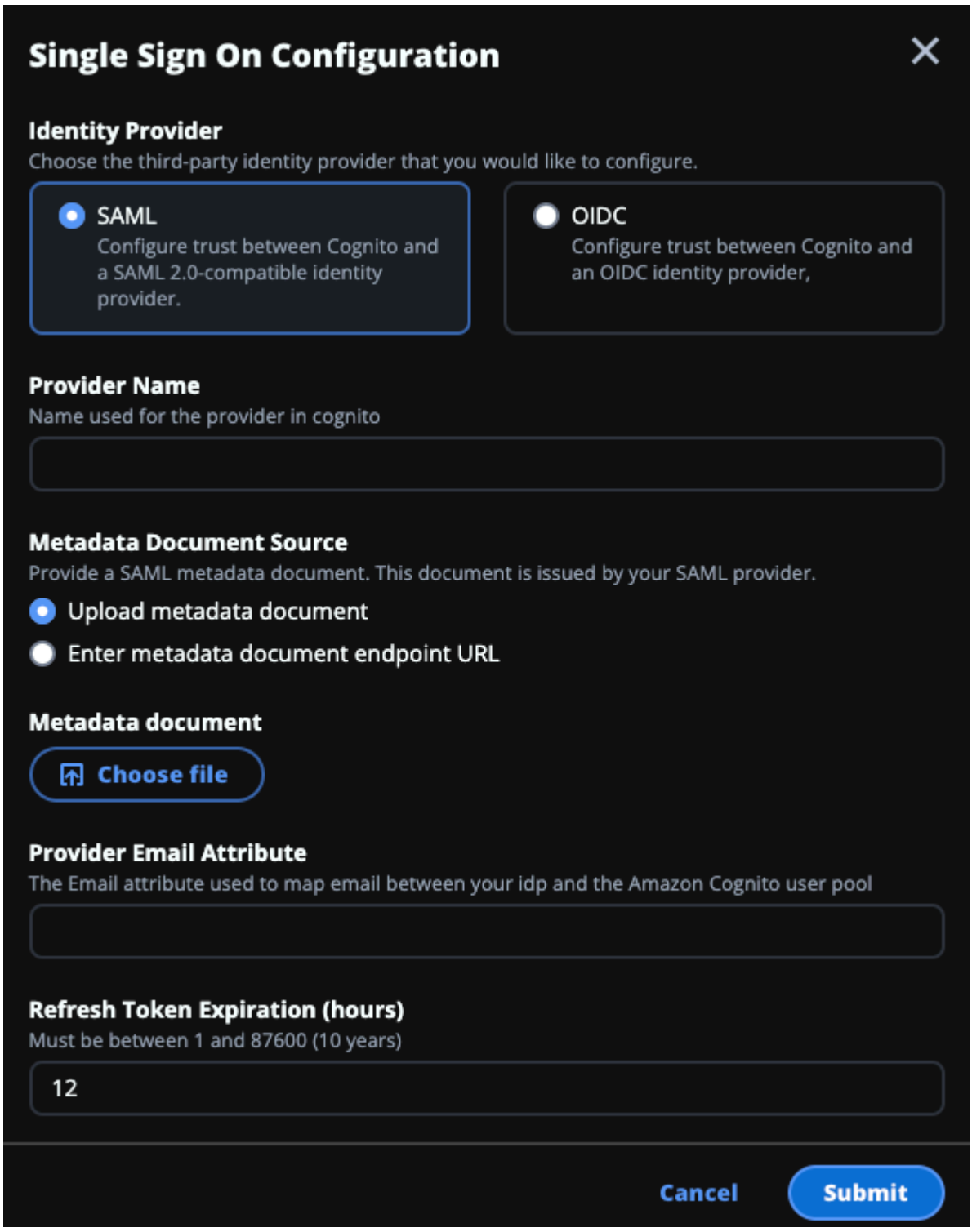
ID プロバイダーを使用するRESように を設定する

のシングルサインオン設定を完了するには RES

1. 管理者または clusteradmin RESとして にサインインします。
2. 環境管理 ⇒ 全般の設定 ⇒ Identity Provider に移動します。



3. シングルサインオン 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、シングルサインオン設定ページを開きます。



a. Identity Provider の場合は、 を選択しますSAML。

b. 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URLから 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. [送信] を選択します。

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。

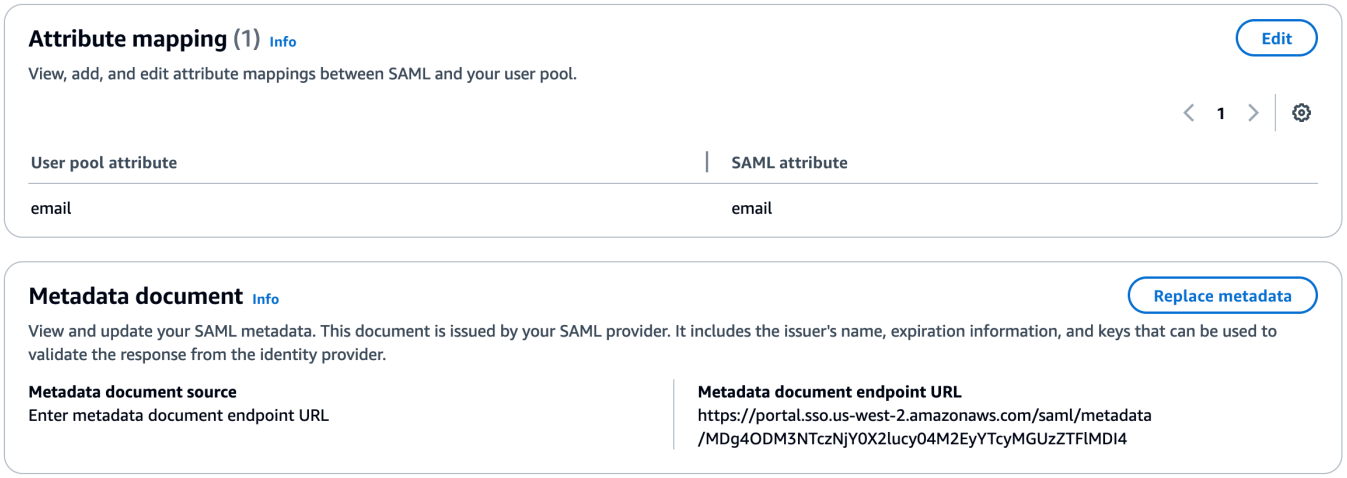
非本番環境での ID プロバイダーの設定

提供された外部リソースを使用して非本番環境を作成しRES、アイデンティティプロバイダーとして IAM Identity Center を設定した場合は、Okta などの別の ID プロバイダーを設定することもできます。RES SSO 有効化フォームでは、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、以下を実行します。

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して、ユーザープールの概要 を表示します。
4. サインインエクスペリエンスタブから、フェデレーティッドアイデンティティプロバイダーのサインインに移動し、設定されたアイデンティティ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せずにおく必要があります。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、「メタデータを置き換える」を選択します。



6. 属性マッピングを編集した場合は、DynamoDB の`<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。

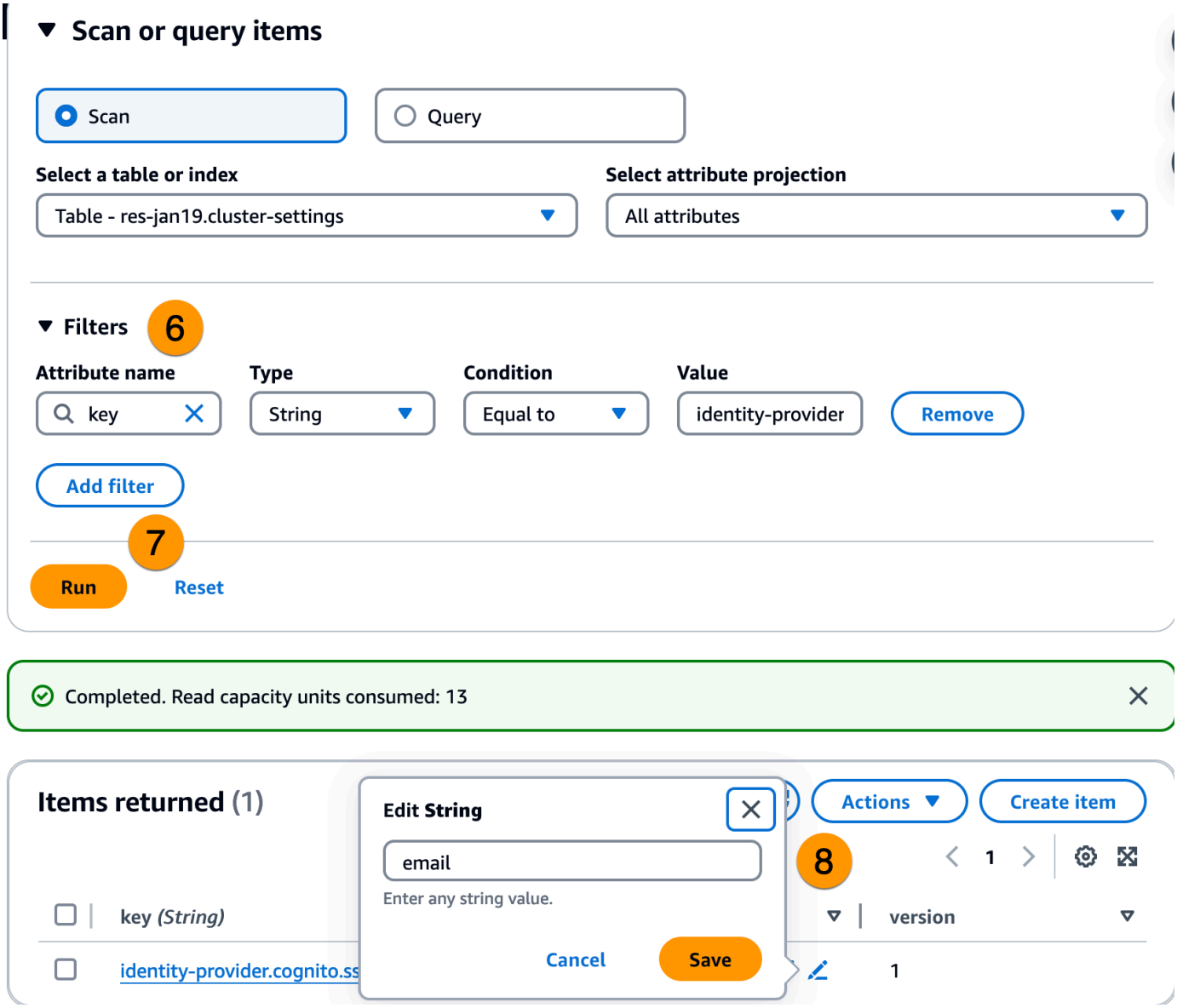
   b. `<environment name>.cluster-settings` テーブルを検索して選択し、アクションメニューから項目を探索 を選択します。

   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 で文字列を検索`identity-provider.cognito.sso_idp_provider_email_attribute`し、編集 を選択して、Amazon Cognito の変更に合わせて文字列を変更します。



IdP SAML 問題のデバッグ

SAML-tracer — この拡張機能を Chrome ブラウザで使用して、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-tracer を参照してください。

SAML 開発者ツール — 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 OneLogin を提供します。詳細については、 OneLogin ウェブサイトの「Base 64 デコード + 膨張」を参照してください。

Amazon CloudWatch Logs — RESログで CloudWatch 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SAMLの統合の詳細については、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. AWS 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、ウェブとポータルVDIの一部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**
>
> AWS GovCloud （ 米国西部) 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. 「ウェブ」をレコード名 として入力します。
4. レコードタイプCNAMEとして を選択します。
5. 値 には、最初の E メールに受信し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VDC、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] を選択します。

c. リソースを選択し、 を開きます<environmentname>-vdc-external-nlb。

d. からDNS名前をコピーしますNLB。

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、 を選択しますCNAME。
12. にNLB、 を入力しますDNS。
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、 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RES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 () 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ACM、クライアントとウェブサービスホスト間の SSL/TLS チャ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するときに、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。(AWS GovCloud 米国西部) 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 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。各証明書には、ステータスとして保留中の検証があります。

> **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 に変更する必要があります。
   - GovCloud デプロイ：

     (AWS GovCloud 米国西部) 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 に変更する必要があります。
8. 新しい証明書をコピーARN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 CloudWatch 中に次のロググループを に作成します。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 ロググループ	Retention
/aws/lambda/ *<installation-stack-name>*-cluster-endpoints	有効期限なし
/aws/lambda/ *<installation-stack-name>*-cluster-manager-scheduled-ad-sync	有効期限なし
/aws/lambda/ *<installation-stack-name>*-cluster-settings	有効期限なし

CloudWatch ロググループ	Retention
/aws/lambda/ *<installation-stack-name>*-oauth-credentials	有効期限なし
/aws/lambda/ *<installation-stack-name>*-self-signed-certificate	有効期限なし
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	有効期限なし
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	有効期限なし
/aws/lambda/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope	有効期限なし
/*<installation-stack-name>* /cluster-manager	3 か月間
/*<installation-stack-name>* /vdc/controller	3 か月間
/*<installation-stack-name>* /vdc/dcv-broker	3 か月間
/*<installation-stack-name>* /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 ログで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を設定する

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RESすることで、 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、 IAMPermissionBoundaryパラ

メータの一部としてアクセス許可の境界を指定することでARN、RES AWS CloudFormation 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、どのRESロールにもアクセス許可の境界は設定されません。以下は、RESロールが操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が、次のアクションを明示的に許可し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:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
```

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

RES-ready を設定する AMIs

準備RESが整った 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 にプレインストールできますAMIs。RES-ready を使用すると、焼き付け済みイメージを使用するVDIインスタンスの起動時間がAMIs短縮されます。EC2 Image Builder を使用すると、 を新しいソフトウェアスタックAMIsとして構築して登録できます。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、 の最新バージョンをデプロイRESする必要があります。

トピック

- RES 環境にアクセスする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の設定
- Image Builder イメージパイプラインの設定
- Image Builder イメージパイプラインの実行
- で新しいソフトウェアスタックを登録する RES

RES 環境にアクセスする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- というIAMロールを作成または変更する必要がありますEC2InstanceProfileForImageBuilder。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。

- 信頼された関係には、Amazon EC2サービスが含まれます。
- A mazonSSMManagedInstanceCore および EC2InstanceProfileForImageBuilderポリシー。
- デプロイされたRES環境への DynamoDB および Amazon S3 アクセスが制限されたカスタムRESポリシー。

  (このポリシーは、カスタマー管理ポリシードキュメントまたはカスタマーインラインポリシードキュメントのいずれかにすることができます。)

信頼されたリレーションシップエンティティ：

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

RES ポリシー：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*",
                        "vdc.host_modules.*"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-Account-
ID}/idea/vdc/res-ready-install-script-packages/*",
```

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

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手順に従ってください。

コンポーネントの詳細を入力します。

1. タイプ の場合は、ビルド を選択します。
2. Image オペレーティングシステム (OS) の場合は、Linux または Windows のいずれかを選択します。
3. コンポーネント名 には、 などの意味のある名前を入力します**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。
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。

   Linux

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

```
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
```

```
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

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

```
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
```

```
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
      - name: Reboot
        action: Reboot
        onFailure: Abort
        maxAttempts: 3
        inputs:
           delaySeconds: 0
```

6. 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 レシピは、新しいイメージを作成するための出発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機能することを検証するために追加するコンポーネントのセットを定義します。レシピを作成または変更して、必要なRESソフトウェア依存関係AMIを持つターゲット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)
- Ubuntu 22.04.3 (x86)
- RHEL 8 (x86)、9 (x86)
- Windows 2019、2022 (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. でサポートされているベースイメージを選択しますRES。

6. インスタンス設定 で、エージェントがプリインストールされていない場合は、SSMエージェントを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 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、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。RES インストールスクリプトは AWS CLI を使用して、DynamoDB クラスター設定の設定値VDIへのアクセスを提供します。Windows では、このコンポーネントは必要ありません。
8. Linux または Windows 環境に作成された EC2 Image Builder コンポーネントを追加し、必要なパラメータ値を入力します。入力には、AWSAccountID、、RESEnvNameRESEnvRegion、 が必要ですRESEnvReleaseVersion。

> **Important**
>
> Linux 環境では、aws-cli-version-2-linuxビルドコンポーネントを最初に追加した状態で、これらのコンポーネントを追加する必要があります。

9. (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、 を起動AMI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。
10. 必要に応じて任意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、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。

1. Linux ベースのレシピの場合、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。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VDIへのアクセスを提供します。Windows では、このコンポーネントは必要ありません。

2. Linux または Windows 環境に作成された EC2 Image Builder コンポーネントを追加し、必要なパラメータ値を入力します。入力には、AWSAccountID、、RESEnvNameRESEnvRegion、 が必要ですRESEnvReleaseVersion。

> **Important**
>
> Linux 環境では、`aws-cli-version-2-linux`ビルドコンポーネントを最初に追加した状態で、これらのコンポーネントを追加する必要があります。

3. 必要に応じて任意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、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の設定

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。で使用するにはRES、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：

1. 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IAMロールを準備する。
2. 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。
3. VPC、サブネット、セキュリティグループ では、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の設定

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-ready 用にイメージパイプラインを設定するにはAMIs、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します。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. 画像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. レシピの選択 で、既存のレシピを使用 を選択し、 で作成され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の定義 では、ユースケースに応じてデフォルト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、で作成され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の設定。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の定義 で、サービスデフォルト 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。出力イメージは、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の実行

設定された出力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. Image pipelines 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の設定。
2. アクション から、パイプラインの実行 を選択します。

で新しいソフトウェアスタックを登録する RES

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、 に組み込まれている出力イメージの AMI ID を入力しますImage Builder イメージパイプラインの実行。

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ついて、技術的な対象者向けの追加の手順を説明します。

トピック

シークレットの管理

Research and Engineering Studio では、 を使用して次のシークレットが保持されます AWS Secrets Manager。RES は、環境の作成中にシークレットを自動的に作成します。環境の作成中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	RES 生成済み	入力された管理者
`<envname> -sso-client-secret`	環境のシングルサインオンOAuth2クライアントシークレット	✓	
`<envname> -vdc-client-secret`	vdc ClientSecret	✓	
`<envname> -vdc-client-id`	vdc ClientId	✓	
`<envname> -vdc-gateway-certificate-private-key`	ドメインの自己署名証明書プライベートキー	✓	
`<envname> -vdc-gateway-`	ドメインの自己署名証明書	✓	

シークレット名	説明	RES 生成済み	入力された管理者
certificate-certificate			
<envname> -cluster-manager-client-secret	クラスターマネージャー ClientSecret	✓	
<envname> -cluster-manager-client-id	クラスターマネージャー ClientId	✓	
<envname> -external-private-key	ドメインの自己署名証明書プライベートキー	✓	
<envname> -external-certificate	ドメインの自己署名証明書	✓	
<envname> -internal-private-key	ドメインの自己署名証明書プライベートキー	✓	
<envname> -internal-certificate	ドメインの自己署名証明書	✓	
<envname> -directoryservice-ServiceAccountUserDN	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。

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

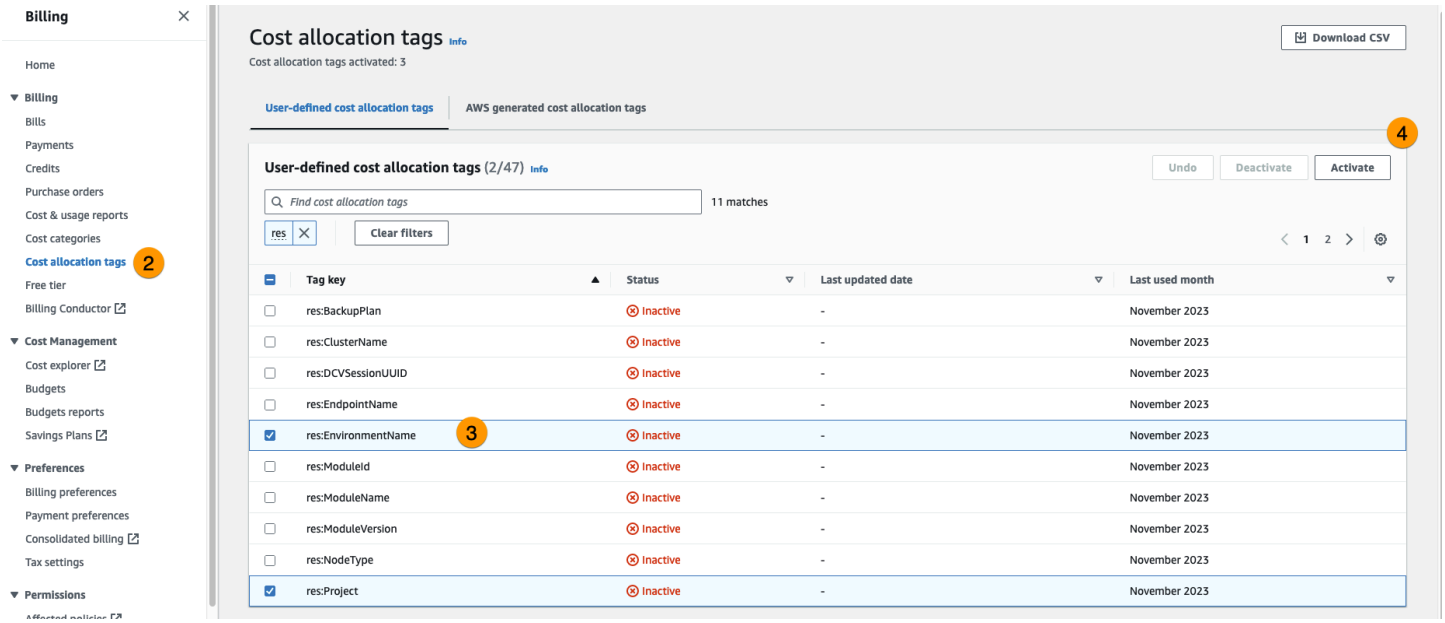
コストのモニタリングと制御

> **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。料金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の環境タグをアクティブ化する必要があります。

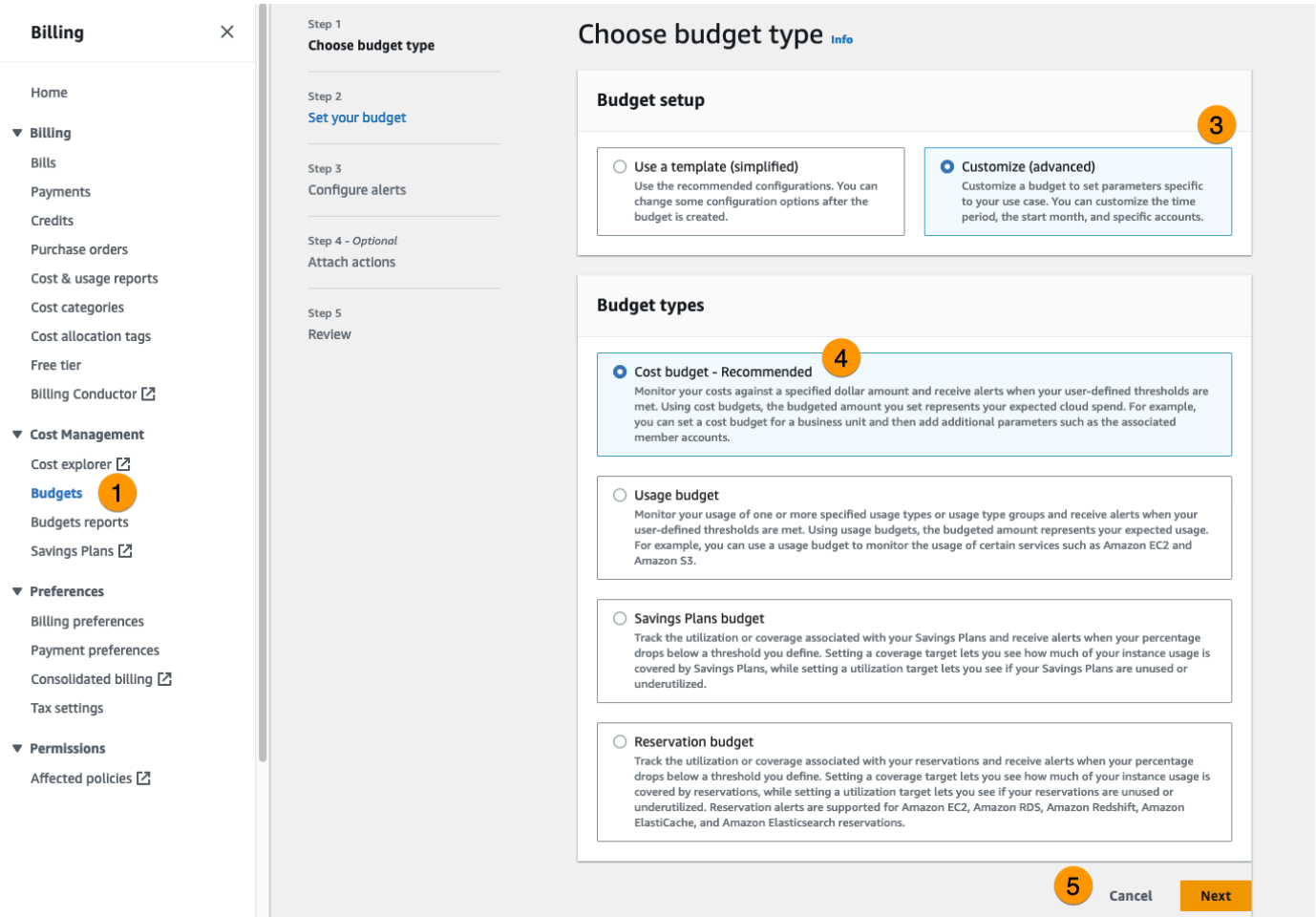
1. にサインイン AWS Management Console し、 で AWS Billing コンソールを開きますhttps://console.aws.amazon.com/billing/。
2. コスト配分タグ を選択します。
3. `res:Project` および `res:EnvironmentName` タグを検索して選択します。
4. [アクティブ化] を選択します。



> **Note**
>
> デプロイ後にRESタグが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. 予算タイプ で、コスト予算 - 推奨 を選択します。
5. [Next (次へ)] を選択します。

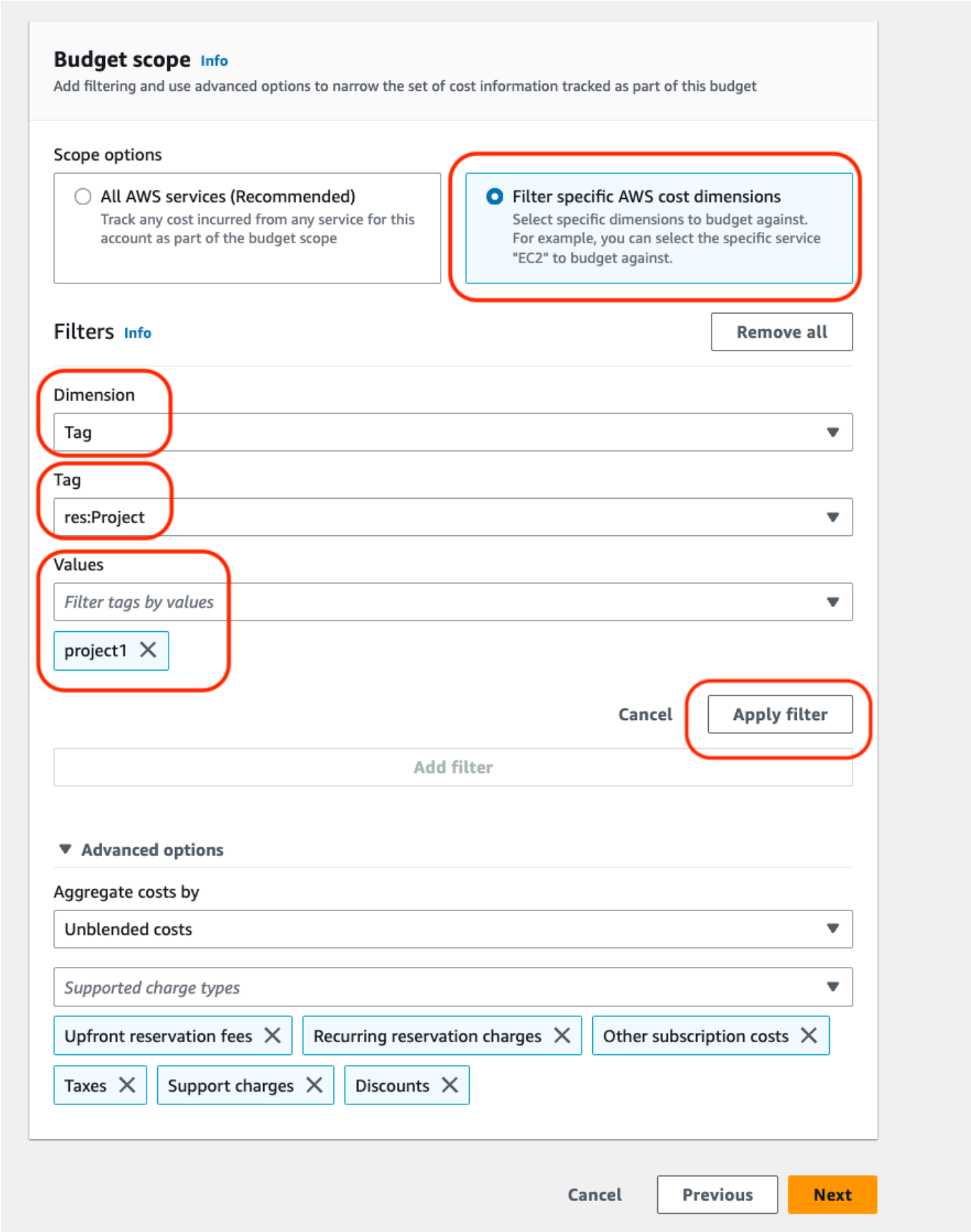


6. 詳細 に、アカウントの他の予算と区別するために、予算の意味のある予算名を入力します。例えば、*<EnvironmentName>-<ProjectName>-<BudgetName>* と指定します。
7. 「予算額を設定する」で、プロジェクトに予算された金額を入力します。

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. ディメンション で、タグ を選択します。
11. タグ で、res:Project を選択します。

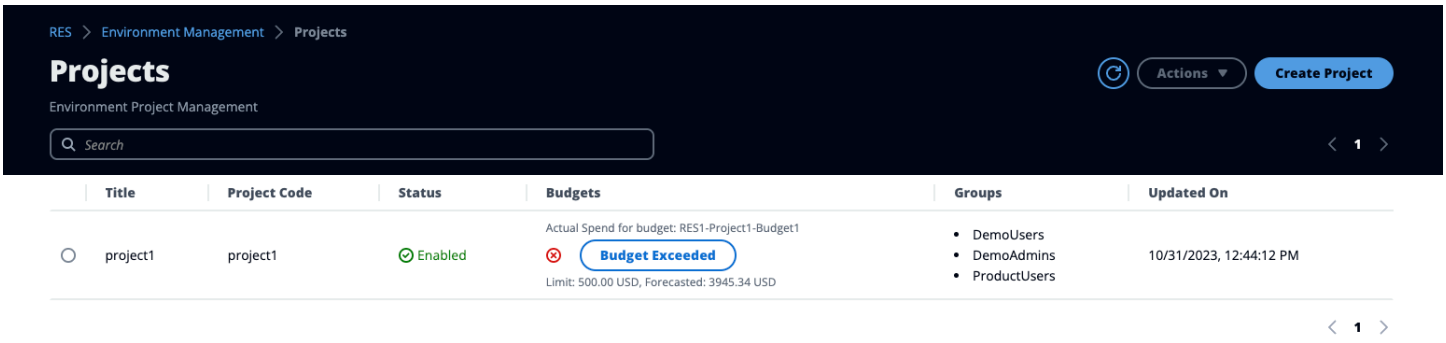
> **Note**
>
> タグと値が使用可能になるまでに最大 2 日かかる場合があります。プロジェクト名が使用可能になったら、予算を作成できます。

12. 値 で、プロジェクト名を選択します。
13. Apply filter 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. [Next (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
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. (オプション) アラートしきい値を追加します。
16. [Next (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. [Next (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”。予算を超えた場合、仮想デスクトップの起動はブロックされます。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。



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。変更が 内で有効になるまでに最大 15 分かかる場合がありますRES。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。

セッション管理

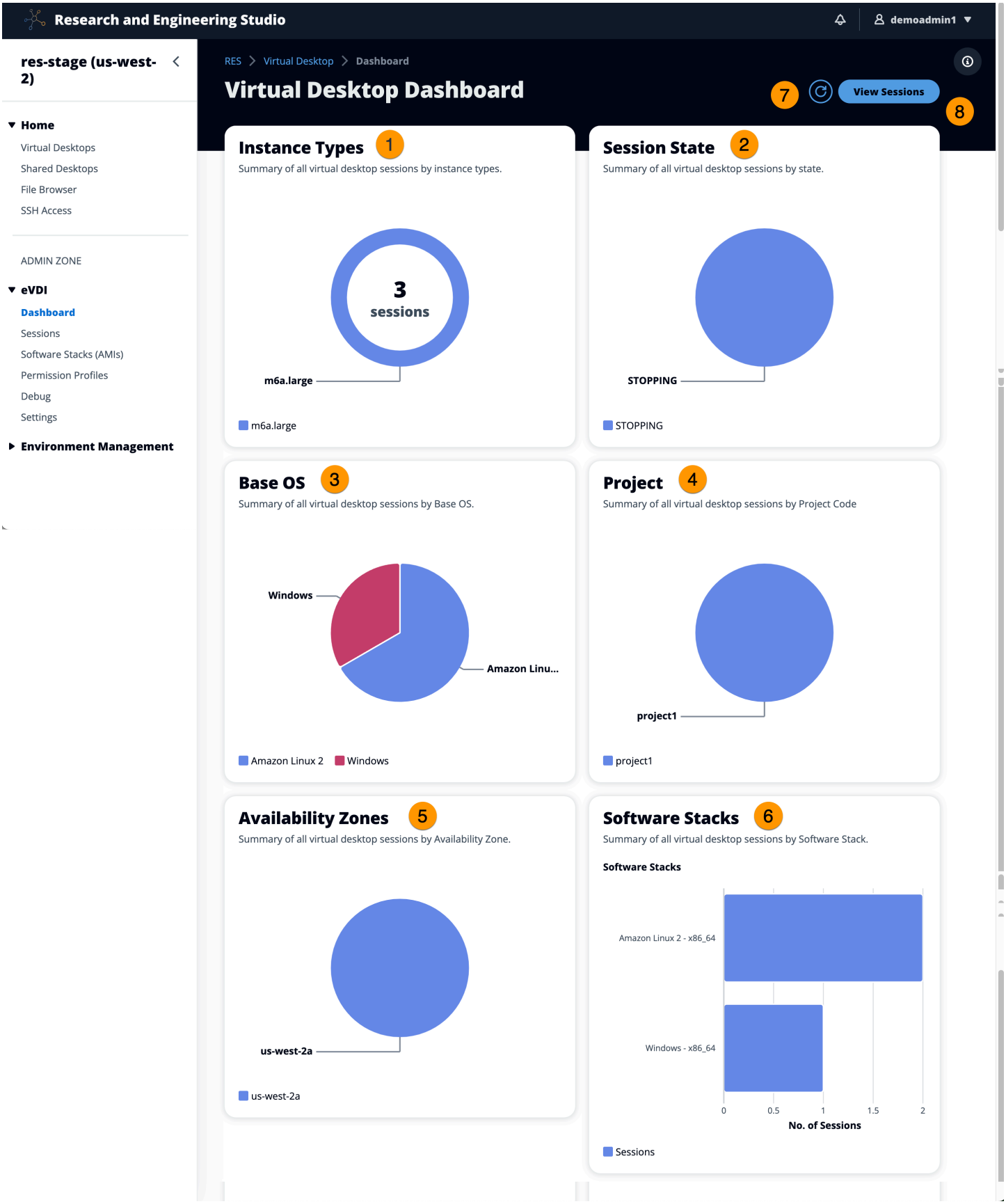
セッション管理は、セッションを開発およびテストするための柔軟でインタラクティブな環境を提供します。管理ユーザーとして、プロジェクト環境内でインタラクティブセッションを作成および管理することをユーザーに許可できます。

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
demoadmin1
res-stage (us-west-2)
Home
Virtual Desktops
Shared Desktops
File Browser
SSH Access
ADMIN ZONE
eVDI
Dashboard
Sessions
Software Stacks (AMIs)
Permission Profiles
Debug
Settings
Environment Management
RES > Virtual Desktop > Dashboard
Virtual Desktop Dashboard
7
View Sessions
8
Instance Types
1
Summary of all virtual desktop sessions by instance types.
3
sessions
m6a.large
m6a.large
Session State
2
Summary of all virtual desktop sessions by state.
STOPPING
STOPPING
Base OS
3
Summary of all virtual desktop sessions by Base OS.
Windows
Amazon Linu...
Amazon Linux 2
Windows
Project
4
Summary of all virtual desktop sessions by Project Code
project1
project1
Availability Zones
5
Summary of all virtual desktop sessions by Availability Zone.
us-west-2a
us-west-2a
Software Stacks
6
Summary of all virtual desktop sessions by Software Stack.
Software Stacks
Amazon Linux 2 - x86_64
Windows - x86_64
0
0.5
1
1.5
2
No. of Sessions
Sessions

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。

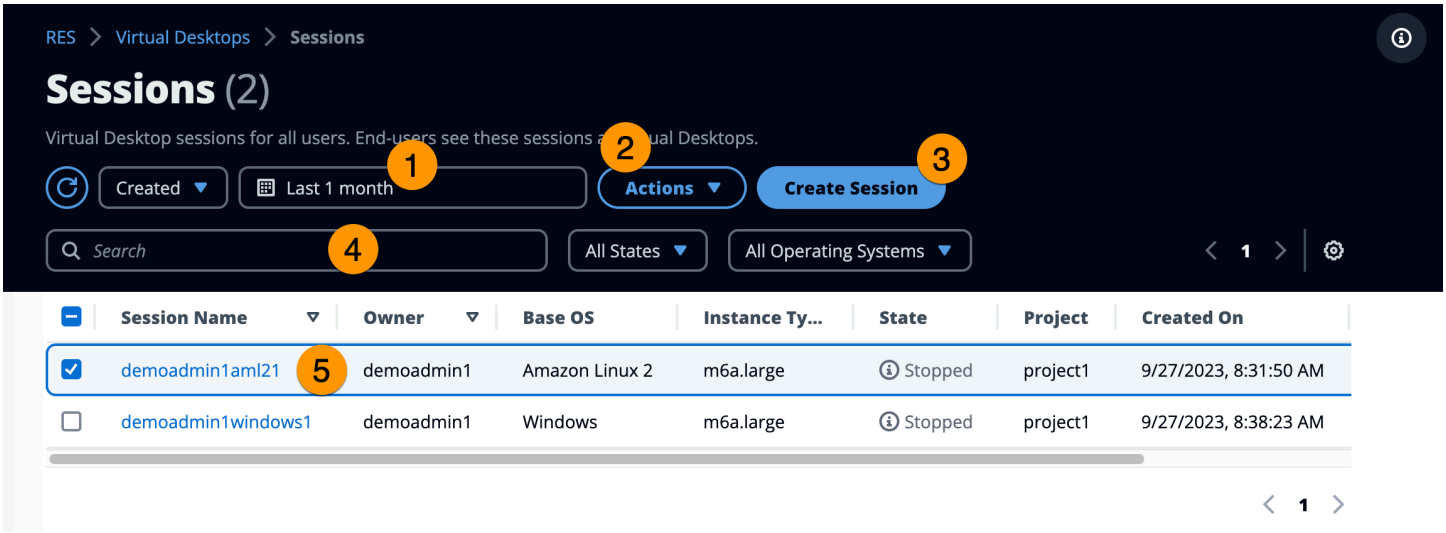
1. インスタンスのタイプ
2. セッションの状態
3. ベース OS
4. プロジェクト
5. アベイラビリティーゾーン
6. ソフトウェアスタック

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。



1. メニューを使用して、指定された時間枠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. 強制終了セッション (複数可)

f. セッションのヘルス (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) 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するには、詳細オプションの表示をオンにします。
4. [送信] を選択します。

Launch New Virtual Desktop

Session Name
Enter a name for the virtual desktop

Session Name is required. Use any characters and form a name of length between 3 and 24 characters, inclusive.

User
Select the user to create the session for

Project
Select the project under which the session will get created

Operating System
Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack
Select the software stack for your virtual desktop

Enable Instance Hibernation
Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

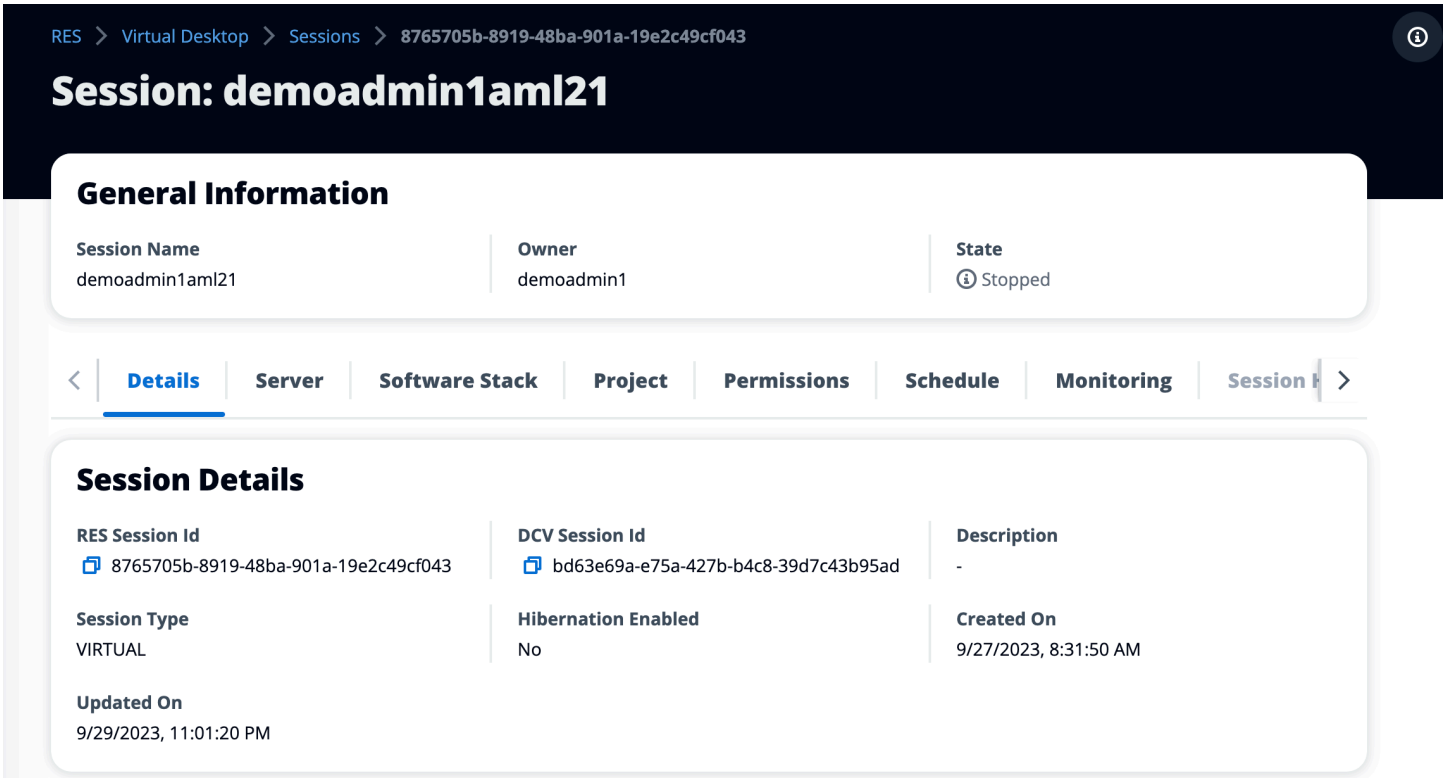
Virtual Desktop Size
Select a virtual desktop instance type

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

10

セッションの詳細

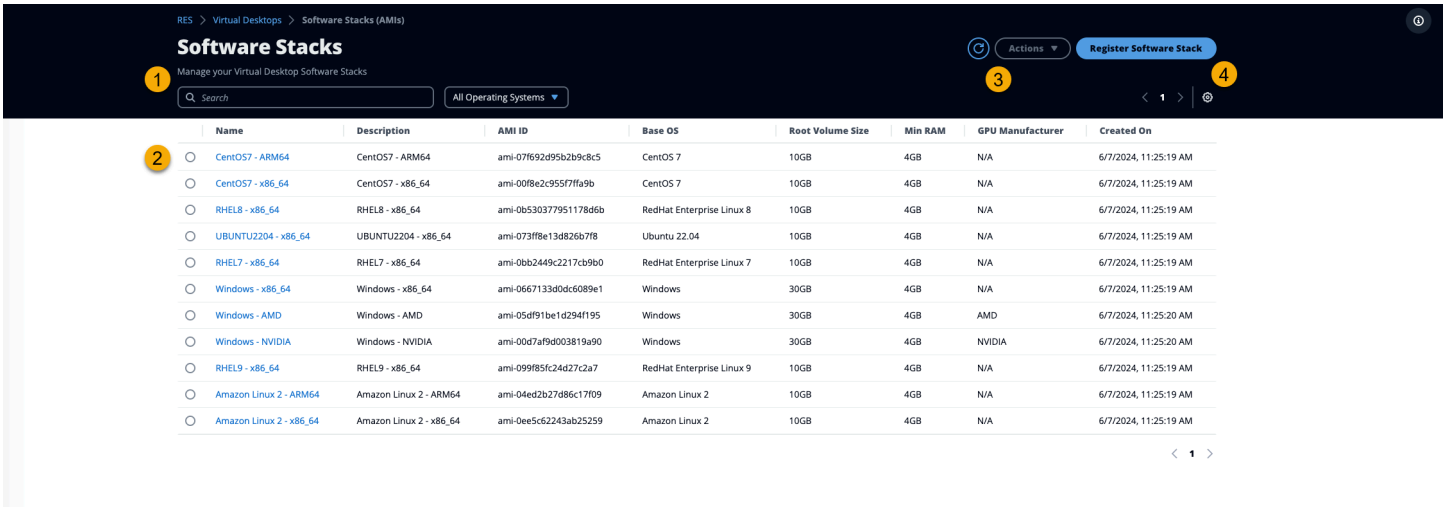
セッションリストから、セッション名を選択してセッションの詳細を表示します。



ソフトウェアスタック (AMIs)

> **Note**
>
> で提供される CentSO7 ソフトウェアスタックを実行するには AWS GovCloud (US)、リンクされた標準アカウント AWS Marketplace を使用して AMI内で をサブスクライブする必要があります。

Software Stacks 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。



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を選択したら、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使用すると、新しいスタックを作成できます。
    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. [送信] を選択します。

Register new Software Stack

Name
Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description
Enter a user friendly description for the software stack

AMI Id
Enter the AMI Id

AMI Id must start with ami-xxx

Operating System
Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer
Select the GPU Manufacturer for the software stack

N/A

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

10

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

10

Projects
Select applicable projects for the software stack

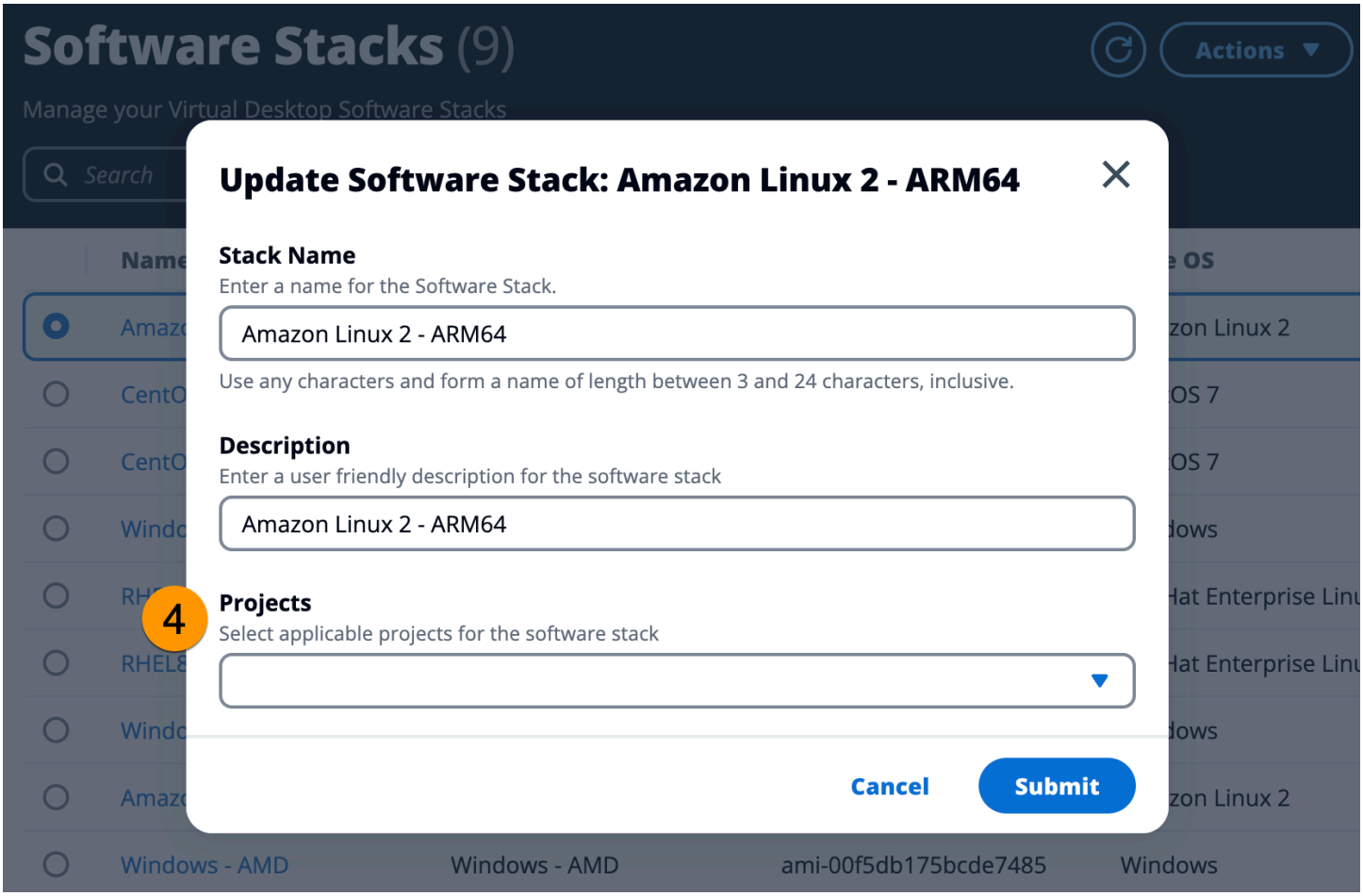
プロジェクトにソフトウェアスタックを割り当てる

新しいソフトウェアスタックを作成するときは、スタックをプロジェクトに割り当てることができます。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、以下を実行します。

> **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. Software Stacks ページから、プロジェクトに追加するソフトウェアスタックを選択します。
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。
5. [送信] を選択します。

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。

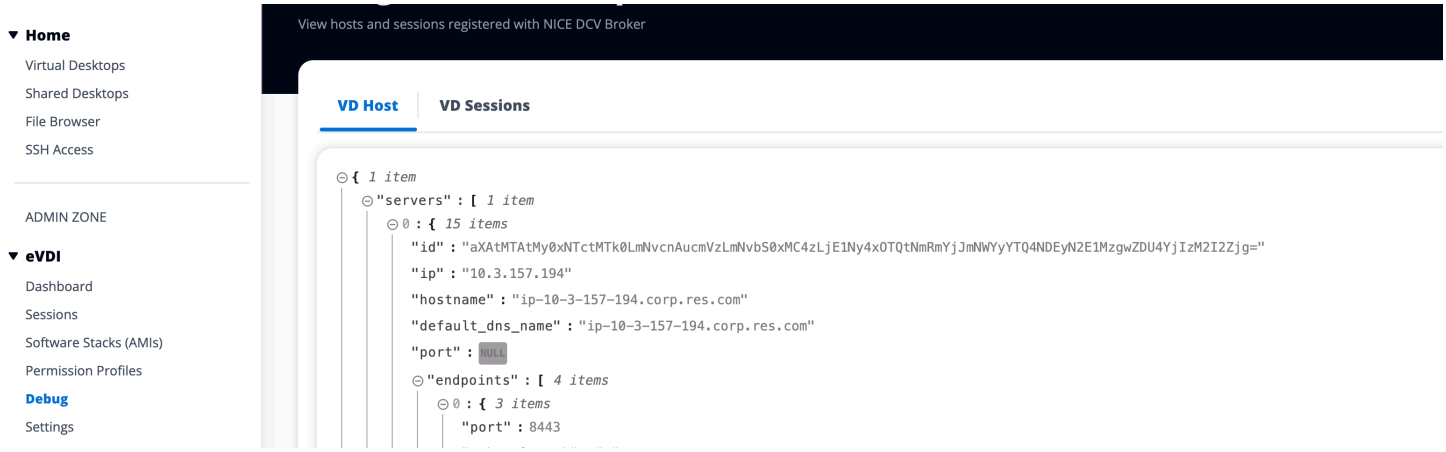


ソフトウェアスタックの詳細を表示する

Software Stacks リストから Software Stack Name を選択して詳細を表示します。詳細ページから、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。

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 Host 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 Sessions 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。



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。Server 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セッションのみが閉じられます。

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。

ユーザーあたりの許可されたセッション

個々のユーザーが一度に持つことができるVDIセッションの数。ユーザーがこの値を満たすか超えると、My Virtual Desktops ページから新しいセッションを起動できなくなります。Sessions ページからセッションを起動する機能は、この値による影響を受けません。

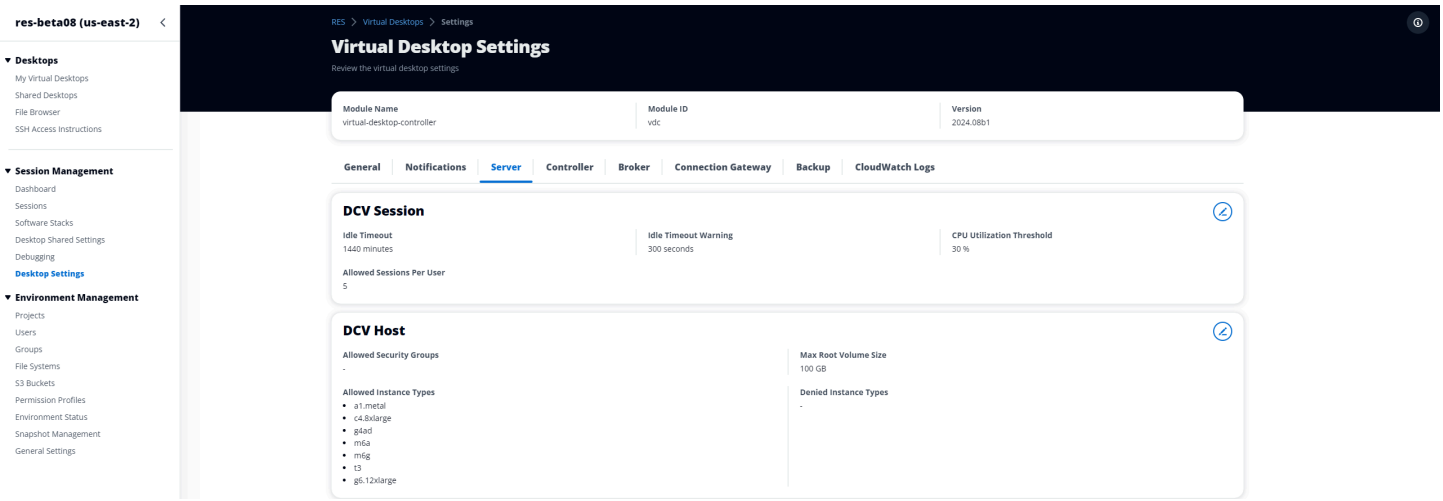
最大ルートボリュームサイズ

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。

許可される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。例えば、「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' を指定すると、m7a.24xlarge のみがVDIセッションとして起動できます。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。



環境管理

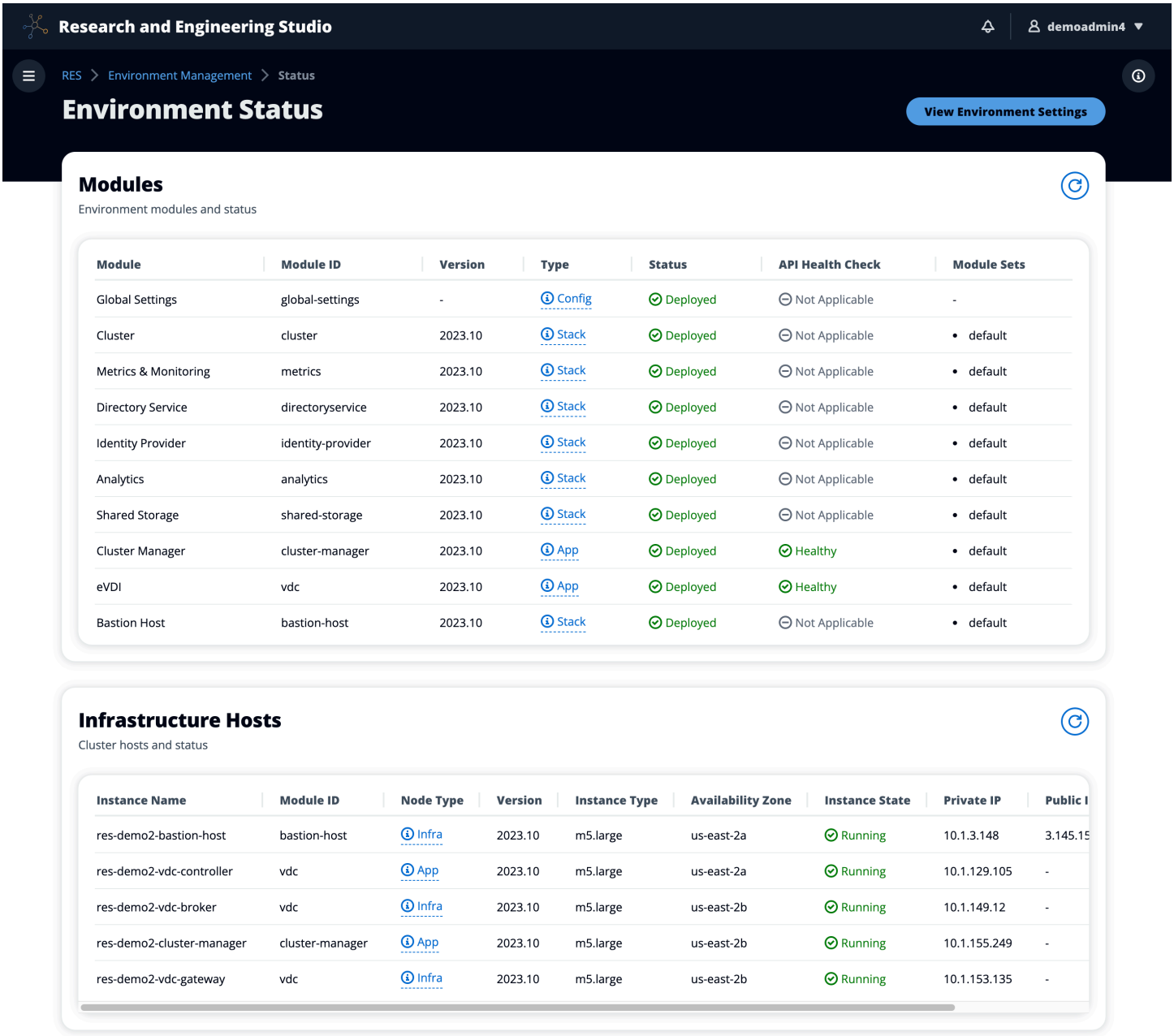
の環境管理セクションからRES、管理ユーザーは、研究およびエンジニアリングプロジェクト用に分離された環境を作成および管理できます。これらの環境には、コンピューティングリソース、ストレージ、その他の必要なコンポーネントがすべて安全な環境内に含まれる場合があります。ユーザーは、プロジェクトの特定の要件を満たすようにこれらの環境を設定およびカスタマイズできるため、他のプロジェクトや環境に影響を与えることなく、ソリューションの実験、テスト、反復を簡単に行うことができます。

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が含まれます。



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。

- 全般

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。ウェブポータルの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。

- ネットワーク

  アクセスIDs用の VPC ID、プレフィックスリストを表示します。

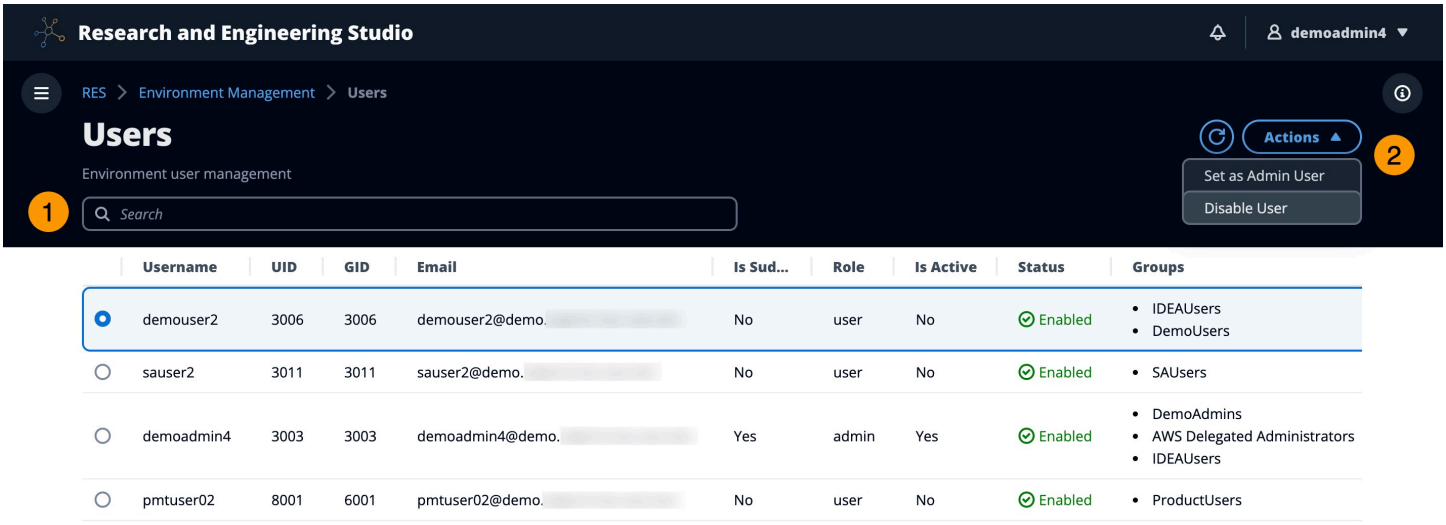
- Directory Service

  ユーザー名とパスワードARN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は、 ユーザーページに表示されます。ユーザーは、製品の設定中にクラスター管理者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。

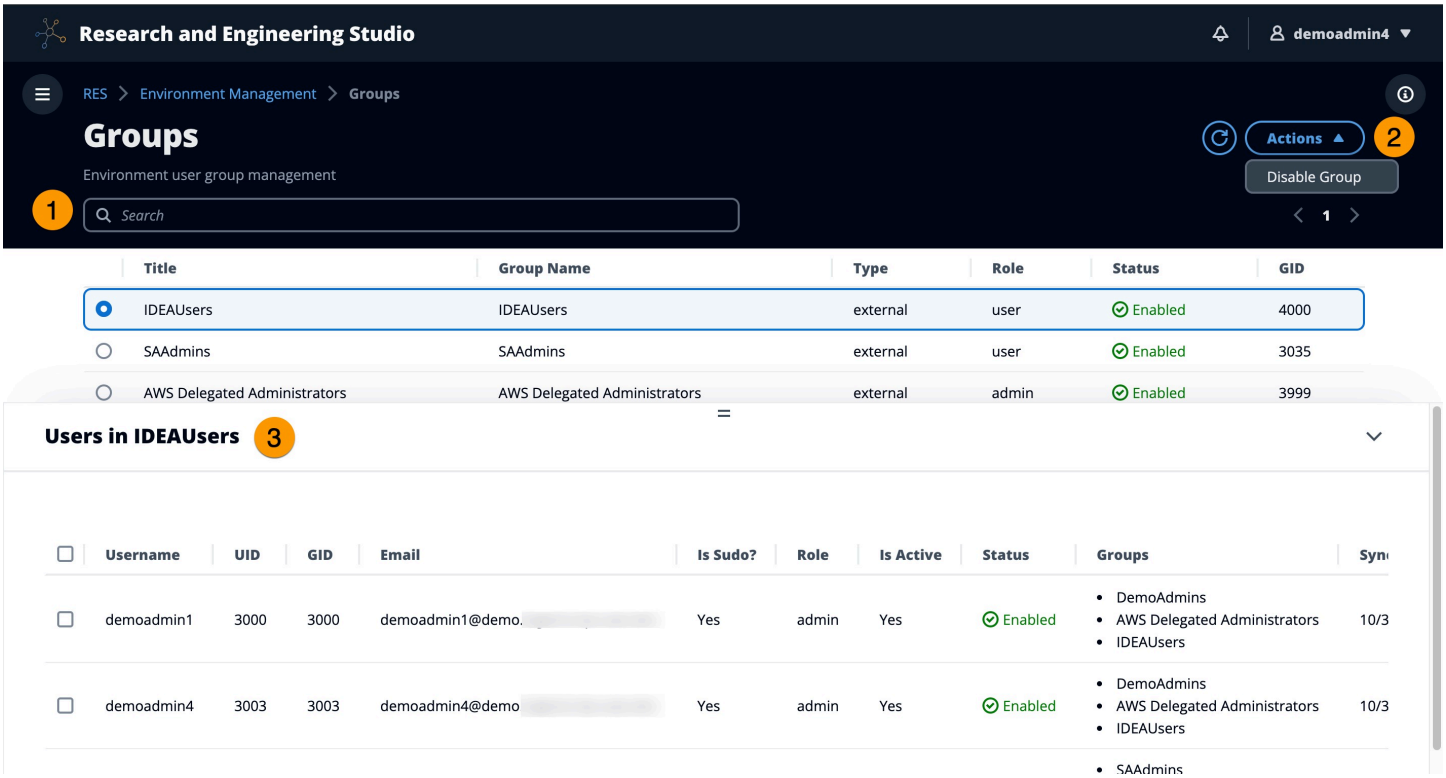


ユーザーページから、次のことができます。

1. ユーザーを検索します。
2. ユーザー名を選択した場合は、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。



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. ユーザーグループが選択されている場合は、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、画面下部のユーザーペインを展開して、グループのユーザーを表示できます。

プロジェクト

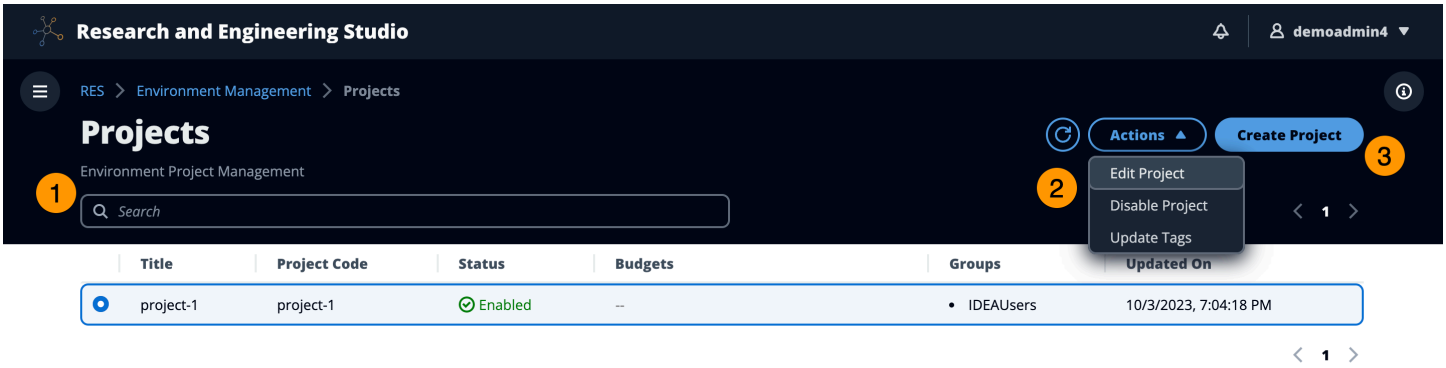
プロジェクトは、仮想デスクトップ、チーム、予算の境界を形成します。プロジェクトを作成するときは、名前、説明、環境設定などの設定を定義します。プロジェクトには、通常、コンピューティングリソースのタイプとサイズ、ソフトウェアスタック、ネットワーク設定など、プロジェクトの特定の要件を満たすようにカスタマイズできる 1 つ以上の環境が含まれます。

トピック

- プロジェクトを表示する
- プロジェクトを作成する
- プロジェクトを編集する

- 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。Projects 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
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。

プロジェクトを作成する

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。

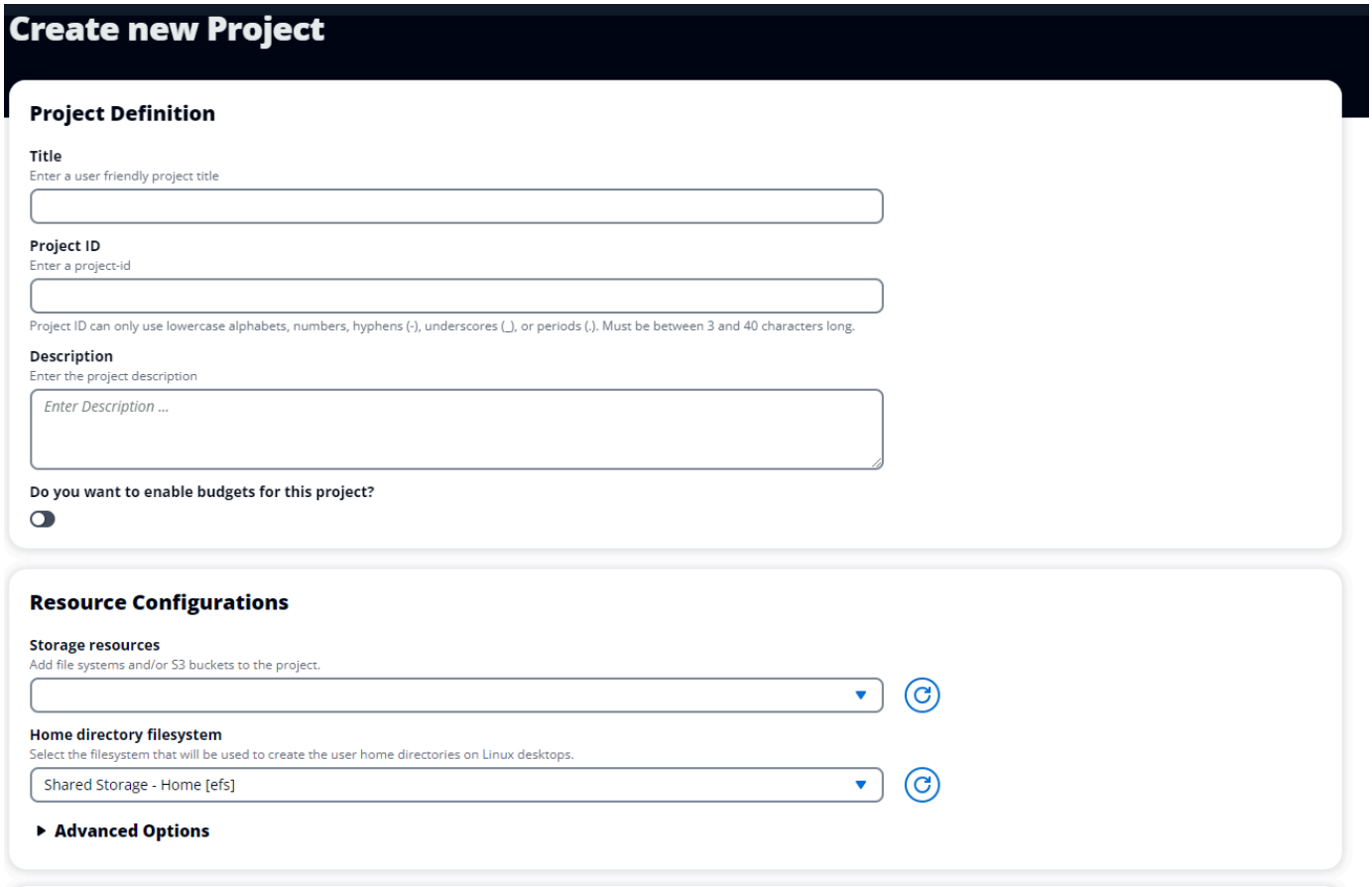
   プロジェクト ID は、 でコスト配分を追跡するために使用できるリソースタグです AWS Cost Explorer Service。詳細については、「ユーザー定義のコスト配分タグのアクティブ化」を参照してください。

> **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。

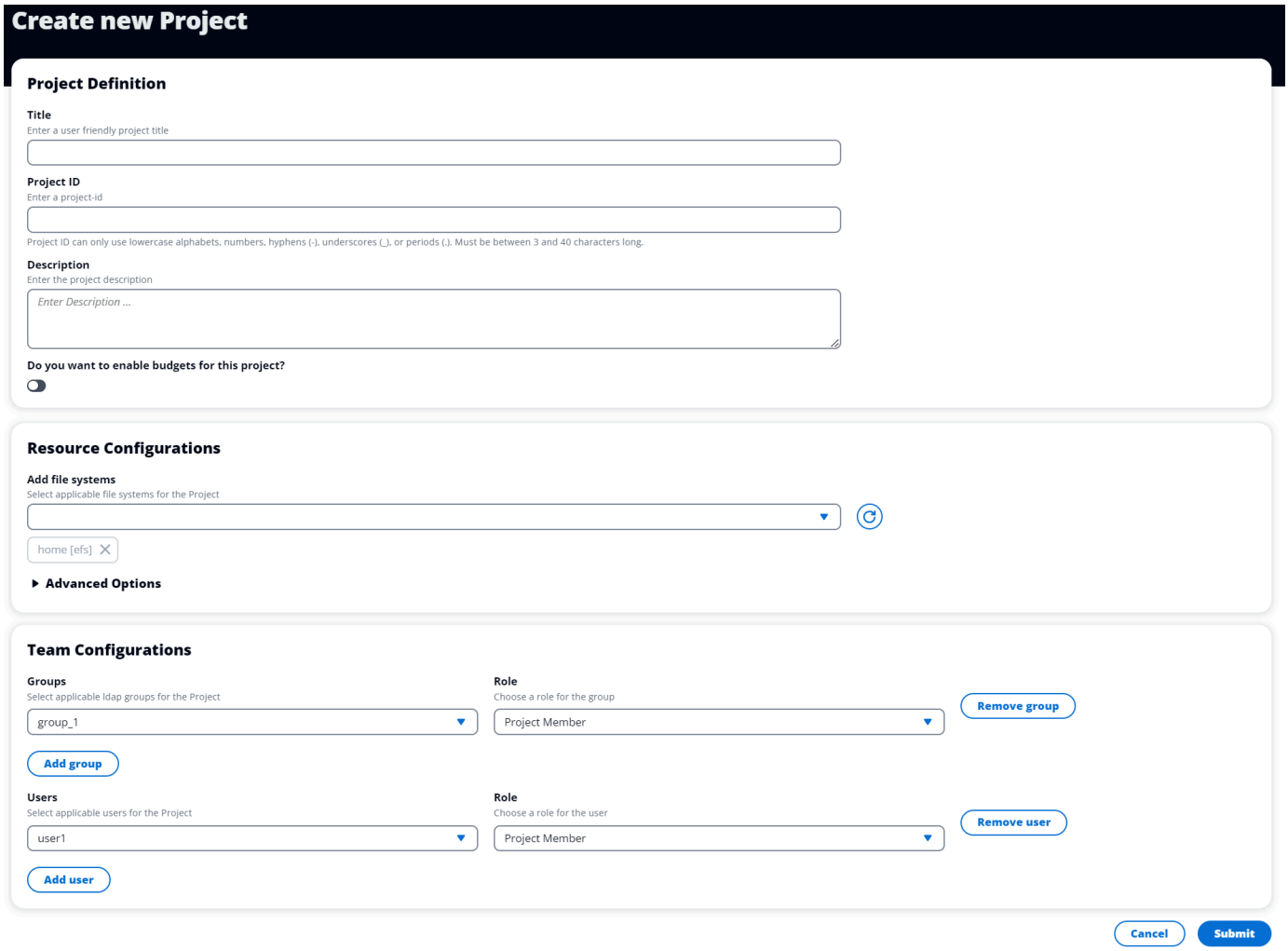
詳細オプション の詳細については、「」を参照してください起動テンプレートを追加する。

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、、Lustre、FSx NetApp ONTAP、またはEBSボリュームストレージFSxのいずれかを使用できます。

   FSx Lustre の共有ホームファイルシステム EFSおよび は、複数のプロジェクトおよび 間で共有FSx NetApp ONTAPできることに注意してくださいVDIs。ただし、EBSボリュームストレージオプションでは、VDIそのプロジェクトのすべての に、他の VDIs 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。

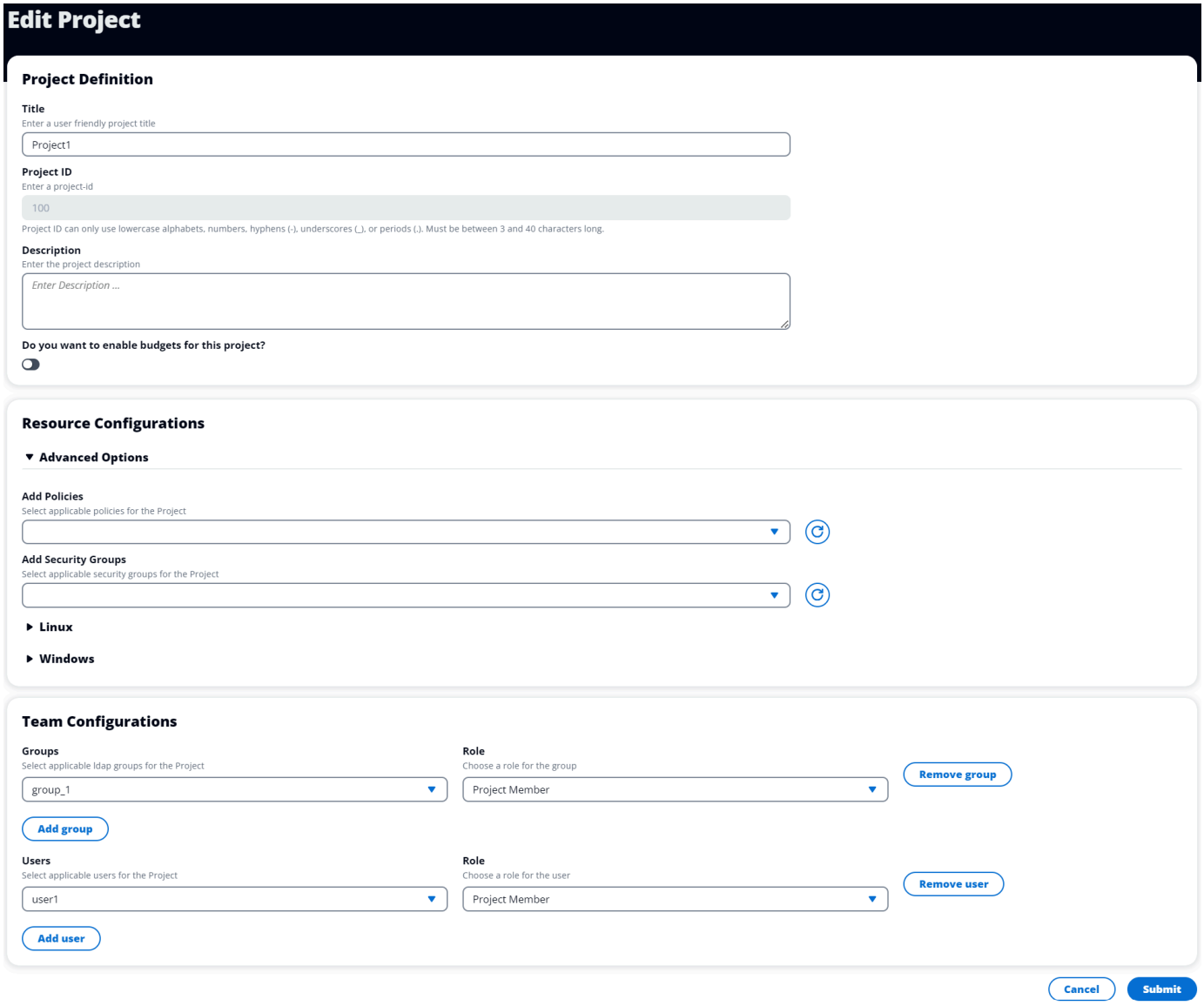


5. ユーザーまたはグループに適切なロール (「プロジェクトメンバー」または「プロジェクト所有者」) を割り当てます。各ロールが実行できるアクションデフォルトのアクセス許可プロファイルについては、「」を参照してください。
6. [送信] を選択します。



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. アクションメニューから、プロジェクトの編集 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。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. [送信] を選択します。



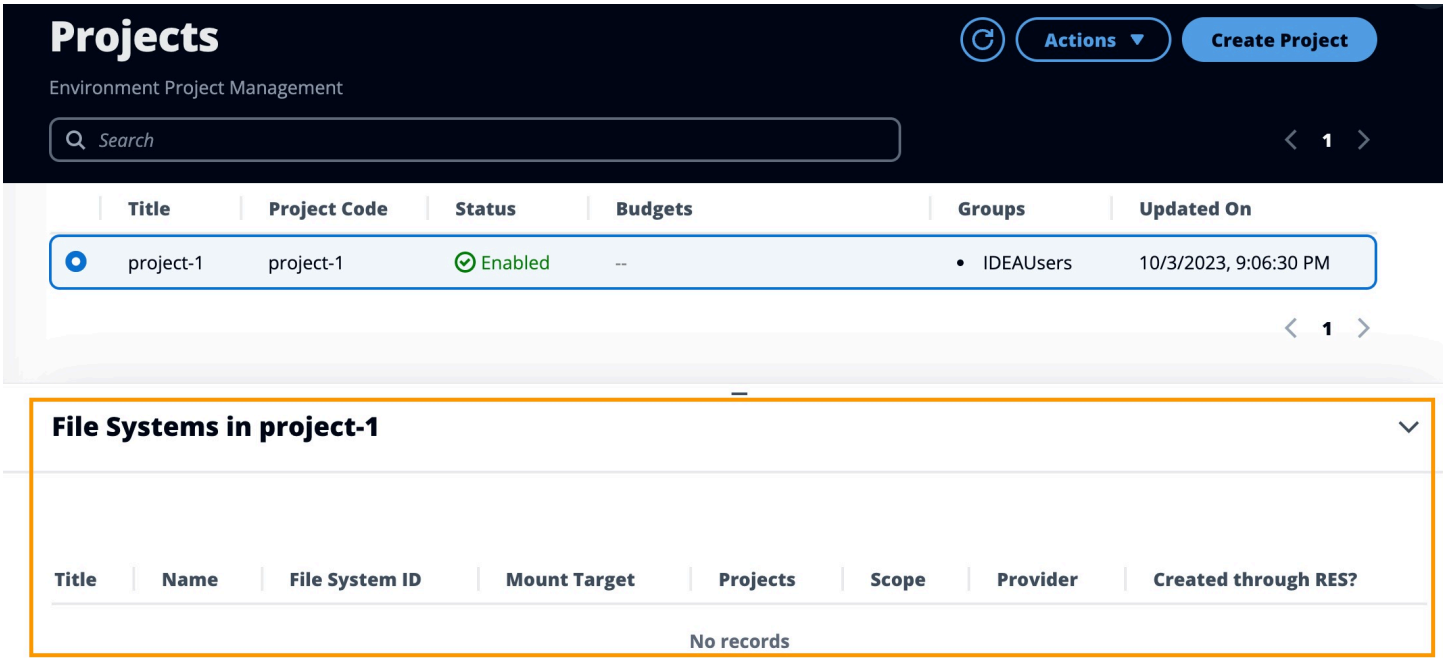
プロジェクトへのタグの追加または削除

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. アクションメニューから、タグの更新 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、画面下部の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。



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ト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

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アクセスを制御するIAMポリシーを追加できます。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、「」の「ポリシーとアクセス許可IAM」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インスタンスの出入り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。

起動スクリプトの追加

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ます。スクリプトの開始には、次のいずれかを選択できます。

VDI 起動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インスタンスの最初にスクリプトを開始します。

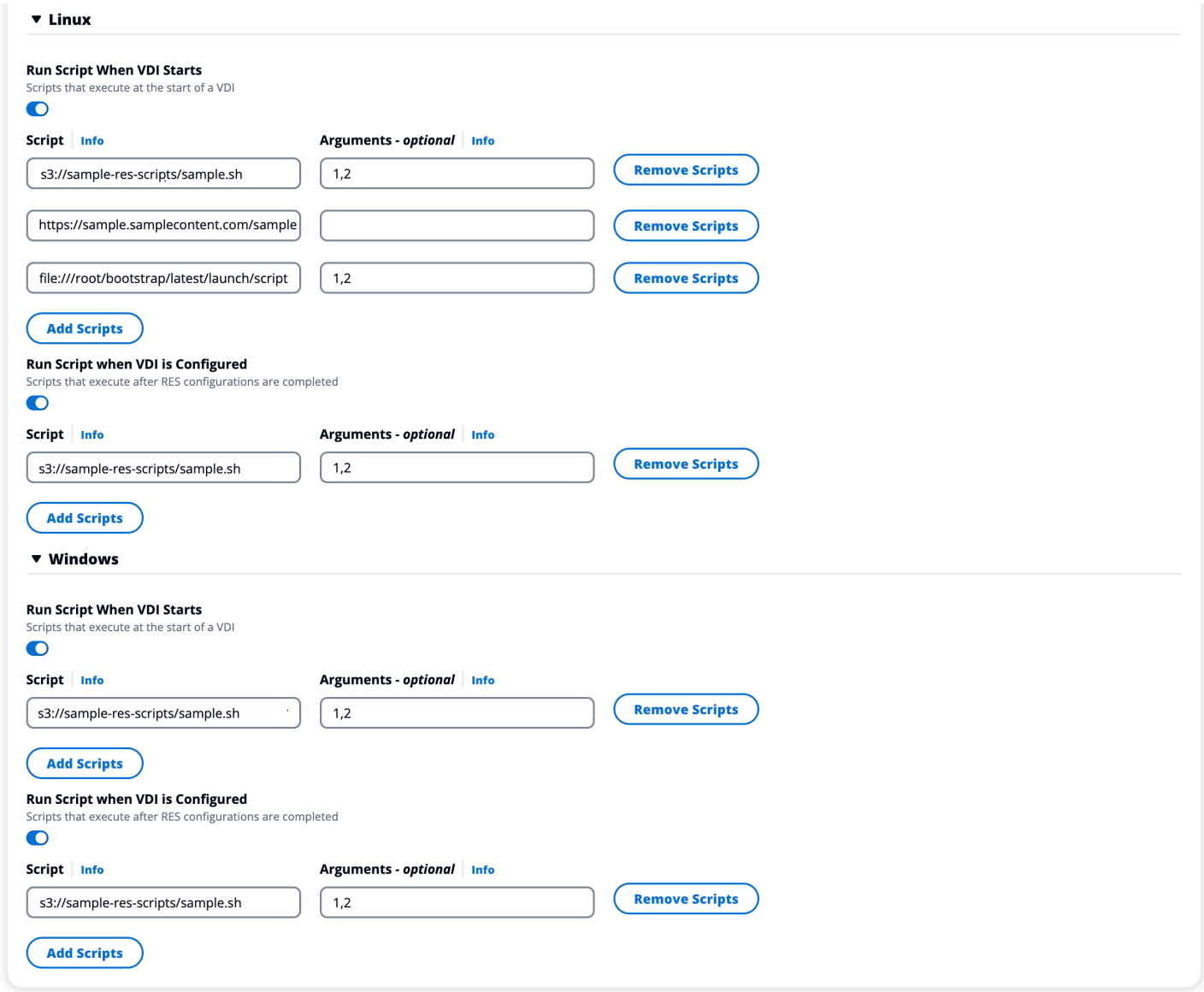
VDI が設定されている場合にスクリプトを実行する

このオプションは、RES設定が完了すると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/サンプル
ローカルファイル	file:///user/scripts/example.sh

引数 には、カンマで区切られた引数を指定します。



プロジェクト設定の例

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. VDI 指定されたユーザーがプロジェクト内で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で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「他のユーザーのセッションの作成/終了」で構成されるセッション管理アクセス許可。

これにより、管理者は、環境内の非管理者にプロジェクトベースのアクセス許可を委任できます。

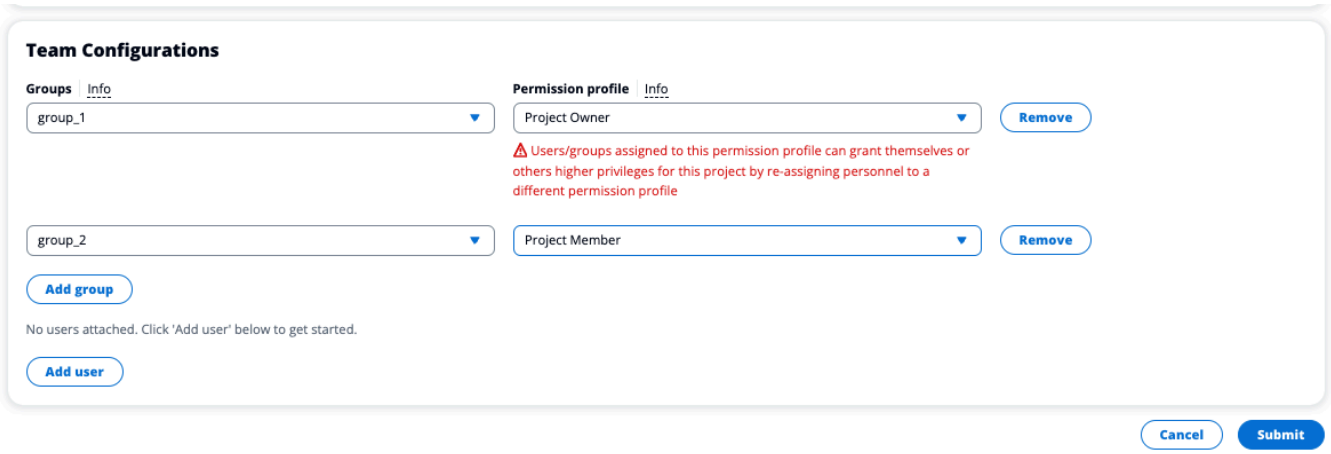
トピック

- 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

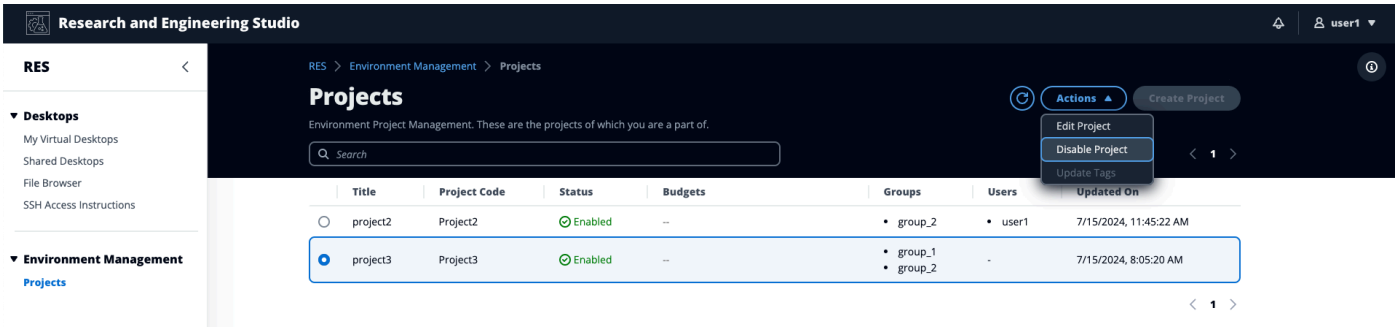
プロジェクトメンバーシップを更新する

このアクセス許可により、権限を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。



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、権限を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。

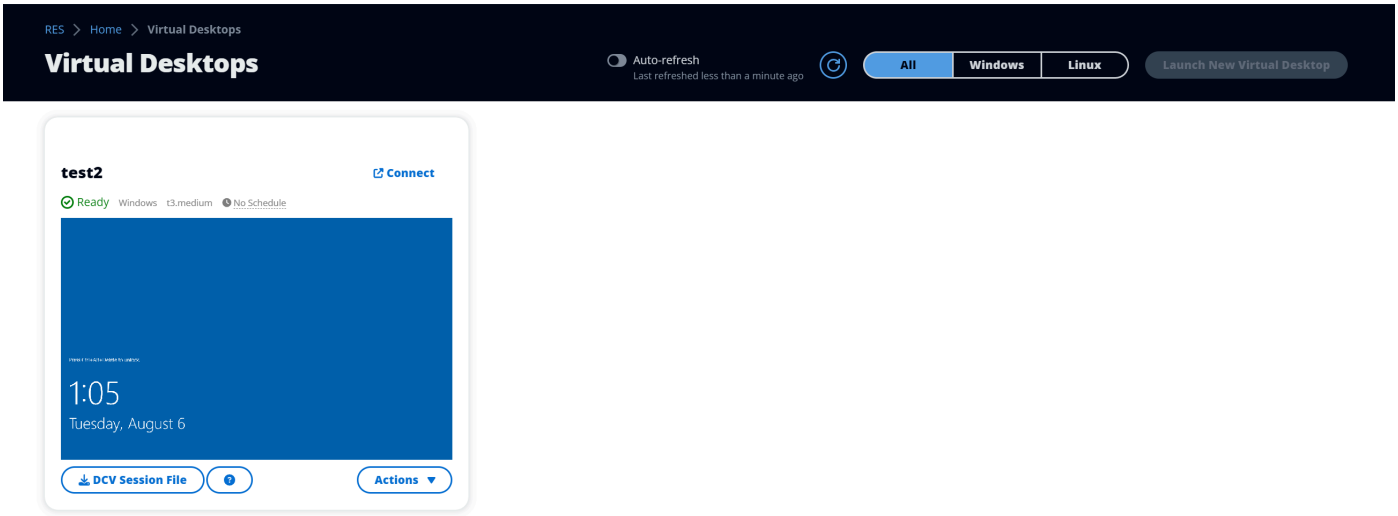


VDI セッション管理のアクセス許可

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。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するには、この操作を無効にします。ユーザーはいつでも自分のVDIセッションを停止および終了できます。

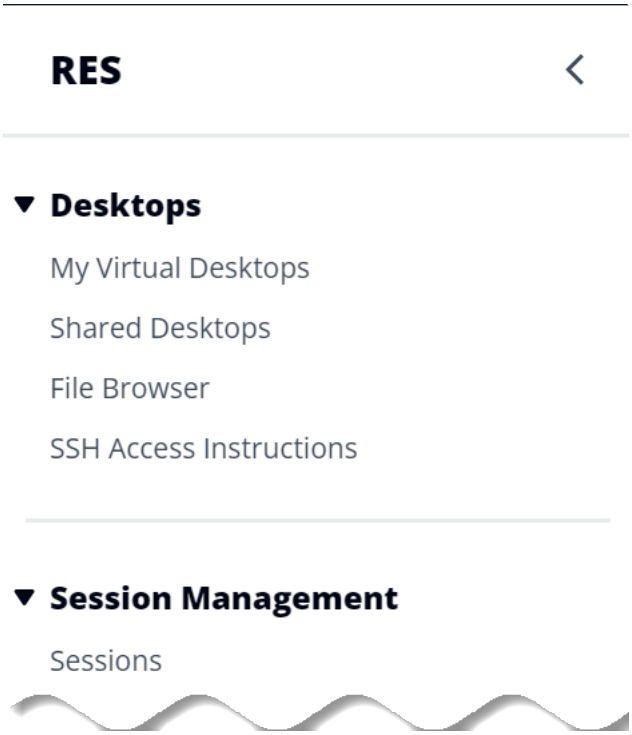
管理者以外のユーザーがセッションを作成するアクセス許可を持っていない場合、次のように、新しい仮想デスクトップを起動ボタンが無効になります。



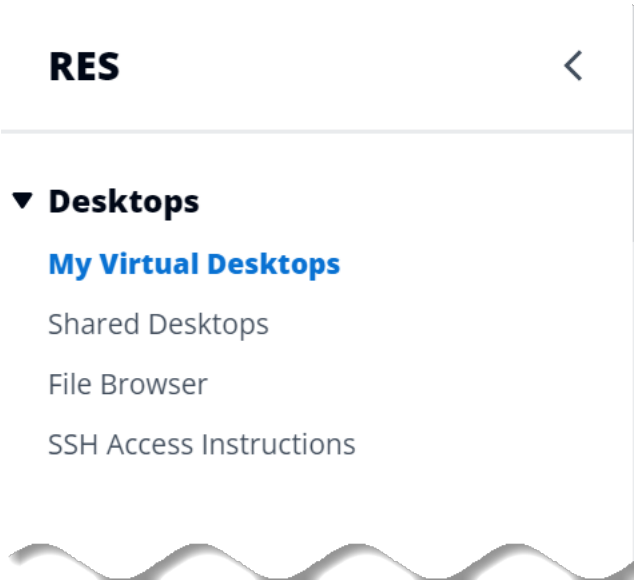
他のユーザーのセッションを作成または終了する

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た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に他のユーザーのセッションを起動するアクセス許可がある場合、左側のナビゲーションペインには、次のようにセッション管理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、次のようにセッション管理が表示されません。

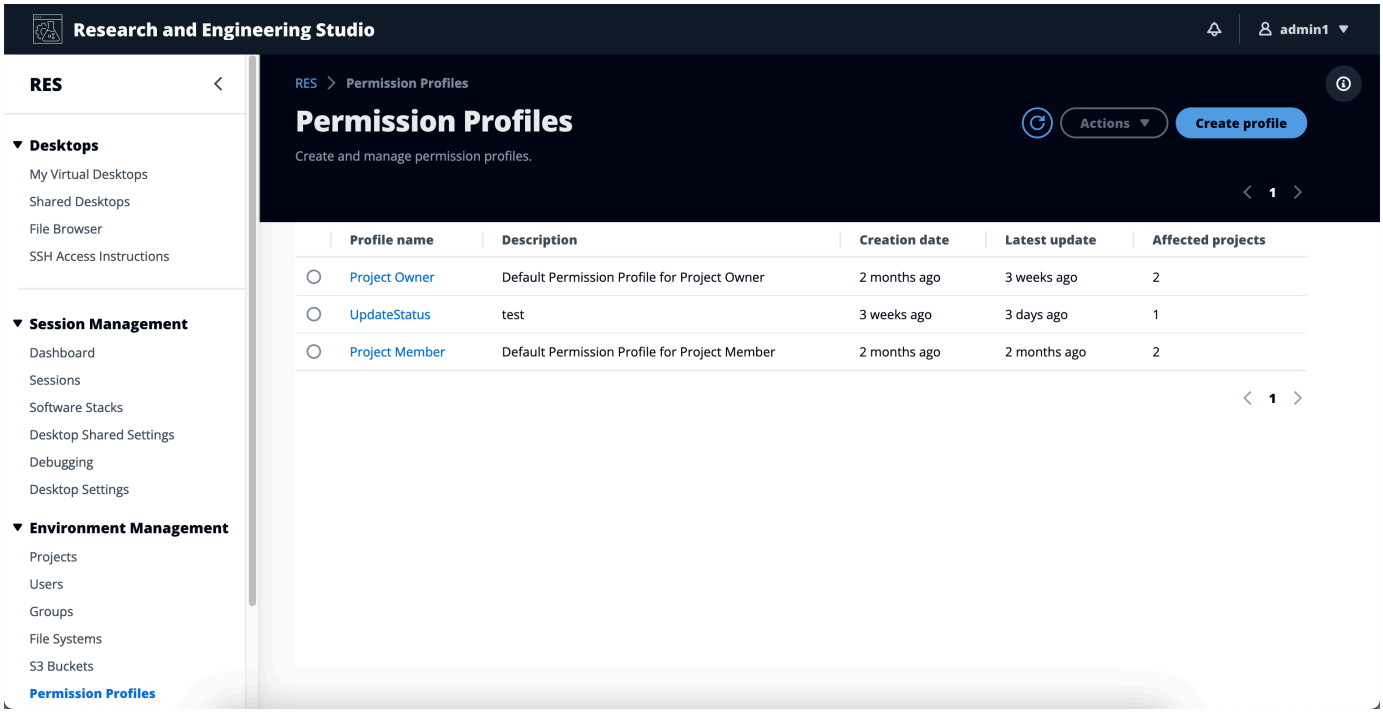


アクセス許可プロファイルの管理

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。

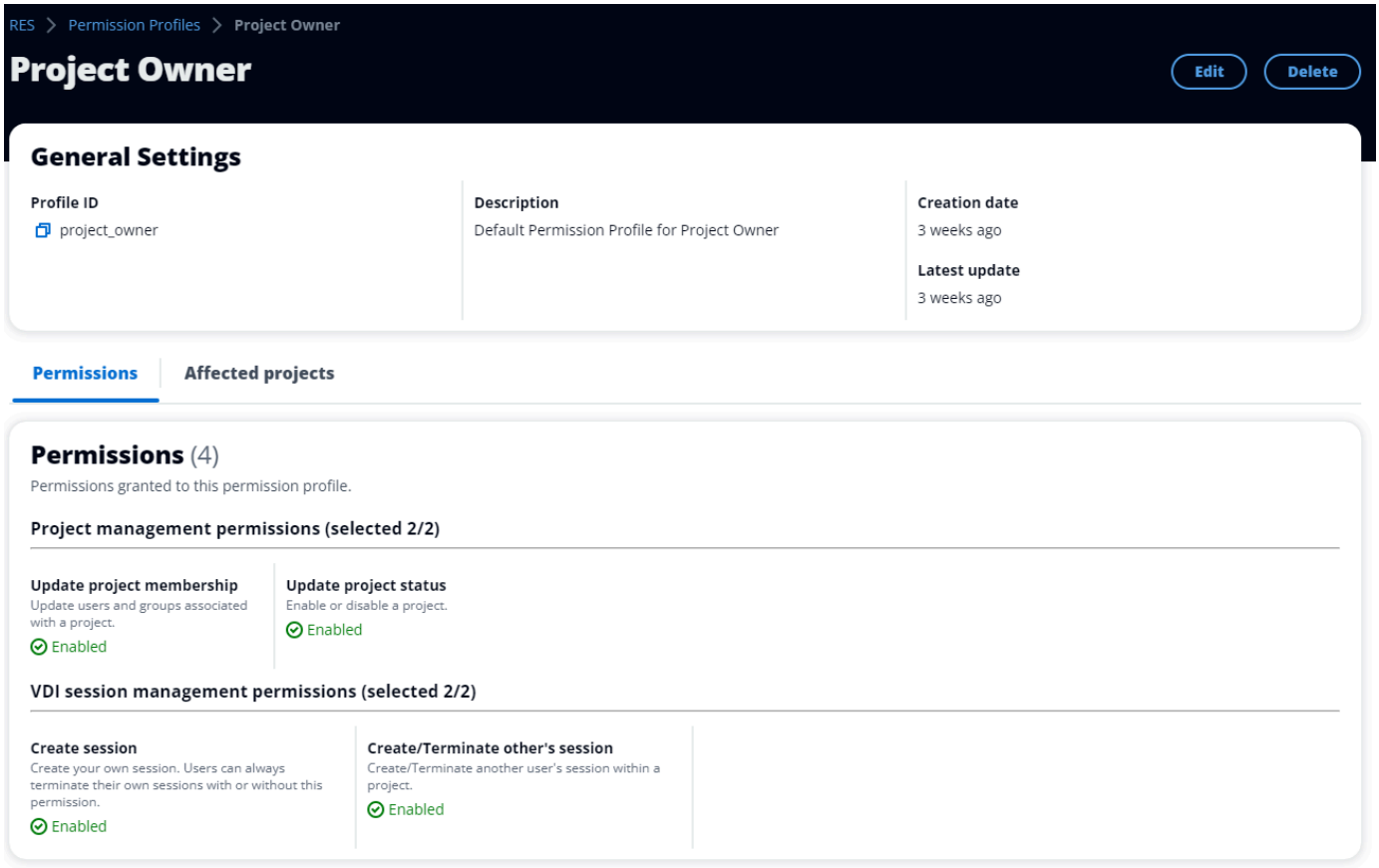
アクセス許可プロファイルを一覧表示する

- 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プロファイルを選択します。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。

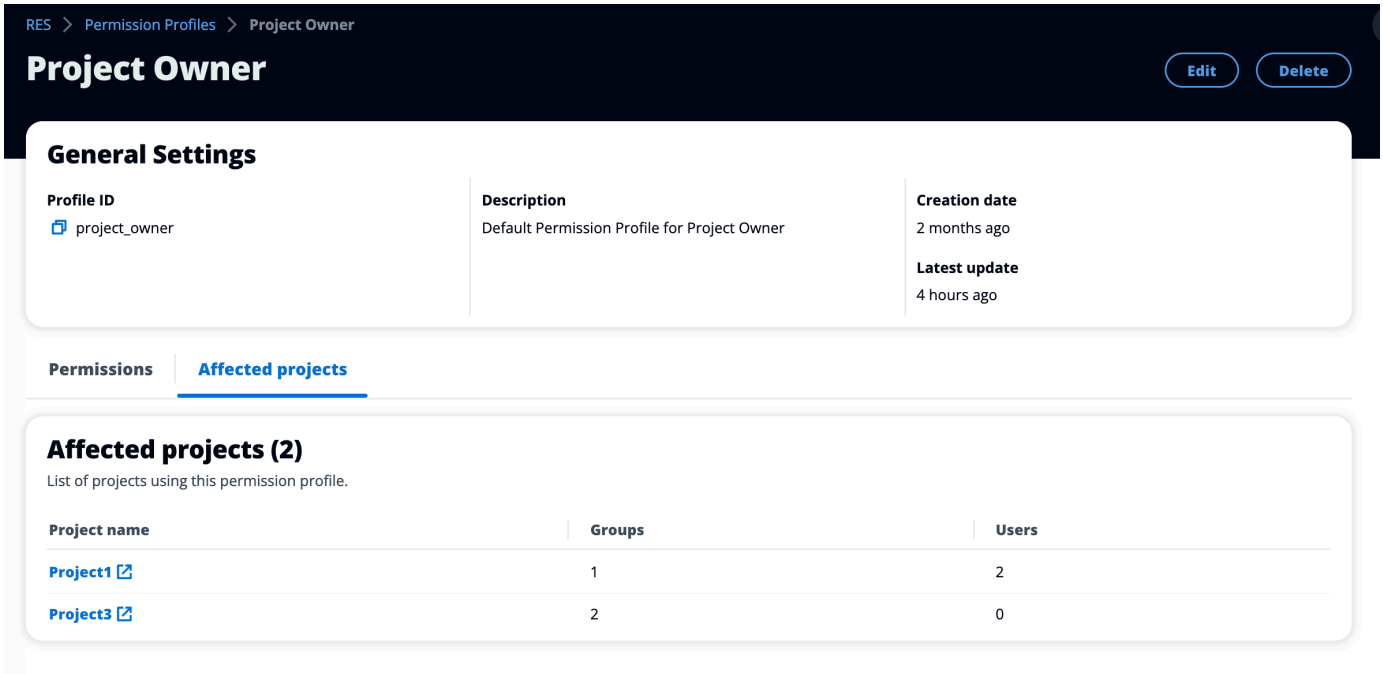


アクセス許可プロファイルを表示する

1. 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。

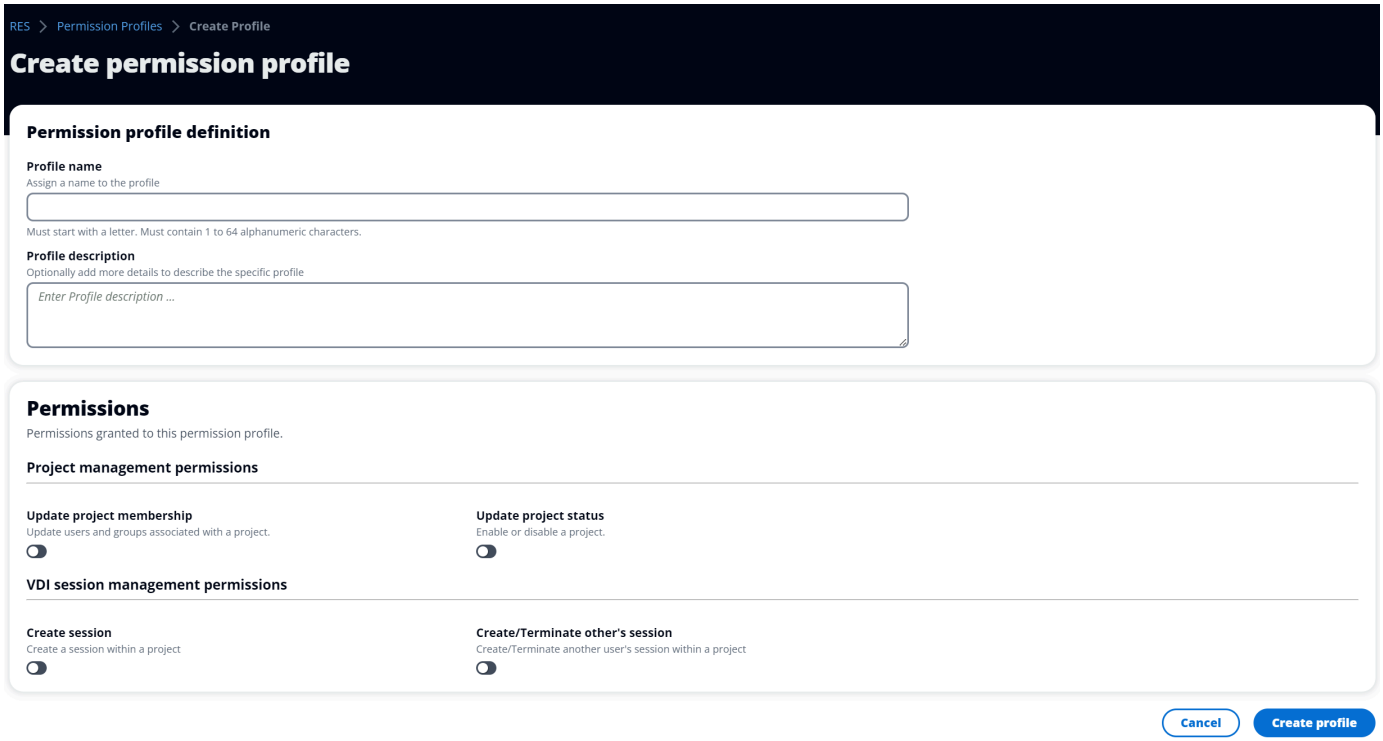


2. 影響を受けるプロジェクトタブを選択すると、現在アクセス許可プロファイルを使用しているプロジェクトが表示されます。



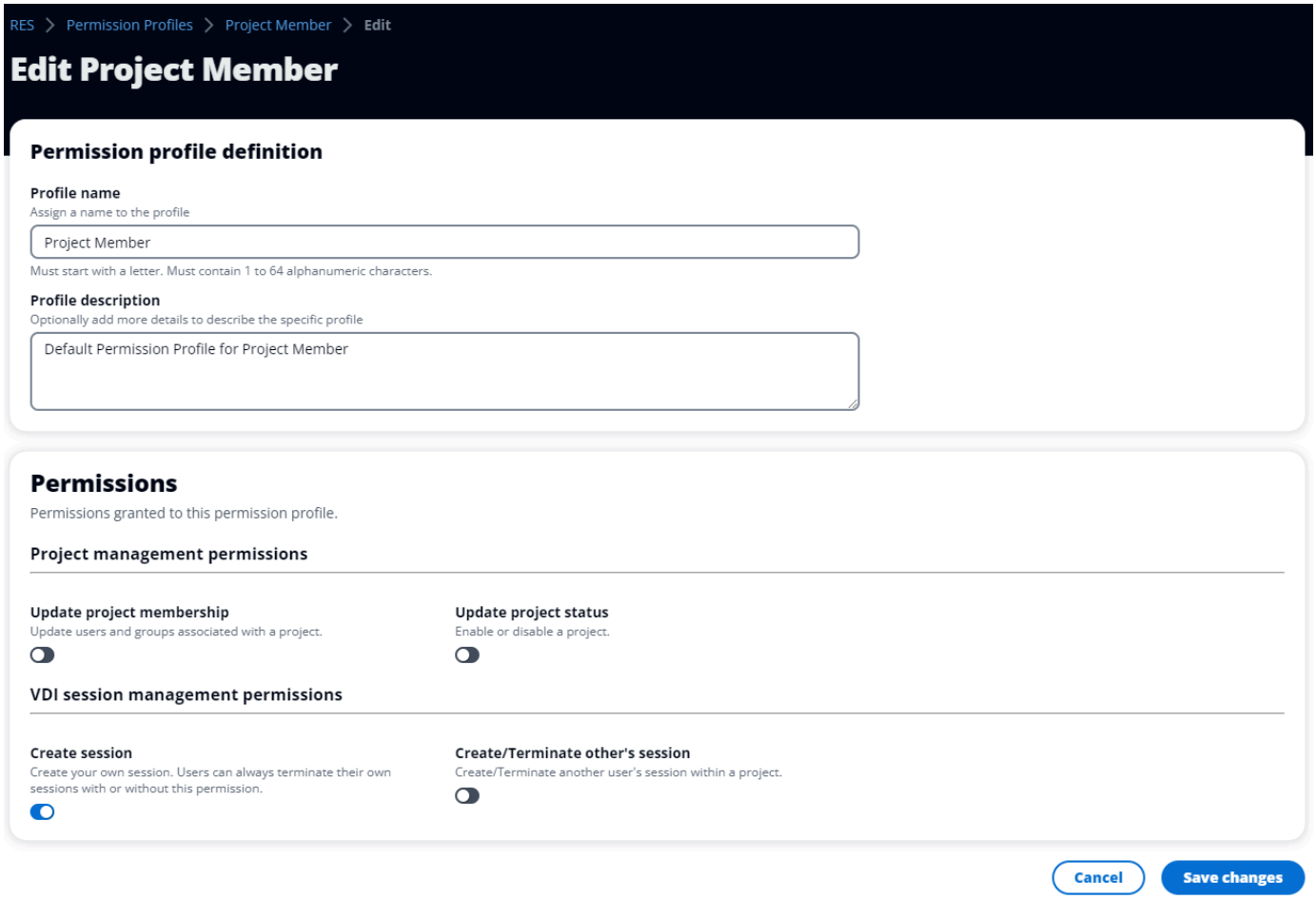
アクセス許可プロファイルを作成する

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。



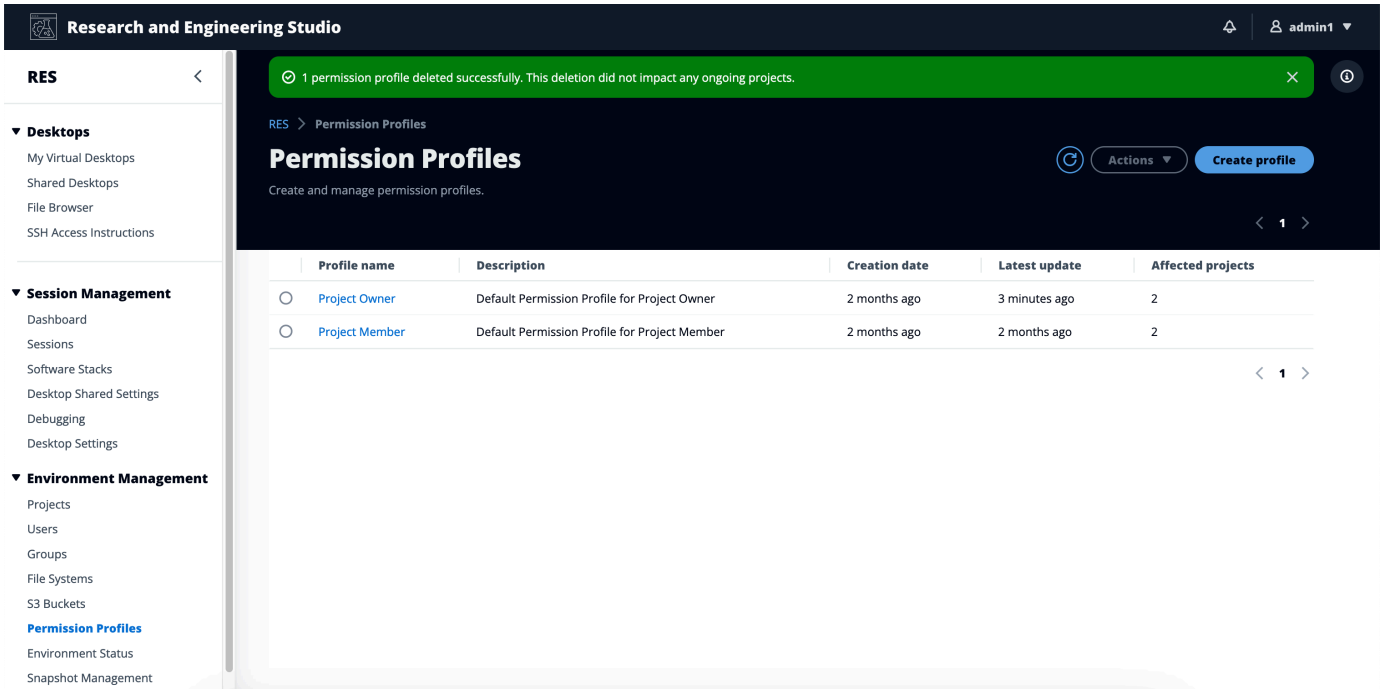
アクセス許可プロファイルを編集する

- メインのアクセス許可プロファイルページで、その横の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、プロファイルを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。



アクセス許可プロファイルを削除する

- メイン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るアクセス許可プロファイルは削除できません。



デフォルトのアクセス許可プロファイル

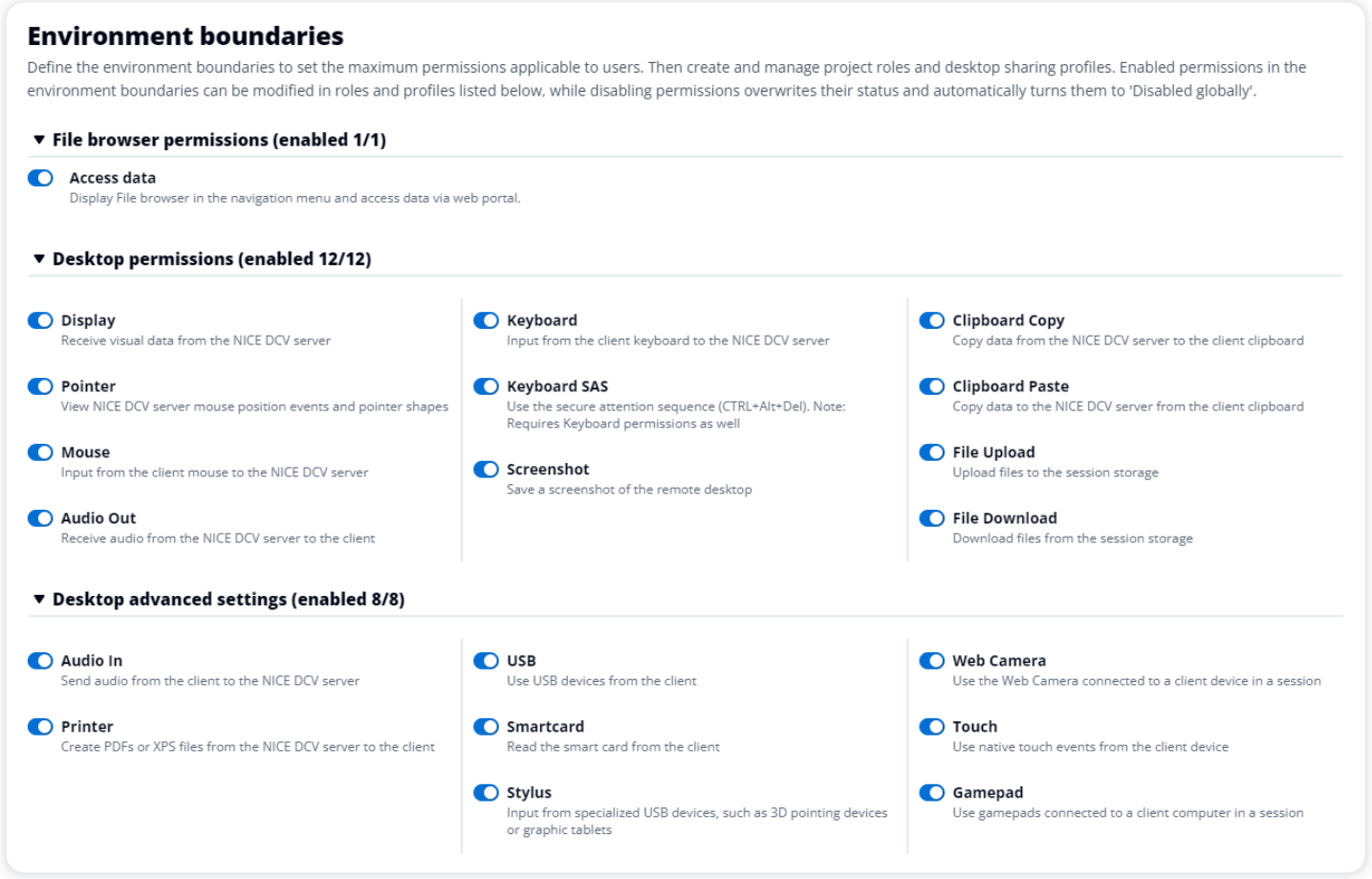
すべてのRESプロジェクトには、グローバル管理者が設定できる 2 つのデフォルトのアクセス許可プロファイルが付属しています。（さらに、グローバル管理者はプロジェクトの新しいアクセス許可プロファイルを作成および変更できます。）次の表は、デフォルトのアクセス許可プロファイルの「プロジェクトメンバー」および「プロジェクト所有者」に対して許可されるアクセス許可を示しています。アクセス許可プロファイル、およびプロジェクトのユーザーを選択するために付与されるアクセス許可は、それらが属するプロジェクトにのみ適用されます。グローバル管理者は、すべてのプロジェクトで以下のすべてのアクセス許可を持つスーパーユーザ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

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す。			
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	

環境境界

環境の境界により、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、ファイルブラウザアクセスやデスクトップアクセス許可などのアクセス許可が含まれます。



ファイルブラウザアクセスの設定

管理者は、ファイルブラウザのアクセス許可 でアクセスデータをオンまたはオフに切り替えることができます。Access 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 File Browser 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。Access データを有効にすると、ユーザーはウェブポータルの File Browser ナビゲーションにアクセスでき、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。

アクセスデータ機能がオンになってからオフにすると、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消えます。

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、デスクトップ共有プロファイルを作成し、デスクトップが共有されているユーザーが実行できるアクショ

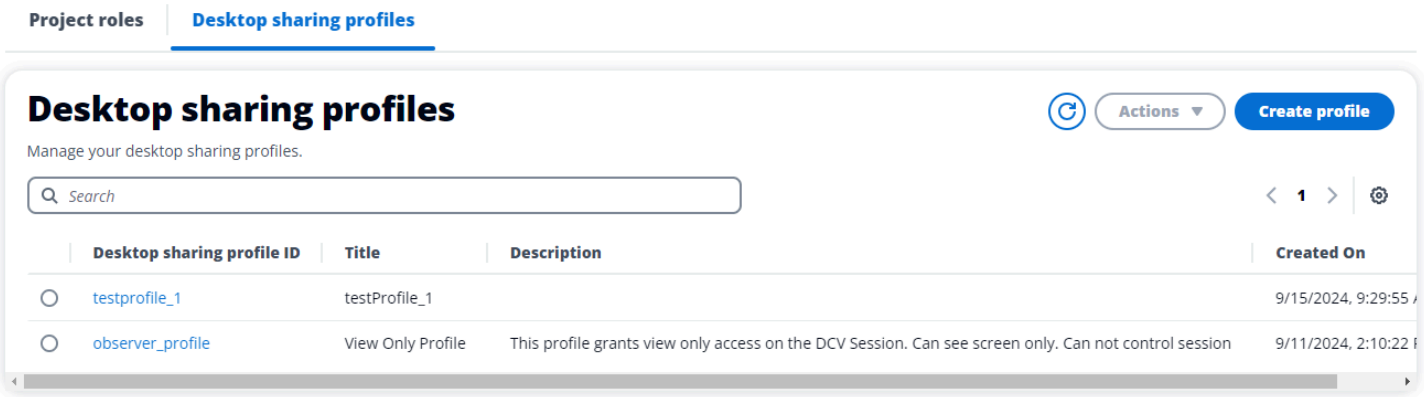
ンを決定できます。デスクトップアクセス許可が無効になっている場合、デスクトップ共有プロファイル の対応するアクセス許可は自動的に無効になります。これらのアクセス許可には「グローバルに無効」というラベルが付けられます。管理者がこのデスクトップアクセス許可を再度有効にしても、管理者が手動で有効にするまで、デスクトップ共有プロファイルのアクセス許可は無効のままになります。

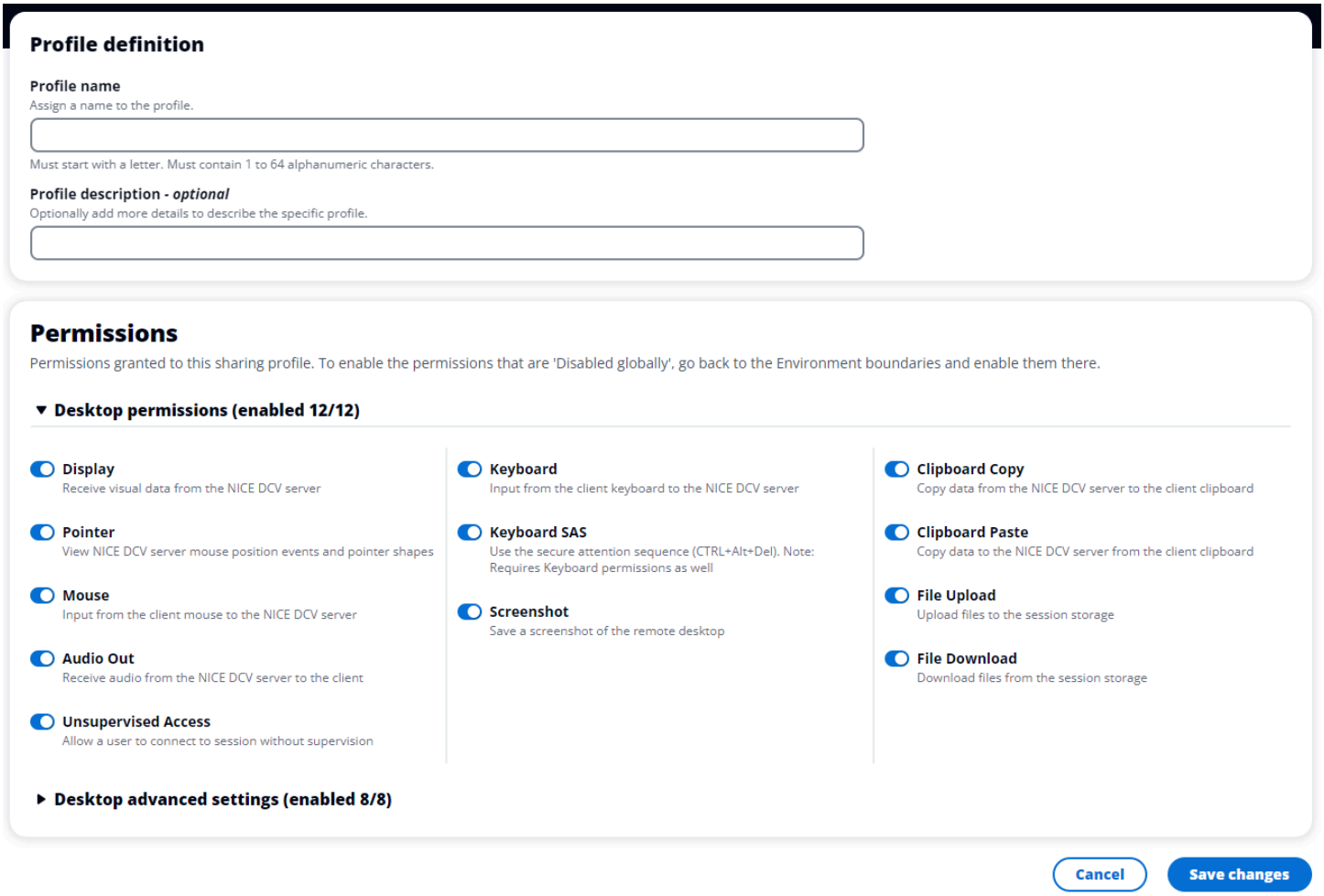
デスクトップ共有プロファイル

管理者は新しいプロファイルを作成し、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際に使用されます。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。



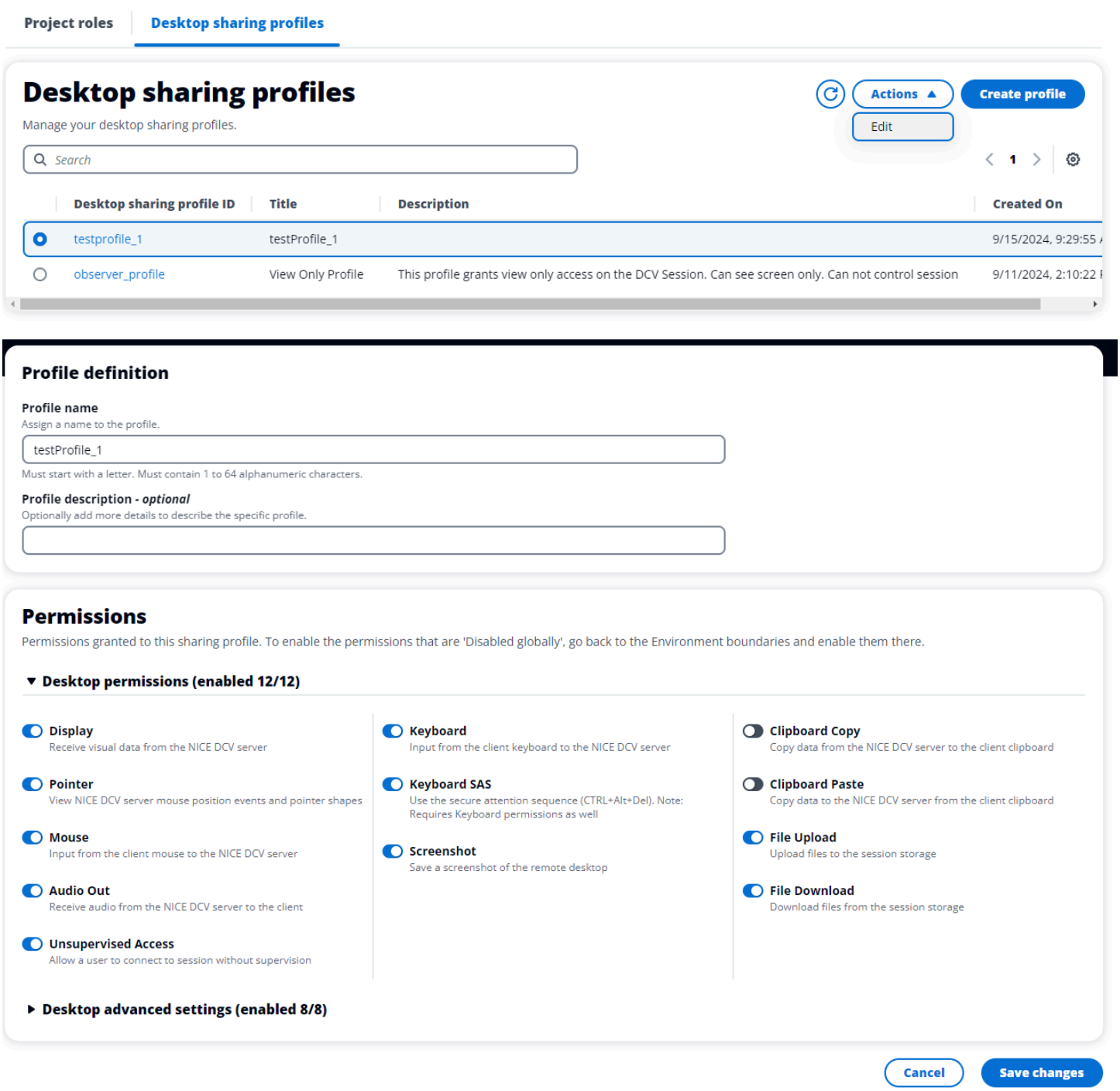


プロファイルの編集

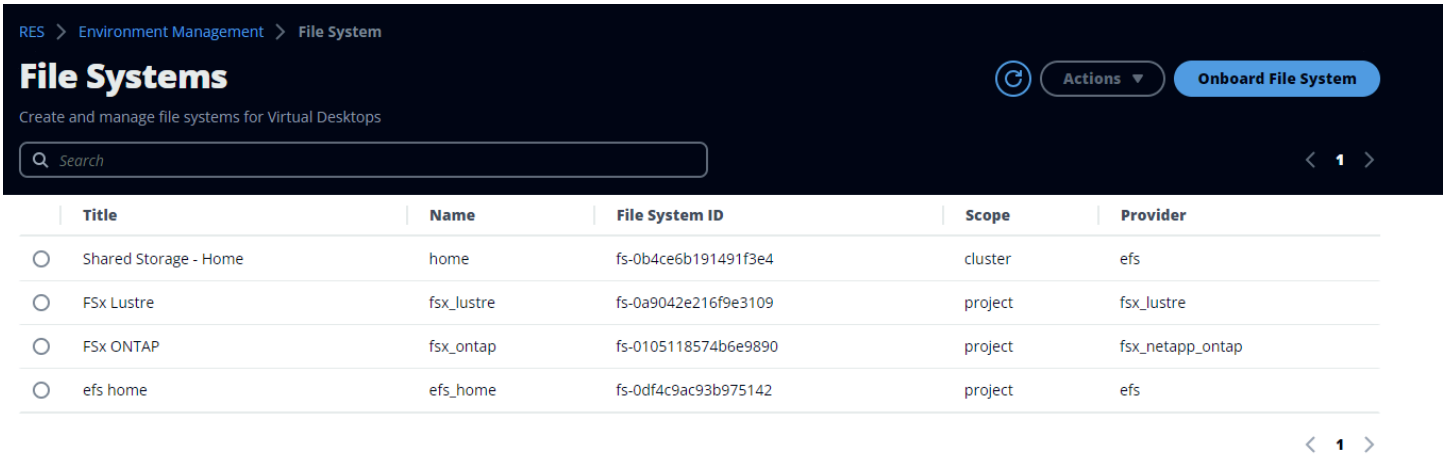
プロファイルを編集するには：

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直ちに適用されます。


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

ファイルシステム



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以下を行います。
   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作成します。
5. ファイルシステムを選択すると、画面下部の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

- ファイルシステムを作成する
- ファイルシステムのオンボード

ファイルシステムを作成する

1. [ファイルシステムの作成] を選択します。
2. 新しいファイルシステムの詳細を入力します。
3. IDs からサブネットを指定しますVPC。は、環境管理 > 設定 > ネットワークタブIDsにあります。

4. [送信] を選択します。

Create new File System

Title

Enter a user friendly file system title

Eg. EFS 01

Name

Enter a file system name

File System name can only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

File System Provider

Select applicable file system type

EFS

Projects

Select applicable project

Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

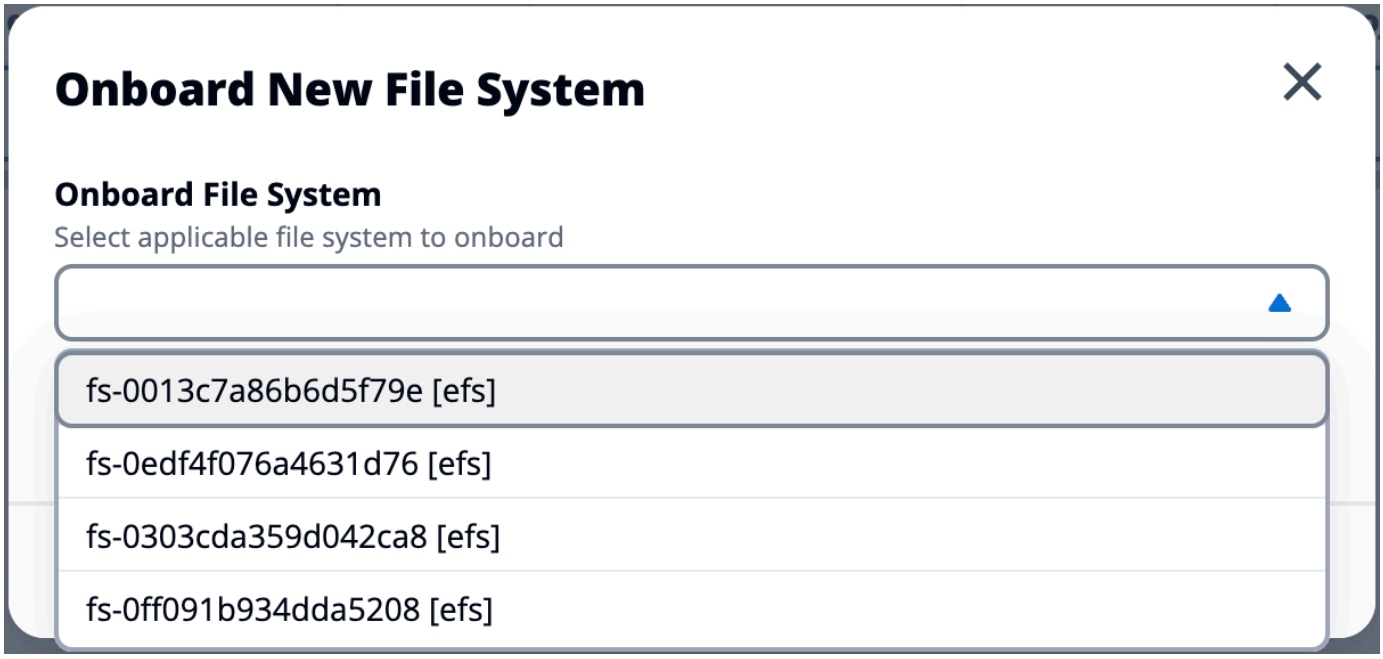
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

Enter directory to mount the file system

ファイルシステムのオンボード

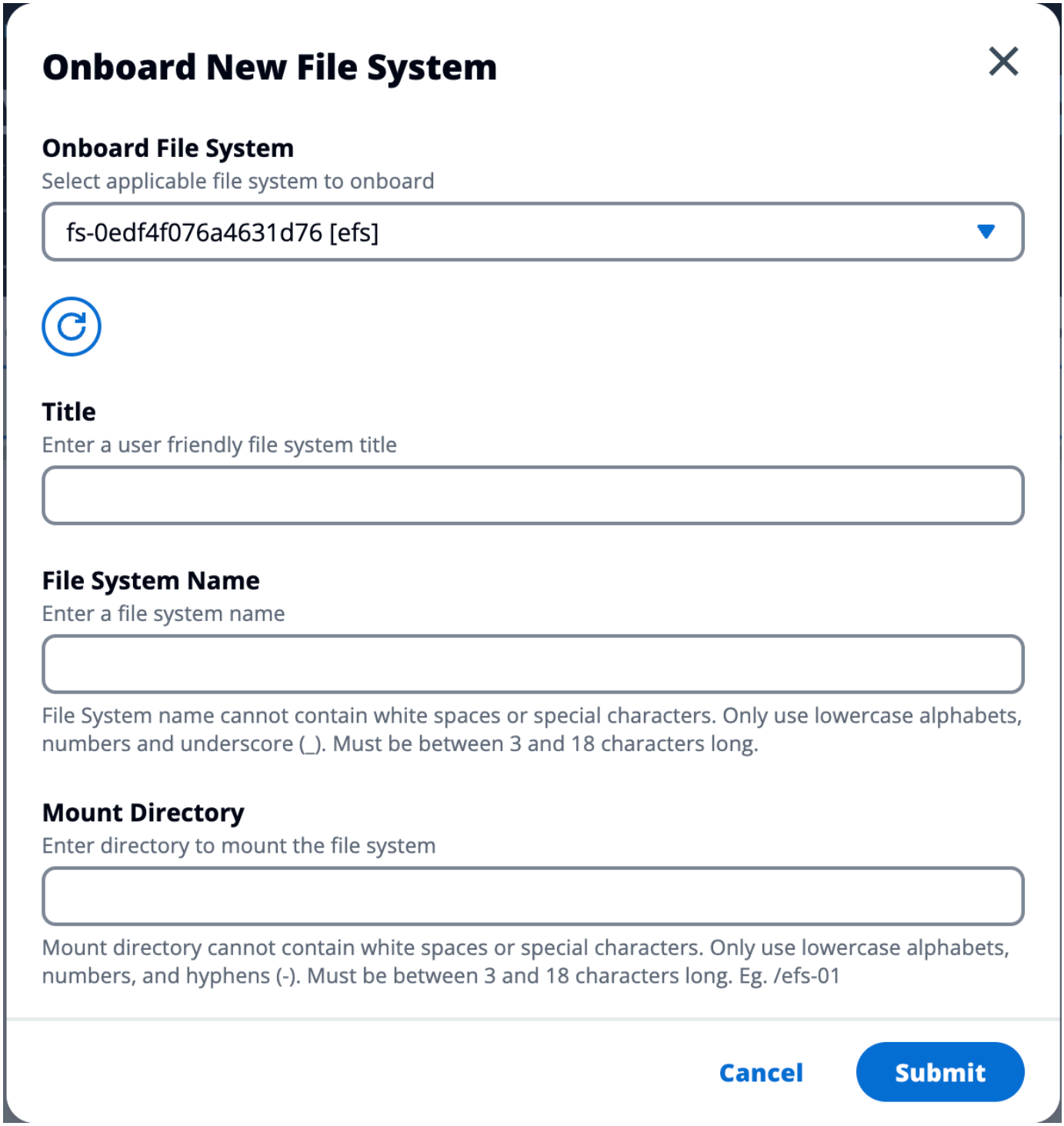
1. オンボードファイルシステム を選択します。
2. ドロップダウンからファイルシステムを選択します。モーダルは、追加の詳細エントリで展開されます。



3. ファイルシステムの詳細を入力します。

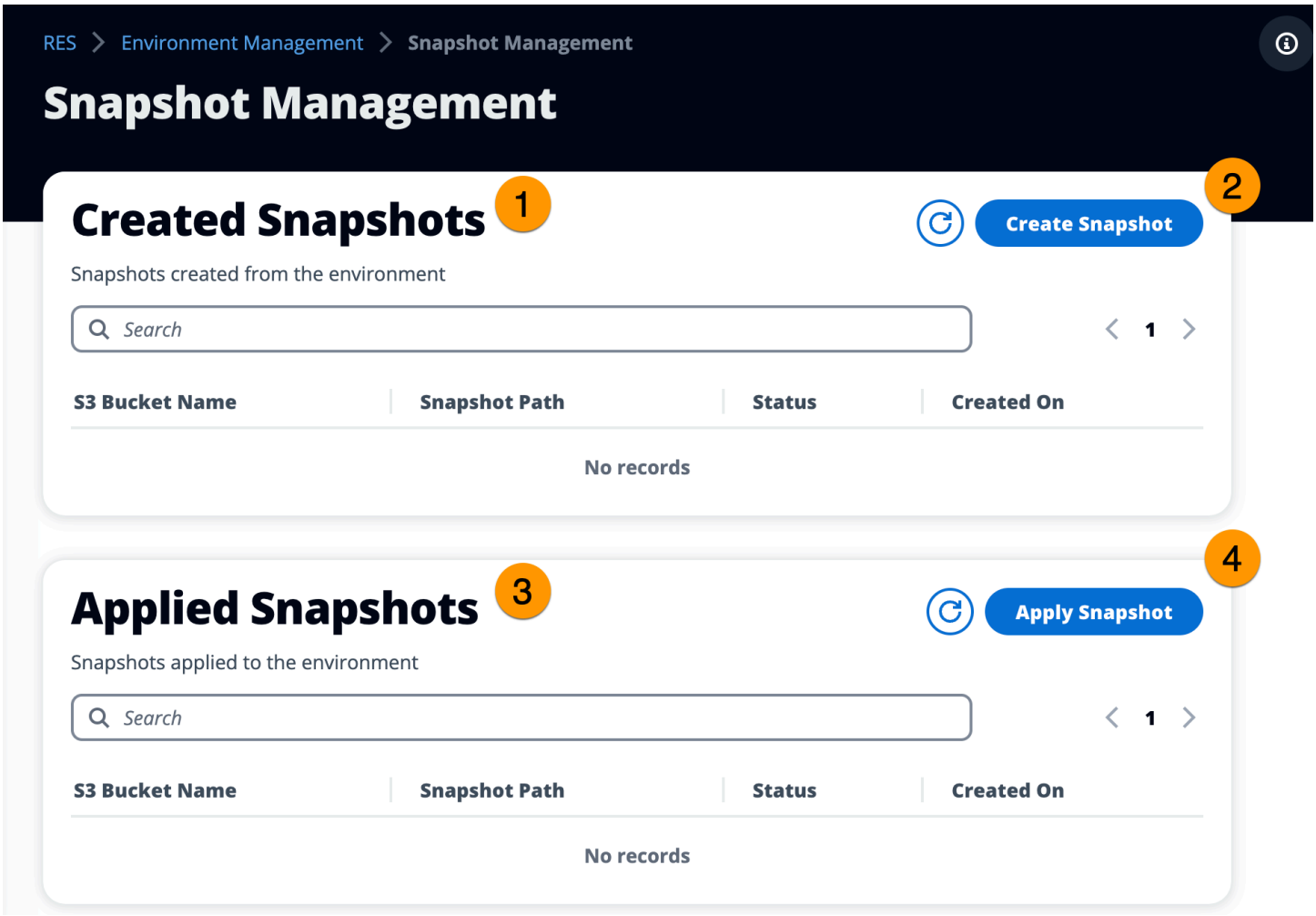
> **Note**
>
> デフォルトでは、管理者とプロジェクト所有者は、新しいプロジェクトを作成するときにホームファイルシステムを選択できます。これは後で編集することはできません。プロジェクトのホームディレクトリとして使用するファイルシステムは、マウントディレクトリパスを に設定してオンボーディングする必要があります/home。これにより、ホームディレクトリのファイルシステムのドロップダウンオプションにオンボーディングされたファイルシステムが入力されます。この機能は、プロジェクトに関連付けられたユーザーのみが を介してファイルシステムにアクセスできるため、プロジェクト間でデータを分離しておくのに役立ちますVDIs。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. [送信] を選択します。


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、環境状態を保存し、同じ状態の新しい環境に移行できます。



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。バケットバージョニングとサーバーアクセス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。バケットのライフサイクルはコンソールから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：

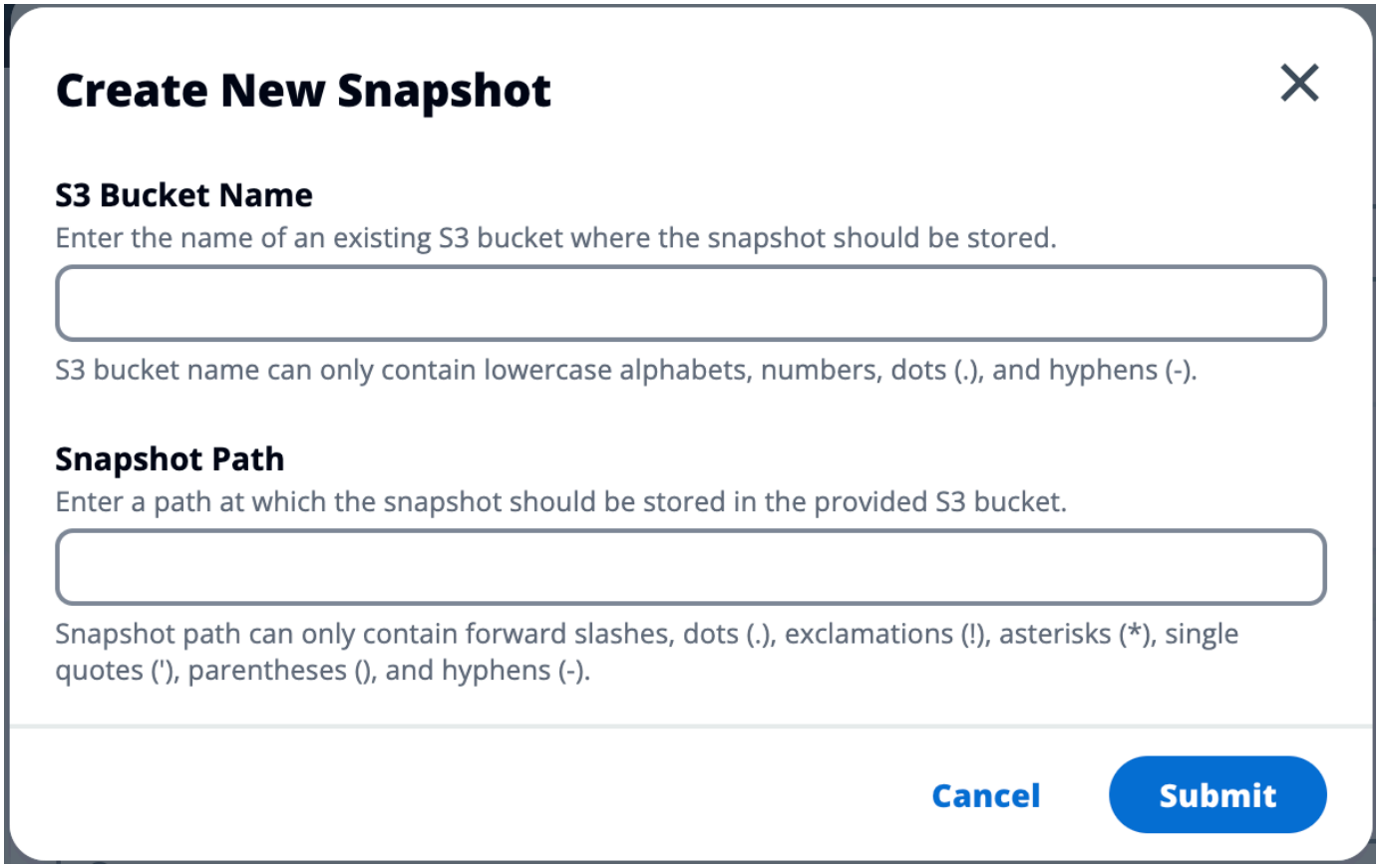
1. バケットリストから作成したバケットを選択します。
2. アクセス許可タブを選択します。
3. [バケットポリシー] で [編集] を選択します。
4. バケットポリシーに次のステートメントを追加します。以下の値を自分の値に置き換えてください。
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

> **Important**
>
> でサポートされている限定バージョン文字列があります AWS。詳細については、「https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}:role/{RES_ENVIRONMENT_NAME}-
cluster-manager-role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

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`** と指定します。
4. [送信] を選択します。



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 に変わるまで有効ではありません COMPLETED。

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、そのスナップショットが既に存在するかどうかを判断します。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、他の基本的なリソース情報が異なる場合は、次の規則を使用して、変更された名前とキーで新しいレコードを作成します。 `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す。

スナップショットアプリケーション中、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。新しい環境で利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。依存リソースが利用できない場合、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した場合は、 CloudWatch ロググループで見つかったログ`/res-<env-name>/cluster-manager`の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。

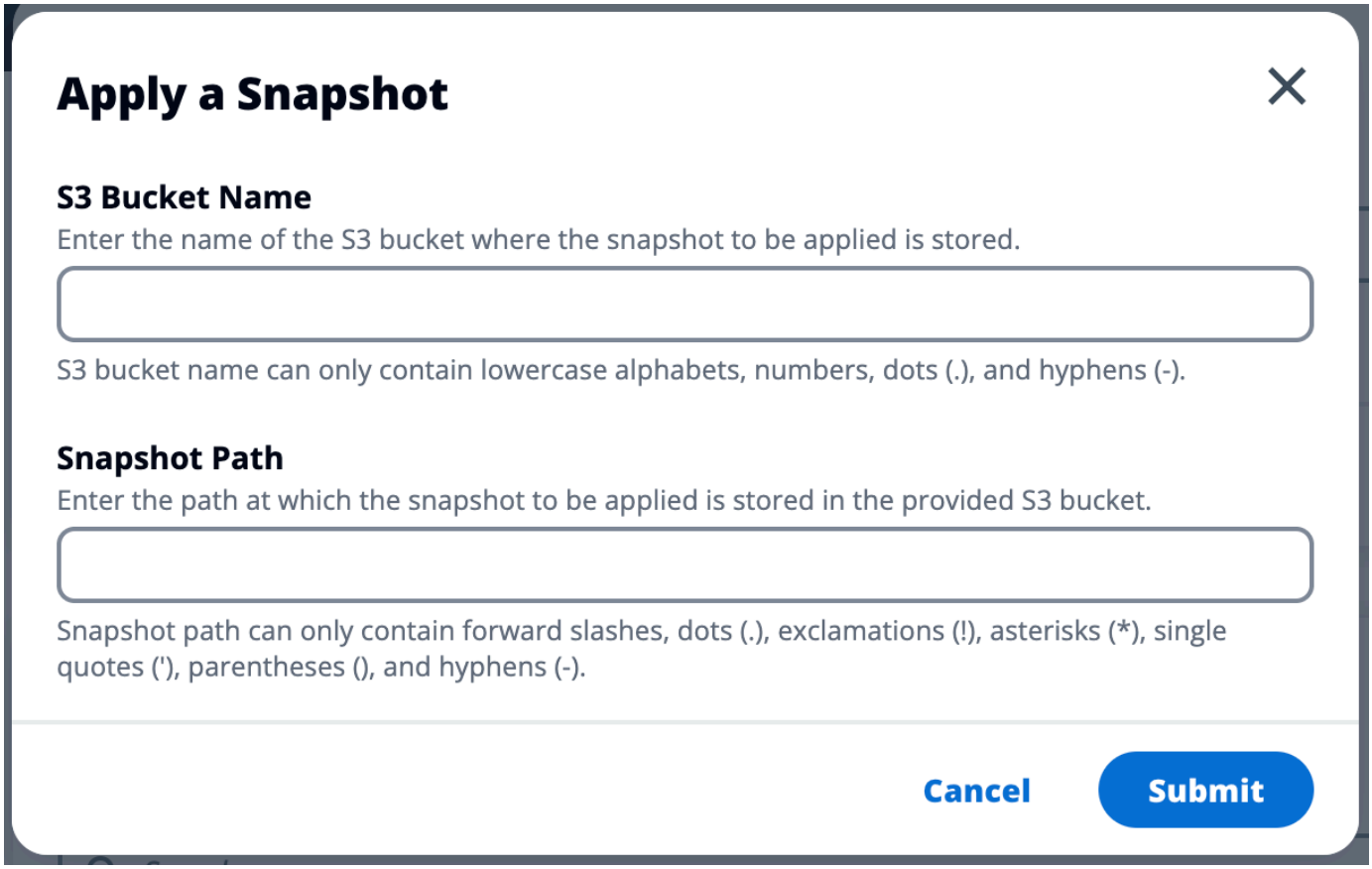
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

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

```
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{AWS_ACCOUNT_ID}:role/{RES_ENVIRONMENT_NAME}-
cluster-manager-role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

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. [送信] を選択します。



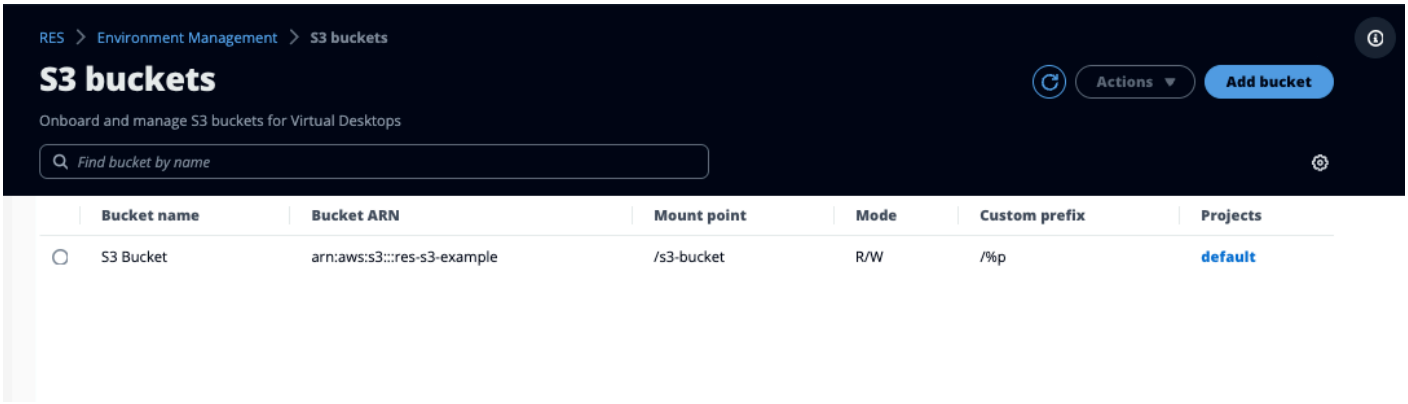
5. 5～10 分後、スナップショット管理ページで更新を選択してステータスを確認します。

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RES、環境管理 の S3 バケットタブで、S3 バケットを 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 にオンボードしますRES。
2. S3 バケットを選択し、アクションメニューを使用して以下を行います。
   - 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。

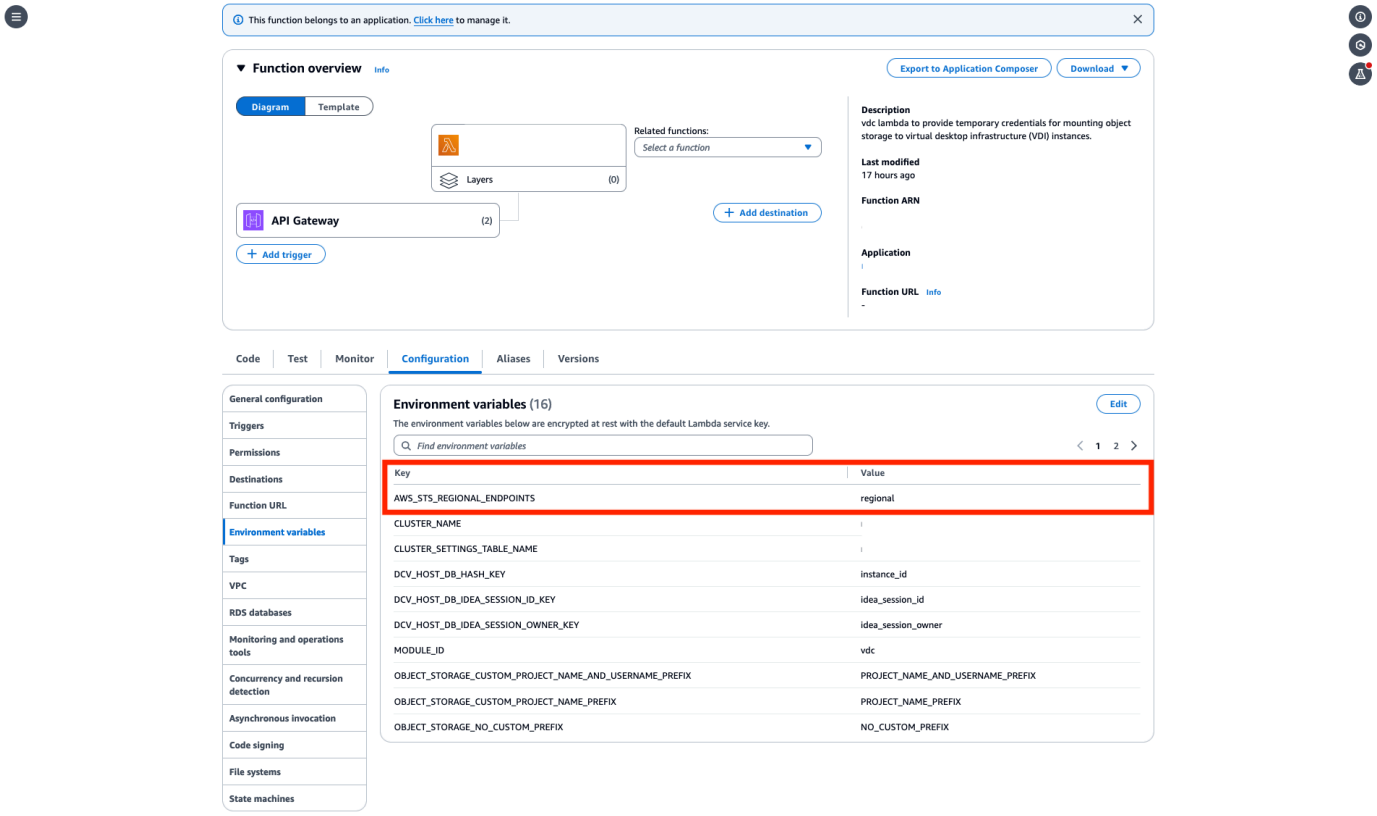
トピック

- 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
- プライベートでのデータ流出の防止 VPC
- トラブルシューティング
- の有効化 CloudTrail

分離VPCデプロイの Amazon S3 バケットの前提条件

分離された に Research and Engineering Studio をデプロイする場合はVPC、以下の手順に従って、RES AWS アカウントにデプロイした後に 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。



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. [Save] 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。

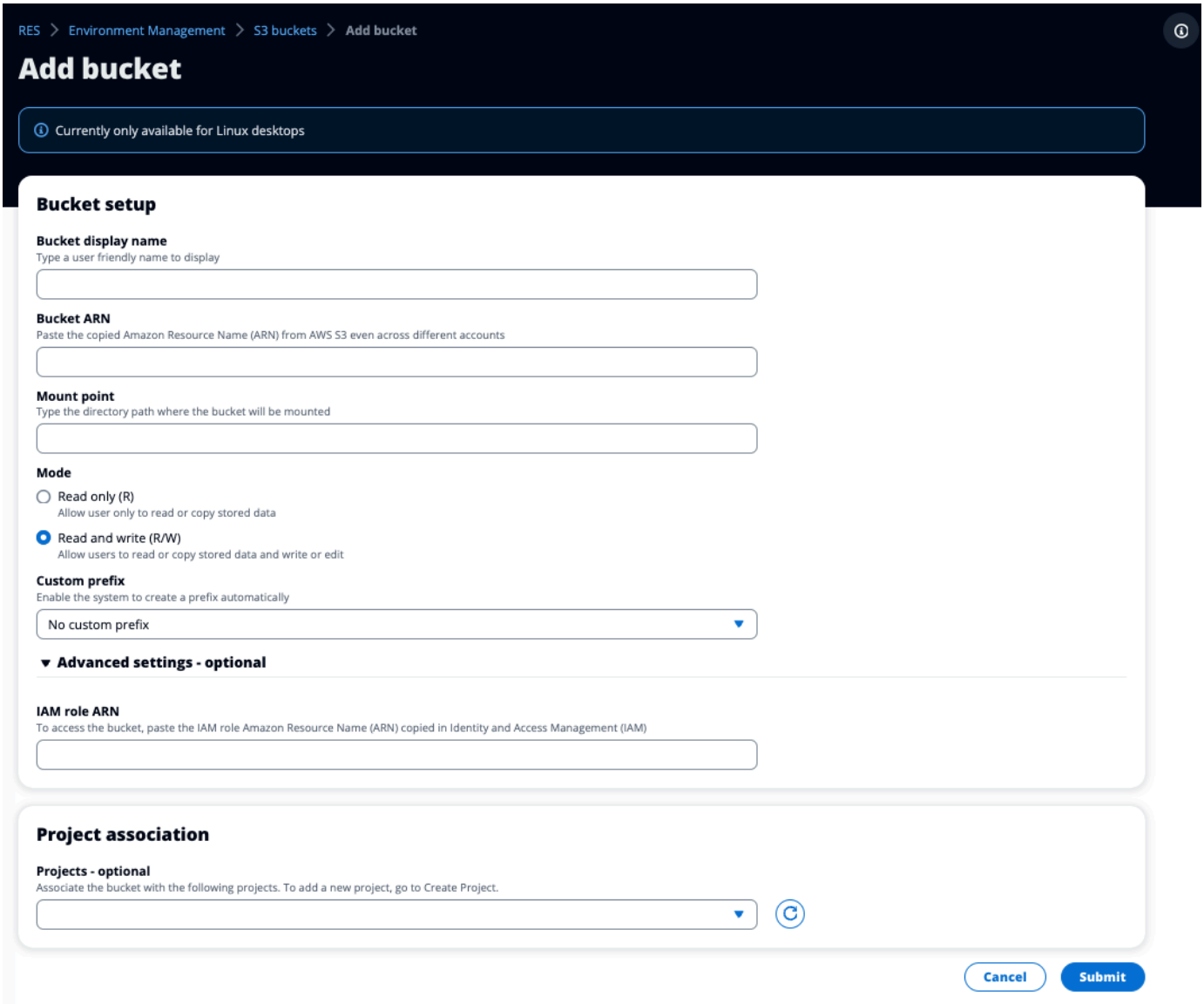
> **Important**
>
> - 指定されたバケット ARN、マウントポイント、およびモードは、作成後に変更することはできません。

- バケットには、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ARN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連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ARNするIAMロールを指定できます。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. [送信] を選択します。



Amazon S3 バケットを編集する

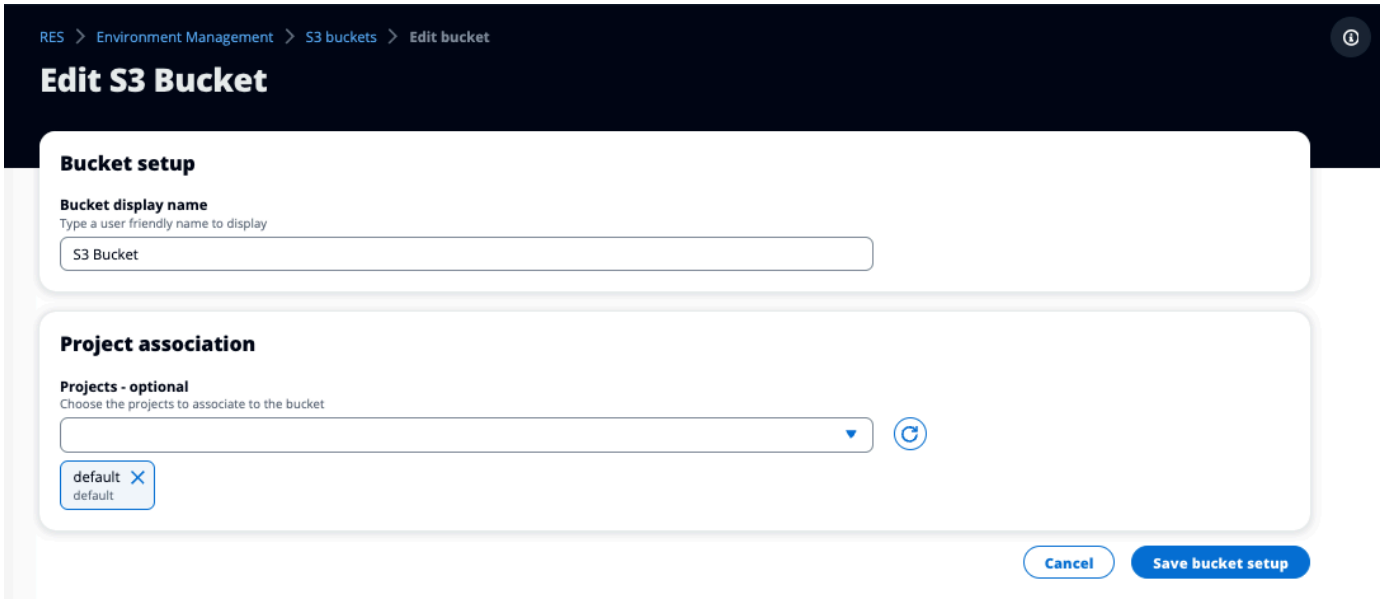
1. S3 バケットリストで S3 バケットを選択します。
2. アクションメニューから、編集 を選択します。
3. 更新を入力します。

> **Important**
>
> - プロジェクトを S3 バケットに関連付けると、バケットは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ている後にのみ、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。



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 バケットの との関連付けのみを削除しますRES。
> - バケットを削除すると、そのVDIセッションの認証情報の有効期限が切れた時点 (約 1 時間) に、既存の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

に S3 バケットを追加するとRES、バケット内のデータを特定のプロジェクトや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。

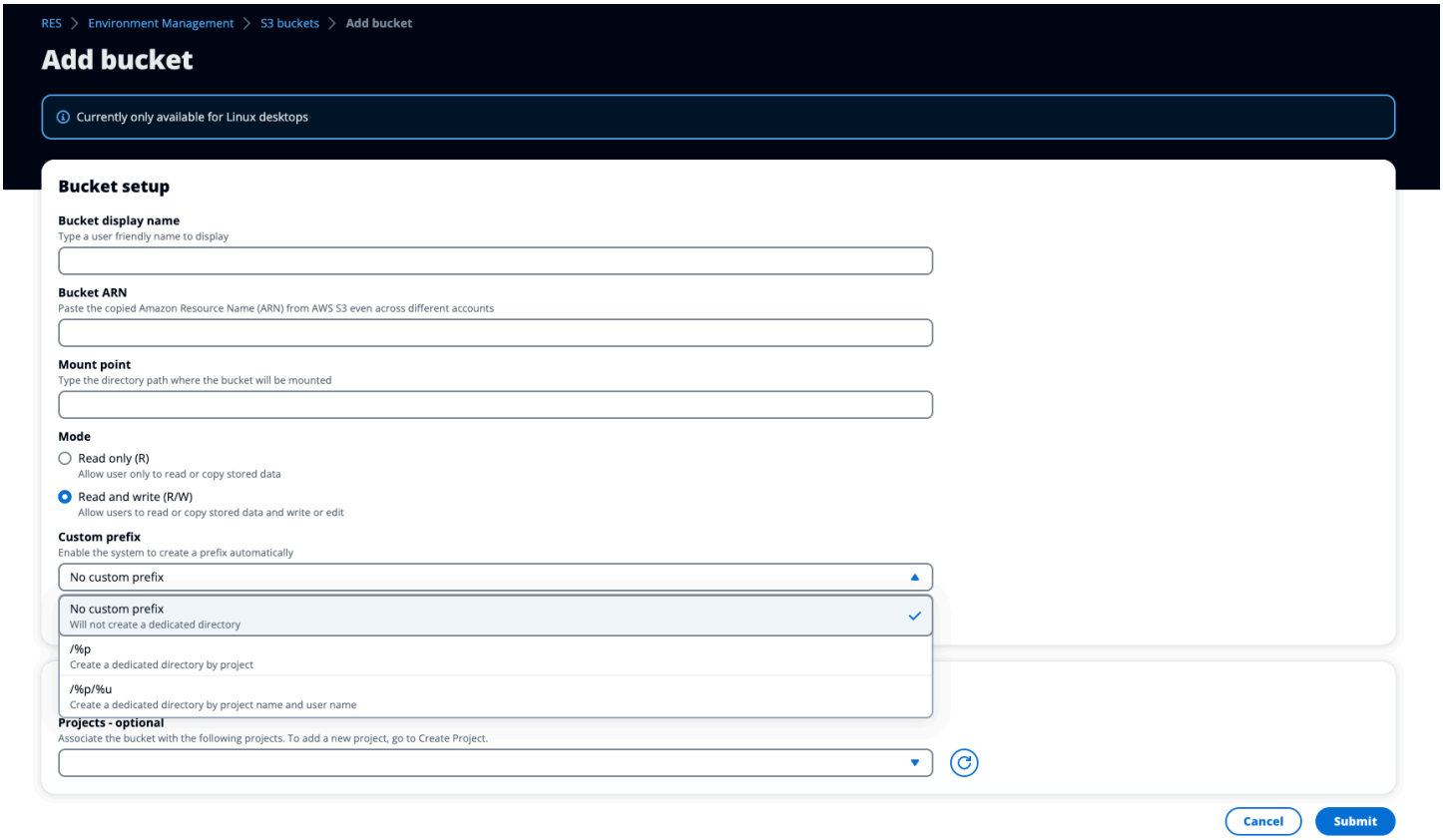
読み取り専用

`Read Only (R)` を選択した場合、バケットのプレフィックス ARN (Amazon リソースネーム) に基づいてデータ分離が適用されます。例えば、管理者が RESを使用して にバケットを追加 ARN`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VDIsから起動するユーザーは、パス *`bucket-name`*の下にある 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 にプレフィックスが追加されていない場合ARN、バケット全体はそれに関連付けられたプロジェクトで使用可能になります。

読み取りと書き込み

`Read and Write (R/W)` を選択した場合でも、前述のようにARN、バケット のプレフィックスに基づいてデータ分離が強制されます。このモードには、管理者が S3 バケットに可変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、以下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



カスタムデータ分離なし

No custom prefix カスタムプレフィックス に 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可能になります。例えば、管理者が ARN arn:aws:s3:::*bucket-name* No custom prefix RESを使用して 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 とプロジェクト B 内VDIsから起動するユーザーには、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が許可されます。

プロジェクトレベルごとのデータ分離

/%p カスタムプレフィックス に を選択すると、バケット内のデータは、バケット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。例えば、管理者が にバケットを追加し、 ARNarn:aws:s3:::*bucket-name*と のマウントポイントが/%p選択されている RESを使用する場合です。*/bucket*、および は、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 にファイルを書き込むことができます。*/bucket*。 プロジェクト A のユーザー B には、ユーザー A が書き込んだファイルも表示されます。*/bucket*。 ただし、ユーザー B がプロジェクト B VDIで を

起動し、*/bucket*、データはプロジェクトによって分離されるため、ユーザー A が書き込んだ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 VDIsからのファイルを使用する/ProjectB場合にのみアクセスできます。

プロジェクト単位、ユーザー単位のデータ分離

/%p/%u カスタムプレフィックス に 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、ユーザー名%uを表します。例えば、管理者が にバケットを追加し、 を/%p/%u選択した ARN arn:aws:s3:::*bucket-name* と のマウントポイントで RES を使用します。*/bucket*。 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 にファイルを書き込むことができます。*/bucket*。 %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、 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。*/bucket*、データは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。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 VDIsで を使用している/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、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: にデプロイRESされているアカウントにIAMロールを作成する （ 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) にアクセスする必要がある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 を選択します。
3. ポリシーの作成：
   a. [Create policy] 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 (アカウント B にある S3 バケットの名前*<BUCKET-NAME>*に置き換えます) 。

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

d. [Next (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ための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) を選択します。

6. ロールを作成する :

a. [ロールの作成] を選択します。

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. 次のJSONポリシーを貼り付けます (*<ACCOUNT_ID>*をアカウント A の実際のアカウント ID、RESデプロイの*<ENVIRONMENT_NAME>*環境名、リージョン AWS RESがデプロイされている *<REGION>*に置き換えます) 。

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

d. [Next (次へ)] を選択します。

7. アクセス許可ポリシーのアタッチ :

a. 前に作成したポリシーを検索して選択します。

b. [Next (次へ)] を選択します。

8. ロールのタグ付け、レビュー、作成 :

a. ロール名 (「S3AccessRole」など) を入力します。

b. ステップ 3 でタグの追加 を選択し、次のキーと値を入力します。

- キー: `res:Resource`
- 値: `s3-bucket-iam-role`

c. ロールを確認し、ロールの作成 を選択します。

9. で IAMロールを使用しますRES。

a. ARN 作成したIAMロールをコピーします。

b. RES コンソールにログインします。

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. バケットを追加 を選択し、クロスアカウント S3 バケット でフォームを入力しますARN。

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. ロールARNフィールドにIAM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 からバケットへのアクセスをIAMロールに付与します (置き換える *<AccountA_ID>* アカウント A の実際のアカウント ID と *<BUCKET-NAME>* S3 バケットの名前を含む):

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

c. [Save] を選択します。

プライベートでのデータ流出の防止 VPC

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 を保護しますVPC。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エンドポイントを作成する方法と、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. で Amazon https://console.aws.amazon.com/vpc/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] を選択します。
   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、「S3」と入力します `com.amazonaws.<region>.s3` (AWS リージョン*<region>*に置き換えます) 。
   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設定：
   a. ではVPC、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、デプロイ時に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. Enable DNS name の場合、 オプションがチェックされ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. ポリシー で、カスタム 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 (置き換える *mybucket* S3 バケット名 および *111122223333* また、*444455556666* アクセスIDsする適切な AWS アカウントを持つ)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::mybucket",
                "arn:aws:s3:::mybucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",   // Your Account ID
                        "444455556666"    // Another Account ID
                    ]
                }
            }
        }
    ]
}
```

5. 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. エンドポイントを作成したら、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 にマウントされないかどうかを確認する方法 VDI

バケットが にマウントできない場合VDI、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 VDIを介して 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 ログを確認する：

   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ゲートウェイ CloudWatch ログの確認：

   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-lambdavdccustomcredentialbrokerapigatewayaccesslogs<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置き換えを入力 `<filesystem_id>` 変更する必要があるファイルシステムの値。
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、正しいIAMロール で値が正しく設定されていることを確認しますARN。

   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。
      - キー属性には、 と入力しますshared-storage.`<filesystem_id>`.s3_bucket.iam_role_arn。
      - 正しいIAMロール を追加しますARN。
   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ロールの影響を受ける VDIs が再度マウントARNされていることを確認します。

の有効化 CloudTrail

CloudTrail コンソールを使用して アカウント CloudTrail で を有効にするには、AWS CloudTrail 「 ユーザーガイド」の「 CloudTrail コンソールを使用した証跡の作成」の手順に従ってください。CloudTrail は、アクセスしたIAMロールを記録して 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際のガイダンスを提供します。

トピック

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をプリインストールして設定して 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

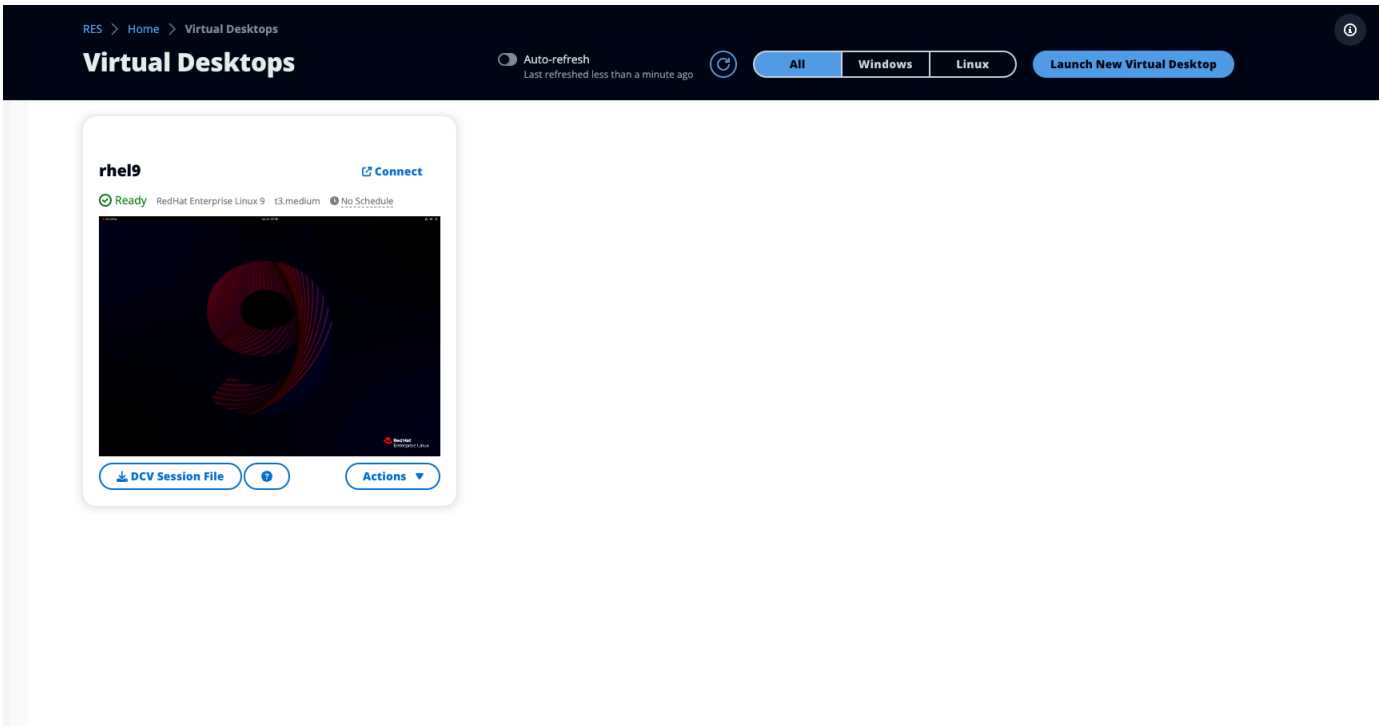
RES 現在、 は、次のオペレーティングシステムを使用した仮想デスクトップの起動をサポートしています。

- Amazon Linux 2 (x86 および ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL 8 (x86)、9 (x86)
- Windows 2019、2022 (x86)

トピック

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の起動 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. [送信] を選択します。

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。

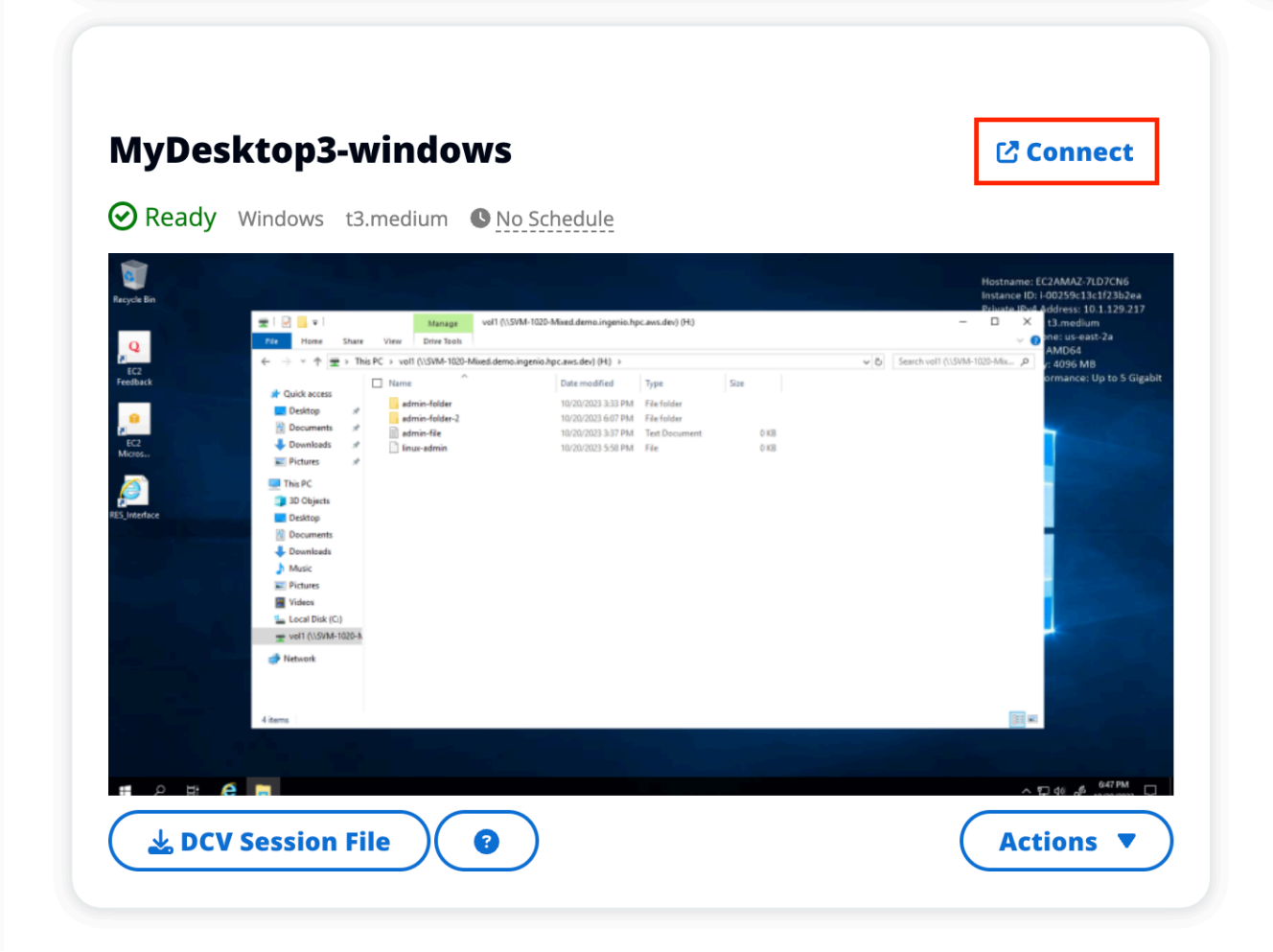
デスクトップにアクセスする

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。

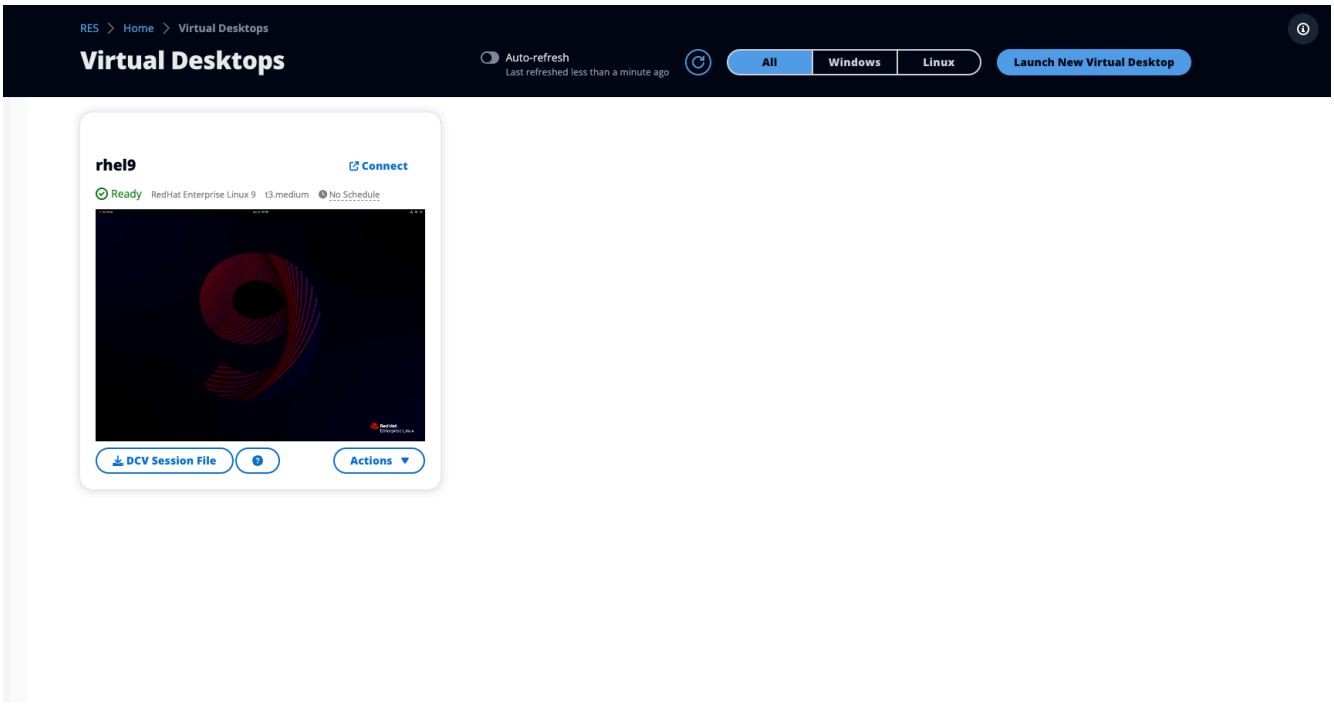
- Connect を選択するか、サムネイルを選択してブラウザから直接デスクトップにアクセスします。



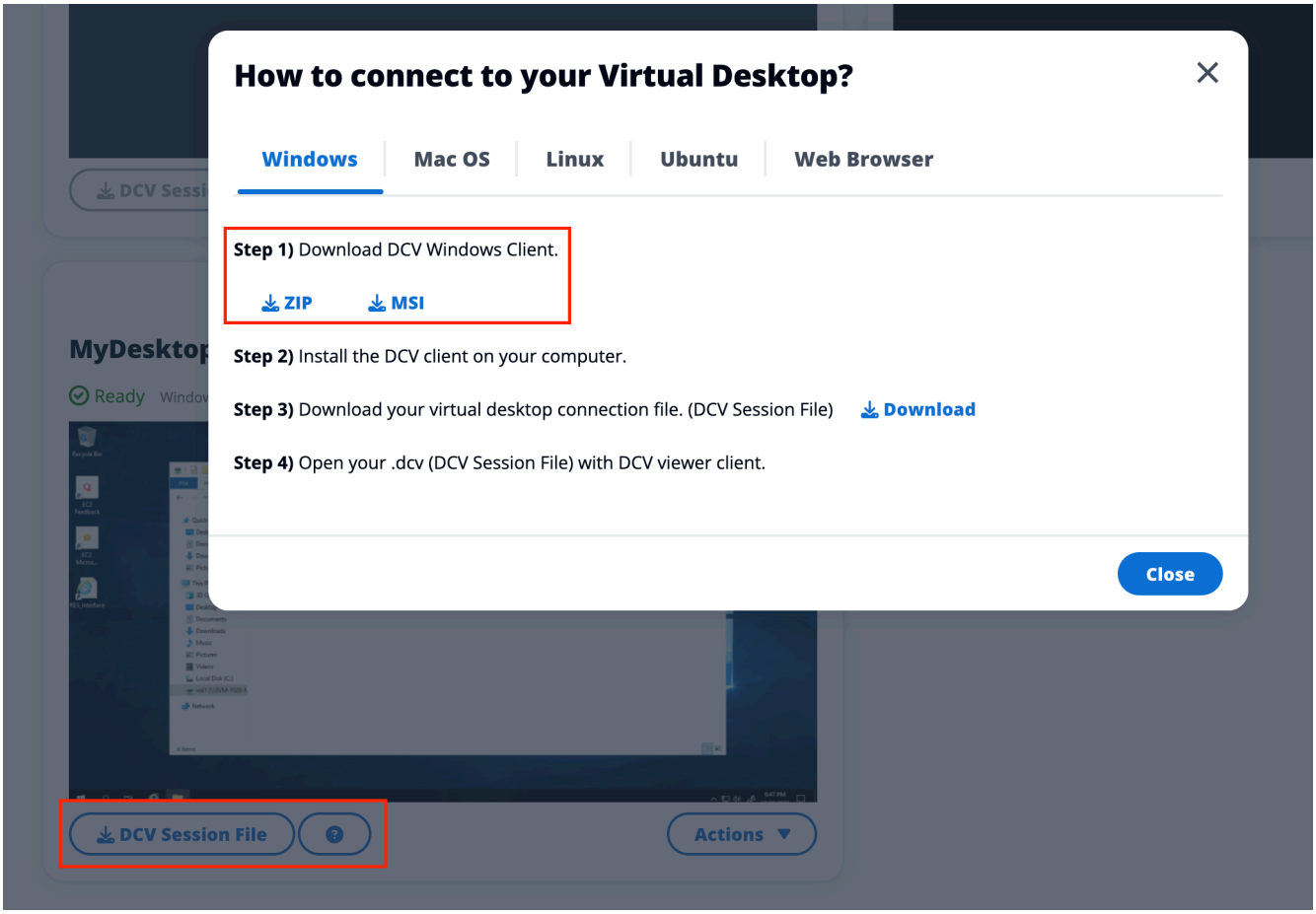
DCV connection

DCV クライアント経由で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。経由で にアクセスするにはDCV :

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。システムにDCV クライアントをインストールする必要があります。



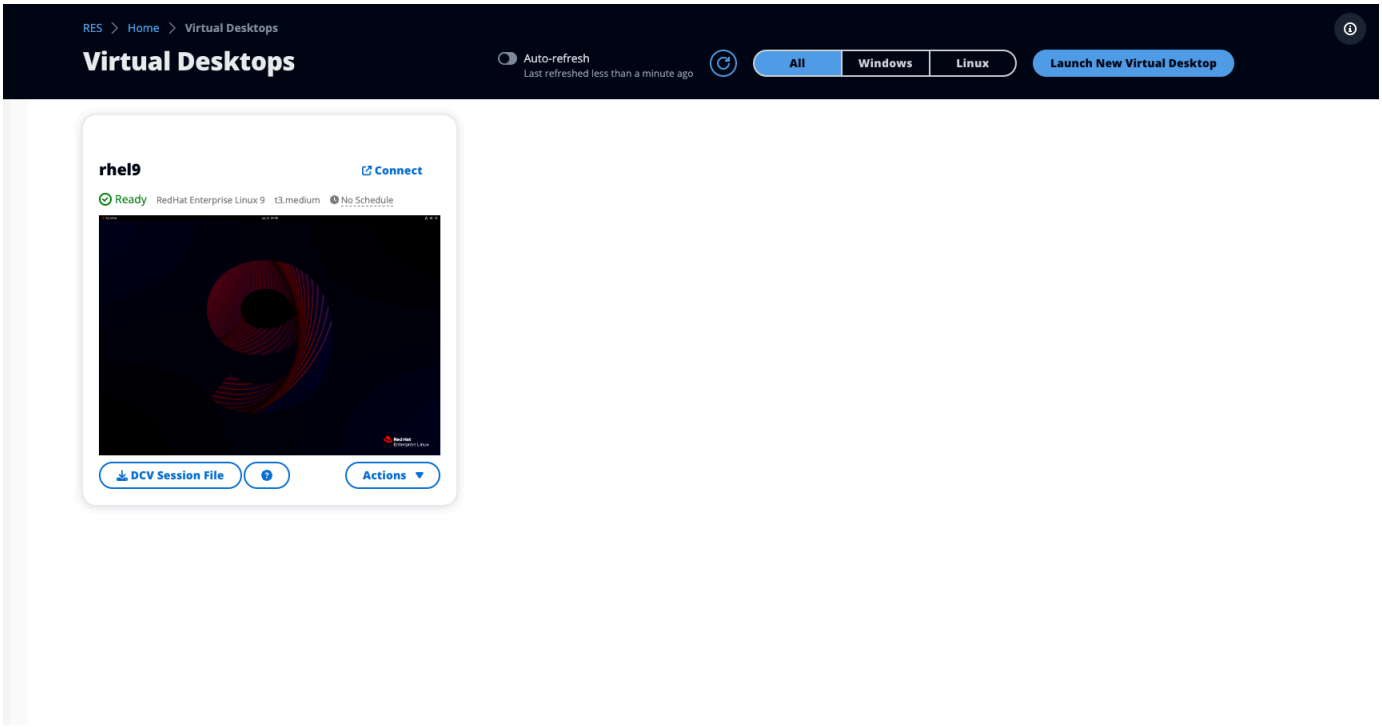
2. インストール手順については、？ アイコンを選択します。



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。

   - [Stop] (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

     セッションを永続的に終了します。一時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

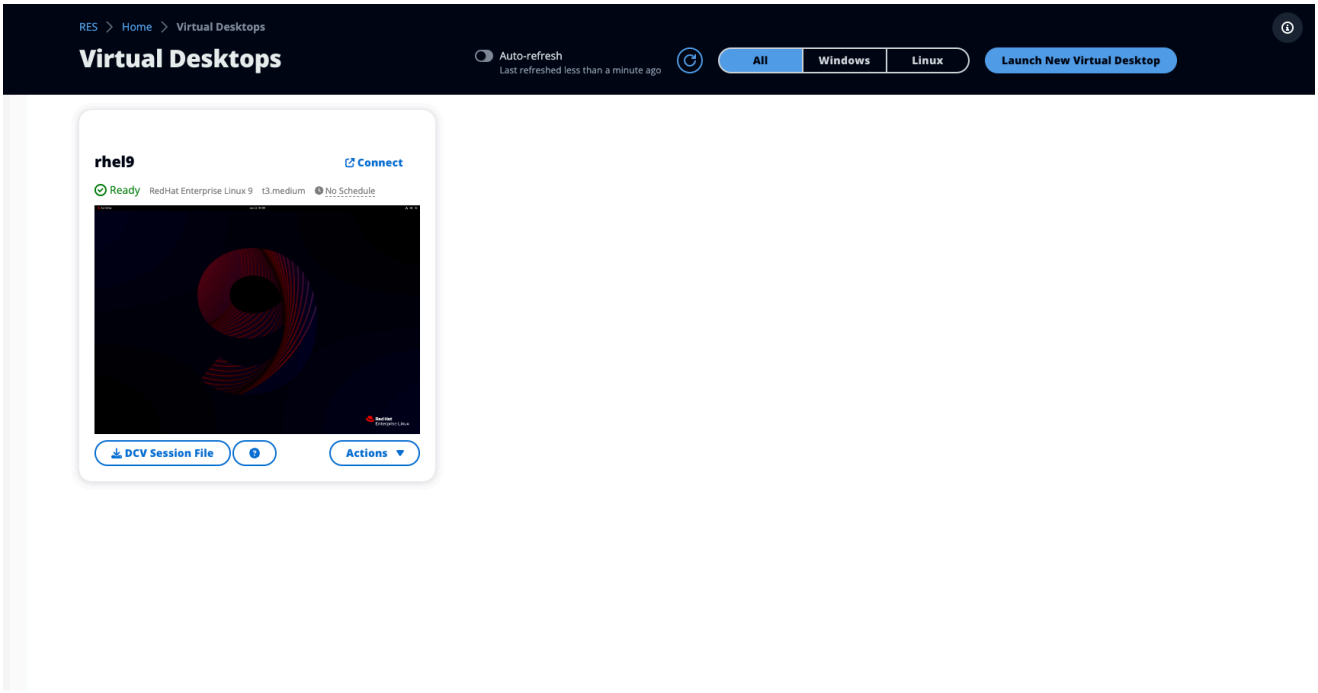
     デスクトップの状態はメモリに保存されます。デスクトップを再起動すると、アプリケーションは再開されますが、リモート接続が失われる可能性があります。すべてのインスタンスが休止をサポートしているわけではなく、このオプションはインスタンスの作成中に有効になっていた場合にのみ使用できます。インスタンスがこの状態をサポートしているかどうかを確認するには、「休止の前提条件」を参照してください。

仮想デスクトップの変更

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. [Stop] (停止) を選択します。

> **Note**
>
> 休止状態のセッションのデスクトップサイズを更新することはできません。

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. [送信] を選択します。
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。

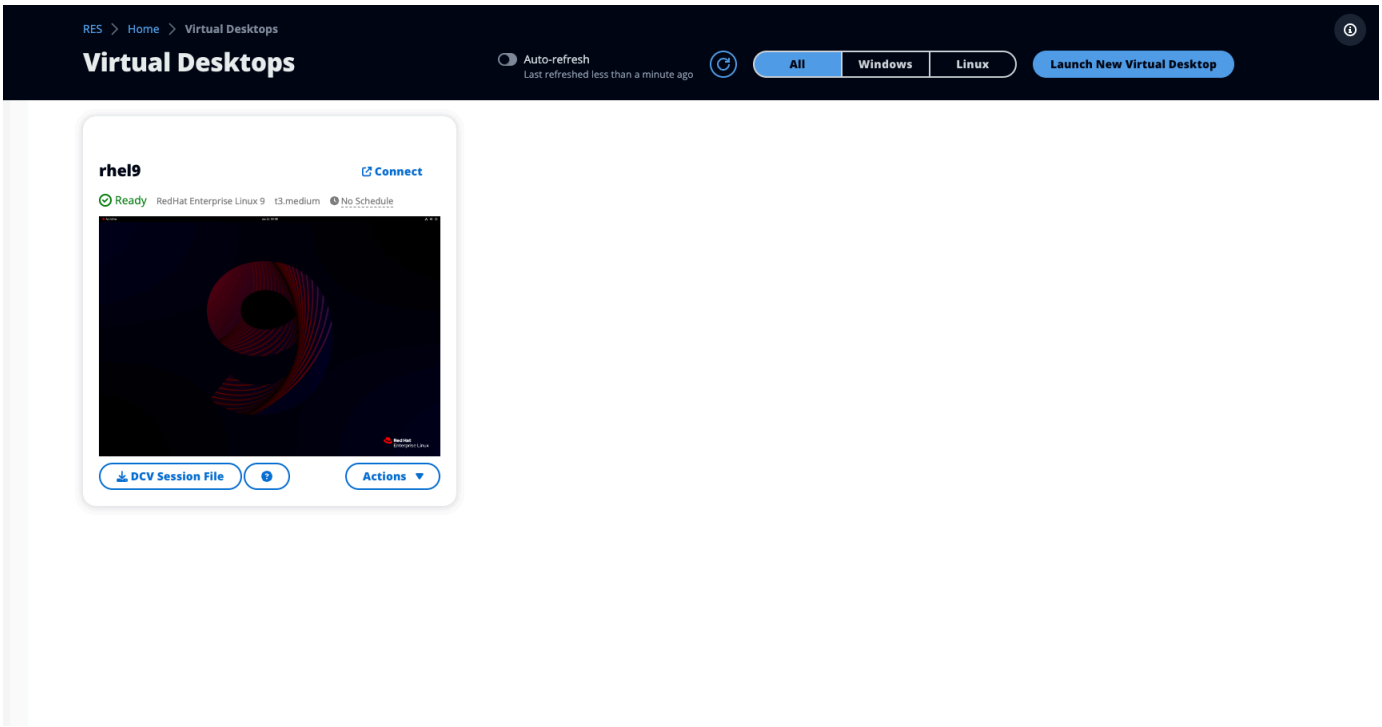
   a. [アクション] を選択します。

b. Virtual Desktop State を選択します。

c. [開始] を選択します。

セッション情報の取得

1. [アクション] を選択します。

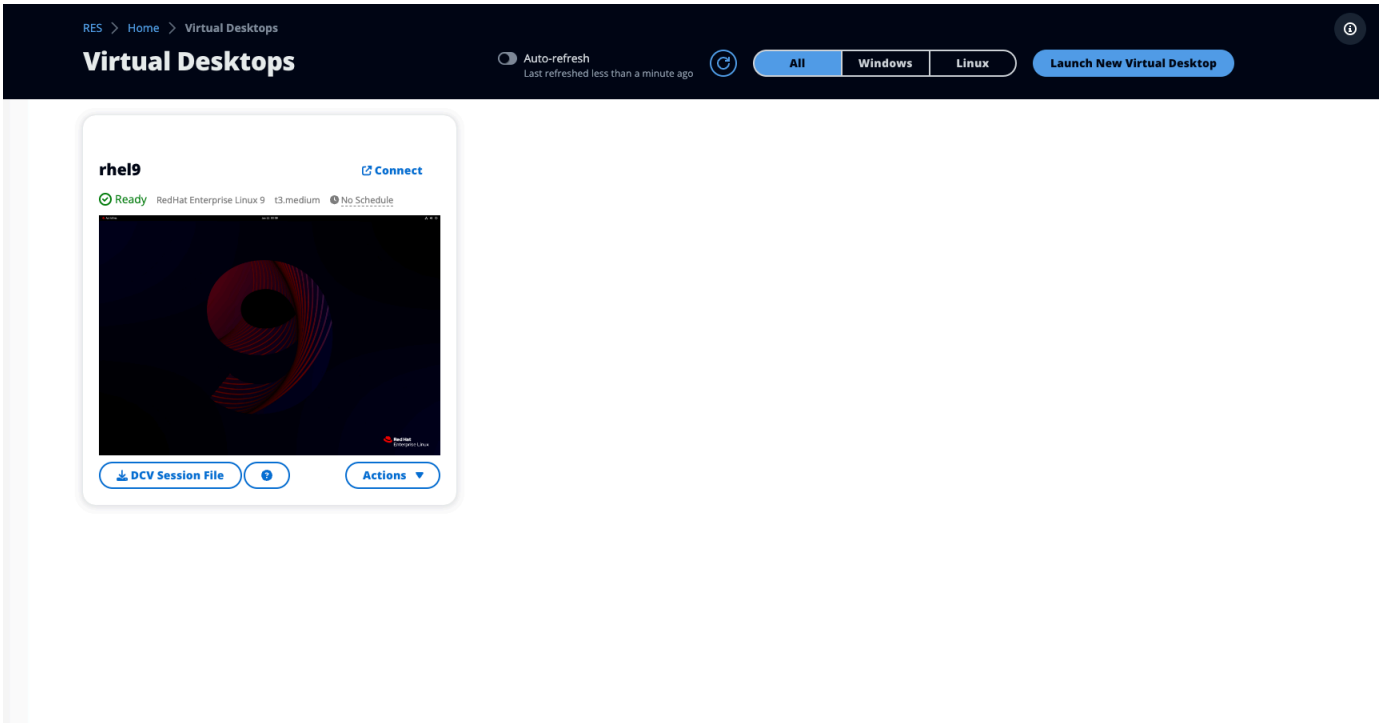


2. 情報の表示 を選択します。

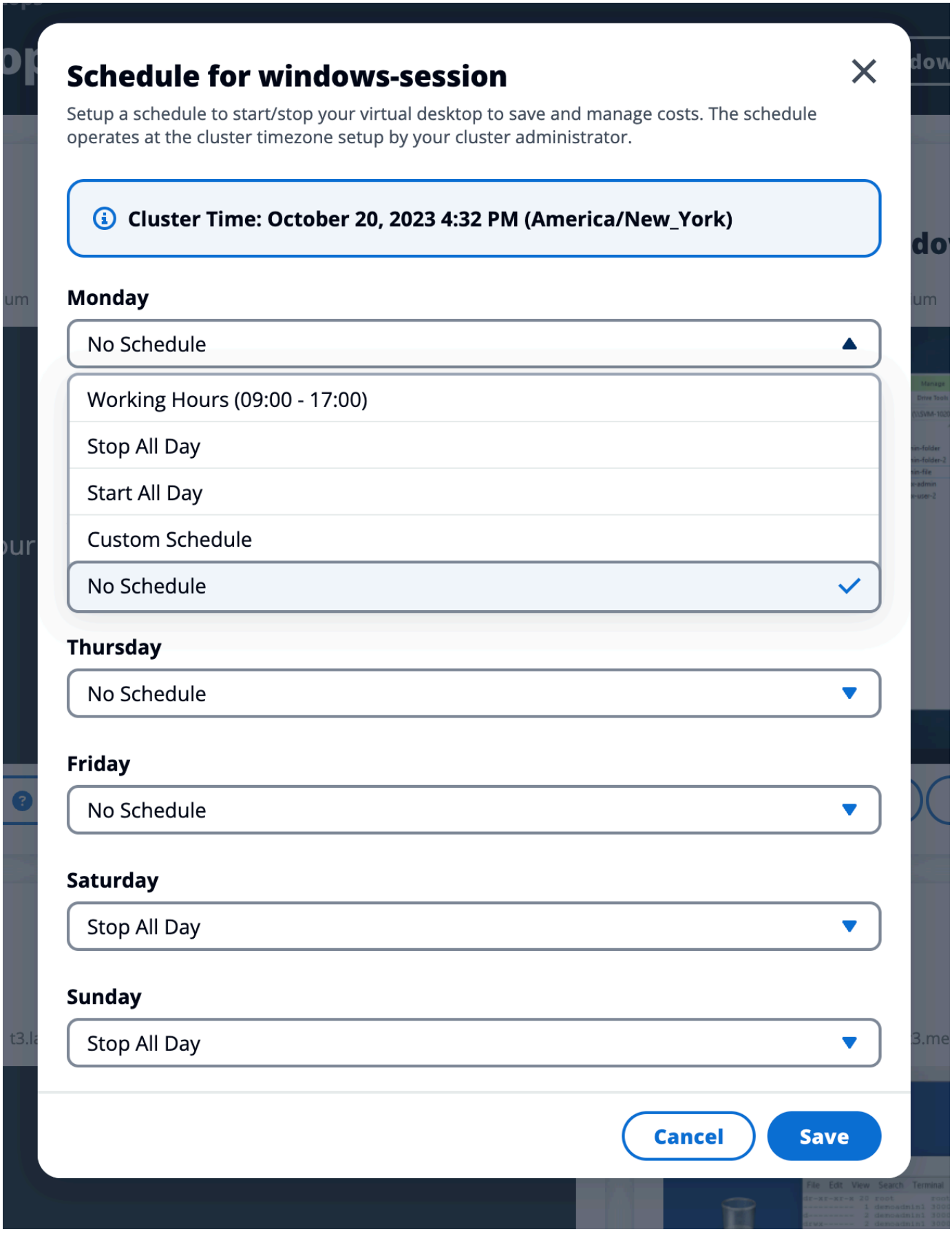
仮想デスクトップをスケジュールする

デフォルトでは、仮想デスクトップにはスケジュールがなく、セッションを停止または終了するまでアクティブのままになります。また、デスクトップはアイドル状態でも停止し、誤って停止しないようにします。アイドル状態は、アクティブな接続がなく、15 分以上 15% 未満のCPU使用状況によって決まります。デスクトップを自動的に開始および停止するようにスケジュールを設定できます。

1. [アクション] を選択します。



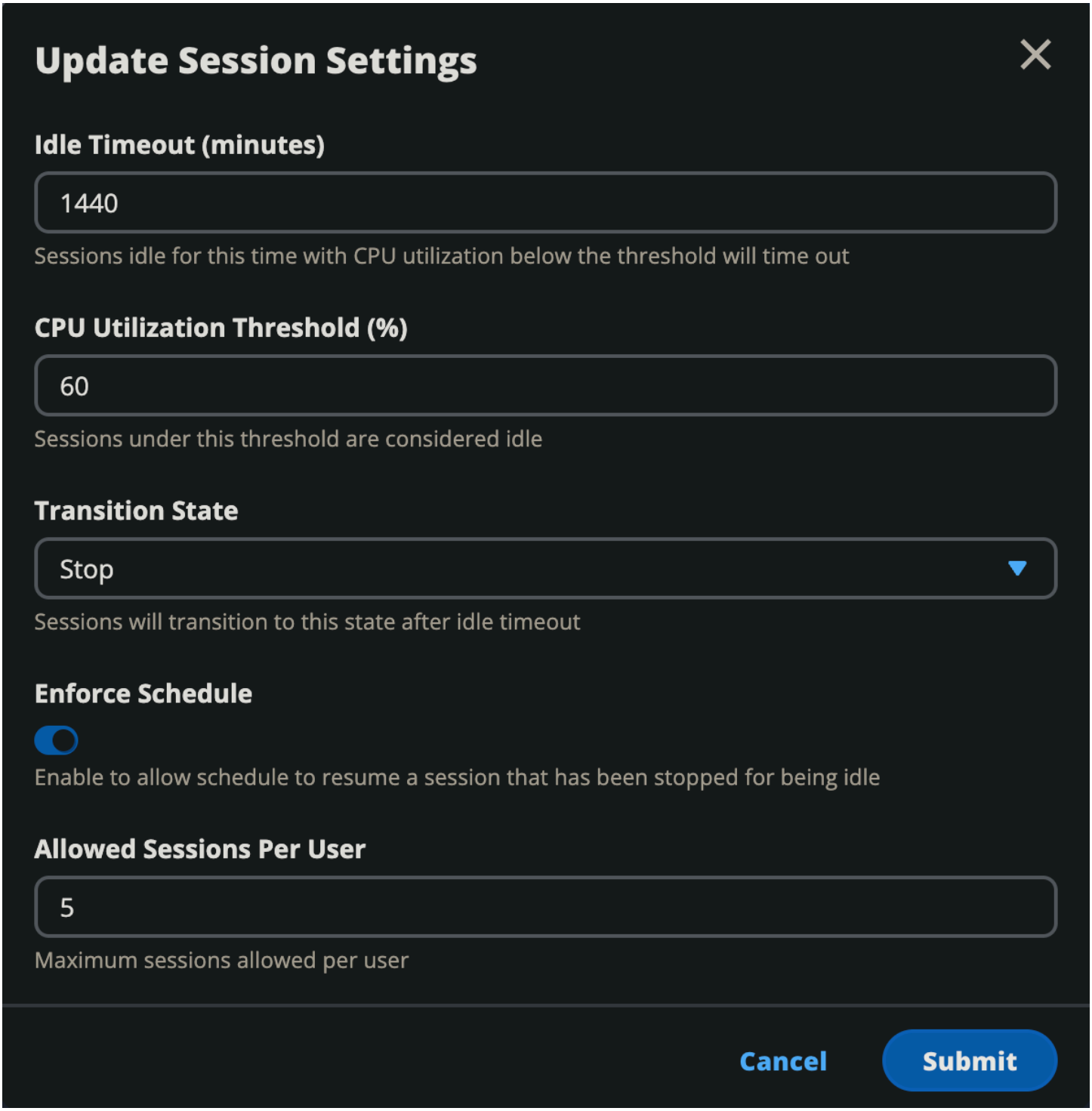
2. [スケジュール] を選択します。
3. 日ごとにスケジュールを設定します。
4. [Save] を選択します。


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

仮想デスクトップインターフェイスの自動停止

管理者は、アイドル状態のVDIs停止または終了を許可するように設定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はみなされません。
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 (停止または終了) に移行します。
4. スケジュールの強制: 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。

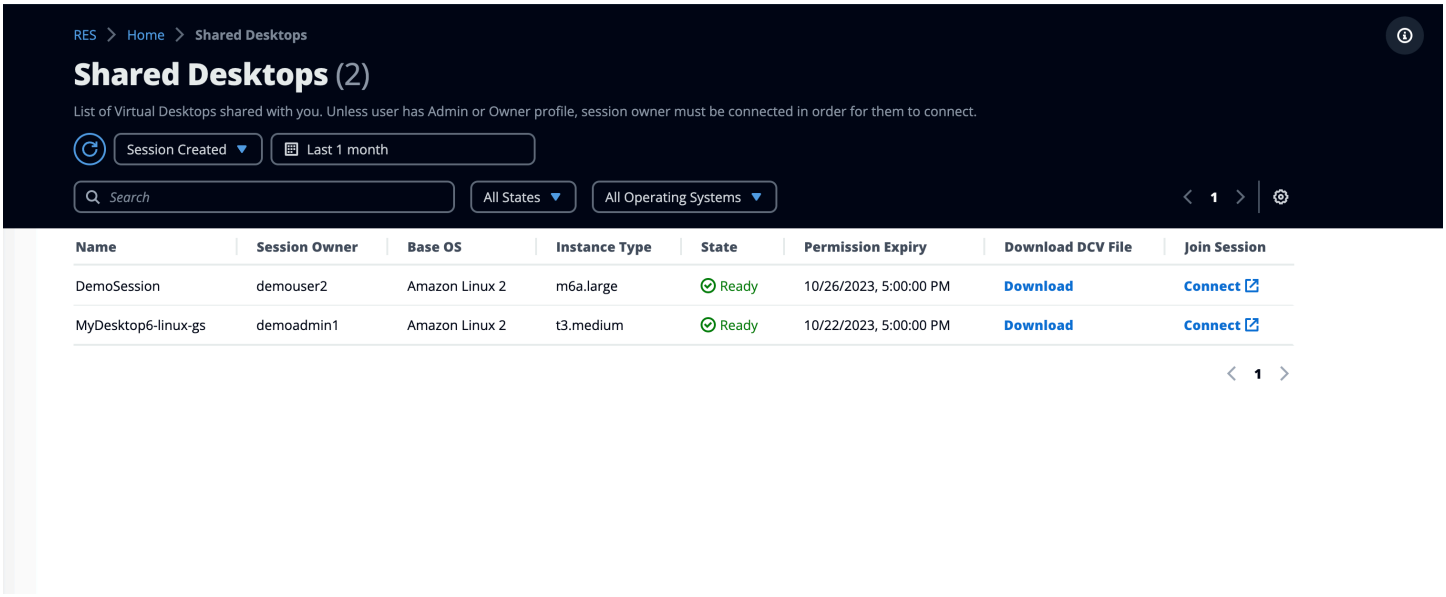


これらの設定は、サーバータブのデスクトップ設定ページにあります。要件に従って設定を更新したら、送信をクリックして設定を保存します。新しいセッションでは、更新された設定が使用されますが、既存のセッションでは、起動時に使用していた設定が引き続き使用されることに注意してください。

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、共有された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、ユーザーが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。



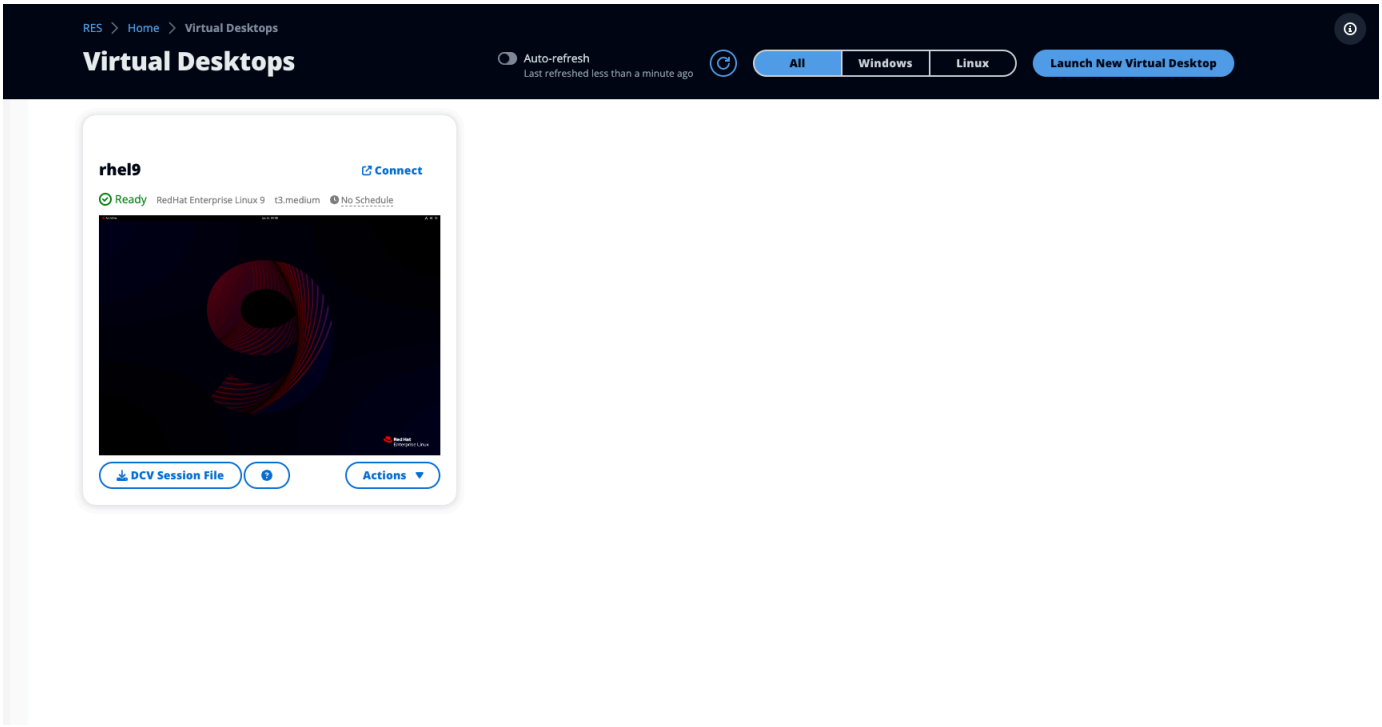
セッションの共有中に、コラボレーターのアクセス許可を設定できます。例えば、コラボレーションしているチームメイトに読み取り専用アクセスを付与できます。

トピック

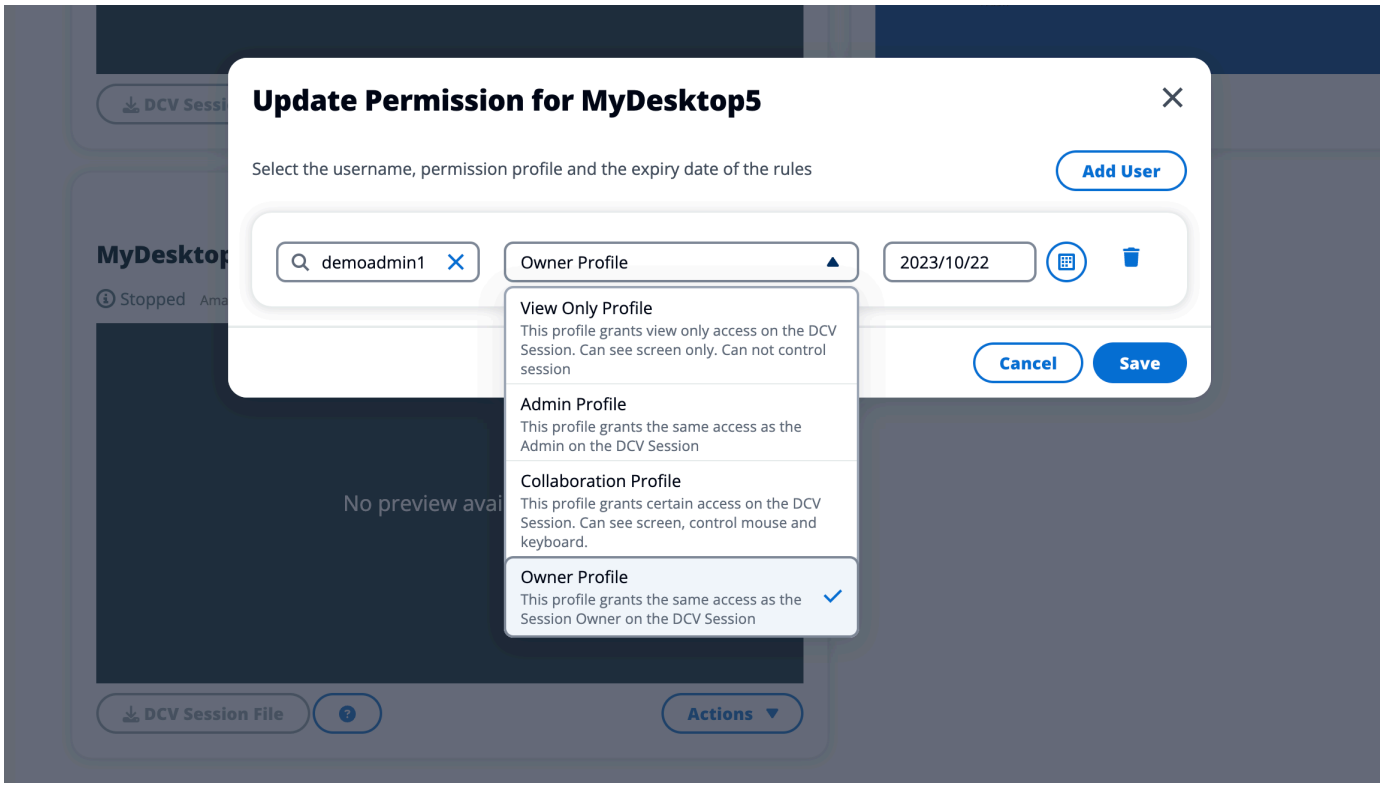
- デスクトップを共有する
- 共有デスクトップにアクセスする

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. [Save] を選択します。



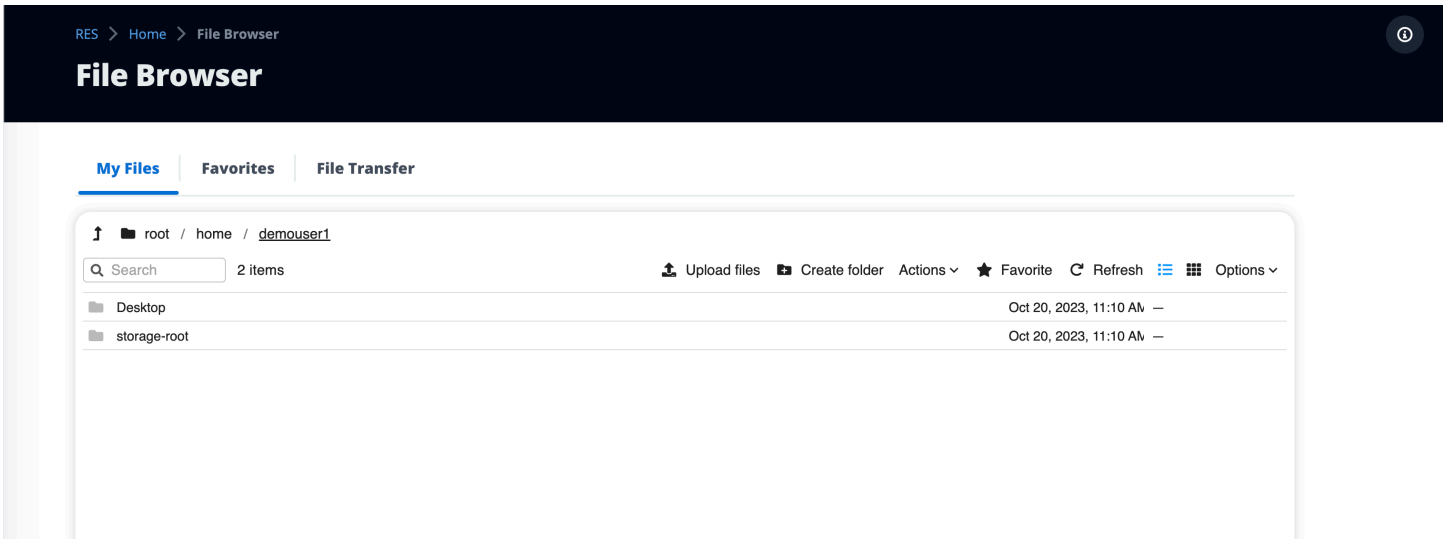
アクセス許可の詳細については、「」を参照してくださいthe section called “アクセス許可ポリシー”。

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 で参加できますDCV。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でアクセスするアクセス許可を持つすべての利用可能なファイルを管理できます。バックエンドストレージ (Amazon EFS) は、すべての Linux ノードで使用できます。Linux ノードと Windows ノードでは、 FSx の ONTAP を使用できます。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。

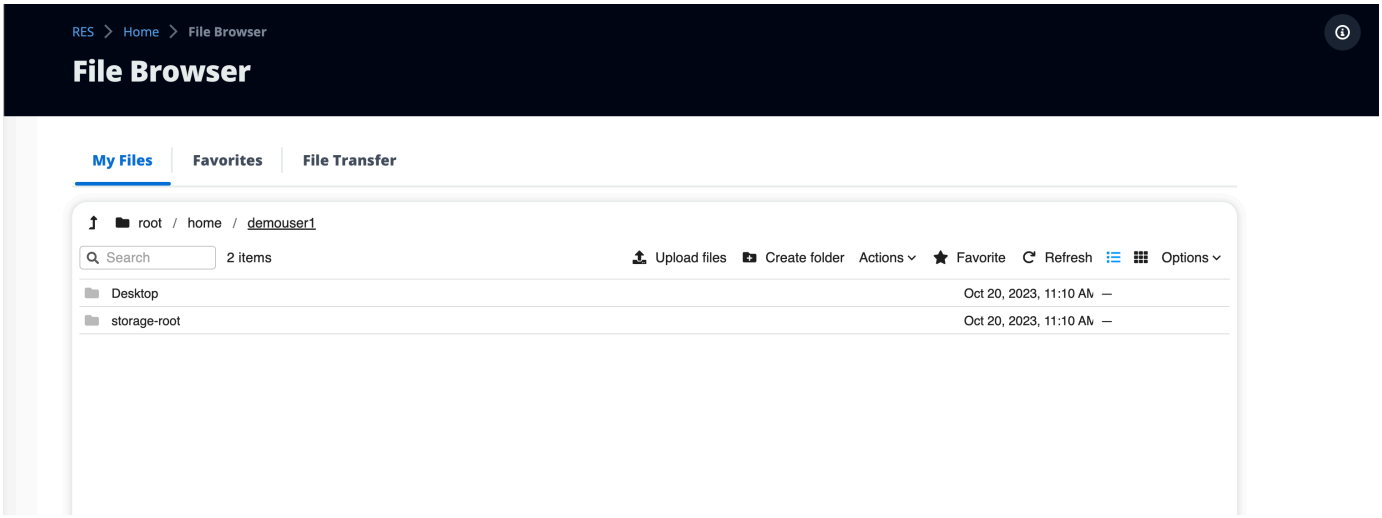


トピック

- 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
- ファイルの編集
- ファイルの転送

ファイルのアップロード (複数可)

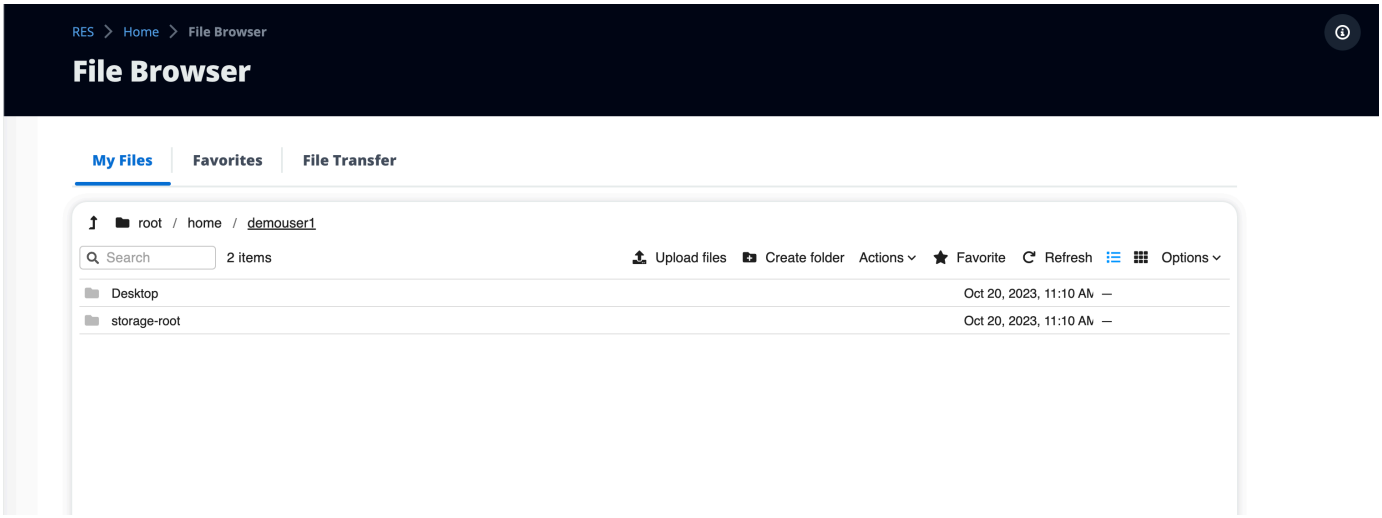
1. ファイルのアップロード を選択します。



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。



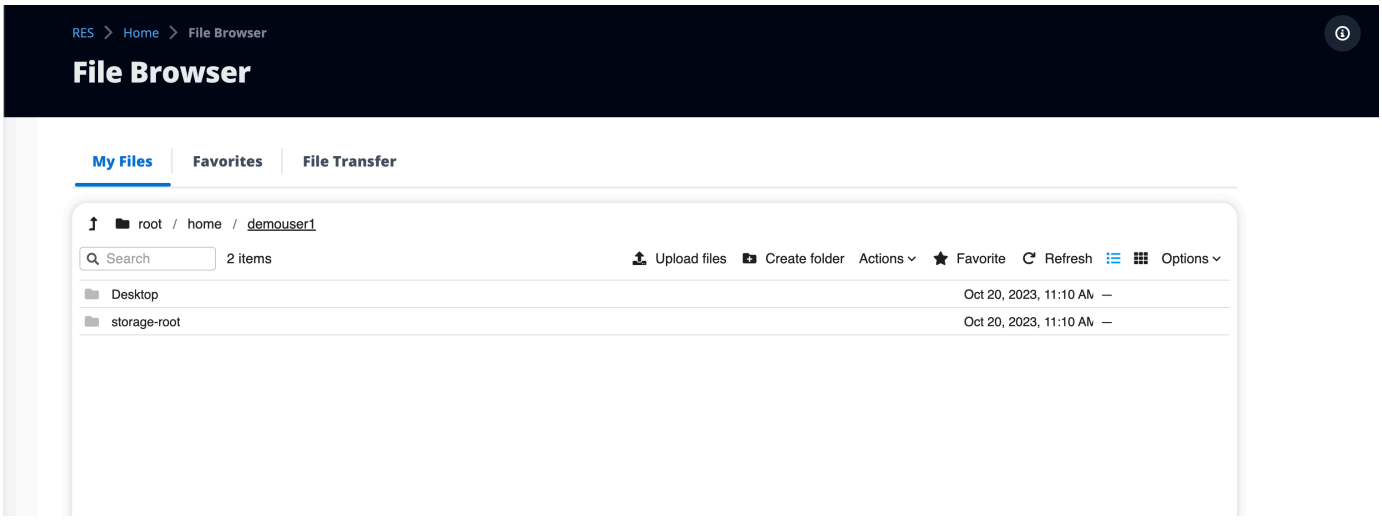
2. [アクション] を選択します。
3. ファイルの削除 を選択します。

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

重要なファイルと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。

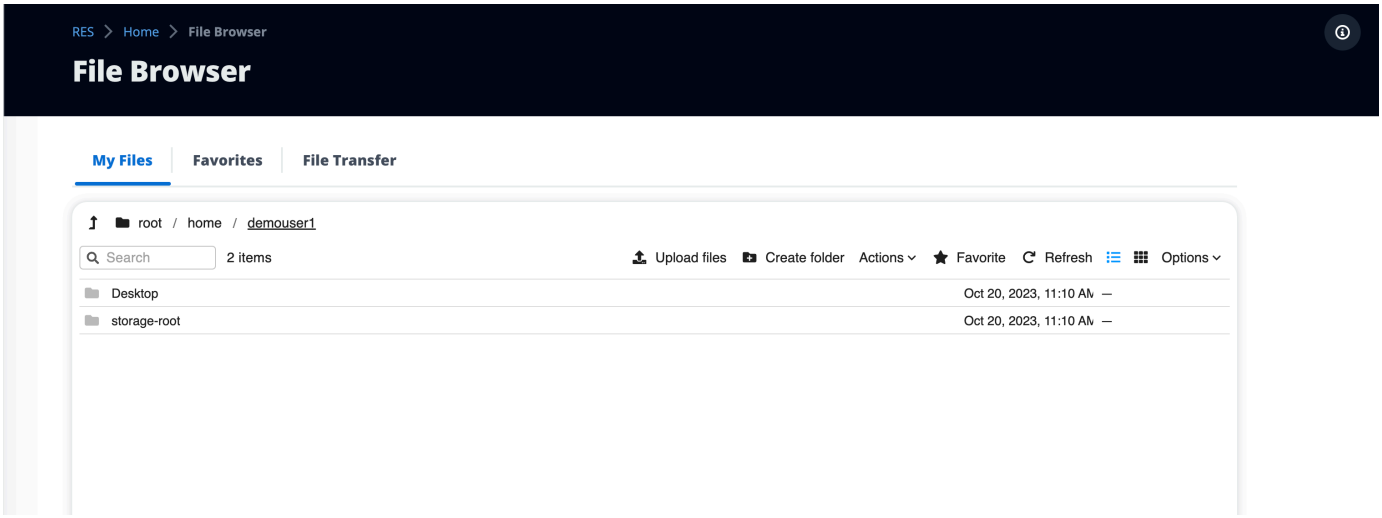
または、任意のファイルまたはフォルダを右クリックし、お気に入り を選択します。

> **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。

ファイルの編集

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。

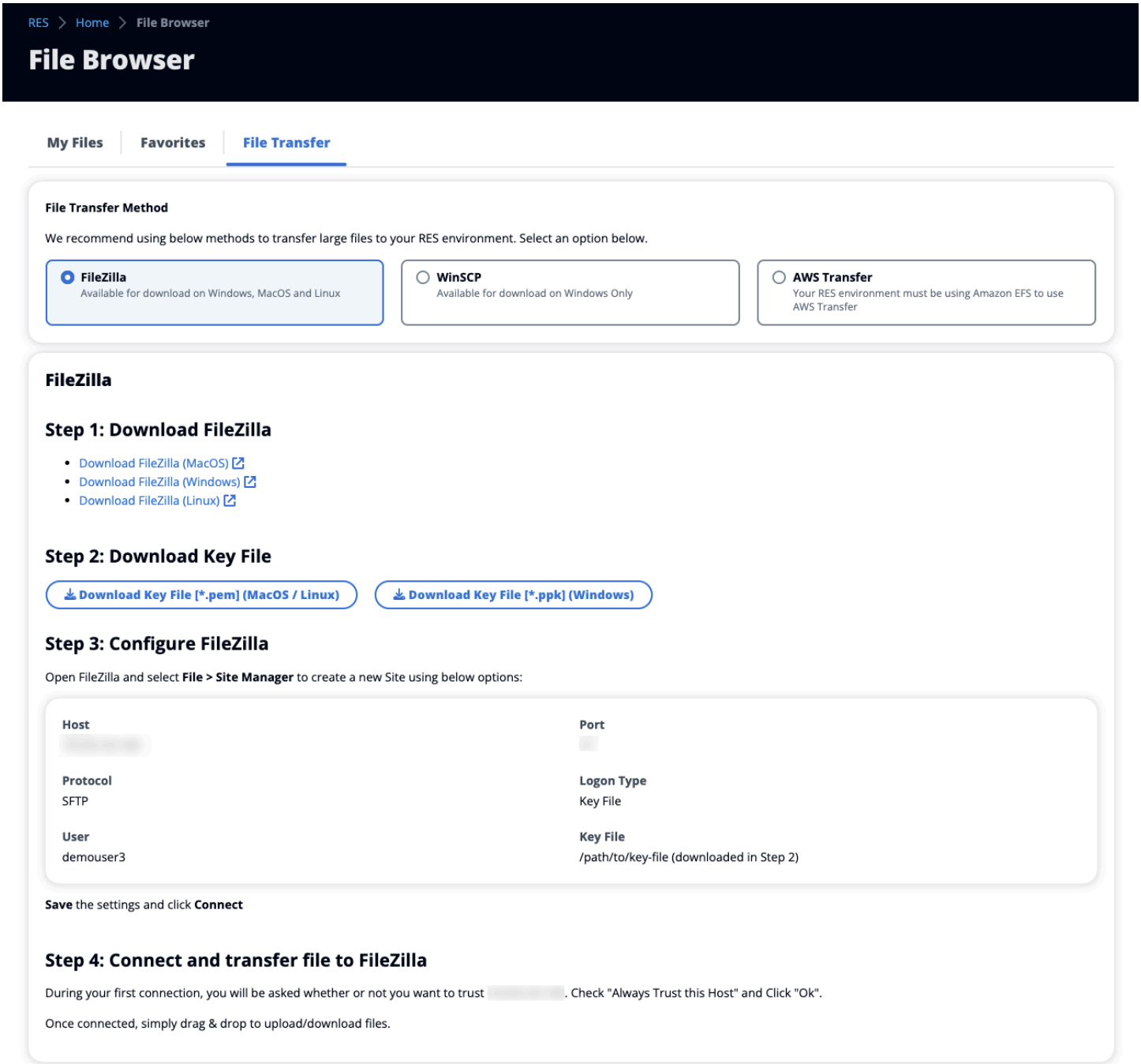


2. 更新を行い、 の保存 を選択します。

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)
- 勝利SCP (Windows)
- AWS Transfer for FTP (Amazon EFS)


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

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
- 問題 RunBooks
- 既知の問題

詳細な内容：

- (2024.04 - 2024.04.02) Linux 仮想デスクトップが再起動時にRESUMING「」ステータスで停止してい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
- (2024.06 以前) AD 同期RES中に 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 のセキュリティ脆弱性 VDIs

一般的なデバッグとモニタリング

このセクションでは、 内の情報の場所について説明しますRES。

- 便利なログおよびイベント情報ソース
  - 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と Amazon EC2 Auto Scaling Group 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

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る保持されている情報源はさまざまです。

環境 Amazon EC2インスタンスのログファイル

ログファイルは、 が使用している Amazon EC2インスタンスに存在しますRES。SSM Session Manager 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にセッションを開くことができます。

クラスターマネージャーや vdc コントローラー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/ssd/
- /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、以下の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

Windows 仮想デスクトップインスタンスのログは、 で確認できます。

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

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\NICEDCV\Server\bin

Windows では、NICEDCV証明書ファイルは以下にあります。

- C:\Windows\System32\config\systemprofile\AppData\Local\NICEdcv\

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。その中のログエントリは、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に有用な情報を提供します。

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
  - 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、記述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"
```

問題を監視するもう 1 つの方法は、目的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。

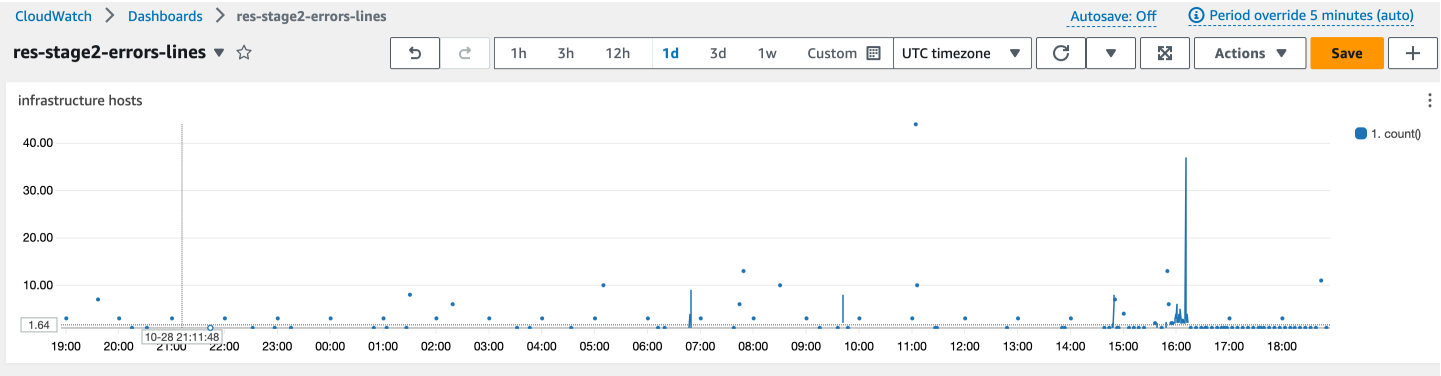
例としては、文字列エラーの発生をカウントERRORし、線としてグラフ化するウィジェットを作成します。この方法により、パターン変更が発生したことを示す潜在的な問題や傾向の発生を簡単に検出できます。

以下は、インフラストラクチャホストの の例です。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

環境の作成中に作成された 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>-bastion-host

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 高性能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

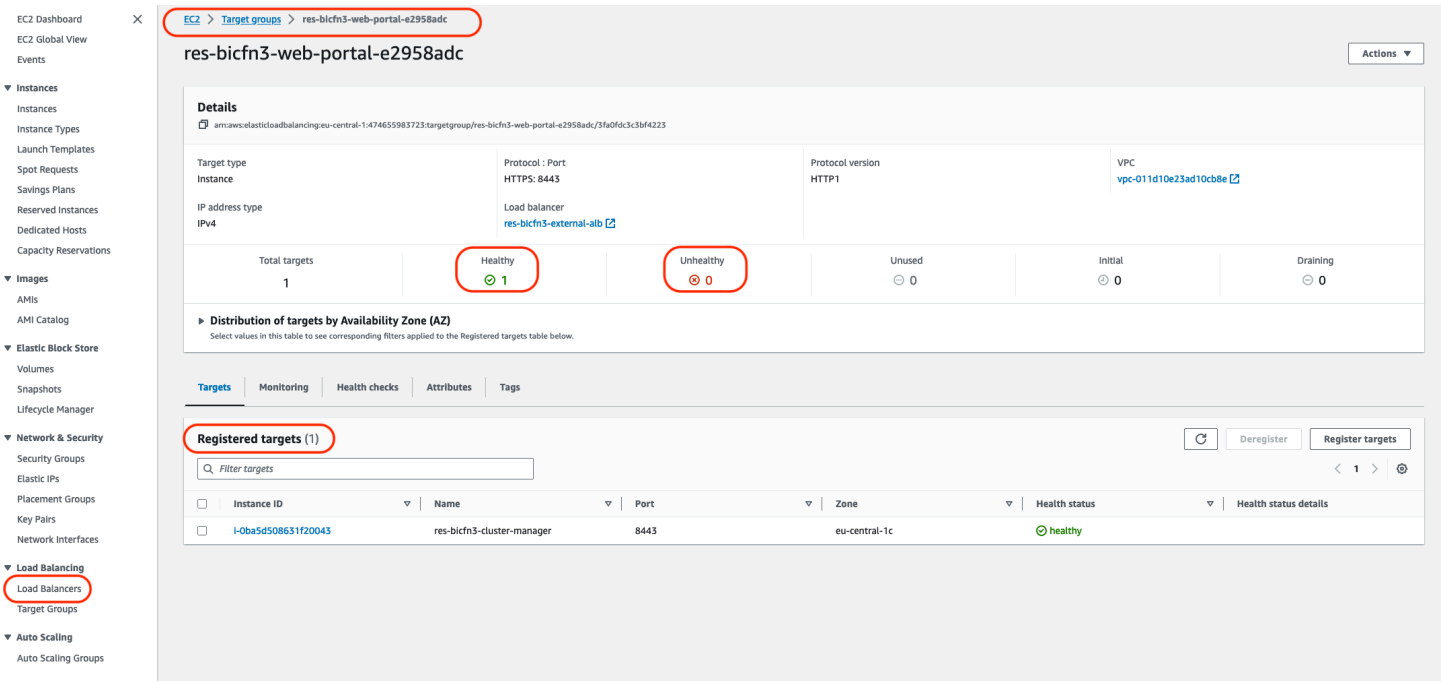
問題によるシステム障害と Amazon EC2 Auto Scaling Group アクティビティに反映される

がサーバーエラーRESUIs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の検出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確認し、関連する の Auto Scaling Group Activity タブをチェックASG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にセッションを開き、インスタンスが異常としてマークされ、 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ASG。

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。

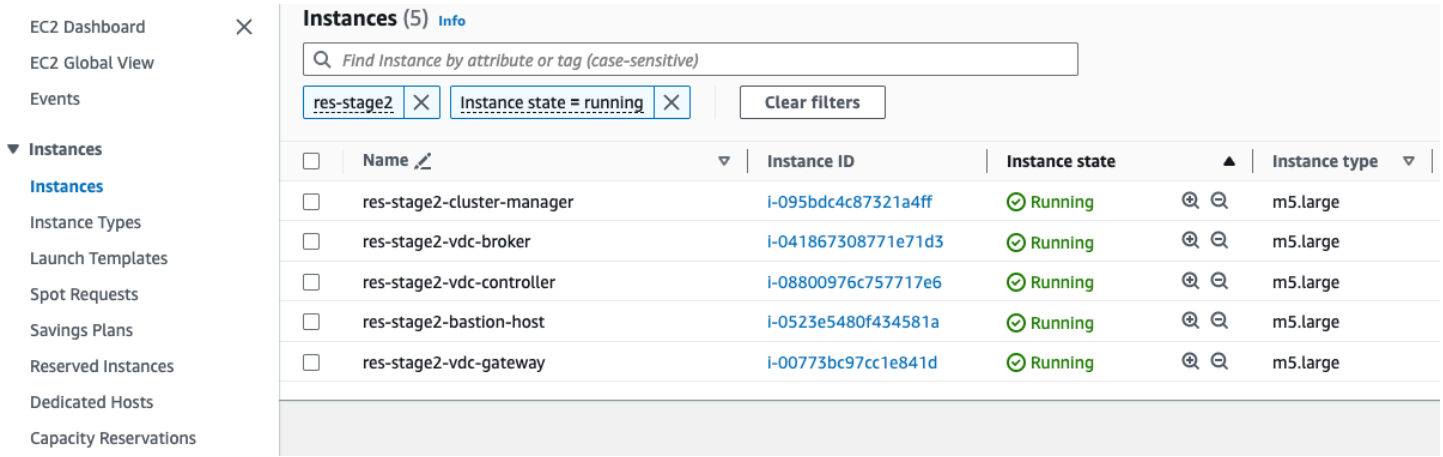


一般的な Amazon EC2 コンソールの外観

このセクションでは、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を示します。

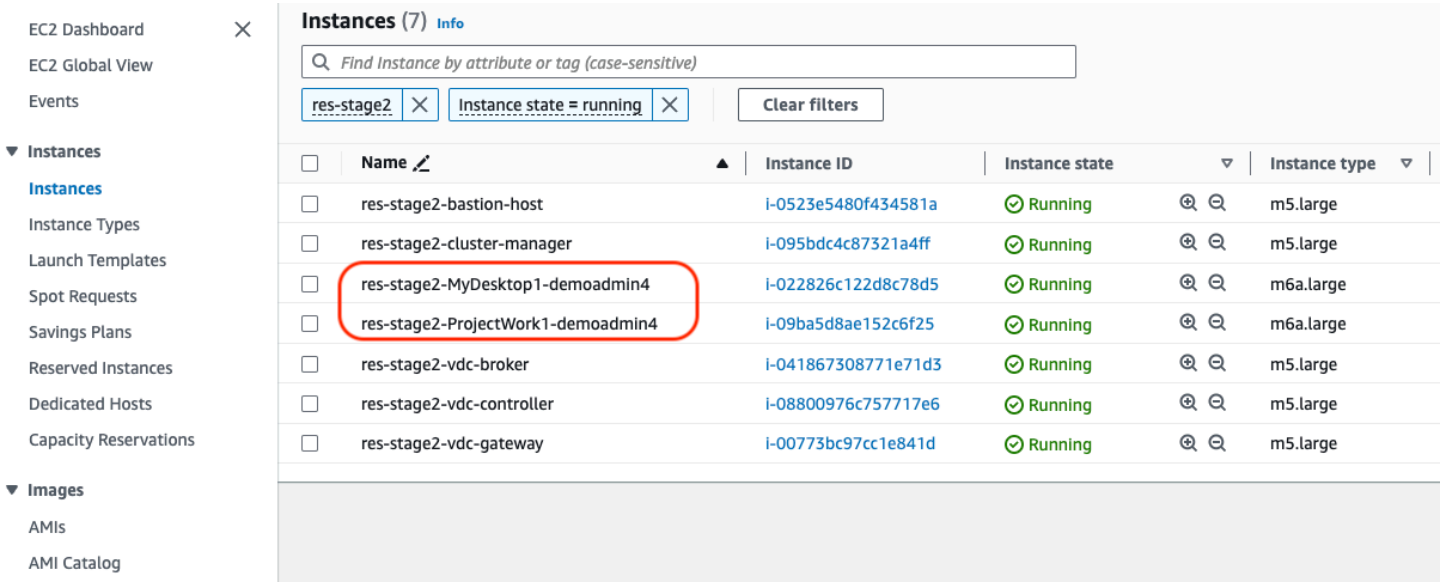
インフラストラクチャホスト

Amazon EC2コンソールは、デスクトップが実行されていない場合、通常次のような状態になります。表示されるインスタンスは、Amazon EC2ホストのRESインフラストラクチャです。インスタンス名のプレフィックスはRES環境名です。



インフラストラクチャホストと仮想デスクトップ

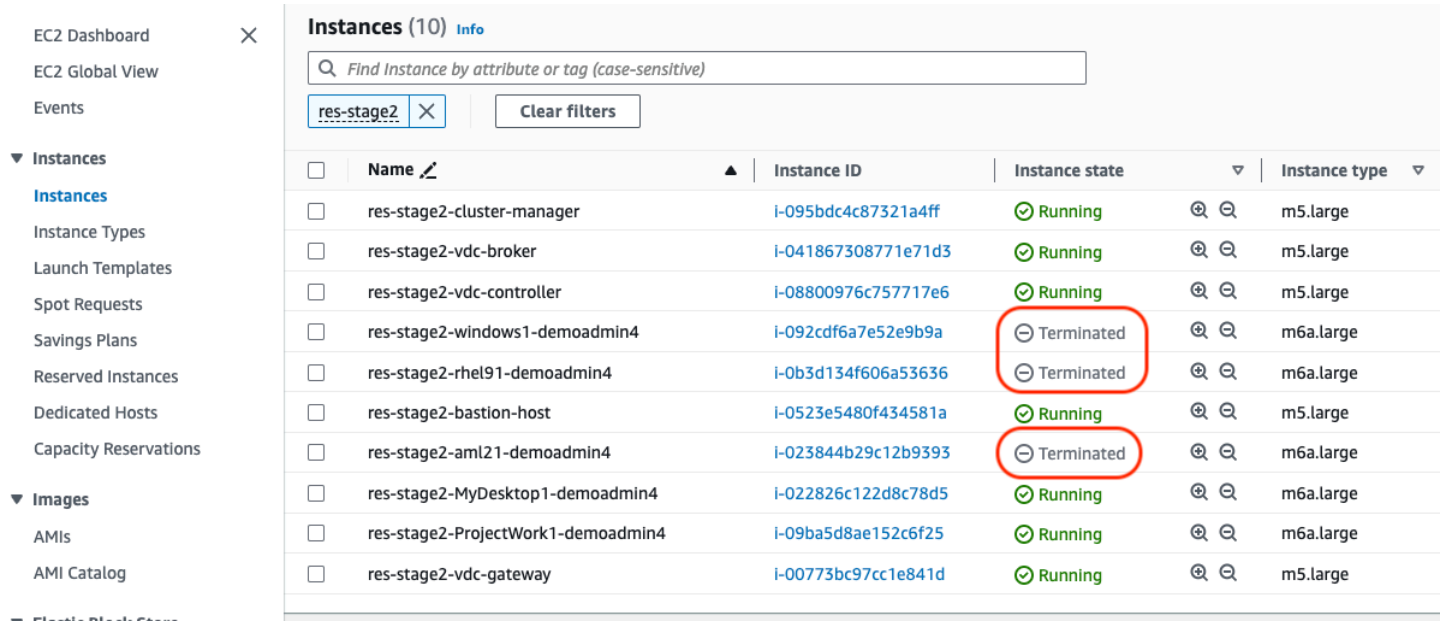
Amazon EC2コンソールでは、仮想デスクトップが実行されていると、次のようになります。この場合、仮想デスクトップは赤で示されます。インスタンス名のサフィックスは、デスクトップを作成したユーザーです。中央の名前は、起動時に設定されたセッション名であり、デフォルトMyDesktop「」またはユーザーが設定した名前です。



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。



参照に便利な Active Directory (AD) 関連のコマンド

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を次に示します。使用するドメインやその他のパラメータは、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.
```

Windows

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

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

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

問題 RunBooks

次のセクションでは、発生する可能性のある問題、検出方法、問題の解決方法に関する提案について説明します。

- インストールの問題
  - インストール後にカスタムドメインをセットアップしたい RES
  - AWS CloudFormation スタックは、「受信した失敗したメッセージWaitCondition 」というメッセージで作成に失敗します。エラー：状態。TaskFailed「
  - スタックが正常に作成された後に AWS CloudFormation E メール通知を受信しない
  - インスタンスのサイクルまたは vdc コントローラーが失敗した状態

- 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している
  - AD に参加できないために vdc-controller インスタンスがサイクルしています / eVDI モジュールに失敗したAPIヘルスチェックが表示されています
  - Software Stack を編集して追加するときに、プロジェクトがプルダウンに表示されない
  - クラスターマネージャーの 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」(アカウントがユーザー名の場合) が表示されます。
  - 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りました」と表示されます。管理者にお問い合わせください」
  - DHCP 外部/顧客の AD 設定に関するオプションの問題
  - Firefox エラー MOZILLA_PKIX_ERROR_REQUIREDTLS_FEATURE_MISSING
- Env 削除
  - res-xxx-cluster スタックがDELETE「_FAILED」状態で、「ロールが無効であるか、想定できない」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

インストールの問題

トピック

- インストール後にカスタムドメインをセットアップしたい RES
- AWS CloudFormation スタックは、「受信した失敗したメッセージWaitCondition 」というメッセージで作成に失敗します。エラー：状態。TaskFailed「
- スタックが正常に作成された後に AWS CloudFormation E メール通知を受信しない
- インスタンスのサイクルまたは vdc コントローラーが失敗した状態
- 依存オブジェクトエラーにより環境 CloudFormation スタックが削除に失敗する

- 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
- CloudFormation 環境作成中のスタック作成失敗
- AdDomainAdminNode CREATE_ で外部リソース (デモ) スタックの作成が失敗するFAILED

.....

インストール後にカスタムドメインをセットアップしたい RES

> **Note**
>
> 前提条件 : これらのステップを実行する前に、証明書と PrivateKey 内容を Secrets Manager シークレットに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. > Load Balancing EC2 > Load Balancer AWS のコンソールでRES外部ロードバランサーに移動します。
   b. 命名規則 に従って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SSL/TLS証明書を持つリスナーを更新します。
   e. 変更を保存します。
2. クラスター設定テーブルで :
   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 — name「key」、type「string」、condition「contains」、value「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 (ARN) に保存されている対応する証明書の Amazon リソースネーム () ですACM。

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 DNSの名前を指定します<env-name>-external-alb。
4. が 環境で既に設定されている場合SSOは、RESウェブポータルの全般設定 > Identity Provider > Single Sign On > Status > Edit ボタンから、最初に使用した入力と同じ入力SSOで再設定します。

に証明書を追加する VDIs

1. 次のタグをシークレットに追加して、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：
   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 — name「key」、type「string」、condition「contains」、value「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アクセス用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ARNの 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ARNの 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. AWS コンソールで、Auto ScalingEC2」のAuto Scaling 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検索して開きます。

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. 詳細 までスクロールダウンします。

f. 最下部までスクロールし、ユーザーデータ に移動します。

g. 単語`CERTIFICATE_SECRET_ARN`と 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ARNs指定された 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) 最近作成された起動テンプレートのバージョン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DNSの名前 を指定します`<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ンアップするのを待ちます。

.....

AWS CloudFormation スタックは、「受信した失敗したメッセージWaitCondition 」というメッセージで作成に失敗します。エラー：状態。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、最初に使用できる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。

.....

スタックが正常に作成された後に AWS CloudFormation E メール通知を受信しない

AWS 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ていることを確認します。

   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. Amazon EC2コンソールでインスタンスのサイクルの証拠を確認します。

   <envname> プレフィックスが として表示され、新しいEC2インスタンスに置き換えられる Amazon インスタンスがある場合、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。のステップを試the section called “インスタンスのサイクルまたは vdc コントローラーが失敗した状態”して問題を解決します。

.....

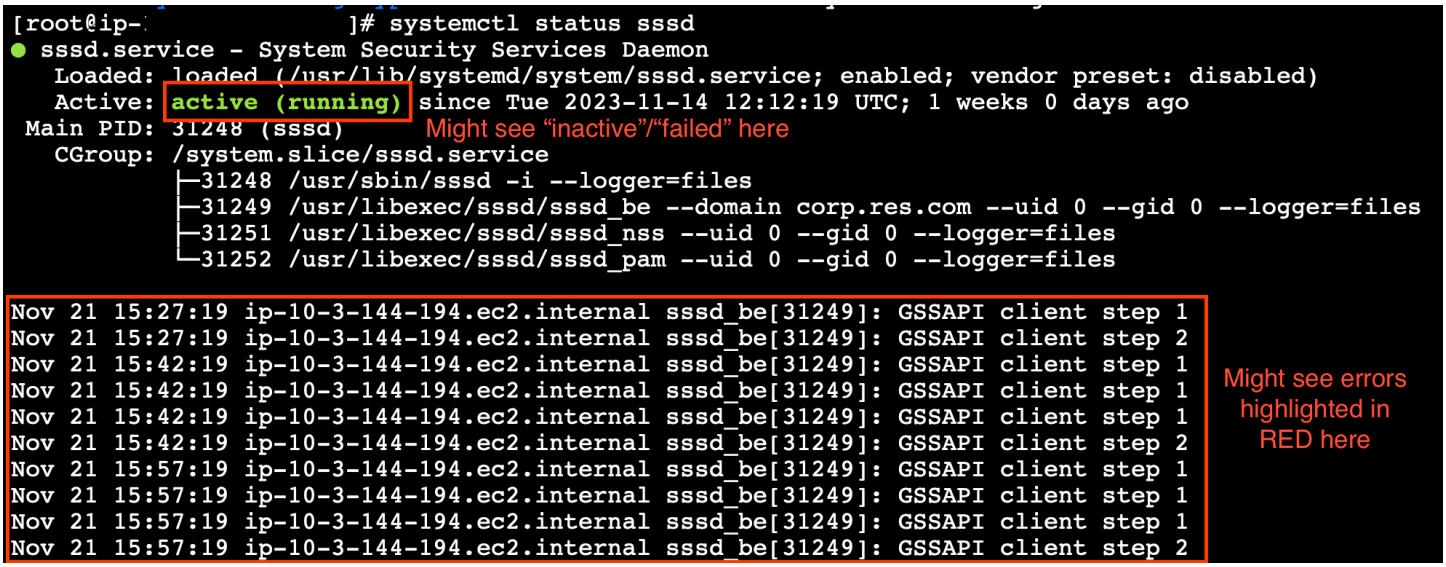
インスタンスのサイクルまたは vdc コントローラーが失敗した状態

この問題の最も可能性の高い原因は、リソースが Active Directory に接続または参加できないことです (複数可) 。

問題を確認するには：

1. コマンドラインから、vdc-controller の実行中のインスタンスSSMで 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。



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、考えられる 3 つの根本原因のいずれかがある可能性があります。

根本原因 1: 不正な ldap 接続の詳細が入力されました

ログを見直します。次のことが複数回繰り返されると、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 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
```

```
+ (( ATTEMPT_COUNT++ ))
```

1. RES スタックの作成中に、次のパラメータ値が正しく入力されていることを確認します。
   - 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 DynamoDB コンソールにあります。テーブル名は である必要があります`<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。自動スケーリングは、DynamoDB テーブルの最新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: 誤った ServiceAccount ユーザー名が入力されました

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 名前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 である必要があります`<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、現在実行中の環境の 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開始します。

根本原因 3: 間違った ServiceAccount パスワードが入力されました

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 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や、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 AWS 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 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、現在実行中の環境の 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、最新の値を使用して新しいインスタンスを開始します。

.....

依存オブジェクトエラーにより環境 CloudFormation スタックが削除に失敗する

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vdcdcvhostsecuritygroup、コンソールを使用して RES AWS 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。

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 [] のCIDRブロックパラメータにエラーが表示されますFAILED。

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には、x.x.x.0/24 または x.x.x.0/32 の形式が想定されます。

CloudFormation 環境作成中のスタック作成失敗

環境の作成には、一連のリソース作成オペレーションが必要です。一部のリージョンでは、キャパシティの問題が発生し、 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_ で外部リソース (デモ) スタックの作成が失敗する FAILED

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
```

障害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 SSOでのセットアップ”
- the section called “の ID プロバイダーの設定 SSO”

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 を実行する権限がありません。PassRole
- 自分の AWS アカウント以外のユーザーにリソースの AWS 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、 から欠落しているユーザー RES
- セッションの作成時に使用できないユーザー

- サイズ制限が CloudWatch クラスターマネージャーログのエラーを超過しました

.....

iam を実行する権限がありません。PassRole

iam:PassRole action 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、 にロールを渡すことができるようにポリシーを更新する必要がありますRES。

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、そのサービスに既存のロールを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権限が必要です。

次のエラー例は、Marymajor という名前のIAMユーザーがコンソールを使用して でアクションを実行しようとすると発生しますRES。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権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
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 iam:PassRole アクションを実行できるように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。サインイン認証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リソースの AWS 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 (ACLs) をサポートするサービスでは、これらのポリシーを使用して、リソースへのアクセスをユーザーに許可できます。

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。

- リソースへのアクセスをサードパーティー AWS アカウントに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の提供」を参照してください。
- ID フェデレーションを介し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「外部認証されたユーザーへのアクセスを提供する (ID フェデレーション) 」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。

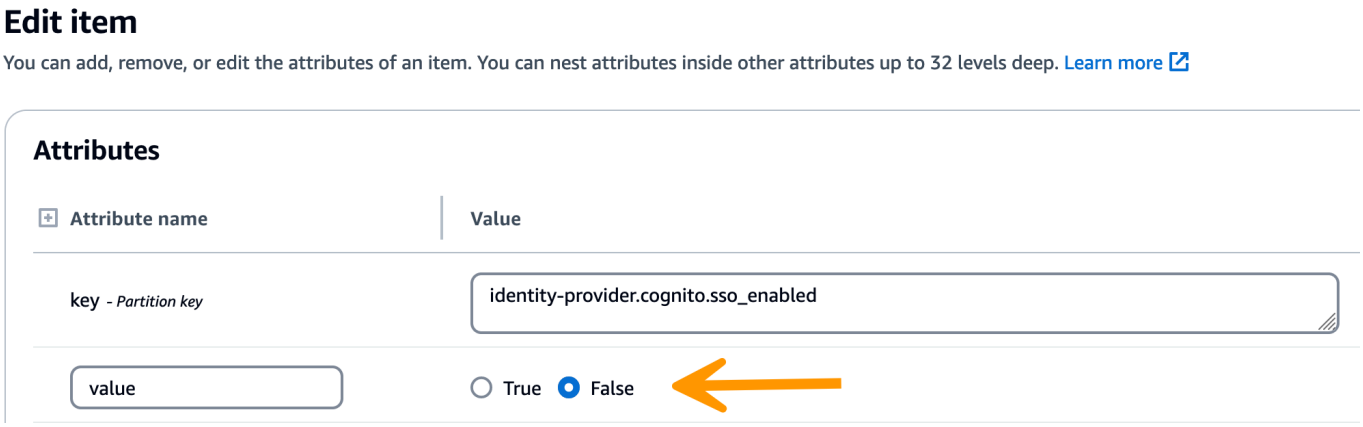
ログを確認するには：

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、テーブル項目 を探索 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。



7. RES ユーザーインターフェイスに戻り、 を再設定しますSSO。

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「ユーザーが見つからない」というエラーを受け取り、そのユーザーが Active Directory に存在する場合：

- ユーザーが に存在しておらずRES、最近 AD にユーザーを追加した場合
  - ユーザーがまだ に同期されていない可能性がありますRES。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、「」のステップに従いますActive Directory に追加されたが、 から欠落しているユーザー RES。
- ユーザーが に存在する場合RES：
  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用の ID プロバイダーの設定 (SSO) 」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、 から欠落しているユーザー RES

Active Directory にユーザーを追加したものの、 にユーザーがない場合RES、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に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使用できない場合は、ユーザーが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 回環境に口グインする必要があります。

.....

サイズ制限が CloudWatch クラスターマネージャーログのエラーを超過しました

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

CloudWatch クラスターマネージャーログでこのエラーが表示された場合、ldap 検索で返され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 検索結果の制限を増やします。

.....

ストレージ

トピック

.....

を通じてファイルシステムを作成しましたRESが、VDIホストには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「利用可能な」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お待ちください。

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. ステータスが でない場合は、VDIホストを起動するまで待ちます。

.....

を通じてファイルシステムをオンボーディングしたRESが、VDIホストにマウントされない

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RES必要があります。これらのファイルシステムは の外部で作成されるためRES、 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。

- NFS Linux VDCホストからのトラフィック (ポート: 2049)
- SMB Windows VDCホストからのトラフィック (ポート: 445)

.....

VDI ホストから読み書きできない

ONTAP はUNIX、ボリュームの 、NTFS、および MIXED セキュリティスタイルをサポートします。セキュリティスタイルは、データアクセスの制御ONTAP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。

例えば、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、SMBクライアントは のマルチプロトコルの性質上、データにアクセスすることができます (ただし、クライアントは適切に認証および承認する必要があります) ONTAP。ただし、 は、ネイティブツールを使用してUNIXクライアントのみが変更できるUNIXアクセス許可ONTAPを使用します。

アクセス許可処理のユースケースの例

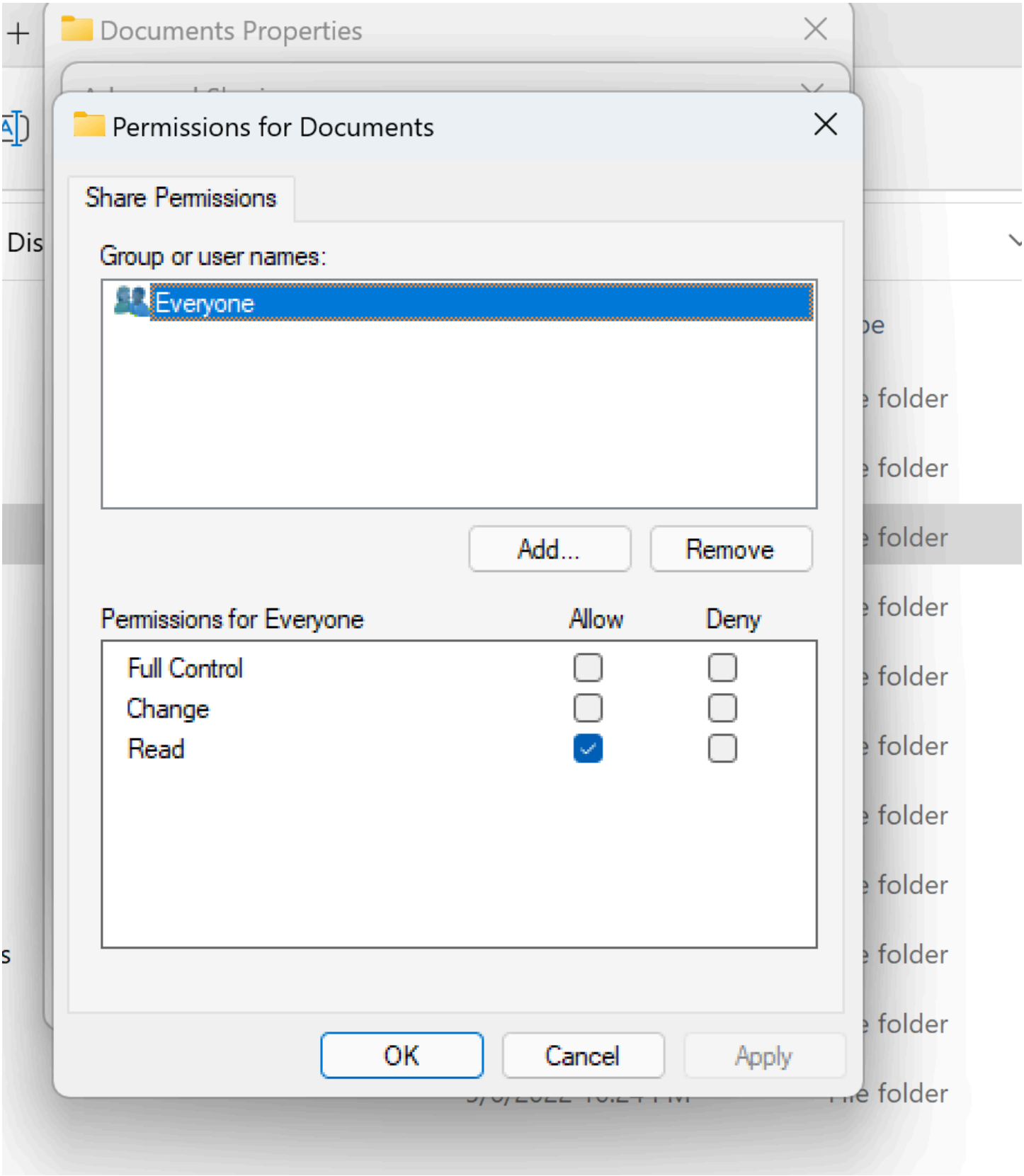
Linux ワークロードでのUNIXスタイルボリュームの使用

アクセス許可は、他のユーザーの sudoer によって設定できます。例えば、以下では、/<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されます。

```
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。例えば、ユーザーuser_01とフォルダ を指定すると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。


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

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、 に名前マッピングを設定する必要があります。SVMこれにより、すべての 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。詳細については、「Amazon FSx for でのマルチプロトコルワークロードの有効化 NetApp ONTAP」を参照してください。

.....

から Amazon FSx for NetApp ONTAP を作成しましたRESが、ドメインに参加しませんでした

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、ドメインに参加しません。作成したONTAPファイルシステムをSVMドメインに結合するには、「Microsoft Active Directory SVMsへの参加」を参照し、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 Service Account に委任されていることを確認します。がドメインに正常にSVM結合したら、SVM概要 > エンドポイント > SMBDNS名前 に移動し、後で必要になるためDNS名前をコピーします。

ドメインに結合したら、クラスター設定 DynamoDB SMB DNS テーブルで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、 を選択します`<stack-name>-cluster-settings`。
3. テーブル項目 を探索 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、項目の編集 を選択します。
5. 前にコピーしたSMBDNS名前で値を更新します。
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 でのファイルシステムアクセスコントロールVPC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、ドメイン参加SVMおよび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、RESOnboard 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 File Systems 、Onboard File System 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「失敗」
- 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「失敗」

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。問題で必要なテーブルクラウドがインポートされないことが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 ExportStatus の のステータスが であることを確認しますCOMPLETED。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。上記のフィールドセットが見つからない場合、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。

2. スナップショットの作成を開始したら、スナップショットのステータスが COMPLETEDで になっていることを確認しますRES。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表示して、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

.....

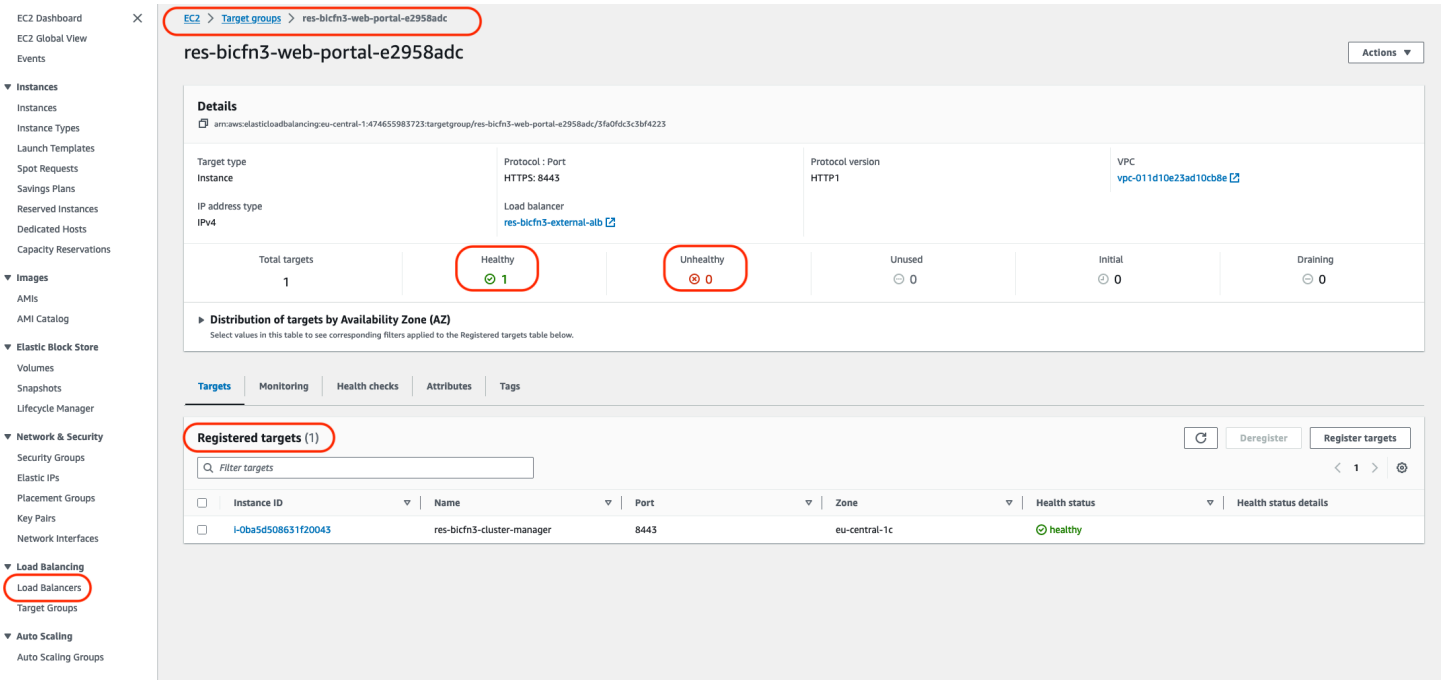
正常なインスタンスのないロードバランサーターゲットグループ

サーバーエラーメッセージなどの問題が UI に表示されたり、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EC2インスタンスに置き換えられているように見える Amazon インスタンスがないかを確認することです。その場合は、Amazon CloudWatch ログをチェックして原因を特定できます。

もう 1 つの方法は、システム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ンスが表示されない場合です。

通常の外観の例を次に示します。



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、インストールされた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。例えば、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 がない場合がありますAZs。この条件が発生した場合、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ことがあります。

.....

Virtual Desktops の起動

トピック

- 以前に動作していた仮想デスクトップは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 接続の試行は「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
- VDIs 起動後にエラー状態になる

.....

以前に動作していた仮想デスクトップは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したり、Amazon EC2インスタンスがRES環境外で終了または停止されたりすることが原因で問題が発生する可能性があります。管理者 UI ステータスは、引き続き準備完了状態を表示する場合がありますが、接続を試みても失敗します。

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ていたデータは、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。
- Server タブを選択します。
- DCV セッションパネルで、右側の編集アイコンをクリックします。
- ユーザーあたりの許可されたセッションの値を、希望する新しい値に変更します。
- [送信] を選択します。
- 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 接続の試行は「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 エラーで失敗した場合「接続は閉じられました。トランスポートエラー「」。原因は、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に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、SSMSession Manager 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、後続の接続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使用して、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

デスクトップ起動が Admin UI のプロビジョニング状態のままである場合、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、有用な CloudWatch 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の関連情報を含むログファイルと Amazon ロググループのリストが含まれています。

この問題の潜在的な原因は次のとおりです。

- 使用された ID AMI はソフトウェアスタックとして登録されていますが、 ではサポートされていませんRES。

  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。AMIs AWS Marketplace から取得した 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 から起動されたときに実行されませんAMI。

  デフォルトでは、ユーザーデータスクリプトは Amazon EC2インスタンスが起動されたときに 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AMIから を作成する場合は、 にソフトウェアスタックを登録し、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AMIと、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。

  問題を解決するには、 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 PowerShell コマンドウィンドウを Administrator として開きAMI、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AMIから新しい を作成します。新しい を使用してAMI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。また、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 から別の仮想デスクトップを起動すると、同じ問題が再度実行されますAMI。

.....

VDIs 起動後にエラー状態になる

考えられる問題 1: ホームファイルシステムには、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 スタックデプロイ中に指定されたホームファイルシステムは、2024.01 RES 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。

解決ステップ : ファイルシステムのユーザーディレクトリを削除します。

1. SSM をクラスターマネージャーホストに送信します。
2. `cd /home`.
3. `ls` - は、、.admin2. 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admin1を一覧表示する必要があります。
4. ディレクトリ を削除しますsudo `rm -r 'dir_name'`。ssm-user および ec2-user ディレクトリを削除しないでください。
5. ユーザーがすでに新しい env 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 - クラスターマネージャー Amazon `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad`で実行しますEC2。
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。が約 20 分で `Ready`状態VDIに移行することを確認します。

.....

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している

- AD に参加できないために vdc-controller インスタンスがサイクルしています / eVDI モジュールに失敗したAPIヘルスチェックが表示されています
- Software Stack を編集して追加するときに、プロジェクトがプルダウンに表示されない
- クラスターマネージャーの 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」 (アカウントがユーザー名の場合) が表示されます。
- 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りました」と表示されます。管理者にお問い合わせください」
- DHCP 外部/顧客の AD 設定に関するオプションの問題
- Firefox エラー MOZILLA_PKIX_ERROR_REQUIREDTLS_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している

インフラストラクチャインスタンスが Amazon EC2コンソールで終了と繰り返し表示される場合、原因はその設定に関連する場合があり、インフラストラクチャインスタンスのタイプによって異なります。以下は、原因を特定する方法です。

Amazon EC2コンソールで vdc コントローラーインスタンスが終了状態が繰り返される場合、これはシークレットタグが正しくない可能性があります。によって維持されるシークレットRESには、インフラストラクチャ 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なります。

```
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:
```

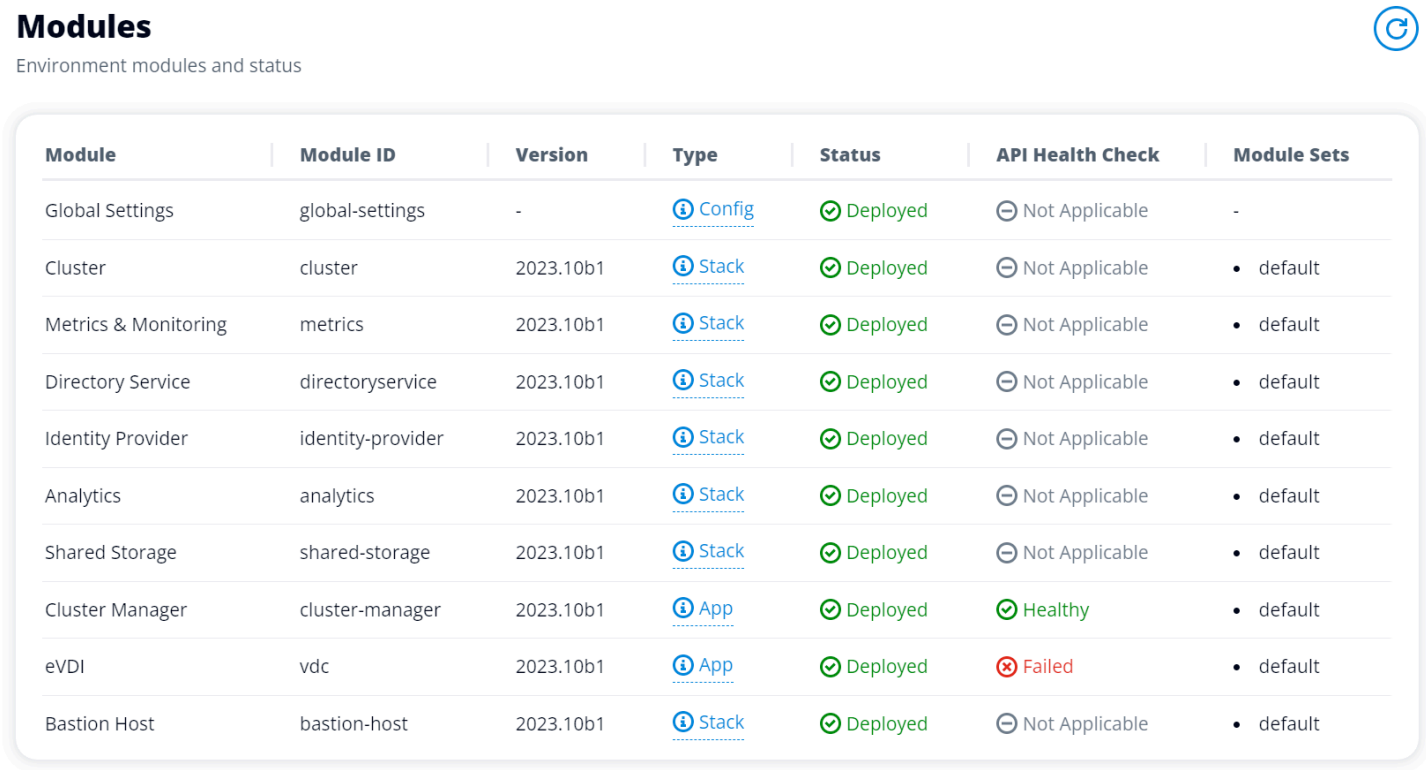
```
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

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 に参加できないために vdc-controller インスタンスがサイクルしています / eVDI モジュールに失敗したAPIヘルスチェックが表示されています

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	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

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CloudWatchログを調べることです。(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 ユーザー名が正しくスペルされていることを確認してください。

ログラインの例：

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

- SecretsManager コンソール から、RESデプロイ中に提供された 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。現在のクラスターマネージャーインスタンスと vdc コントローラー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。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RES、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。

  ログラインの例：

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

  - env の作成中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。現在のクラスターマネージャーインスタンスと vdc コントローラー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 を選択します。
2. アクション を選択し、ユーザーパスワードをリセットしてから、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 (など) のパスワードを更新します`<env_name>directoryserviceServiceAccountPassword`。
4. 現在のクラスターマネージャーインスタンスと vdc コントローラー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。

.....

Software Stack を編集して追加するときに、プロジェクトがプルダウンに表示されない

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。この問題が表示された場合は、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。

.....

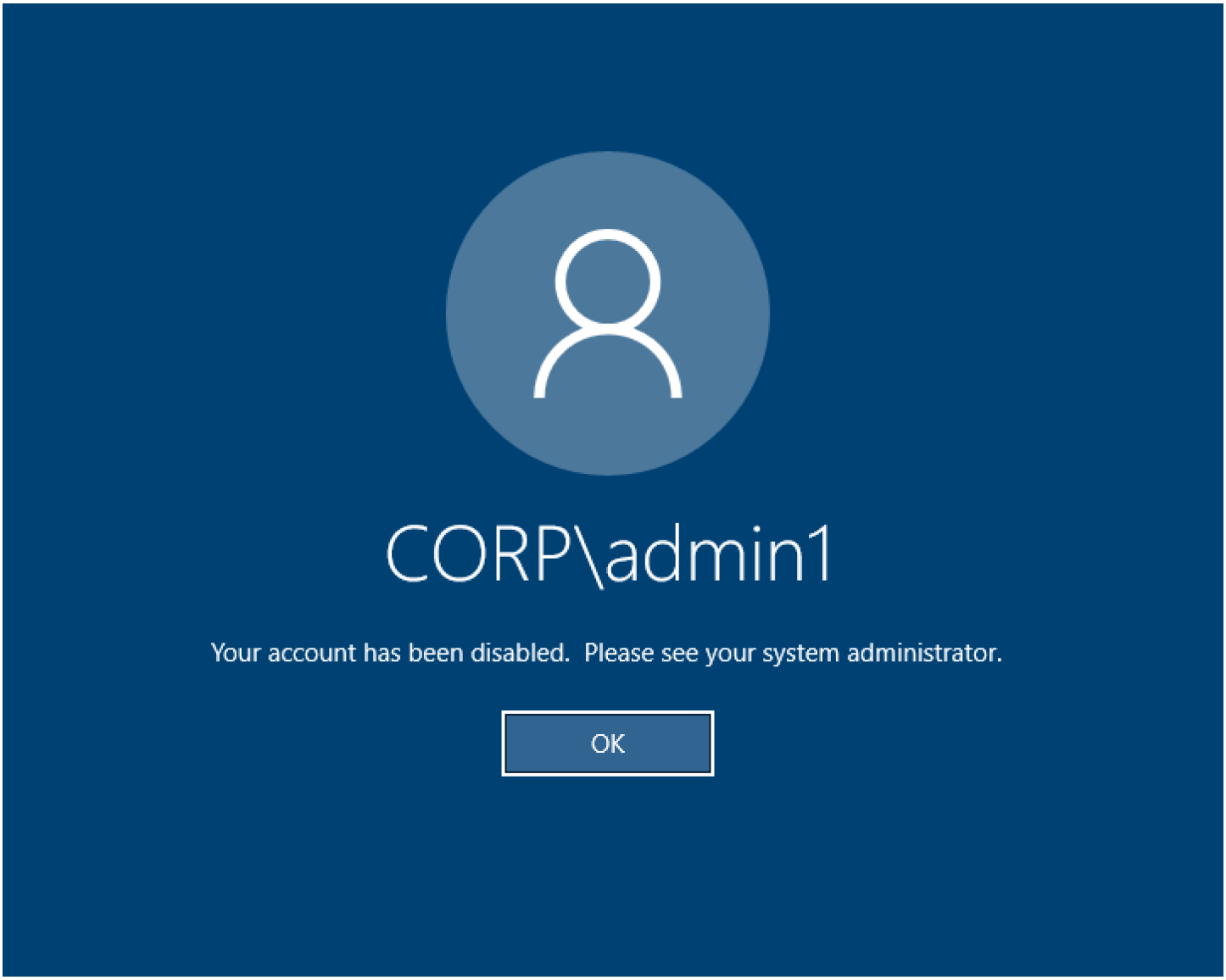
クラスターマネージャーの Amazon CloudWatch ログには、「 < user-home-init> アカウントはまだ利用できません。ユーザーの同期を待っています」 (アカウントがユーザー名の場合) が表示されます。

サブSQS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、ビジー状態になり、無限ループに閉じ込められます。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するとトリガーされます。

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 に対して正しく設定RESされていない可能性があります。例としては、BI/RES環境の作成で使用されたServiceAccountCredentialsSecretArnパラメータの値が正しくない場合があります。

.....

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りました」と表示されます。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、 経由で正常にサインインRESした後、に設定されている AD でユーザーが無効化されている可能性がありますSSO。

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。

.....

DHCP 外部/顧客の AD 設定に関するオプションの問題

を独自の Active Directory "The connection has been closed. Transport error"で使用するときに Windows 仮想デスクトップRESで というエラーが発生した場合は、Amazon CloudWatch ログで dcv-connection-gateway次のようなものがないか確認してください。

```
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 DHCP のオプションに AD ドメインコントローラーを使用している場合はVPC、以下を行う必要があります。

1. を 2 つのドメインコントローラー AmazonProvidedDNSに追加しますIPs。
2. ドメイン名を ec2.internal に設定します。

ここに例を示します。この設定がない場合、Windows デスクトップはトランスポートエラー を提供します。これは、RES/DCV が ip-10-0-x-xx.ec2.internal hostname を検索するためです。

.....

Firefox エラー MOZILLA_PKIX_ERROR_REQUIREDTLS_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、エラーメッセージタイプ MOZILLA_PKIX_ERRORREQUIRED_TLS_FEATURE_ MISSING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 の指示に従って修正できます。

.....

Env 削除

トピック

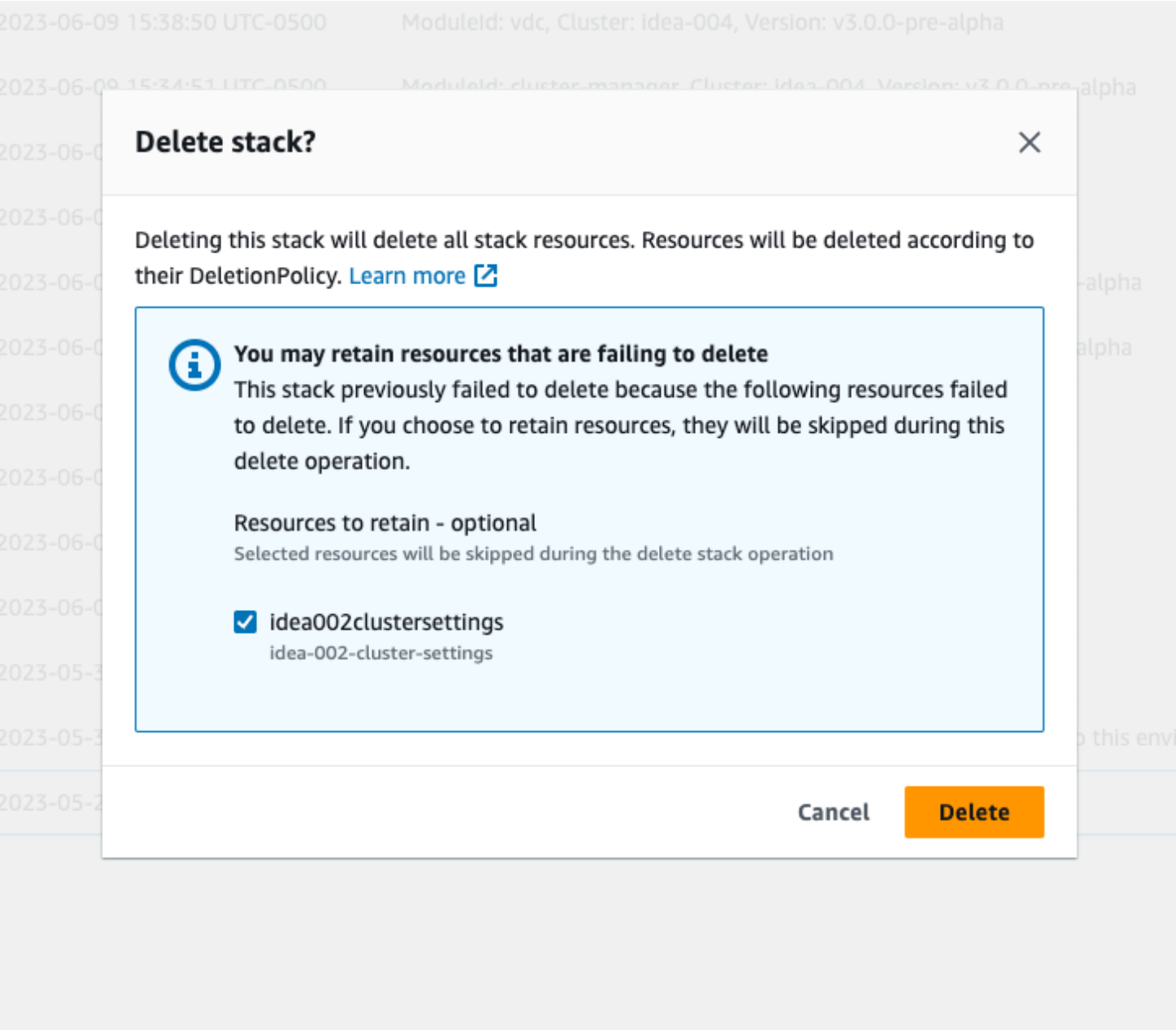
- res-xxx-cluster スタックがDELETE「_FAILED」状態で、「ロールが無効であるか、想定できない」エラーのため手動で削除できない
- ログの収集
- VDI ログのダウンロード
- Linux EC2インスタンスからのログのダウンロード
- Windows EC2インスタンスからのログのダウンロード
- WaitCondition エラーのECSログの収集

.....

res-xxx-cluster スタックがDELETE「_FAILED」状態で、「ロールが無効であるか、想定できない」エラーのため手動で削除できない

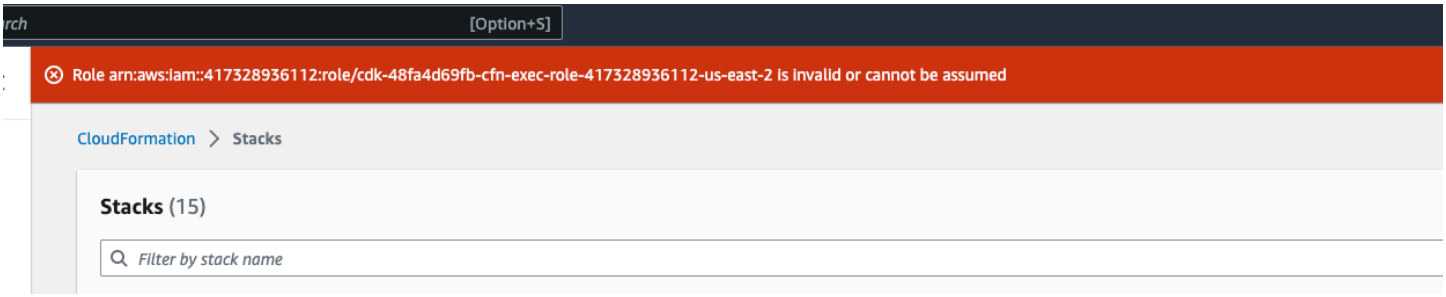
res-xxx-cluster「」スタックがDELETE「_FAILED」状態であり、手動で削除できない場合、次の手順を実行して削除できます。

スタックがDELETE「_FAILED」状態にある場合は、まず手動で削除してみてください。Delete Stack 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。



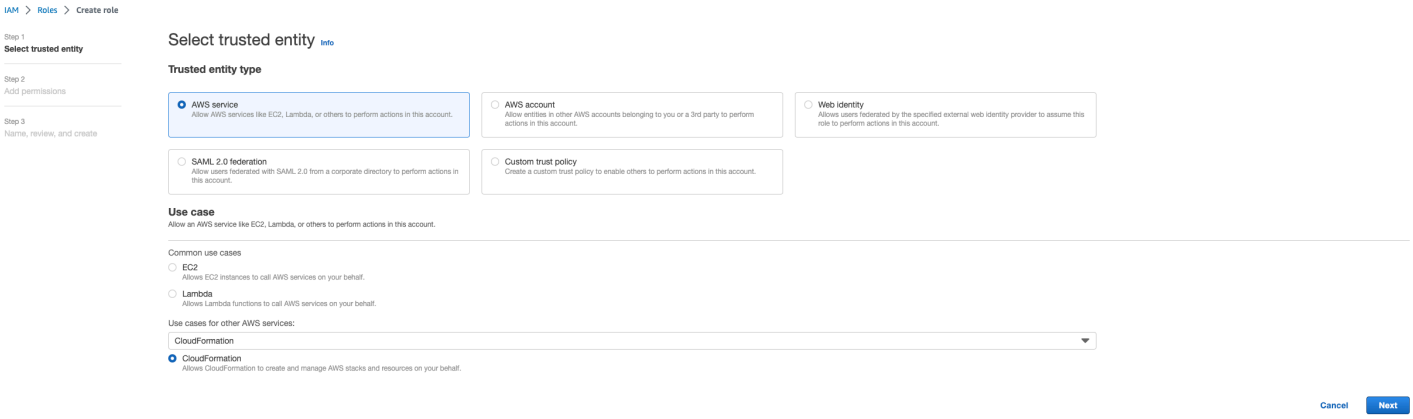
場合によっては、必要なスタックリソースをすべて削除しても、保持するリソースを選択するメッセージが表示されることがあります。その場合は、保持するリソースとしてすべてのリソースを選択し、「削除」を選択します。

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`

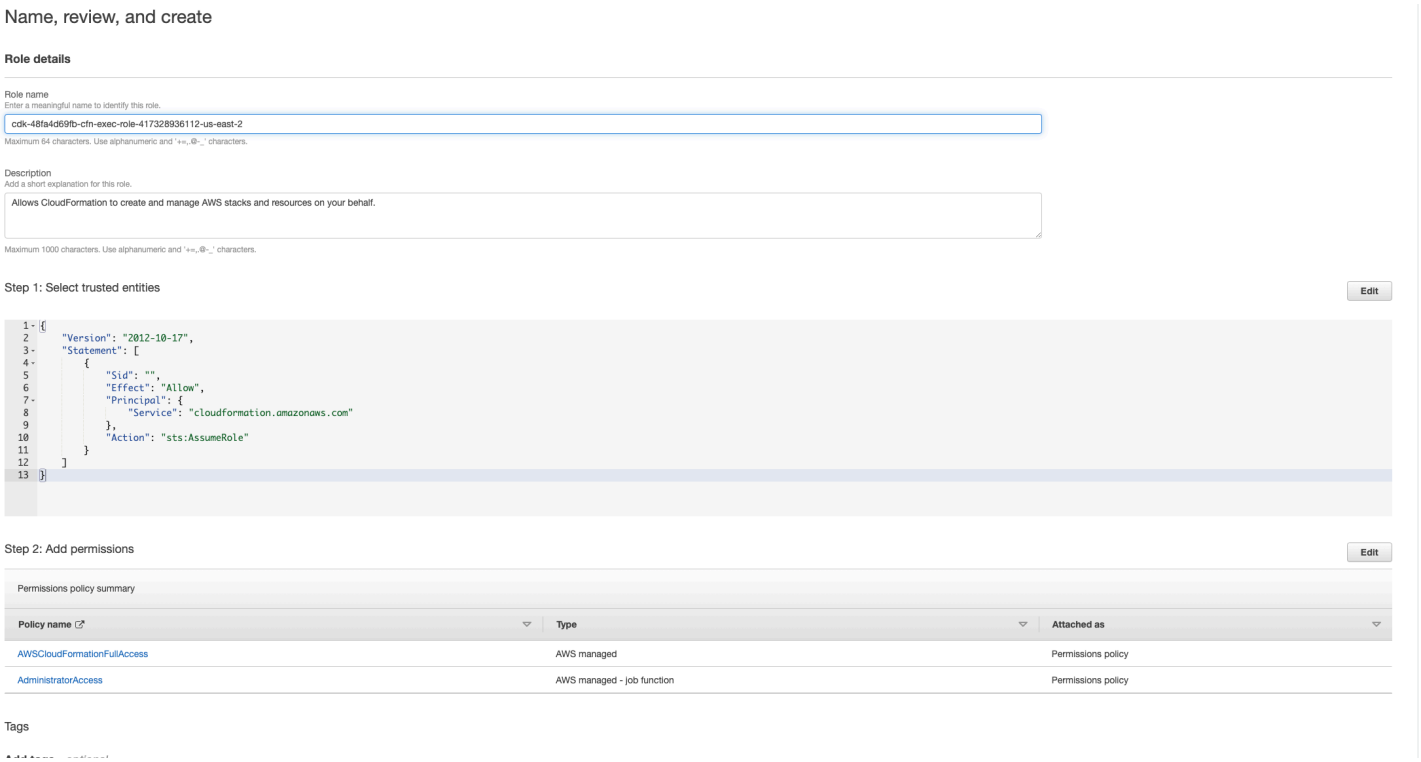


つまり、スタックの削除に必要なロールが、スタックの前に最初に削除されたことを意味します。これを回避するには、ロールの名前をコピーします。IAM コンソールに移動し、次のパラメータを使用して、その名前のロールを作成します。

- 信頼できるエンティティタイプの場合は、AWS サービス を選択します。
- ユースケース の場合は、 `Use cases for other AWS services` を選択しますCloudFormation。



[Next (次へ)] を選択します。ロール 'AWSCloudFormationFullAccess' と 'AdministratorAccess' のアクセス許可を付与していることを確認してください。レビューページは次のようになります。



次に、 CloudFormation コンソールに戻り、スタックを削除します。ロールを作成した後、削除できるようになりました。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 PowerShell 、Windows を開いてコマンドを実行します。

Infrastructure ホストログの収集

1. クラスターマネージャー: 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。
   a. ロググループ のすべての CloudWatch ログ`<env-name>/cluster-manager`。
   b. `<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。このセクションの先頭にある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。

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. ロググループ のすべての CloudWatch 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。このセクションの先頭にある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手順に従うことです。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 VDIで を起動した場合VDI1、Amazon EC2コンソール上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

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するには、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」の「」にリンクされた手順に従ってください。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。そのためには、以下の手順に従って 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

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するには、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」の「」に

リンクされた手順に従ってください。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. S3 アクセスを許可するようにVDIEC2インスタンスIAMロールを更新します。
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 と同じIAMロールVDIs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 バケットを選択し、以前にアップロードされた<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 バケットを選択し、以前にアップロードされた<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 → を展開しLogGroup、ロググループを選択して CloudWatch ログを開きます。
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

.....

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

ID プロバイダーへの認証リクエストを処理するときにログインしようとして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、 として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 でサービスアカウントのパスワードを更新して、上記で入力した新しいパスワードと一致させます。
   - Keycloak スタックの場合: PasswordSecret-...RESExternal--...DirectoryService--...、説明: Microsoft Active Directory のパスワード
   - for RES: res-ServiceAccountPassword-... with Description: Active Directory Service 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。

既知の問題

既知の問題 2024.x

(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 (つまり、VDI) 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 ARN (`arn:aws:s3:::example-bucket`) インスタンスに読み取り/書き込み S3 バケットをマウントできません。

この問題の影響を受けないバケット設定には以下が含まれます。

- 読み取り専用バケット
- バケットの一部としてプレフィックス (つまり、arn:aws:s3:::example-bucket/example-folder-prefix) とカスタムプレフィックス ARN (プロジェクト名またはプロジェクト名とユーザー名) を含むバケットの読み取り/書き込み
- ルートバケット を持つがARN、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。のマウントディレクトリは存在しますVDIが、ディレクトリは空になり、バケットの現在の内容は含まれません。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 と 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、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<output-directory>ディレクトリとRES環境の名前<environment-name>に置き換えます。

   a. パッチは 2024.08 RES 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 を設定し AWS CLI、 によって作成されたバケットに書き込む Amazon S3 アクセス許可があることを確認しますRES。

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

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

2. 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。(最初のステップでは、 ENVIRONMENT_NAME変数をRES環境の名前に既に設定しています。)

```
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}
```

> **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 Environment variable を持つ を追加してくださいregional。詳細については、「分離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*<RES-EnvironmentName>*-vdc-extが正常になったら、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 を起動VDIs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

RES AD グループの名前にスペースが含まれている場合、2024.06 は以前のバージョンのスナップショットの適用に失敗します。

クラスターマネージャー 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、次の要件を満たすグループ名RESのみを受け入れることによって発生します。

- 小文字と大文字ASCII、数字、ダッシュ(-)、ピリオド (.)、アンダースコア (_) のみを使用できます。
- 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 と 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<output-directory>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 2024.06 RES 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 を設定し AWS CLI、 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RES。

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

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

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

2. 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ASCII、数字、ダッシュ(-)、ピリオド (.)、アンダースコア (_)、および 1～30 のスペースを含めることができます。

.....

(2024.04-2024.04.02) IAM VDIインスタンスのロールにアタッチされていないアクセス許可境界を提供

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境界設定を適切に継承していない。これは、 IAMPermissionBoundaryパラメータによって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なかった結果です。

影響を受けるバージョン

2024.04 - 2024.04.02

緩和策

VDIs 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、を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 2024.04.02 RES 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関する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 を設定し AWS CLI、 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RES。

```
OUTPUT_DIRECTORY=<output-directory>

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

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

2. 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. を環境の名前<environment-name>に置き換えて、このコマンドを実行してRES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しない

問題

Amazon マシンイメージ (AMIs) は、特定の設定RESで 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。ap-southeast-2 (シドニー) で Windows Nvidia インスタンスを起動RESするように で設定された AMI ID は現在正しくありません。

AMIこのタイプのインスタンス設定`ami-0e190f8939a996caf`の -ID は、ap-southeast-2 (シドニー) に誤ってリストされています。AMI 代わりに ID `ami-027cf6e71e2e442f4`を使用する必要があります。

デフォルトの でインスタンスを起動しようとすると、次のエラーが発生しますami-0e190f8939a996cafAMI。

```
An error occured (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RESにデプロイします。
- Windows NVIDIAデフォルトの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

2024.04.02 以前のすべてのRESバージョンが影響を受けます

緩和策

RES バージョン 2024.01.01 では、以下の緩和策が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) でRESの削除失敗 GovCloud

問題

RES 削除ワークフロー中、`UnprotectCognitoUserPoolLambda` は後で削除される Cognito ユーザープールの削除保護を非アクティブ化します。Lambda の実行は、 によって開始されます`InstallerStateMachine`。

商用リージョンと GovCloud リージョンではデフォルトの 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RESで を削除しようとすると、次のエラーが発生します。

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

バグを再現する手順 :

- GovCloud リージョンRESにデプロイする
- 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、以下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 Python 3.11-> 保存 を選択します。
- を開きます CloudFormation。
- RES スタックを削除する -> インストーラリソースを保持する UNCHECKED -> を削除する。

.....

(2024.04 - 2024.04.02) Linux 仮想デスクトップが再起動時にRESUMING「」ステータスで停止してい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「」ステータスで停止する可能性があります。

インスタンスを再起動すると、 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/controller CloudWatch 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

2024.04 - 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. SSH EC2コンソールから問題インスタンスに移動します。
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で実行され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 2024.04.02 RES 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の を設定し AWS CLI、 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RES。

```
OUTPUT_DIRECTORY=<output-directory>

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

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

2. 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、 RES をデプロイしたリージョン<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 VDC 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

RES SSOは、 が少なくとも 2 時間 (AD 同期サイクルが 2 回) 設定されると、AD ユーザーの同期を失敗します。クラスターマネージャー 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}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

このエラーは、次の要件を満たすSAMAccountユーザー名RESのみを受け入れることによって発生します。

- 小文字ASCII、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 2024.04.02 RES 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の を設定し AWS CLI、 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RES。

```
OUTPUT_DIRECTORY=<output-directory>

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

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

2. 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、キーのフォーマットが不適切になります。複数の行が 1 行としてダウンロードされるため、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と、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-----BEGIN PRIVATE KEY-----、 の直前に別の行を作成することで、キーファイルのフォーマットを変更することもできます-----END PRIVATE KEY-----。

.....

(2024.06 以前) AD 同期RES中に 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RES場合、グループメンバーは に適切に同期されません。 UserOU

RES AD グループからユーザーを同期しようとすると、 は ldapsearch フィルターを作成します。現在のフィルターは、UserOUパラメータの代わりに UserOU パラメータを誤って使用します。

GroupOU 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 が異なる場合にのみ発生します。

影響を受けるバージョン

この問題は、すべてのRESバージョン 2024.06 以前に影響します。

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<output-directory>ローカルディレクトリに置き換え、 をパッチを適用する のバージョン<res_version>に置き換えRES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 を設定し AWS CLI、 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RES。
> - パッチはRESバージョン 2024.04.02 と 2024.06 のみをサポートします。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 のセキュリティ脆弱性 VDIs

バグの説明

CVE-2024-6387 と呼ばれ、OpenSSH サーバーで識別regreSSHionされました。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することができ、Open SSHを使用して安全な通信を行うシステムに重大なリスクをもたらします。

の場合RES、標準設定は踏み台ホストを経由して仮想デスクトップSSHに入り、踏み台ホストはこの脆弱性の影響を受けません。ただし、 ALL RES バージョンで RHEL9および Ubuntu2024 AMI (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 VDIs (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と Ubuntu2024 VDIsは悪用される可能性がありますが、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、 を参照してください。

影響を受けるバージョン

この問題は、すべてのRESバージョン 2024.06 以前に影響します。

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 がある場合はVDIs、以下のPATCHEXISTINGVDIs手順に従ってください。今後の にパッチを適用するにはVDIs、PATCHFUTUREVDIs以下の手順に従うことをお勧めします。これらの手順では、スクリプトを実行して にプラットフォームの更新を適用する方法について説明しますVDIs。

PATCH EXISTING VDIs

1. 既存のすべての Ubuntu と RHEL9 にパッチを適用する次のコマンドを実行しますVDIs。

   a. パッチスクリプトには AWS CLIv2 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 を設定し AWS CLI、 AWS Systems Manager Run Command を送信する Systems Manager の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にSUCCESSメッセージIDsがあることを確認します。

PATCH FUTURE VDIs

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 2024.06 RES 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の AWS CLIのコピーを設定し、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RES。

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

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

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

2. 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 VDC 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

パッチ適用の将来VDIs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VDIsRES環境で将来の にパッチを適用するには、まずの手順を使用して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。

.....

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ライセンスRDPを必要とせずに Amazon EC2インスタンスへのリモットが可能になります。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、リモートデスクトップユーザーを Microsoft または Microsoft ライセンスリセラーから購入CALs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CALsを持つリモートデスクトップユーザーにはライセンスモビリティの利点があり、デフォルトの (共有) テナント環境に移行 AWS できます。Software Assurance または License Mobility のメリットのないライセンスの持ち込みについては、 のこのセクションを参照してくださいFAQ。

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) は、現在の製品の提供と慣行を表 AWS し、 予告なく変更される場合があります。 および (c) は、 AWS およびその関連会社からのコミットメントまたは保証を一切作成しません。 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、 明示的か黙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すべての契約。

の Research and Engineering Studio AWS は、The Apache Software Foundation で利用可能な Apache ライセンスバージョン 2.0 の条項に基づいてライセンスされます。

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。

日付	変更

2024 年 10 月	• リリースバージョン 2024.10: のサポートが追加されました —
	  • 環境境界.
	  • デスクトップ共有プロファイル.
	  • 仮想デスクトップインターフェイスの自動停止.

2024 年 8 月	• リリースバージョン 2024.08: のサポートが追加されました —
	  • 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。「Amazon S3 バケット」を参照してください。
	  • 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。「アクセス許可ポリシー」を参照してください。
	• ユーザーガイド: トラブルシューティングセクションを展開しました。

2024 年 6 月	• 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。 • ユーザーガイド: を追加 デモ環境を作成する
2024 年 4 月	リリースバージョン 2024.04 — RES- レディ AMIsおよびプロジェクト起動テンプレート

日付	変更
2024 年 3 月	その他のトラブルシューティングトピック、CloudWatch ログ保持、マイナーバージョンのアンインストール
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 指示とテンプレートが追加されました
2023 年 11 月	初回リリース

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。