aws

Guide de l’utilisateur

Studio de recherche et d'ingénierie

Studio de recherche et d'ingénierie: Guide de l’utilisateur

Table of Contents

Présentation

Research and Engineering Studio (RES) est un produit open source AWS pris en charge qui permet aux administrateurs informatiques de fournir un portail Web aux scientifiques et aux ingénieurs pour exécuter des charges de travail informatiques techniques. AWS RES fournit aux utilisateurs une interface unique leur permettant de lancer des bureaux virtuels sécurisés pour mener des recherches scientifiques, concevoir des produits, effectuer des simulations techniques ou effectuer des analyses de données. Les utilisateurs peuvent se connecter au portail RES en utilisant leurs identifiants d'entreprise existants et travailler sur des projets individuels ou collaboratifs.

Les administrateurs peuvent créer des espaces de collaboration virtuels appelés projets pour un ensemble spécifique d'utilisateurs afin d'accéder à des ressources partagées et de collaborer. Les administrateurs peuvent créer leurs propres piles de logiciels d'application (AMI) et autoriser les utilisateurs de RES à lancer des bureaux virtuels Windows ou Linux, ainsi qu'à accéder aux données du projet via des systèmes de fichiers partagés. Les administrateurs peuvent attribuer des piles de logiciels et des systèmes de fichiers et restreindre l'accès aux seuls utilisateurs du projet. Les administrateurs peuvent utiliser la télémétrie intégrée pour surveiller l'utilisation de l'environnement et résoudre les problèmes des utilisateurs. Ils peuvent également établir des budgets pour des projets individuels afin d'éviter une surconsommation de ressources. Le produit étant open source, les clients peuvent également personnaliser l'expérience utilisateur du portail RES en fonction de leurs propres besoins.

RES est disponible sans frais supplémentaires et vous ne payez que pour les AWS ressources nécessaires à l'exécution de vos applications.

Ce guide fournit une présentation de Research and Engineering Studio on AWS, de son architecture de référence et de ses composants, des considérations relatives à la planification du déploiement et des étapes de configuration pour le déploiement de RES sur le cloud Amazon Web Services (AWS).

Fonctionnalités et avantages

Research and Engineering Studio on AWS fournit les fonctionnalités suivantes :

Interface utilisateur basée sur le Web

RES fournit un portail Web que les administrateurs, les chercheurs et les ingénieurs peuvent utiliser pour accéder à leurs espaces de travail de recherche et d'ingénierie et les gérer. Les scientifiques et

les ingénieurs n'ont pas besoin d'une expertise Compte AWS ou d'une expertise dans le cloud pour utiliser RES.

Configuration basée sur le projet

Utilisez des projets pour définir des autorisations d'accès, allouer des ressources et gérer les budgets pour un ensemble de tâches ou d'activités. Attribuez des piles logicielles spécifiques (systèmes d'exploitation et applications approuvées) et des ressources de stockage à un projet pour garantir la cohérence et la conformité. Surveillez et gérez les dépenses par projet.

Outils de collaboration

Les scientifiques et les ingénieurs peuvent inviter d'autres membres de leur projet à collaborer avec eux, en définissant les niveaux d'autorisation qu'ils souhaitent que ces collègues aient. Ces personnes peuvent se connecter à RES pour se connecter à ces ordinateurs de bureau.

Intégration à l'infrastructure de gestion des identités existante

Intégrez votre infrastructure de gestion des identités et de services d'annuaire existante pour permettre la connexion au portail RES avec l'identité d'entreprise existante d'un utilisateur et attribuer des autorisations aux projets en utilisant les appartenances d'utilisateurs et de groupes existantes.

Stockage permanent et accès aux données partagées

Pour permettre aux utilisateurs d'accéder aux données partagées par le biais de sessions de bureau virtuel, connectez-vous à vos systèmes de fichiers existants ou créez de nouveaux systèmes de fichiers dans RES. Les services de stockage pris en charge incluent Amazon Elastic File System pour les postes de travail Linux et Amazon FSx NetApp for ONTAP pour les ordinateurs de bureau Windows et Linux.

Surveillance et établissement de rapports

Utilisez le tableau de bord d'analyse pour surveiller l'utilisation des ressources par type d'instance, de pile logicielle et de type de système d'exploitation. Le tableau de bord fournit également une ventilation de l'utilisation des ressources par projet à des fins de reporting.

Gestion du budget et des coûts

Créez un lien AWS Budgets vers vos projets RES pour suivre les coûts de chaque projet. Si vous dépassez votre budget, vous pouvez limiter le lancement de sessions VDI.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à ce produit :

Navigateur de fichiers

Un navigateur de fichiers fait partie de l'interface utilisateur RES où les utilisateurs actuellement connectés peuvent consulter leur système de fichiers.

Système de fichiers

Le système de fichiers agit comme un conteneur pour les données de projet, souvent appelées ensembles de données, qui fournit une solution de stockage dans les limites d'un projet et améliore la collaboration et le contrôle d'accès aux données.

Projet

Un projet est une partition logique au sein de l'application qui sert de limite distincte pour les données et les ressources de calcul, garantissant la gouvernance du flux de données et empêchant le partage des données et des hôtes VDI entre les projets.

Autorisations basées sur le projet

Les autorisations basées sur les projets décrivent une partition logique des données et des hôtes VDI dans un système où plusieurs projets peuvent exister. L'accès d'un utilisateur aux données et aux hôtes VDI au sein d'un projet est déterminé par le ou les rôles qui lui sont associés. Un utilisateur doit disposer d'un accès (ou d'une adhésion au projet) pour chaque projet auquel il a besoin d'accéder. Dans le cas contraire, un utilisateur ne pourra pas accéder aux données du projet et aux VDI s'il n'a pas obtenu l'adhésion.

Pile logicielle

Les piles logicielles sont des Amazon Machine Images (AMI) avec des métadonnées spécifiques aux RES basées sur le système d'exploitation qu'un utilisateur a sélectionné pour approvisionner son hôte VDI.

Hôtes VDI

Les hôtes d'instances de bureau virtuel (VDI) permettent aux membres du projet d'accéder aux données et aux environnements informatiques spécifiques au projet, garantissant ainsi des espaces de travail sécurisés et isolés.

Pour une référence générale des AWS termes, voir le AWS glossaire dans la référence AWS générale.

Présentation de l'architecture

Cette section fournit un schéma d'architecture des composants déployés avec ce produit.

Diagramme d'architecture

Le déploiement de ce produit avec les paramètres par défaut déploie les composants suivants dans votreCompte AWS.

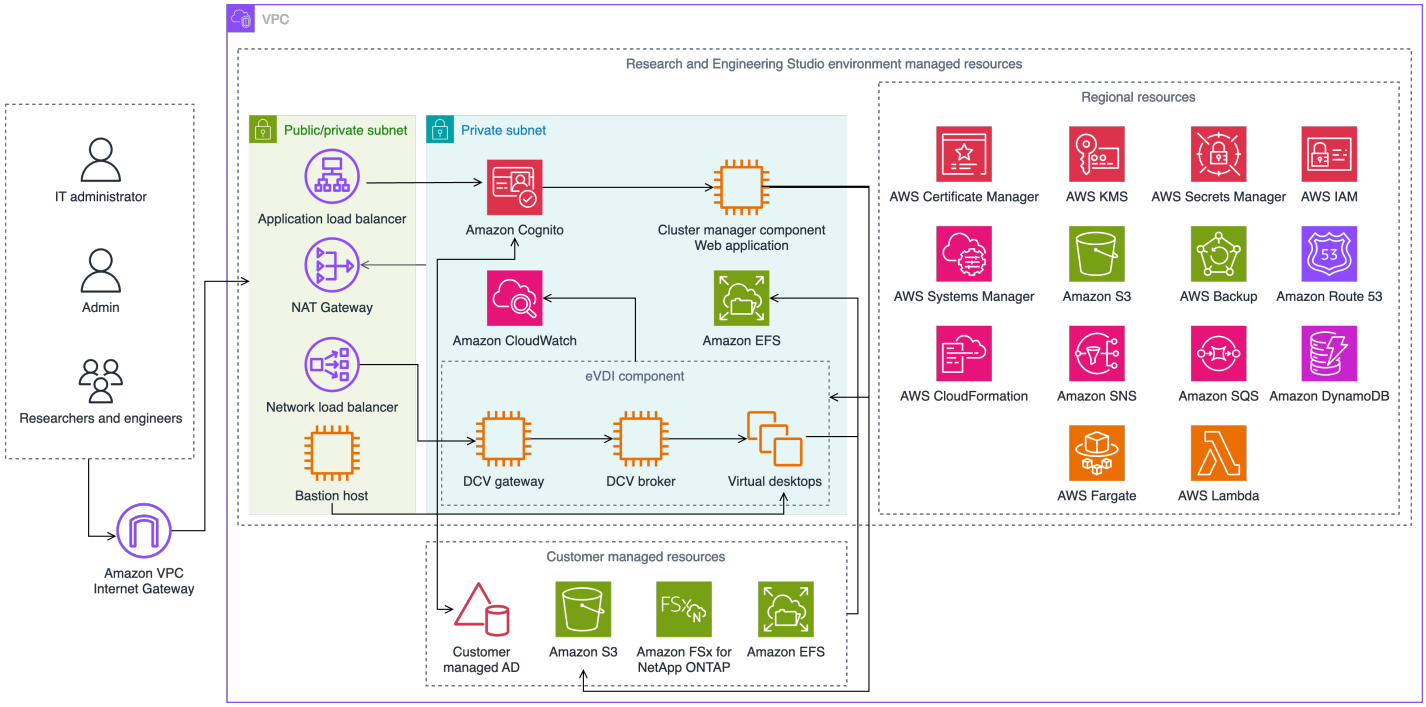


Figure 1 : Studio de recherche et d'ingénierie sur AWS l'architecture

> **Note**
>
> AWS CloudFormationles ressources sont créées à partir de AWS Cloud Development Kit (AWS CDK) constructions.

Le flux de processus de haut niveau pour les composants du produit déployés avec le AWS CloudFormation modèle est le suivant :

1. RES installe des composants pour le portail Web ainsi que :
   a. Composant de bureau virtuel d'ingénierie (eVDI) pour les charges de travail interactives

b. Composant Metrics

   Amazon CloudWatch reçoit les métriques des composants eVDI.

c. Composant Bastion Host

   Les administrateurs peuvent se connecter au composant hôte Bastion via SSH pour gérer l'infrastructure sous-jacente.

2. RES installe les composants dans des sous-réseaux privés situés derrière une passerelle NAT. Les administrateurs accèdent aux sous-réseaux privés via l'Application Load Balancer (ALB) ou le composant Bastion Host.
3. Amazon DynamoDB stocke la configuration de l'environnement.
4. AWS Certificate Manager(ACM) génère et stocke un certificat public pour l'Application Load Balancer (ALB).

> **Note**
>
> Nous vous recommandons AWS Certificate Manager de l'utiliser pour générer un certificat fiable pour votre domaine.

5. Amazon Elastic File System (EFS) héberge le système de `/home` fichiers par défaut monté sur tous les hôtes d'infrastructure et sessions eVDI Linux applicables.
6. RES utilise Amazon Cognito pour créer un utilisateur bootstrap initial appelé clusteradmin et envoie des informations d'identification temporaires à l'adresse e-mail fournie lors de l'installation. L'administrateur du cluster doit changer le mot de passe lors de la première connexion.
7. Amazon Cognito s'intègre à l'Active Directory et aux identités des utilisateurs de votre organisation pour la gestion des autorisations.
8. Les zones de sécurité permettent aux administrateurs de restreindre l'accès à des composants spécifiques du produit en fonction des autorisations.

AWSservices inclus dans ce produit

Service AWS	Description
Amazon Elastic Compute Cloud	Noyau. Fournit les services informatiques sous-jacents pour créer des bureaux virtuels avec

Service AWS	Description
	le système d'exploitation et la pile logicielle choisis.
Elastic Load Balancing	Noyau. Les hôtes Bastion, cluster-manager et VDI sont créés dans des groupes Auto Scaling situés derrière l'équilibreur de charge. ELB équilibre le trafic du portail Web entre les hôtes RES.
Amazon Virtual Private Cloud	Noyau. Tous les principaux composants du produit sont créés au sein de votre VPC.
Amazon Cognito	Noyau. Gère les identités et l'authentification des utilisateurs. Les utilisateurs d'Active Directory sont mappés aux utilisateurs et aux groupes Amazon Cognito afin d'authentifier les niveaux d'accès.
Amazon Elastic File System	Noyau. Fournit le système de `/home` fichiers pour le navigateur de fichiers et les hôtes VDI, ainsi que pour les systèmes de fichiers externes partagés.
Amazon DynamoDB	Noyau. Stocke les données de configura tion telles que les utilisateurs, les groupes, les projets, les systèmes de fichiers et les paramètres des composants.
AWS Systems Manager	Noyau. Stocke les documents permettant d'exécuter des commandes pour la gestion des sessions VDI.

Service AWS	Description
AWS Lambda	Noyau. Prend en charge les fonctionnalités du produit telles que la mise à jour des paramètre s dans la table DynamoDB, le démarrage des flux de travail de synchronisation Active Directory et la mise à jour de la liste des préfixes.
Amazon CloudWatch	Soutenir. Fournit des métriques et des journaux d'activité pour tous les hôtes Amazon EC2 et les fonctions Lambda.
Amazon Simple Storage Service	Soutenir. Stocke les fichiers binaires des applications pour le démarrage et la configura tion de l'hôte.
AWS Key Management Service	Soutenir. Utilisé pour le chiffrement au repos avec les files d'attente Amazon SQS, les tables DynamoDB et les rubriques Amazon SNS.
AWS Secrets Manager	Soutenir. Stocke les informations d'identification des comptes de service dans Active Directory et les certificats auto-signés pour les VDI.
AWS CloudFormation	Soutenir. Fournit un mécanisme de déploieme nt pour le produit.
AWS Identity and Access Management	Soutenir. Limite le niveau d'accès pour les hôtes.
Amazon Route 53	Soutenir. Crée une zone hébergée privée pour résoudre l'équilibreur de charge interne et le nom de domaine hôte du bastion.
Amazon Simple Queue Service	Soutenir. Crée des files de tâches pour prendre en charge les exécutions asynchrones.

Service AWS	Description
Amazon Simple Notification Service	Soutenir. Prend en charge le modèle publicati on-abonné entre les composants VDI tels que le contrôleur et les hôtes.
AWS Fargate	Soutenir. Installe, met à jour et supprime des environnements à l'aide de tâches Fargate.
Passerelle de fichiers Amazon FSx	Facultatif. Fournit un système de fichiers partagé externe.
Amazon FSx pour ONTAP NetApp	Facultatif. Fournit un système de fichiers partagé externe.
AWS Certificate Manager	Facultatif. Génère un certificat fiable pour votre domaine personnalisé.
AWS Backup	Facultatif. Offre des fonctionnalités de sauvegarde pour les hôtes Amazon EC2, les systèmes de fichiers et DynamoDB.

Planifiez votre déploiement

Coût

Research and Engineering Studio on AWS est disponible sans frais supplémentaires et vous ne payez que pour les AWS ressources nécessaires à l'exécution de vos applications. Pour plus d'informations, consultez AWSservices inclus dans ce produit.

> **Note**
>
> Vous êtes responsable du coût des AWS services utilisés lors de l'utilisation de ce produit. Nous vous recommandons de créer un budget AWS Cost Explorerpour aider à gérer les coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque AWS service utilisé dans ce produit.

Sécurité

Lorsque vous créez des systèmes sur une AWS infrastructure, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce modèle de responsabilité partagée réduit votre charge opérationnelle car il AWS exploite, gère et contrôle les composants, notamment le système d'exploitation hôte, la couche de virtualisation et la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur AWS la sécurité, consultez AWS Cloud la section Sécurité.

Rôles IAM

AWS Identity and Access Management Les rôles (IAM) permettent aux clients d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs du. AWS Cloud Ce produit crée des rôles IAM qui accordent aux AWS Lambda fonctions du produit et aux instances Amazon EC2 l'accès pour créer des ressources régionales.

RES prend en charge les politiques basées sur l'identité au sein d'IAM. Lors du déploiement, RES crée des politiques pour définir les autorisations et les accès de l'administrateur. L'administrateur qui implémente le produit crée et gère les utilisateurs finaux et les chefs de projet au sein de l'Active Directory du client existant intégré à RES. Pour plus d'informations, consultez la section Création de politiques IAM dans le guide de l'utilisateur AWS d'Identity and Access Management.

L'administrateur de votre organisation peut gérer l'accès des utilisateurs à l'aide d'un Active Directory. Lorsque les utilisateurs finaux accèdent à l'interface utilisateur RES, RES s'authentifie auprès d'Amazon Cognito.

Groupes de sécurité

Les groupes de sécurité créés dans ce produit sont conçus pour contrôler et isoler le trafic réseau entre les fonctions Lambda, les instances EC2, les instances CSR des systèmes de fichiers et les points de terminaison VPN distants. Nous vous recommandons de passer en revue les groupes de sécurité et de restreindre davantage l'accès selon les besoins une fois le produit déployé.

Chiffrement des données

Par défaut, Research and Engineering Studio on AWS (RES) chiffre les données clients au repos et en transit à l'aide d'une clé détenue par RES. Lorsque vous déployez RES, vous pouvez spécifier un AWS KMS key. RES utilise vos informations d'identification pour accorder un accès clé. Si vous fournissez un produit détenu et géré par un client AWS KMS key, les données du client au repos seront cryptées à l'aide de cette clé.

RES chiffre les données des clients en transit à l'aide du protocole SSL/TLS. Nous avons besoin du protocole TLS 1.2, mais nous recommandons le protocole TLS 1.3.

Soutenu Régions AWS

Ce produit utilise des services qui ne sont pas tous disponibles actuellement Régions AWS. Vous devez lancer ce produit dans un Région AWS endroit où tous les services sont disponibles. Pour connaître la disponibilité la plus récente des AWS services par région, consultez la Région AWS liste complète des services.

Le studio de recherche et d'ingénierie sur AWS est soutenu dans les domaines suivants Régions AWS :

Nom de la région	
USA Est (Ohio)	Canada (Centre)
USA Est (Virginie du Nord)	Europe (Francfort)
USA Ouest (Californie du Nord)	Europe (Irlande)

Nom de la région	
USA Ouest (Oregon)	Europe (Londres)
Asie-Pacifique (Mumbai)	Europe (Milan)
Asie-Pacifique (Séoul)	Europe (Paris)
Asie-Pacifique (Singapour)	Israël (Tel Aviv)
Asie-Pacifique (Sydney)	AWS GovCloud (US-Ouest)
Asie-Pacifique (Tokyo)	

Quotas

Les quotas de service, également appelés limites, sont le nombre maximal de ressources ou d'opérations de service pour vous Compte AWS.

Quotas pour AWS les services inclus dans ce produit

Assurez-vous de disposer d'un quota suffisant pour chacun des services mis en œuvre dans ce produit. Pour de plus amples informations, veuillez consulter les Service Quotas AWS.

Pour ce produit, nous recommandons d'augmenter les quotas pour les services suivants :

- Amazon Virtual Private Cloud
- Amazon EC2

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

AWS CloudFormation quotas

Vous avez Compte AWS AWS CloudFormation des quotas dont vous devez tenir compte lorsque vous lancez le stack de ce produit. En comprenant ces quotas, vous pouvez éviter les erreurs de

limitation qui vous empêcheraient de déployer correctement ce produit. Pour plus d'informations, consultez les AWS CloudFormation quotas dans le guide de l'AWS CloudFormation utilisateur.

Planification de la résilience

Le produit déploie une infrastructure par défaut avec le nombre et la taille minimum d'instances Amazon EC2 pour faire fonctionner le système. Pour améliorer la résilience dans les environnements de production à grande échelle, nous recommandons d'augmenter les paramètres de capacité minimale par défaut au sein des groupes Auto Scaling (ASG) de l'infrastructure. L'augmentation de la valeur d'une instance à deux instances permet de tirer parti de plusieurs zones de disponibilité (AZ) et de réduire le délai de restauration des fonctionnalités du système en cas de perte de données inattendue.

Les paramètres ASG peuvent être personnalisés dans la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/. Le produit crée quatre ASG par défaut, chaque nom se terminant `-asg` par. Vous pouvez modifier les valeurs minimales et souhaitées en fonction de votre environnement de production. Choisissez le groupe que vous souhaitez modifier, puis sélectionnez Actions et Modifier. Pour plus d'informations sur les ASG, consultez la section Scale the size of your Auto Scaling group dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Déployez le produit

> **Note**
>
> Ce produit utilise des AWS CloudFormation modèles et des piles pour automatiser son déploiement. Le ou les CloudFormation modèles décrivent les AWS ressources incluses dans ce produit et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans le ou les modèles.

Avant de lancer le produit, examinez le coût, l'architecture, la sécurité du réseau et les autres considérations abordées précédemment dans ce guide.

Rubriques

Prérequis

Rubriques

Créez un Compte AWS avec un utilisateur administratif

Vous devez avoir Compte AWS un utilisateur administratif :

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Création d'une paire de clés SSH Amazon EC2

Si vous ne possédez pas de paire de clés SSH Amazon EC2, vous devez en créer une. Pour plus d'informations, consultez la section Création d'une paire de clés à l'aide d'Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Augmenter les quotas de service

Nous recommandons d'augmenter les quotas de service pour :

- Amazon VPC
  - Augmenter le quota d'adresses IP Elastic par passerelle NAT de cinq à huit
  - Augmenter le nombre de passerelles NAT par zone de disponibilité de cinq à dix
- Amazon EC2
  - Augmenter les adresses IP élastiques EC2-VPC de cinq à dix

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés. Pour plus d'informations, consultez the section called "Quotas pour AWS les services inclus dans ce produit".

Création d'un domaine public (facultatif)

Nous vous recommandons d'utiliser un domaine personnalisé pour le produit afin de disposer d'une URL conviviale. Vous devez enregistrer un domaine auprès d'Amazon Route 53 ou d'un autre fournisseur et importer un certificat pour le domaine en question AWS Certificate Manager. Si vous possédez déjà un domaine public et un certificat, vous pouvez ignorer cette étape.

1. Suivez les instructions pour enregistrer un domaine auprès de Route53. Vous devriez recevoir un e-mail de confirmation.
2. Récupérez la zone hébergée pour votre domaine. Ceci est créé automatiquement par Route53.
    a. Ouvrez la console Route53.
    b. Choisissez Zones hébergées dans le menu de navigation de gauche.
    c. Ouvrez la zone hébergée créée pour votre nom de domaine et copiez l'ID de zone hébergée.
3. Ouvrez AWS Certificate Manager et suivez ces étapes pour demander un certificat de domaine. Assurez-vous que vous vous trouvez dans la région où vous prévoyez de déployer la solution.
4. Choisissez Lister les certificats dans le menu de navigation et recherchez votre demande de certificat. La demande devrait être en attente.
5. Choisissez votre numéro de certificat pour ouvrir la demande.
6. Dans la section Domaines, choisissez Créer des enregistrements dans Route53. Le traitement de la demande prendra environ dix minutes.
7. Une fois le certificat émis, copiez l'ARN depuis la section État du certificat.

Créer un domaine (GovCloud uniquement)

Si vous déployez un dans la région AWS GovCloud (ouest des États-Unis), vous devrez suivre ces étapes préalables.

1. Déployez la AWS CloudFormation pile de certificats dans le AWS compte de partition commerciale où le domaine public hébergé a été créé.
2. Dans les CloudFormation sorties du certificat, recherchez et notez le `CertificateARN` et`PrivateKeySecretARN`.

3. Dans le compte de GovCloud partition, créez un secret avec la valeur de la `CertificateARN` sortie. Notez le nouvel ARN secret et ajoutez deux balises au secret pour `vdc-gateway` pouvoir accéder à la valeur du secret :

   a. rouge : ModuleName = virtual-desktop-controller

   b. res : EnvironmentName = [nom de l'environnement] (Cela pourrait être res-demo.)

4. Dans le compte de GovCloud partition, créez un secret avec la valeur de la `PrivateKeySecretArn` sortie. Notez le nouvel ARN secret et ajoutez deux balises au secret pour `vdc-gateway` pouvoir accéder à la valeur du secret :

   a. rouge : ModuleName = virtual-desktop-controller

   b. res : EnvironmentName = [nom de l'environnement] (Cela pourrait être res-demo.)

Fournir des ressources externes

Lorsque vous déployez Research and Engineering Studio sur AWS, des ressources externes sont utilisées par le produit dont vous aurez besoin. RES s'attend à ce que ces ressources existent une fois déployées.

- Mise en réseau (VPC, sous-réseaux publics et privés)

  C'est ici que vous exécuterez les instances EC2 utilisées pour héberger l'environnement, Active Directory (AD) et le stockage partagé.

- Stockage (Amazon EFS)

  Les volumes de stockage contiennent les fichiers et les données nécessaires à l'infrastructure de bureau virtuel (VDI).

- Service d'annuaire (AWS Directory Service for Microsoft Active Directory)

  Le service d'annuaire authentifie les utilisateurs sur les pages de l'environnement.

> **Tip**
>
> Si vous déployez un environnement de démonstration et que ces ressources externes ne sont pas disponibles, vous pouvez utiliser des recettes de calcul AWS haute performance pour générer des ressources pour un environnement de démonstration. Consultez la section

suivante pour déployer des ressources dans votre compte. the section called “Création d'un environnement de démonstration”
Pour les déploiements de démonstration dans la région AWS GovCloud (ouest des États-Unis), vous devrez suivre les étapes requises dans. Créer un domaine (GovCloud uniquement)

Configurer LDAPS dans votre environnement (facultatif)

Si vous envisagez d'utiliser la communication LDAPS dans votre environnement, vous devez suivre ces étapes pour créer et joindre des certificats au contrôleur de domaine AWS Managed Microsoft AD (AD) afin d'assurer la communication entre AD et RES.

1. Suivez les étapes indiquées dans Comment activer le protocole LDAPS côté serveur pour votre. AWS Managed Microsoft AD Vous pouvez ignorer cette étape si vous avez déjà activé LDAPS.
2. Après avoir confirmé que LDAPS est configuré sur l'AD, exportez le certificat AD :
   a. Accédez à votre serveur Active Directory.
   b. Ouvrez PowerShell en tant qu'administrateur.
   c. Exécutez `certmgr.msc` pour ouvrir la liste des certificats.
   d. Ouvrez la liste des certificats en ouvrant d'abord les Autorités de certification racine fiables, puis les certificats.
   e. Sélectionnez et maintenez (ou cliquez avec le bouton droit) le certificat portant le même nom que votre serveur AD et choisissez Toutes les tâches, puis Exporter.
   f. Choisissez X.509 codé en Base-64 (.CER), puis Next.
   g. Sélectionnez un répertoire, puis cliquez sur Suivant.
3. Créez un secret dans AWS Secrets Manager :

   Lorsque vous créez votre secret dans Secrets Manager, choisissez Autre type de secrets sous Type de secret et collez votre certificat codé PEM dans le champ Texte en clair.
4. Notez l'ARN créé et saisissez-le comme `DomainTLSCertificateSecretARN` paramètre dansthe section called “Étape 1 : Lancez le produit”.

Configuration d'un VPC privé (facultatif)

Le déploiement d'un studio de recherche et d'ingénierie dans un VPC isolé offre une sécurité renforcée pour répondre aux exigences de conformité et de gouvernance de votre entreprise. Cependant, le déploiement standard de RES repose sur un accès Internet pour installer les dépendances. Pour installer RES dans un VPC privé, vous devez satisfaire aux conditions préalables suivantes :

Rubriques

Préparation d'Amazon Machine Images (AMI)

1. Téléchargez les dépendances. Pour être déployée dans un VPC isolé, l'infrastructure RES nécessite la disponibilité de dépendances sans accès public à Internet.
2. Créez un rôle IAM avec un accès en lecture seule à Amazon S3 et une identité fiable en tant qu'Amazon EC2.
    a. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
    b. Dans Rôles, sélectionnez Créer un rôle.
    c. Sur la page Sélectionner une entité de confiance :
        - Sous Type d'entité de confiance, sélectionnez Service AWS.
        - Pour Cas d'utilisation sous Service ou cas d'utilisation, sélectionnez EC2, puis Next.
    d. Dans Ajouter des autorisations, sélectionnez les politiques d'autorisation suivantes, puis cliquez sur Suivant :
        - Amazon S3 ReadOnlyAccess
        - Amazon SMS ManagedInstanceCore
        - EC2 InstanceProfileForImageBuilder
    e. Ajoutez un nom et une description du rôle, puis choisissez Créer un rôle.
3. Créez le composant du générateur d'images EC2 :

a. Ouvrez la console https://console.aws.amazon.com/imagebuilder EC2 Image Builder à l'adresse.

b. Sous Ressources enregistrées, sélectionnez Composants, puis Créer un composant.

c. Sur la page Créer un composant, entrez les informations suivantes :

- Pour Type de composant, choisissez Construire.
- Pour les détails du composant, choisissez :

Paramètre	Entrée utilisateur
Système d'exploitation d'images (OS)	Linux
Versions de systèmes d'exploitation compatibles	Amazon Linux 2
Nom du composant	Choisissez un nom tel que : *< research-and-engineering-studio -infrastructure>*
Version du composant	Nous vous recommandons de commencer par la version 1.0.0.
Description	Entrée utilisateur facultative.

d. Sur la page Créer un composant, choisissez Définir le contenu du document.

i. Avant de saisir le contenu du document de définition, vous aurez besoin d'un URI pour le fichier tar.gz. Téléchargez le fichier tar.gz fourni par RES dans un compartiment Amazon S3 et copiez l'URI du fichier depuis les propriétés du compartiment.

ii. Saisissez :

> **Note**
>
> `AddEnvironmentVariables`est facultatif, et vous pouvez le supprimer si vous n'avez pas besoin de variables d'environnement personnalisées dans vos hôtes d'infrastructure.
> Si vous configurez `http_proxy` des variables d' `https_proxy`environnement, les `no_proxy` paramètres sont nécessaires

pour empêcher l'instance d'utiliser un proxy pour interroger localhost, les adresses IP des métadonnées de l'instance et les services prenant en charge les points de terminaison VPC.

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

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
```

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

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.local,{{ 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. Choisissez Créer un composant.

4. Créez une recette d'image Image Builder.

a. Sur la page Créer une recette, entrez les informations suivantes :

Section	Paramètre	Entrée utilisateur
Détails de la recette	Nom	Entrez un nom approprié , tel que res-recipe-linux-x 86.
	Version	Entrez une version, commençant généralement par 1.0.0.
	Description	Ajoutez une description facultative.
Image de base	Sélectionnez une image	Sélectionnez les images gérées.
	SE	Amazon Linux
	Origine de l'image	Démarrage rapide (géré par Amazon)
	Nom de l'image	Amazon Linux 2 x86
	Options de gestion automatique des versions	Utilisez la dernière version du système d'exploitation disponible.
Configuration de l'instance	–	Conservez tout dans les paramètres par défaut

Section	Paramètre	Entrée utilisateur
		et assurez-vous que l'option Supprimer l'agent SSM après l'exécution du pipeline n'est pas sélection née.
Répertoire de travail	Chemin du répertoire de travail	/root/bootstrap/re s_dependencies
Composants	Construire des composants	Recherchez et sélectionnez les éléments suivants : • Géré par Amazon : -2-linux aws-cli-version • Géré par Amazon : amazon-cloudwatch-agent-linux • Détenu par vous : composant Amazon EC2 créé précédemm ent. Entrez votre Compte AWS identifia nt et votre actuel Région AWS dans les champs.
	Composants de test	Recherchez et sélection nez : • Géré par Amazon : simple-boot-test-linux

b. Choisissez Créer une recette.

5. Créez la configuration de l'infrastructure Image Builder.

a. Sous Ressources enregistrées, sélectionnez Configurations d'infrastructure.

b. Choisissez Créer une configuration d'infrastructure.

c. Sur la page Créer une configuration d'infrastructure, entrez ce qui suit :

Section	Paramètre	Entrée utilisateur
Général	Nom	Entrez un nom approprié, tel que res-infra-linux-x 86.
	Description	Ajoutez une description facultative.
	Rôle IAM	Sélectionnez le rôle IAM créé précédemment.
AWS infrastructure	Type d’instance	Choisissez t3.medium.

	VPC, sous-réseau et groupes de sécurité	Sélectionnez une option qui autorise l'accès à Internet et au compartim ent Amazon S3. Si vous devez créer un groupe de sécurité, vous pouvez en créer un depuis la console Amazon EC2 avec les entrées suivantes :
		• VPC : sélectionnez le même VPC utilisé pour la configuration de l'infrast ructure. Ce VPC doit avoir accès à Internet.
		• Règle entrante :
		  • Type : SSH
		  • Source : Personnalisé
		  • Bloc CIDR : 0.0.0.0/0

d. Choisissez Créer une configuration d'infrastructure.

6. Créez un nouveau pipeline EC2 Image Builder :

a. Accédez à Pipelines d'images, puis choisissez Créer un pipeline d'images.

b. Sur la page Spécifier les détails du pipeline, entrez ce qui suit et choisissez Next :

- Nom du pipeline et description facultative
- Pour le calendrier de création, définissez un calendrier ou choisissez Manuel si vous souhaitez démarrer le processus de cuisson des AMI manuellement.

c. Sur la page Choisir une recette, choisissez Utiliser une recette existante et entrez le nom de la recette créée précédemment. Choisissez Suivant.

d. Sur la page Définir le traitement d'image, sélectionnez les flux de travail par défaut, puis cliquez sur Suivant.

e. Sur la page Définir la configuration de l'infrastructure, choisissez Utiliser la configuration d'infrastructure existante et entrez le nom de la configuration d'infrastructure créée précédemment. Choisissez Suivant.

f. Sur la page Définir les paramètres de distribution, tenez compte des points suivants pour vos sélections :

- L'image de sortie doit résider dans la même région que l'environnement RES déployé, afin que RES puisse lancer correctement les instances hôtes de l'infrastructure à partir de celui-ci. À l'aide des valeurs par défaut du service, l'image de sortie sera créée dans la région où le service EC2 Image Builder est utilisé.
- Si vous souhaitez déployer RES dans plusieurs régions, vous pouvez choisir Créer de nouveaux paramètres de distribution et y ajouter d'autres régions.

g. Passez en revue vos sélections et choisissez Créer un pipeline.

7. Exécutez le pipeline EC2 Image Builder :

a. Dans Pipelines d'images, recherchez et sélectionnez le pipeline que vous avez créé.

b. Choisissez Actions, puis Run pipeline.

Le pipeline peut prendre entre 45 minutes et une heure pour créer une image AMI.

8. Notez l'ID d'AMI de l'AMI générée et utilisez-le comme entrée pour le paramètre InfrastructureHost AMI dansthe section called “Étape 1 : Lancez le produit”.

Configuration des points de terminaison VPC

Pour déployer RES et lancer des bureaux virtuels, vous devez Services AWS accéder à votre sous-réseau privé. Vous devez configurer les points de terminaison VPC pour fournir l'accès requis, et vous devrez répéter ces étapes pour chaque point de terminaison.

1. Si aucun point de terminaison n'a été configuré auparavant, suivez les instructions fournies dans Accès et Service AWS utilisation d'un point de terminaison VPC d'interface.
2. Sélectionnez un sous-réseau privé dans chacune des deux zones de disponibilité.

Service AWS	Nom du service
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*.cloudformation
Amazon CloudWatch	com.amazonaws.*region*.monitoring
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
Amazon DynamoDB	com.amazonaws. *region* .dynamodb (nécessite un point de terminaison de passerelle)
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

Service AWS	Nom du service
Amazon S3	com.amazonaws. *region* .s3 (Nécessite un point de terminaison de passerelle créé par défaut dans RES.)
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
Amazon SES	com.amazonaws. *region* .email-smtp (Non pris en charge dans les zones de disponibilité suivantes : use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 et 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*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssmmessages

Connectez-vous aux services sans points de terminaison VPC

Pour intégrer des services qui ne prennent pas en charge les points de terminaison VPC, vous pouvez configurer un serveur proxy dans un sous-réseau public de votre VPC. Suivez ces étapes pour créer un serveur proxy avec l'accès minimum nécessaire pour un déploiement de Research and Engineering Studio en utilisant AWS Identity Center comme fournisseur d'identité.

1. Lancez une instance Linux dans le sous-réseau public du VPC que vous utiliserez pour votre déploiement RES.

   - Famille Linux — Amazon Linux 2 ou Amazon Linux 3
   - Architecture — x86
   - Type d'instance : t2.micro ou supérieur
   - Groupe de sécurité — TCP sur le port 3128 à partir de 0.0.0.0/0

2. Connectez-vous à l'instance pour configurer un serveur proxy.

    a. Ouvrez la connexion HTTP.

    b. Autorisez la connexion aux domaines suivants à partir de tous les sous-réseaux concernés :

    - .amazonaws.com (pour les services génériques) AWS
    - .amazoncognito.com (pour Amazon Cognito)
    - .awsapps.com (pour Identity Center)
    - .signin.aws (pour Identity Center)
    - . amazonaws-us-gov.com (pour Gov Cloud)

    c. Refusez toutes les autres connexions.

    d. Activez et démarrez le serveur proxy.

    e. Notez le PORT sur lequel le serveur proxy écoute.

3. Configurez votre table de routage pour autoriser l'accès au serveur proxy.

    a. Accédez à votre console VPC et identifiez les tables de routage pour les sous-réseaux que vous utiliserez pour les hôtes d'infrastructure et les hôtes VDI.

    b. Modifiez la table de routage pour autoriser toutes les connexions entrantes à accéder à l'instance de serveur proxy créée lors des étapes précédentes.

    c. Procédez ainsi pour les tables de routage de tous les sous-réseaux (sans accès Internet) que vous allez utiliser pour l'infrastructure/les VDI.

4. Modifiez le groupe de sécurité de l'instance EC2 du serveur proxy et assurez-vous qu'il autorise les connexions TCP entrantes sur le PORT sur lequel le serveur proxy écoute.

Définir les paramètres de déploiement d'un VPC privé

Dansthe section called “Étape 1 : Lancez le produit”, vous devez saisir certains paramètres dans le AWS CloudFormation modèle. Assurez-vous de définir les paramètres suivants comme indiqué pour réussir le déploiement dans le VPC privé que vous venez de configurer.

Paramètre	Entrée
InfrastructureHostAMI	Utilisez l'ID d'AMI d'infrastructure créé dansthe section called “Préparation d'Amazon Machine Images (AMI)”.

Paramètre	Entrée
IsLoadBalancerInternetFacing	Réglé sur false.
LoadBalancerSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
InfrastructureHostSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
VdiSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
ClientIP	Vous pouvez choisir votre adresse CIDR VPC pour autoriser l'accès à toutes les adresses IP VPC.

Création d'un environnement de démonstration

Si vous effectuez un déploiement dans un environnement hors production et que vous ne disposez pas de ressources externes, vous pouvez commencer par déployer la pile de recettes HPC. Si vous effectuez un déploiement dans un environnement de production et que des ressources externes sont disponibles, vous pouvez passer àthe section called “Étape 1 : Lancez le produit”.

Après avoir déployé les ressources externes, vous pouvez éventuellement suivre les étapes décrites the section called “Configurer LDAPS dans votre environnement (facultatif)” pour tester la communication LDAPS (Secure Lightweight Directory Access Protocol) dans votre environnement de démonstration.

Création de ressources externes

Cette CloudFormation pile crée des certificats de réseau, de stockage, d'Active Directory et de domaine (si un PortalDomainName est fourni). Vous devez disposer de ces ressources externes pour déployer le produit.

Vous pouvez télécharger le modèle de recettes avant le déploiement.

Temps de déploiement : environ 40 à 90 minutes

1. Connectez-vous à la AWS CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.

   > **Note**
   >
   > Vérifiez que vous êtes connecté à votre compte administrateur.

2. Lancez le modèle dans la console.

   Si vous déployez dans la région AWS GovCloud (ouest des États-Unis), lancez le modèle dans le compte de GovCloud partition.

3. Entrez les paramètres du modèle :

Paramètre	Par défaut	Description
DomainName	`corp.res.com`	Domaine utilisé pour l'Active Directory. La valeur par défaut est fournie dans le `LDIF` fichier qui définit les utilisateurs de bootstrap. Si vous souhaitez utiliser les utilisateurs par défaut, laissez la valeur par défaut. Pour modifier la valeur, mettez-la à jour et fournissez un `LDIF` fichier distinct. Il n'est pas nécessaire que cela corresponde au domaine utilisé pour Active Directory.
SubDomain (GovCloud uniquement)		Ce paramètre est facultatif pour les régions commerciales, mais obligatoire pour les GovCloud régions. Si vous fournissez un SubDomain, le paramètre

Paramètre	Par défaut	Description
		sera préfixé DomainNam e par le paramètre fourni. Le nom de domaine Active Directory fourni deviendra un sous-domaine.
AdminPassword		Le mot de passe de l'adminis trateur Active Directory (nom d'utilisateur`Admin`). Cet utilisateur est créé dans le répertoire actif pour la phase d'amorçage initiale et n'est plus utilisé par la suite. Remarque : Le mot de passe de cet utilisateur doit répondre aux exigences de complexité du mot de passe d'Active Directory.
ServiceAccountPassword		Mot de passe utilisé pour créer un compte de service (`ReadOnlyUser`). Ce compte est utilisé pour la synchronisation. Remarque : Le mot de passe de cet utilisateur doit répondre aux exigences de complexité du mot de passe d'Active Directory.

Paramètre	Par défaut	Description
Paire de clés		Connecte les instances administratives à l'aide d'un client SSH. Remarque : Le gestionnaire de AWS Systems Manager session peut également être utilisé pour se connecter à des instances.
Chemin LDIFS3	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	Le chemin Amazon S3 vers un fichier LDIF importé pendant la phase de démarrage de la configuration d'Active Directory. Pour plus d'informations, consultez la section Support LDIF. Le paramètre est prérempli avec un fichier qui crée un certain nombre d'utilisateurs dans Active Directory. Pour consulter le fichier, consultez le fichier res.ldif disponible dans. GitHub

Paramètre	Par défaut	Description
ClientIpCidr		Adresse IP à partir de laquelle vous allez accéder au site. Par exemple, vous pouvez sélectionner votre adresse IP et l'utiliser `[IPADDRESS]/32` pour n'autoriser l'accès qu'à partir de votre hébergeur. Vous pouvez le mettre à jour après le déploiement.
ClientPrefixList		Entrez une liste de préfixes pour permettre l'accès aux nœuds de gestion Active Directory. Pour plus d'informations sur la création d'une liste de préfixes gérée, voir Utilisation de listes de préfixes gérées par le client.
EnvironmentName	`res-`*`[environment name]`*	S'il `PortalDomainName` est fourni, ce paramètre est utilisé pour ajouter des balises aux secrets générés afin qu'ils puissent être utilisés dans l'environnement. Cela devra correspondre au `EnvironmentName` paramètre utilisé lors de la création de la pile RES. Si vous déployez plusieurs environnements dans votre compte, celui-ci doit être unique.

Paramètre	Par défaut	Description
PortalDomainName		Pour les GovCloud déploiements, ne saisissez pas ce paramètre. Les certificats et les secrets ont été créés manuellement lors des prérequis. Le nom de domaine du compte dans Amazon Route 53. Si cela est fourni, un certificat public et un fichier clé seront générés et téléchargés sur AWS Secrets Manager. Si vous avez votre propre domaine et vos propres certificats, ce paramètre `EnvironmentName` peut être laissé vide.

4. Reconnaissez toutes les cases à cocher dans Capabilities, puis choisissez Create stack.

Étape 1 : Lancez le produit

Suivez les step-by-step instructions de cette section pour configurer et déployer le produit dans votre compte.

Temps de déploiement : environ 60 minutes

Vous pouvez télécharger le CloudFormation modèle de ce produit avant de le déployer.

Si vous déployez dans AWS GovCloud (ouest des États-Unis), utilisez ce modèle.

res-stack - Utilisez ce modèle pour lancer le produit et tous les composants associés. La configuration par défaut déploie la pile principale RES et les ressources d'authentification, de frontend et de backend.

> **Note**
>
> AWS CloudFormation les ressources sont créées à partir de constructions AWS Cloud Development Kit (AWS CDK) (AWS CDK).

Le AWS CloudFormation modèle déploie Research and Engineering Studio AWS dans le AWS Cloud. Vous devez remplir les prérequis avant de lancer la pile.

1. Connectez-vous à la AWS CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.
2. Lancez le modèle.

   Pour effectuer un déploiement dans AWS GovCloud (ouest des États-Unis), lancez ce modèle.
3. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer la solution sous une autre forme Région AWS, utilisez le sélecteur de région dans la barre de navigation de la console.

   > **Note**
   >
   > Ce produit utilise le service Amazon Cognito, qui n'est actuellement pas disponible dans tous les cas. Régions AWS Vous devez lancer ce produit Région AWS là où Amazon Cognito est disponible. Pour connaître la disponibilité la plus récente par région, consultez la Région AWS liste complète des services.
4. Sous Paramètres, passez en revue les paramètres de ce modèle de produit et modifiez-les si nécessaire. Si vous avez déployé les ressources externes automatisées, vous pouvez trouver ces paramètres dans l'onglet Sorties de la pile de ressources externes.

Paramètre	Par défaut	Description
EnvironmentName	*< re-démo >*	Nom unique attribué à votre environnement RES, commençant par res- et ne dépassant pas 11 caractères.

Paramètre	Par défaut	Description
AdministratorEmail		Adresse e-mail de l'utilisateur qui termine la configuration du produit. Cet utilisateur joue également le rôle d'un utilisateur hors pair en cas d'échec de l'intégration de l'authentification unique dans Active Directory.
InfrastructureHostAMI	ami- *[chiffres ou lettres uniquement]*	(Facultatif) Vous pouvez fournir un identifiant d'AMI personnalisé à utiliser pour tous les hôtes de l'infrastructure. Le système d'exploitation de base actuellement pris en charge est Amazon Linux 2. Pour plus d'informations, consultez the section called "Configurer des AMI prêtes pour les RES".
SSH KeyPair		La paire de clés utilisée pour se connecter aux hôtes de l'infrastructure.
ClientIP	*x.x.x .0/24 ou x.x.x .0/32*	Filtre d'adresse IP qui limite la connexion au système. Vous pouvez le mettre à jour ClientIpCidr après le déploiement.

Paramètre	Par défaut	Description
ClientPrefixList		(Facultatif) Fournissez une liste de préfixes gérés pour les adresses IP autorisée s à accéder directement à l'interface utilisateur Web et au protocole SSH sur l'hôte Bastion.
IAM PermissionBoundary		(Facultatif) Vous pouvez fournir un ARN de politique géré qui sera attaché en tant que limite d'autorisation à tous les rôles créés dans RES. Pour plus d'informa tions, consultez the section called "Définition de limites d'autorisation personnal isées".
VpcId		IP du VPC où les instances seront lancées.
IsLoadBalancerInternetFacin g		Sélectionnez true pour déployer un équilibreur de charge connecté à Internet (nécessite des sous-réseaux publics pour l'équilibreur de charge). Pour les déploieme nts nécessitant un accès Internet restreint, sélection nez false.

Paramètre	Par défaut	Description
LoadBalancerSubnets		Sélectionnez au moins deux sous-réseaux dans différentes zones de disponibilité où les équilibreurs de charge seront lancés. Pour les déploiements nécessitant un accès Internet restreint, choisissez des sous-réseaux privés. Pour les déploiements nécessitant un accès à Internet, choisissez des sous-réseaux publics. Si plus de deux ont été créés par la pile réseau externe, sélectionnez tous ceux qui ont été créés.
InfrastructureHostSubnets		Sélectionnez au moins deux sous-réseaux privés dans différentes zones de disponibilité où les hôtes de l'infrastructure seront lancés. Si plus de deux ont été créés par la pile réseau externe, sélectionnez tous ceux qui ont été créés.

Paramètre	Par défaut	Description
VdiSubnets		Sélectionnez au moins deux sous-réseaux privés dans différentes zones de disponibilité où les instances VDI seront lancées. Si plus de deux ont été créés par la pile réseau externe, sélectionnez tous ceux qui ont été créés.
ActiveDirectoryName	`corp.res.com`	Domaine de l'Active Directory. Il n'est pas nécessaire qu'il corresponde au nom de domaine du portail.
ANNONCE ShortName	`corp`	Nom abrégé de l'Active Directory. Ce nom est également appelé le nom NetBIOS.
Base LDAP	**`DC=corp,DC=res,DC=com`**	Un chemin LDAP vers la base au sein de la hiérarchie LDAP.
URI de connexion LDAP		Un chemin ldap ://unique accessible par le serveur hôte d'Active Directory . Si vous avez déployé les ressources externes automatisées avec le domaine AD par défaut, vous pouvez utiliser ldap : // corp.res.com.

Paramètre	Par défaut	Description
ServiceAccountUserName	ServiceAccount	Nom d'utilisateur d'un compte de service utilisé pour se connecter à AD. Ce compte doit avoir accès pour créer des ordinateurs dans le ComputerSOU.
ServiceAccountPassword		Mot de passe créé pour ServiceAccountUserName.
Utilisateur Sou		Unité organisationnelle au sein d'AD pour les utilisate urs qui se synchroniseront.
Grupo Sou		Unité organisationnelle au sein d'AD pour les groupes qui seront synchronisés.
Sudo Ersou		Unité organisationnelle au sein d'AD pour les sudoers mondiaux.
SudoersGroupName	Administrateurs RES	Nom du groupe contenant tous les utilisateurs disposant d'un accès sudoer sur les instances lors de l'installation et d'un accès administrateur sur RES.
Ordinateur SOU		Unité organisationnelle au sein d'AD que les instances rejoindront.

Paramètre	Par défaut	Description
Domaine : TLS Certificat eSecret (ARN)		(Facultatif) Fournissez un ARN secret de certificat TLS de domaine pour permettre la communication TLS avec AD.
EnableLdapCartographie d'identité		Détermine si les numéros UID et GID sont générés par SSSD ou si les numéros fournis par l'AD sont utilisés. Définissez sur True pour utiliser l'UID et le GID générés par SSSD, ou sur False pour utiliser l'UID et le GID fournis par l'AD.
Désactiver Adjoin	False	Pour empêcher les hôtes Linux de rejoindre le domaine du répertoire, passez à True. Dans le cas contraire, conservez le paramètre par défaut False.
ServiceAccountUserDN		Indiquez le nom distinctif (DN) de l'utilisateur du compte de service dans le répertoire.
SharedHomeFilesystemID		ID EFS à utiliser pour le système de fichiers de base partagé pour les hôtes Linux VDI.

Paramètre	Par défaut	Description
CustomDomainNamefo rWebApp		(Facultatif) Sous-domaine utilisé par le portail Web pour fournir des liens vers la partie Web du système.
CustomDomainNameforVDI		(Facultatif) Sous-domaine utilisé par le portail Web pour fournir des liens vers la partie VDI du système.
Certificat ACM AR NforWebApp		(Facultatif) Lorsque vous utilisez la configuration par défaut, le produit héberge l'application Web sous le domaine amazonaws.com. Vous pouvez héberger les produits et services sous votre domaine. Si vous avez déployé les ressource s externes automatisées, celles-ci ont été générées pour vous et les informations se trouvent dans les sorties de la pile res-bi. Si vous devez générer un certificat pour votre application Web, consultezGuide de configura tion.

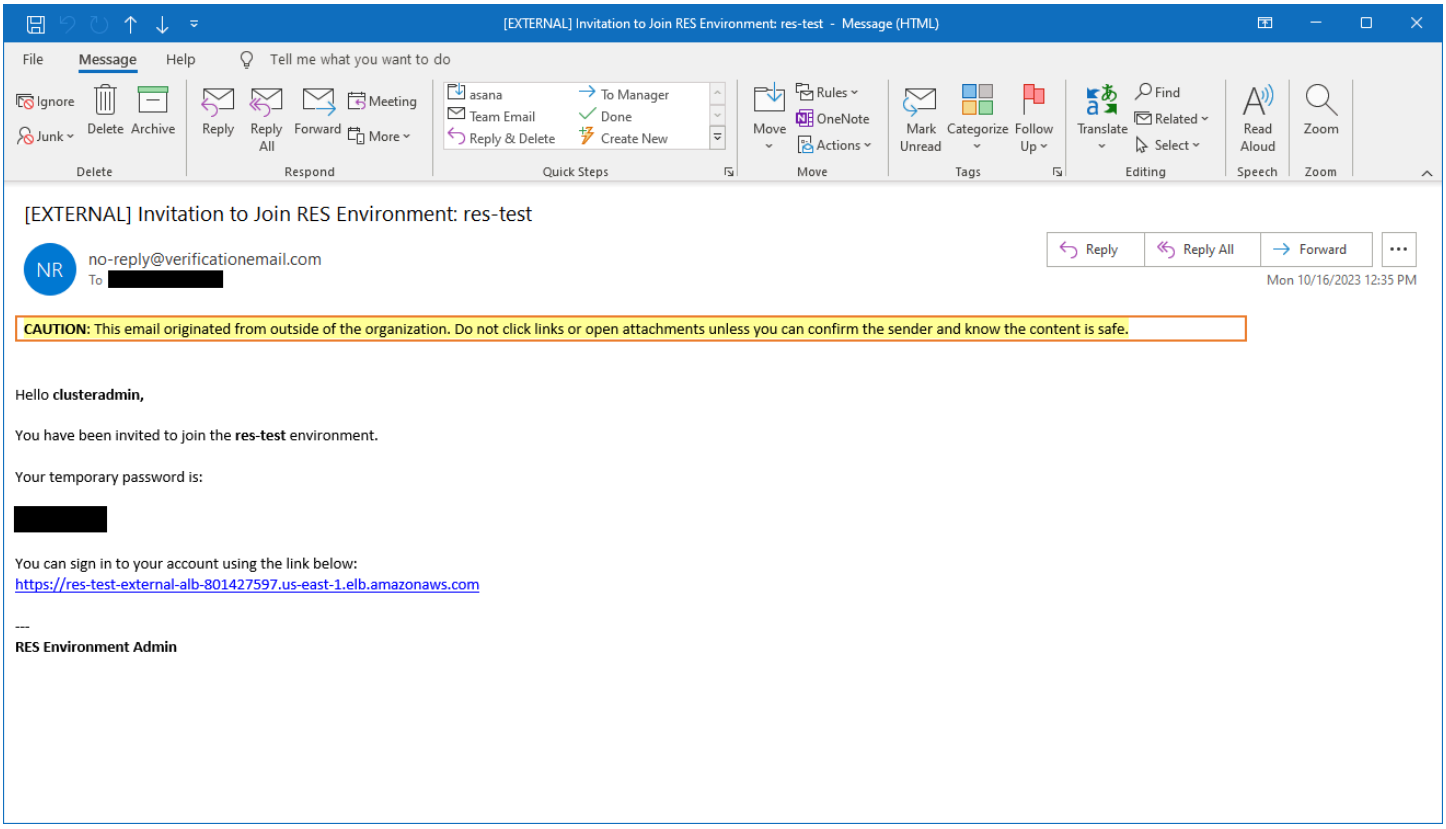
Paramètre	Par défaut	Description
CertificateSecretARN pour VDI		(Facultatif) Ce secret ARN stocke le certificat public du certificat public de votre portail Web. Si vous définissez un nom de domaine de portail pour vos ressources externes automatisées, vous pouvez trouver cette valeur sous l'onglet Outputs de la pile res-bi.
PrivateKeySecretARN pour VDI		(Facultatif) Ce secret ARN stocke la clé privée du certificat de votre portail Web. Si vous définissez un nom de domaine de portail pour vos ressources externes automatisées, vous pouvez trouver cette valeur sous l'onglet Outputs de la pile res-bi.

5. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 60 minutes.

Étape 2 : Connectez-vous pour la première fois

Une fois la pile de produits déployée sur votre compte, vous recevrez un e-mail contenant vos informations d'identification. Utilisez l'URL pour vous connecter à votre compte et configurer l'espace de travail pour les autres utilisateurs.



Une fois que vous vous êtes connecté pour la première fois, vous pouvez configurer les paramètres du portail Web pour vous connecter au fournisseur SSO. Pour obtenir des informations de configuration après le déploiement, consultez leGuide de configuration.

Mettre à jour le produit

Research and Engineering Studio (RES) dispose de deux méthodes pour mettre à jour le produit, selon qu'il s'agit d'une mise à jour majeure ou mineure.

RES utilise un schéma de version basé sur la date. Une version majeure utilise l'année et le mois, et une version mineure ajoute un numéro de séquence si nécessaire. Par exemple, la version 2024.01 a été publiée en janvier 2024 en tant que version majeure ; la version 2024.01.01 était une mise à jour mineure de cette version.

Rubriques

Mises à jour majeures des versions

Research and Engineering Studio utilise des instantanés pour faciliter la migration d'un environnement RES antérieur vers le dernier sans perdre les paramètres de votre environnement. Vous pouvez également utiliser ce processus pour tester et vérifier les mises à jour de votre environnement avant d'intégrer des utilisateurs.

Pour mettre à jour votre environnement avec la dernière version de RES :

1. Créez un instantané de votre environnement actuel. veuillez consulter the section called “Créer un instantané”.
2. Redéployez RES avec la nouvelle version. veuillez consulter the section called “Étape 1 : Lancez le produit”.
3. Appliquez l'instantané à votre environnement mis à jour. veuillez consulter the section called “Appliquer un instantané”.
4. Vérifiez que toutes les données ont bien migré vers le nouvel environnement.

Mises à jour de versions mineures

Pour les mises à jour mineures de RES, aucune nouvelle installation n'est requise. Vous pouvez mettre à jour la pile RES existante en mettant à jour son AWS CloudFormation modèle. Vérifiez la

version de votre environnement RES actuel AWS CloudFormation avant de déployer la mise à jour. Vous trouverez le numéro de version au début du modèle.

Par exemple : `"Description": "RES_2024.1"`

Pour effectuer une mise à jour de version mineure :

1. Téléchargez le dernier AWS CloudFormation modèle enthe section called "Étape 1 : Lancez le produit".
2. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
3. Dans Stacks, recherchez et sélectionnez la pile principale. Il doit apparaître sous la forme*<stack-name>*.
4. Choisissez Mettre à jour.
5. Choisissez Remplacer le modèle actuel.
6. Pour Source du modèle, choisissez Charger un fichier de modèle.
7. Choisissez Choisir un fichier et chargez le modèle que vous avez téléchargé.
8. Dans Spécifier les détails de la pile, choisissez Next. Il n'est pas nécessaire de mettre à jour les paramètres.
9. Dans Configurer les options de pile, choisissez Next.
10. Lors de la révision<stack-name>, choisissez Soumettre.

Désinstallez le produit

Vous pouvez désinstaller le studio de recherche et d'ingénierie AWS du produit depuis AWS Management Console ou en utilisant le AWS Command Line Interface. Vous devez supprimer manuellement les compartiments Amazon Simple Storage Service (Amazon S3) créés par ce produit. Ce produit ne supprime pas automatiquement < EnvironmentName >- shared-storage-security-group si vous avez enregistré des données à conserver.

À l'aide du AWS Management Console

1. Connectez-vous à la console AWS CloudFormation.
2. Sur la page Stacks, sélectionnez la pile d'installation de ce produit.
3. Sélectionnez Delete (Supprimer).

En utilisant AWS Command Line Interface

Déterminez si le AWS Command Line Interface (AWS CLI) est disponible dans votre environnement. Pour les instructions d'installation, reportez-vous à la section « Qu'est-ce qu'il y a AWS Command Line Interface dans le guide de AWS CLI l'utilisateur ? » Après avoir confirmé que le produit AWS CLI est disponible et configuré sur le compte administrateur de la région où le produit a été déployé, exécutez la commande suivante.

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

Suppression du shared-storage-security-group

> **Warning**
>
> Le produit conserve ce système de fichiers par défaut pour éviter toute perte de données involontaire. Si vous choisissez de supprimer le groupe de sécurité et les systèmes de fichiers associés, toutes les données conservées dans ces systèmes seront définitivement supprimées. Nous vous recommandons de sauvegarder les données ou de les réaffecter à un nouveau groupe de sécurité.

1. Connectez-vous à la console Amazon EFS AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/efs/.
2. Supprimez tous les systèmes de fichiers associés à <RES-stack-name>-shared-storage-security-group. Vous pouvez également réaffecter ces systèmes de fichiers à un autre groupe de sécurité pour conserver les données.
3. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
4. Supprimez le <RES-stack-name>-shared-storage-security-group.

Suppression des compartiments Amazon S3

Ce produit est configuré pour conserver le compartiment Amazon S3 créé par le produit (à déployer dans une région optionnelle) si vous décidez de supprimer la AWS CloudFormation pile afin d'éviter toute perte de données accidentelle. Après avoir désinstallé le produit, vous pouvez supprimer manuellement ce compartiment S3 si vous n'avez pas besoin de conserver les données. Suivez ces étapes pour supprimer le compartiment Amazon S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Buckets dans le volet de navigation.
3. Localisez les compartiments `stack-name` S3.
4. Sélectionnez chaque compartiment Amazon S3, puis choisissez Empty. Vous devez vider chaque seau.
5. Sélectionnez le compartiment S3, puis choisissez Supprimer.

Pour supprimer des compartiments S3 à l'aide de AWS CLI, exécutez la commande suivante :

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

> **Note**
>
> La `--force` commande vide le compartiment de son contenu.

Guide de configuration

Ce guide de configuration fournit des instructions post-déploiement destinées à un public technique sur la manière de personnaliser et d'intégrer davantage le studio de recherche et d'ingénierie AWS du produit.

Rubriques

Gestion des utilisateurs et des groupes

Research and Engineering Studio peut utiliser n'importe quel fournisseur d'identité conforme à la norme SAML 2.0. Si vous avez déployé RES à l'aide de ressources externes ou si vous prévoyez d'utiliser le centre d'identité IAM, consultezthe section called “Configuration du SSO avec IAM Identity Center”. Si vous avez votre propre fournisseur d'identité conforme à la norme SAML 2.0, consultezthe section called “Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)”.

Rubriques

Configuration du SSO avec IAM Identity Center

Si aucun centre d'identité n'est déjà connecté à l'Active Directory géré, commencez parthe section called “Mettre en place un centre d'identité”. Si vous avez déjà un centre d'identité connecté à l'Active Directory géré, commencez parthe section called “Connectez-vous à un centre d'identité”.

> **Note**
>
> Si vous effectuez un déploiement dans la région AWS GovCloud (ouest des États-Unis), configurez le SSO dans le compte de AWS GovCloud (US) partition sur lequel vous avez déployé Research and Engineering Studio.

Étape 1 : configurer un centre d'identité

Activation du centre d'identité

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Ouvrez le Identity Center.
3. Sélectionnez Activer.
4. Choisissez Activer avec AWS Organizations.
5. Choisissez Continuer.

> **Note**
>
> Assurez-vous que vous vous trouvez dans la même région que celle dans laquelle vous avez géré Active Directory.

Connexion du centre d'identité à un Active Directory géré

Après avoir activé le centre d'identité, suivez les étapes de configuration recommandées ci-dessous :

1. Dans le menu de navigation, choisissez Réglages.
2. Sous Source d'identité, choisissez Actions, puis Modifier la source d'identité.
3. Sous Répertoires existants, sélectionnez votre répertoire.
4. Choisissez Suivant.
5. Vérifiez vos modifications et entrez **`ACCEPT`** dans le champ de confirmation.
6. Choisissez Modifier la source d'identité.

Synchronisation des utilisateurs et des groupes avec le centre d'identité

Une fois les modifications the section called “Connexion du centre d'identité à un Active Directory géré” terminées, une bannière verte devrait apparaître.

1. Dans le bandeau de confirmation, sélectionnez Démarrer la configuration guidée.
2. Dans Configurer les mappages d'attributs, choisissez Next.
3. Dans la section Utilisateur, entrez les utilisateurs que vous souhaitez synchroniser.
4. Choisissez Ajouter.
5. Choisissez Suivant.
6. Passez en revue vos modifications et choisissez Enregistrer la configuration.
7. Le processus de synchronisation peut prendre quelques minutes. Si vous recevez un message d'avertissement indiquant que les utilisateurs ne se synchronisent pas, choisissez Reprendre la synchronisation.

Activation des utilisateurs

1. Dans le menu, sélectionnez Utilisateurs.
2. Choisissez le ou les utilisateurs pour lesquels vous souhaitez activer l'accès.
3. Choisissez Activer l'accès utilisateur.

Étape 2 : Se connecter à un centre d'identité

Configuration de l'application dans Identity Center

1. Connectez-vous au IAM Identity Center AWS Management Console et ouvrez-le à l'adresse https://console.aws.amazon.com/singlesignon/.
2. Choisissez Applications.
3. Choisissez Add application (Ajouter une application).
4. Dans les préférences de configuration, choisissez J'ai une application que je souhaite configurer.
5. Sous Type d'application, choisissez SAML 2.0.
6. Choisissez Suivant.
7. Entrez le nom d'affichage et la description que vous souhaitez utiliser.
8. Sous métadonnées IAM Identity Center, copiez le lien vers le fichier de métadonnées SAML IAM Identity Center. Vous en aurez besoin pour configurer le SSO avec le portail RES.

9. Sous Propriétés de l'application, entrez l'URL de démarrage de votre application. Par exemple, < your-portal-domain >/sso.
10. Sous URL ACS de l'application, entrez l'URL de redirection depuis le portail RES. Pour le trouver :
    a. Sous Gestion de l'environnement, sélectionnez Paramètres généraux.
    b. Choisissez l'onglet Identity provider.
    c. Sous Single Sign-On, vous trouverez l'URL de redirection SAML.
11. Sous Audience SAML de l'application, entrez l'URN Amazon Cognito. Pour créer l'urne :
    a. Depuis le portail RES, ouvrez les paramètres généraux.
    b. Une fois dans l'onglet Fournisseur d'identité, localisez l'ID du groupe d'utilisateurs.
    c. Ajoutez l'ID du groupe d'utilisateurs à cette chaîne :

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

12. Sélectionnez Envoyer.

Configuration des mappages d'attributs pour l'application

1. Dans le Identity Center, ouvrez les informations relatives à l'application que vous avez créée.
2. Choisissez Actions, puis Modifier les mappages d'attributs.
3. Dans le champ Objet, saisissez $ {user:email}.
4. Sous Format, choisissez EmailAddress.
5. Choisissez Ajouter un nouveau mappage d'attributs.
6. Sous Attribut utilisateur dans l'application, entrez e-mail.
7. Sous Correspond à cette valeur de chaîne ou à cet attribut utilisateur dans IAM Identity Center, entrez $ {user:email}.
8. Dans Format, entrez non spécifié.
9. Sélectionnez Enregistrer les modifications.

Ajouter des utilisateurs à l'application dans Identity Center

1. Dans le Identity Center, ouvrez Utilisateurs assignés pour l'application que vous avez créée et choisissez Attribuer des utilisateurs.

2. Sélectionnez les utilisateurs auxquels vous souhaitez attribuer l'accès à l'application.
3. Choisissez Assign users (Affecter des utilisateurs).

Configuration du SSO dans l'environnement RES

1. Dans l'environnement du studio de recherche et d'ingénierie, ouvrez les paramètres généraux sous Gestion de l'environnement.
2. Ouvrez l'onglet Fournisseur d'identité.
3. Sous Single Sign-On, cliquez sur le bouton Modifier à côté de Status.
4. Complétez le formulaire avec les informations suivantes :
    a. Choisissez SAML.
    b. Sous Nom du fournisseur, entrez un nom convivial.
    c. Sélectionnez Entrer l'URL du point de terminaison du document de métadonnées.
    d. Entrez l'URL que vous avez copiée pendant the section called “Configuration de l'application dans Identity Center”
    e. Sous Attribut e-mail du fournisseur, entrez e-mail.
    f. Sélectionnez Envoyer.
5. Actualisez la page et vérifiez que le statut s'affiche comme activé.

Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)

Research and Engineering Studio s'intègre à n'importe quel fournisseur d'identité SAML 2.0 pour authentifier l'accès des utilisateurs au portail RES. Ces étapes indiquent comment intégrer le fournisseur d'identité SAML 2.0 que vous avez choisi. Si vous avez l'intention d'utiliser IAM Identity Center, consultezthe section called “Configuration du SSO avec IAM Identity Center”.

> **Note**
>
> L'adresse e-mail de l'utilisateur doit correspondre dans l'assertion SAML de l'IDP et dans Active Directory. Vous devrez connecter votre fournisseur d'identité à votre Active Directory et synchroniser régulièrement les utilisateurs.

Rubriques

Configurez votre fournisseur d'identité

Cette section décrit les étapes à suivre pour configurer votre fournisseur d'identité avec les informations du groupe d'utilisateurs RES Amazon Cognito.

1. RES suppose que vous disposez d'un AD (AWS Managed AD ou AD auto-provisionné) avec les identités d'utilisateur autorisées à accéder au portail et aux projets RES. Connectez votre AD à votre fournisseur de services d'identité et synchronisez les identités des utilisateurs. Consultez la documentation de votre fournisseur d'identité pour savoir comment connecter votre AD et synchroniser les identités des utilisateurs. Par exemple, consultez la section Utilisation d'Active Directory comme source d'identité dans le Guide de AWS IAM Identity Center l'utilisateur.
2. Configurez une application SAML 2.0 pour RES dans votre fournisseur d'identité (IdP). Cette configuration nécessite les paramètres suivants :
   - URL de redirection SAML : URL utilisée par votre IdP pour envoyer la réponse SAML 2.0 au fournisseur de services.

     > **Note**
     >
     > En fonction de l'IdP, l'URL de redirection SAML peut porter un nom différent :
     >
     > - URL de l'application
     > - URL du service Assertion Consumer (ACS)
     > - URL de liaison ACS POST

     Pour obtenir l'URL

     1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
     2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
     3. Choisissez l'URL de redirection SAML.

- URI d'audience SAML : ID unique de l'entité d'audience SAML du côté du fournisseur de services.

  > **Note**
  >
  > En fonction de l'IdP, l'URI d'audience SAML peut porter un nom différent :
  >
  > - ClientID
  > - Audience SAML de l'application
  > - ID de l'entité SP

  Fournissez l'entrée dans le format suivant.

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

  Pour trouver l'URI de votre audience SAML

  1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
  2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
  3. Choisissez User Pool Id.

3. L'assertion SAML publiée sur RES doit comporter les champs/revendications suivants définis sur l'adresse e-mail de l'utilisateur :
   - Sujet ou NameID SAML
   - Courrier électronique SAML
4. Votre IdP ajoute des champs/revendications à l'assertion SAML, en fonction de la configuration. RES nécessite ces champs. La plupart des fournisseurs remplissent automatiquement ces champs par défaut. Reportez-vous aux entrées et valeurs de champ suivantes si vous devez les configurer.

   - AudienceRestriction— Réglé sur`urn:amazon:cognito:sp:user-pool-id`. *user-pool-id*Remplacez-le par l'ID de votre groupe d'utilisateurs Amazon Cognito.

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

```
</saml:AudienceRestriction>
```

- Réponse — Réglé `InResponseTo` surhttps://*user-pool-domain*/saml2/idpresponse. *user-pool-domain*Remplacez-le par le nom de domaine de votre groupe d'utilisateurs Amazon Cognito.

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

- SubjectConfirmationData— Réglé sur `Recipient` le point de `saml2/idpresponse` terminaison de votre groupe d'utilisateurs et `InResponseTo` sur l'ID de demande SAML d'origine.

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

- AuthnStatement— Configurez comme suit :

```
<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. Si votre application SAML possède un champ URL de déconnexion, définissez-le sur :. <*domain-url*>/saml2/logout

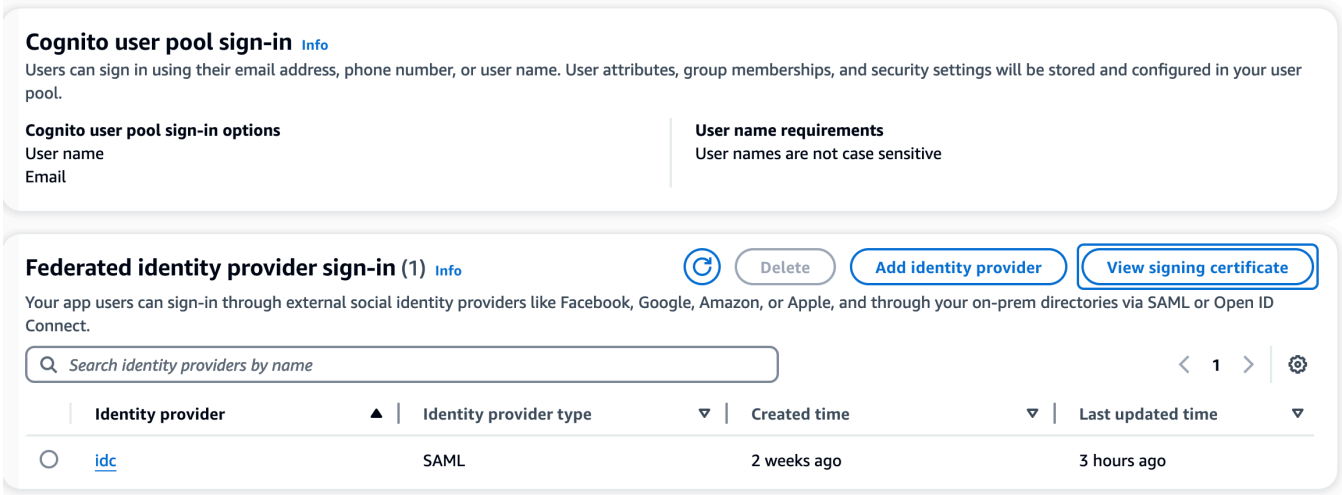
Pour obtenir l'URL du domaine

1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.
3. Choisissez l'URL du domaine.

6. Si votre IdP accepte un certificat de signature pour établir la confiance avec Amazon Cognito, téléchargez le certificat de signature Amazon Cognito et chargez-le dans votre IdP.

Pour obtenir le certificat de signature

1. Ouvrez la console Amazon Cognito dans la section Getting Started with AWS Management Console
2. Sélectionnez votre groupe d'utilisateurs. Votre groupe d'utilisateurs doit être`res-<environment name>-user-pool`.
3. Choisissez l'onglet Sign-in experience (Expérience de connexion).
4. Dans la section Connexion au fournisseur d'identité fédéré, choisissez Afficher le certificat de signature.



Vous pouvez utiliser ce certificat pour configurer Active Directory IDP, en ajouter un `relying party trust` et activer le support SAML sur cette partie utilisatrice.

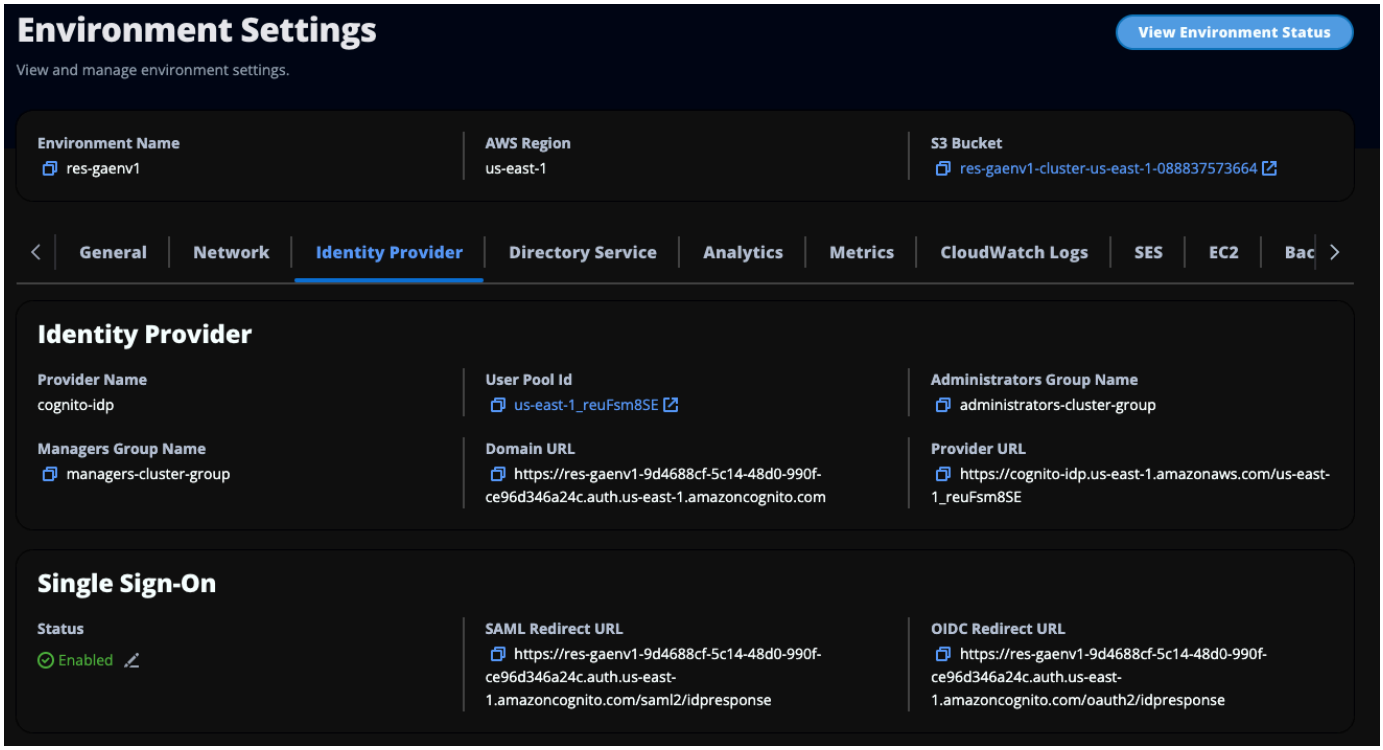
> **Note**
>
> Cela ne s'applique pas à Keycloak et IDC.

5. Une fois la configuration de l'application terminée, téléchargez le XML ou l'URL des métadonnées de l'application SAML 2.0. Vous l'utiliserez dans la section suivante.

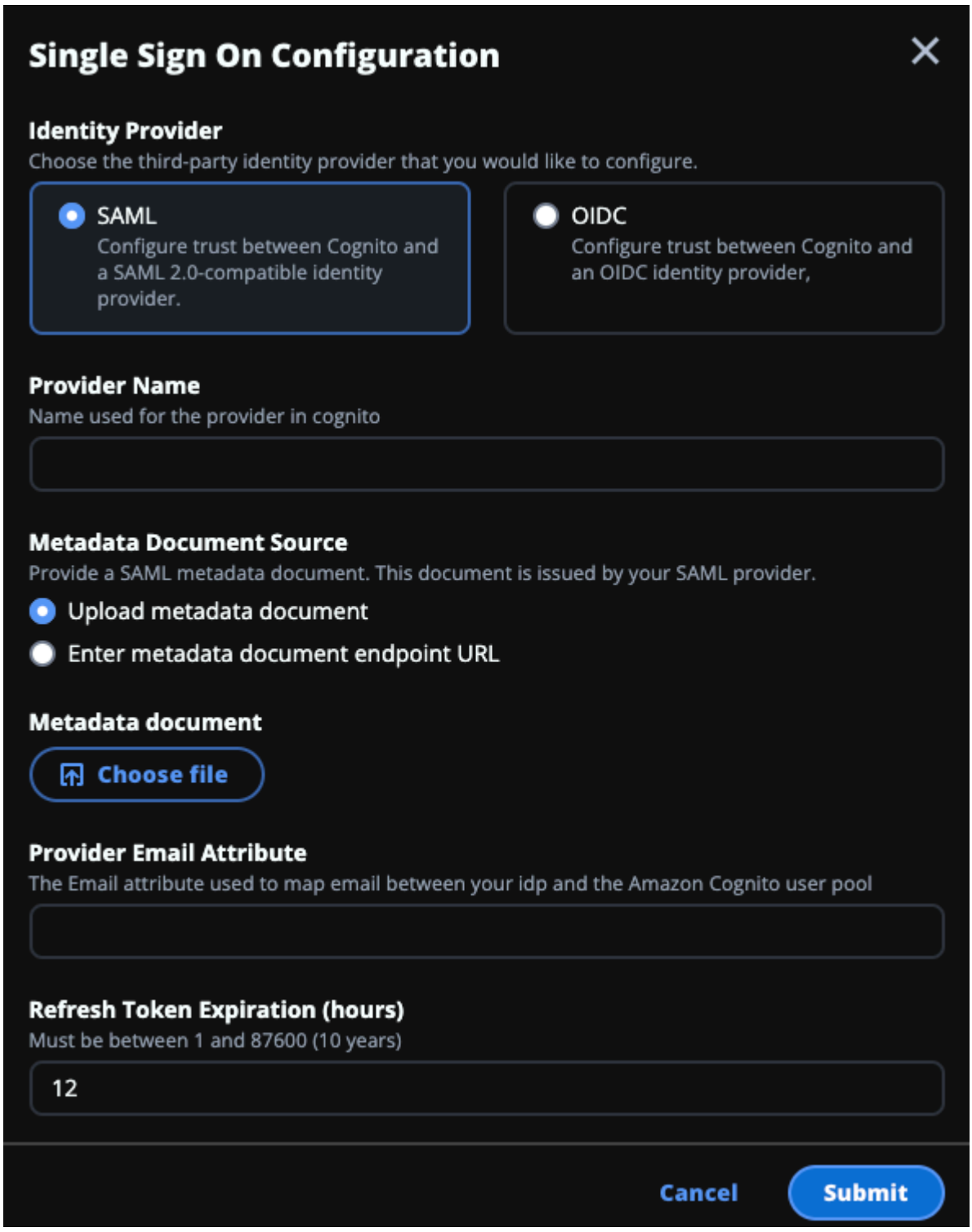
Configurez RES pour utiliser votre fournisseur d'identité

Pour terminer la configuration de l'authentification unique pour RES

1. Connectez-vous à RES en tant qu'administrateur ou clusteradmin.
2. Accédez à Gestion de l'environnement ⇒ Paramètres généraux ⇒ Fournisseur d'identité.



3. Sous Single Sign-On, cliquez sur l'icône de modification à côté de l'indicateur d'état pour ouvrir la page de configuration de Single Sign-On.



a. Pour le fournisseur d'identité, choisissez SAML.

b. Dans Nom du fournisseur, entrez un nom unique pour votre fournisseur d'identité.

> **Note**
>
> Les noms suivants ne sont pas autorisés :
>
> - Cognito
> - IdentityCenter

c. Sous Source du document de métadonnées, choisissez l'option appropriée et téléchargez le document XML de métadonnées ou fournissez l'URL du fournisseur d'identité.

d. Pour Attribut d'e-mail du fournisseur, entrez la valeur du texte`email`.

e. Sélectionnez Envoyer.

4. Rechargez la page des paramètres d'environnement. L'authentification unique est activée si la configuration est correcte.

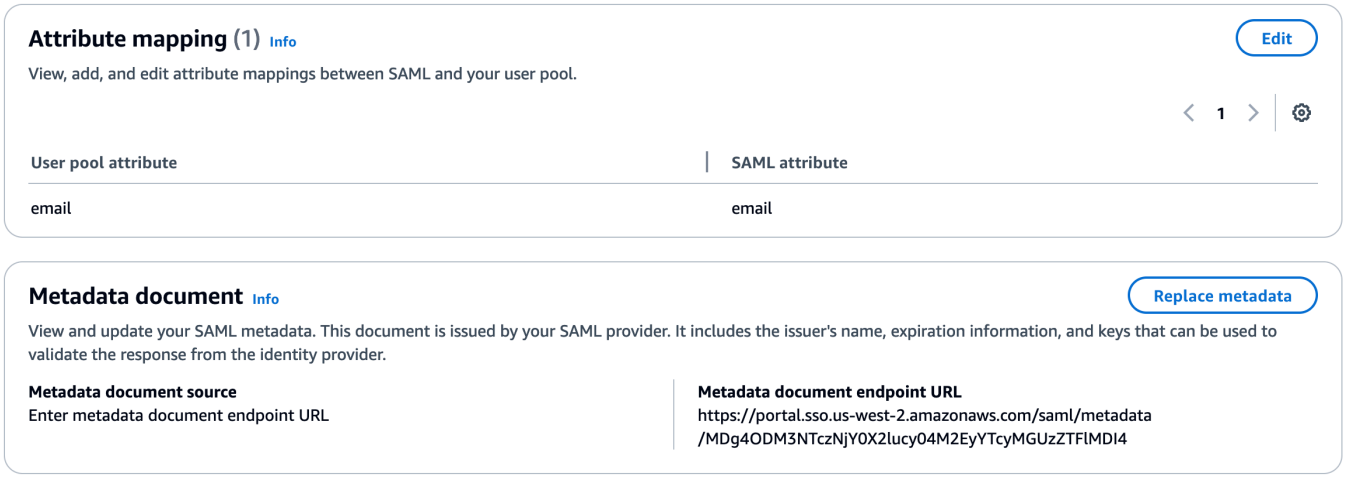
Configuration de votre fournisseur d'identité dans un environnement hors production

Si vous avez utilisé les ressources externes fournies pour créer un environnement RES hors production et que vous avez configuré IAM Identity Center comme fournisseur d'identité, vous souhaiterez peut-être configurer un autre fournisseur d'identité tel qu'Okta. Le formulaire d'activation de RES SSO demande trois paramètres de configuration :

1. Nom du fournisseur : ne peut pas être modifié
2. Document de métadonnées ou URL — Peut être modifié
3. Attribut e-mail du fournisseur — Peut être modifié

Pour modifier le document de métadonnées et l'attribut e-mail du fournisseur, procédez comme suit :

1. Accédez à la console Amazon Cognito.
2. Dans le menu de navigation, sélectionnez Groupes d'utilisateurs.
3. Choisissez votre groupe d'utilisateurs pour afficher l'aperçu du groupe d'utilisateurs.
4. Dans l'onglet Expérience de connexion, accédez à Connexion au fournisseur d'identité fédéré et ouvrez votre fournisseur d'identité configuré.
5. En règle générale, il vous suffit de modifier les métadonnées et de laisser le mappage des attributs inchangé. Pour mettre à jour le mappage des attributs, choisissez Modifier. Pour mettre à jour le document de métadonnées, choisissez Remplacer les métadonnées.



6. Si vous avez modifié le mappage des attributs, vous devez mettre à jour la `<environment name>.cluster-settings` table dans DynamoDB.

   a. Ouvrez la console DynamoDB et choisissez Tables dans le menu de navigation.

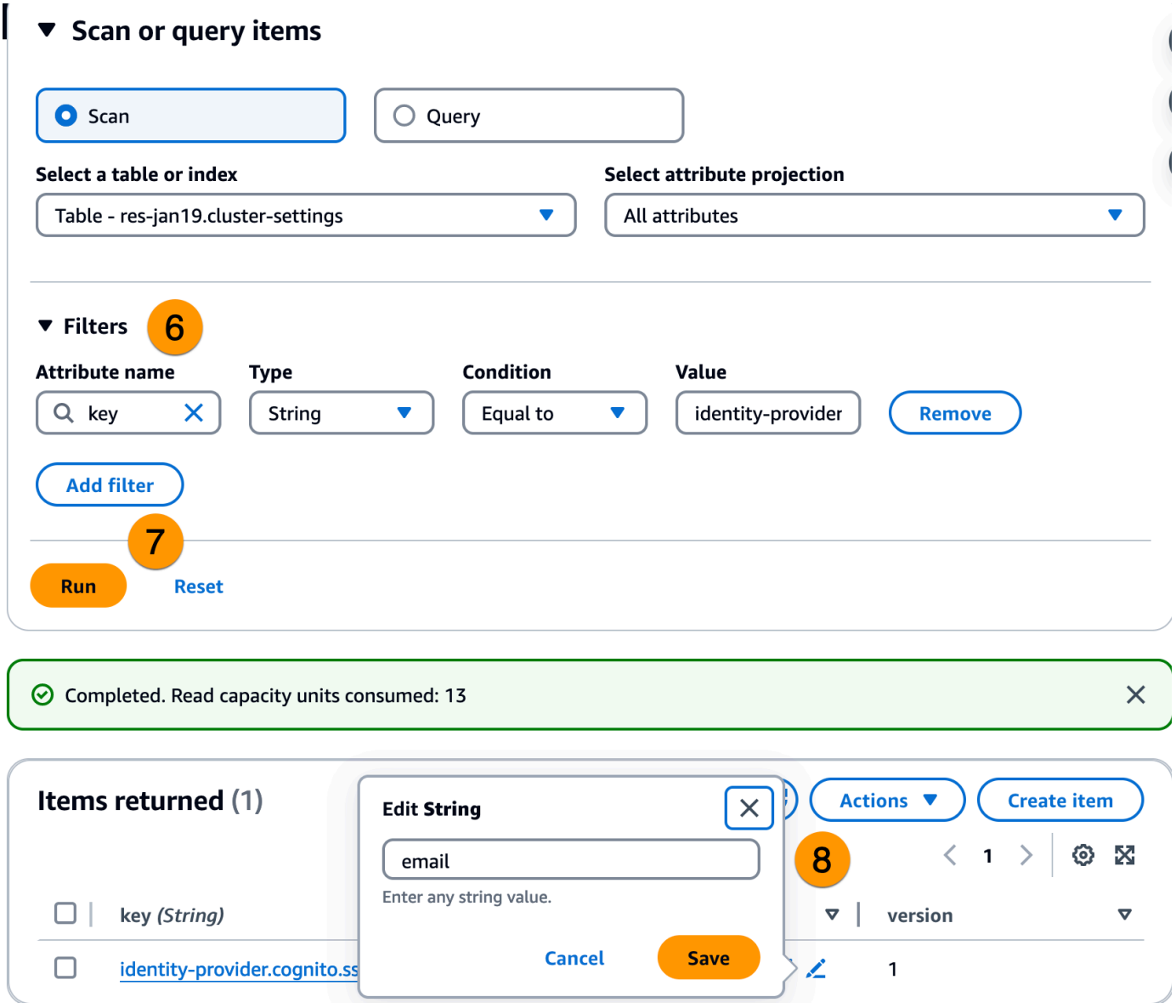
   b. Recherchez et sélectionnez le `<environment name>.cluster-settings` tableau, puis dans le menu Actions, choisissez Explorer les éléments.

   c. Sous Numériser ou interroger des éléments, accédez à Filtres et entrez les paramètres suivants :

      - Nom de l'attribut — `key`
      - Valeur — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Cliquez sur Exécuter.

7. Sous Articles renvoyés, recherchez la `identity-provider.cognito.sso_idp_provider_email_attribute` chaîne et choisissez Modifier pour modifier la chaîne en fonction de vos modifications dans Amazon Cognito.



Débogage des problèmes liés à l'IdP SAML

Traceur SAML — Vous pouvez utiliser cette extension pour le navigateur Chrome afin de suivre les requêtes SAML et de vérifier les valeurs d'assertion SAML. Pour plus d'informations, consultez SAML-Tracer sur le Chrome Web Store.

Outils de développement SAML : OneLogin fournit des outils que vous pouvez utiliser pour décoder la valeur codée SAML et vérifier les champs obligatoires dans l'assertion SAML. Pour plus d'informations, voir Base 64 Decode + Inflate sur le OneLogin site Web.

Amazon CloudWatch Logs — Vous pouvez vérifier la présence d'erreurs ou d'avertissements dans vos CloudWatch journaux RES dans Logs. Vos journaux se trouvent dans un groupe de journaux au format de nom*res-environment-name*/cluster-manager.

Documentation Amazon Cognito — Pour plus d'informations sur l'intégration de SAML à Amazon Cognito, consultez la section Ajouter des fournisseurs d'identité SAML à un groupe d'utilisateurs dans le manuel Amazon Cognito Developer Guide.

Définition de mots de passe pour les utilisateurs

1. Dans la AWS Directory Service console, sélectionnez le répertoire de la pile créée.
2. Dans le menu Actions, choisissez Réinitialiser le mot de passe utilisateur.
3. Choisissez l'utilisateur et entrez un nouveau mot de passe.
4. Choisissez Réinitialiser le mot de passe.

Création de sous-domaines

Si vous utilisez un domaine personnalisé, vous devez configurer des sous-domaines pour prendre en charge les parties Web et VDI de votre portail.

> **Note**
>
> Si vous effectuez un déploiement dans la région AWS GovCloud (ouest des États-Unis), configurez l'application Web et les sous-domaines VDI dans le compte de partition commerciale hébergeant la zone hébergée publique du domaine.

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Recherchez le domaine que vous avez créé et choisissez Créer un enregistrement.
3. Entrez web comme nom de l'enregistrement.
4. Choisissez CNAME comme type d'enregistrement.
5. Dans Value, saisissez le lien que vous avez reçu dans l'e-mail initial.
6. Choisissez Create records (Créer des registres).
7. Pour créer un enregistrement pour le VDC, récupérez l'adresse NLB.

a. Connectez-vous à la AWS CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.
b. Sélectionnez `<environment-name>-vdc`.
c. Choisissez Ressources et ouvrez`<environmentname>-vdc-external-nlb`.
d. Copiez le nom DNS depuis le NLB.

8. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
9. Trouvez votre domaine et choisissez Créer un enregistrement.
10. Sous Nom de l'enregistrement, entrez`vdc`.
11. Sous Record type (Type d'enregistrement), sélectionnez CNAME.
12. Pour le NLB, entrez le DNS.
13. Choisissez Créer un registre.

Création d'un certificat ACM

Par défaut, RES héberge le portail Web sous un équilibreur de charge d'application utilisant le domaine amazonaws.com. Pour utiliser votre propre domaine, vous devez configurer un certificat SSL/TLS public que vous avez fourni ou demandé à AWS Certificate Manager (ACM). Si vous utilisez ACM, vous recevrez un nom de AWS ressource que vous devrez fournir en paramètre pour chiffrer le canal SSL/TLS entre le client et l'hôte des services Web.

> **Tip**
>
> Si vous déployez le package de démonstration des ressources externes, vous devrez saisir le domaine de votre choix `PortalDomainName` lors du déploiement de la pile de ressources externesthe section called “Création de ressources externes”.

Pour créer un certificat pour des domaines personnalisés, procédez comme suit :

1. Depuis la console, ouvrez AWS Certificate Managerpour demander un certificat public. Si vous déployez dans AWS GovCloud l'ouest des États-Unis, créez le certificat dans votre compte de GovCloud partition.
2. Choisissez Demander un certificat public, puis cliquez sur Suivant.

3. Sous Noms de domaine, demandez un certificat pour les deux `*.PortalDomainName` et`PortalDomainName`.
4. Sous Méthode de validation, choisissez Validation DNS.
5. Choisissez Request (Demander).
6. Dans la liste des certificats, ouvrez les certificats demandés. Chaque certificat aura le statut En attente de validation.

> **Note**
>
> Si vous ne voyez pas vos certificats, actualisez la liste.

7. Effectuez l'une des actions suivantes :
   - Déploiement commercial : dans les détails du certificat pour chaque certificat demandé, choisissez Create records in Route 53. Le statut du certificat doit passer à Émis.
   - GovCloud déploiement : si vous déployez dans AWS GovCloud (ouest des États-Unis), copiez la clé et la valeur CNAME. À partir du compte de partition commerciale, utilisez les valeurs pour créer un nouvel enregistrement dans la zone hébergée publique. Le statut du certificat doit passer à Émis.
8. Copiez le nouvel ARN du certificat à saisir comme paramètre pour`ACMCertificateARNforWebApp`.

Amazon CloudWatch Logs

Research and Engineering Studio crée les groupes de journaux suivants CloudWatch lors de l'installation. Consultez le tableau suivant pour les rétentions par défaut :

CloudWatch Groupes de journaux	Retention
/aws/lambda/ < >-points de terminaison du cluster installation-stack-name	N'expire jamais
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	N'expire jamais
/aws/lambda/ < >-paramètres du cluster installation-stack-name	N'expire jamais

CloudWatch Groupes de journaux	Retention
/aws/lambda/ < >-oauth-credentials installation-stack-name	N'expire jamais
/aws/lambda/ < >- installation-stack-name self-signed-certificate	N'expire jamais
/aws/lambda/ < >- installation-stack-name update-cluster-prefix-list	N'expire jamais
/aws/lambda/ < >- installation-stack-name vdc-scheduled-event-transformer	N'expire jamais
/aws/lambda/ < >- -client-scope installation-stack-name vdc-update-cluster-manager	N'expire jamais
/< >/gestionnaire installation-stack-name de clusters	3 mois
/< >/vdc/contrôleur installation-stack-name	3 mois
/< >/vdc/dcv-broker installation-stack-name	3 mois
/< >/vdc/ installation-stack-name dcv-connection-gateway	3 mois

Si vous souhaitez modifier la rétention par défaut d'un groupe de journaux, vous pouvez accéder à la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/ et suivre les instructions de la section Modifier la conservation des données des CloudWatch journaux dans les journaux.

Définition de limites d'autorisation personnalisées

À partir du 2024.04, vous pouvez éventuellement modifier les rôles créés par RES en attachant des limites d'autorisation personnalisées. Une limite d'autorisation personnalisée peut être définie dans le cadre de l' AWS CloudFormation installation RES en fournissant l'ARN de la limite d'autorisation dans le cadre du PermissionBoundary paramètre IAM. Aucune limite d'autorisation n'est définie pour

les rôles RES si ce paramètre est laissé vide. Vous trouverez ci-dessous la liste des actions dont les rôles RES ont besoin pour fonctionner. Assurez-vous que toute limite d'autorisation que vous prévoyez d'utiliser explicitement autorise les actions suivantes :

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

Configurer des AMI prêtes pour les RES

Avec les AMI compatibles RES, vous pouvez préinstaller les dépendances RES pour les instances de bureau virtuel (VDI) sur vos AMI personnalisées. L'utilisation d'AMI compatibles RES améliore les temps de démarrage des instances VDI à l'aide des images préfabriquées. À l'aide d'EC2 Image Builder, vous pouvez créer et enregistrer vos AMI en tant que nouvelles piles de logiciels. Pour plus d'informations sur Image Builder, consultez le guide de l'utilisateur d'Image Builder.

Avant de commencer, vous devez déployer la dernière version de RES.

Rubriques

Préparer le rôle IAM pour accéder à l'environnement RES

Pour accéder au service d'environnement RES depuis EC2 Image Builder, vous devez créer ou modifier un rôle IAM appelé RES-EC2. InstanceProfileForImageBuilder Pour plus d'informations sur la configuration d'un rôle IAM à utiliser dans Image Builder, consultez AWS Identity and Access Management (IAM) dans le guide de l'utilisateur d'Image Builder.

Votre rôle nécessite :

- Les relations de confiance incluent le service Amazon EC2
- Politiques Amazon SSM ManagedInstanceCore et EC2 InstanceProfileForImageBuilder
- Politique RES personnalisée avec accès limité à DynamoDB et Amazon S3 à l'environnement RES déployé

  (Cette politique peut être soit un document de politique géré par le client, soit un document de politique intégré au client.)

Entité relationnelle de confiance :

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

Politique RES :

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

```
}
```

Création d'un composant EC2 Image Builder

Suivez les instructions pour créer un composant à l'aide de la console Image Builder dans le guide de l'utilisateur d'Image Builder.

Entrez les détails de votre composant :

1. Dans Type, choisissez Build.
2. Pour le système d'exploitation Image (OS), choisissez Linux ou Windows.
3. Pour Nom du composant, entrez un nom significatif tel que**`research-and-engineering-studio-vdi-<operating-system>`**.
4. Entrez le numéro de version de votre composant et ajoutez éventuellement une description.
5. Pour le document de définition, entrez le fichier de définition suivant. Si vous rencontrez des erreurs, le fichier YAML est sensible à l'espace et en est la cause la plus probable.

   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. Créez des balises facultatives et choisissez Créer un composant.

Préparez votre recette pour EC2 Image Builder

Une recette EC2 Image Builder définit l'image de base à utiliser comme point de départ pour créer une nouvelle image, ainsi que l'ensemble des composants que vous ajoutez pour personnaliser votre image et vérifier que tout fonctionne comme prévu. Vous devez créer ou modifier une recette pour construire l'AMI cible avec les dépendances logicielles RES nécessaires. Pour plus d'informations sur les recettes, voir Gérer les recettes.

RES prend en charge les systèmes d'exploitation d'image suivants :

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

Create a new recipe

1. Ouvrez la console https://console.aws.amazon.com/imagebuilder EC2 Image Builder à l'adresse.
2. Sous Ressources enregistrées, choisissez Image recipes.
3. Choisissez Créer une recette d'image.
4. Entrez un nom unique et un numéro de version.
5. Choisissez une image de base prise en charge par RES.
6. Sous Configuration de l'instance, installez un agent SSM s'il n'en existe pas un préinstallé. Entrez les informations dans Données utilisateur et toute autre donnée utilisateur nécessaire.

> **Note**
>
> Pour plus d'informations sur l'installation d'un agent SSM, voir :
>
> - Installation manuelle de l'agent SSM sur les instances EC2 pour Linux

- Installation et désinstallation manuelles de l'agent SSM sur les instances EC2 pour Windows Server

7. Pour les recettes basées sur Linux, ajoutez le composant de `aws-cli-version-2-linux` compilation géré par Amazon à la recette. Les scripts d'installation RES utilisent le AWS CLI pour fournir un accès VDI aux valeurs de configuration des paramètres du cluster DynamoDB. Windows n'a pas besoin de ce composant.
8. Ajoutez le composant EC2 Image Builder créé pour votre environnement Linux ou Windows et entrez les valeurs de paramètres requises. Les paramètres suivants sont des entrées obligatoires : RES AWSAccountID EnvNameEnvRegion, RES et RESEnvReleaseVersion.

> **Important**
>
> Pour les environnements Linux, vous devez ajouter ces composants afin que le composant de `aws-cli-version-2-linux` compilation soit ajouté en premier.

9. (Recommandé) Ajoutez le composant de `simple-boot-test-<linux-or-windows>` test géré par Amazon pour vérifier que l'AMI peut être lancée. Il s'agit d'une recommandation minimale. Vous pouvez sélectionner d'autres composants de test qui répondent à vos exigences.
10. Complétez les sections facultatives si nécessaire, ajoutez les autres composants souhaités et choisissez Créer une recette.

Modify a recipe

Si vous possédez déjà une recette EC2 Image Builder, vous pouvez l'utiliser en ajoutant les composants suivants :

1. Pour les recettes basées sur Linux, ajoutez le composant de `aws-cli-version-2-linux` compilation géré par Amazon à la recette. Les scripts d'installation RES utilisent le AWS CLI pour fournir un accès VDI aux valeurs de configuration des paramètres du cluster DynamoDB. Windows n'a pas besoin de ce composant.
2. Ajoutez le composant EC2 Image Builder créé pour votre environnement Linux ou Windows et entrez les valeurs de paramètres requises. Les paramètres suivants sont des entrées obligatoires : RES AWSAccountID EnvNameEnvRegion, RES et RESEnvReleaseVersion.

> **Important**
>
> Pour les environnements Linux, vous devez ajouter ces composants afin que le composant de `aws-cli-version-2-linux` compilation soit ajouté en premier.

3. Complétez les sections facultatives si nécessaire, ajoutez les autres composants souhaités et choisissez Créer une recette.

Configuration de l'infrastructure EC2 Image Builder

Vous pouvez utiliser les configurations d'infrastructure pour spécifier l'infrastructure Amazon EC2 qu'Image Builder utilise pour créer et tester votre image Image Builder. Pour une utilisation avec RES, vous pouvez choisir de créer une nouvelle configuration d'infrastructure ou d'utiliser une configuration existante.

- Pour créer une nouvelle configuration d'infrastructure, voir Création d'une configuration d'infrastructure.
- Pour utiliser une configuration d'infrastructure existante, mettez à jour une configuration d'infrastructure.

Pour configurer votre infrastructure Image Builder :

1. Pour le rôle IAM, entrez le rôle que vous avez configuré précédemment. the section called “Préparer le rôle IAM pour accéder à l'environnement RES”
2. Pour le type d'instance, choisissez un type avec au moins 4 Go de mémoire et compatible avec l'architecture AMI de base que vous avez choisie. Consultez la section Types d'instances Amazon EC2.
3. Pour les VPC, les sous-réseaux et les groupes de sécurité, vous devez autoriser l'accès à Internet pour télécharger des packages logiciels. L'accès doit également être autorisé à la table `cluster-settings` DynamoDB et au compartiment de cluster Amazon S3 de l'environnement RES.

Configurer le pipeline d'images Image Builder

Le pipeline d'images Image Builder assemble l'image de base, les composants pour la création et les tests, la configuration de l'infrastructure et les paramètres de distribution. Pour configurer un pipeline d'images pour les AMI compatibles RES, vous pouvez choisir de créer un nouveau pipeline ou d'utiliser un pipeline existant. Pour plus d'informations, consultez la section Création et mise à jour de pipelines d'images AMI dans le guide de l'utilisateur d'Image Builder.

Create a new Image Builder pipeline

1. Ouvrez la console Image Builder à l'adressehttps://console.aws.amazon.com/imagebuilder.
2. Dans le menu de navigation, choisissez Image pipelines.
3. Choisissez Créer un pipeline d'images.
4. Spécifiez les détails de votre pipeline en saisissant un nom unique, une description facultative, un calendrier et une fréquence.
5. Pour Choisir une recette, choisissez Utiliser une recette existante et sélectionnez la recette créée dansthe section called “Préparez votre recette pour EC2 Image Builder”. Vérifiez que les détails de votre recette sont corrects.
6. Pour Définir le processus de création d'image, choisissez le flux de travail par défaut ou personnalisé selon le cas d'utilisation. Dans la plupart des cas, les flux de travail par défaut sont suffisants. Pour plus d'informations, consultez Configurer les flux de travail d'imagerie pour votre pipeline EC2 Image Builder.
7. Pour Définir la configuration de l'infrastructure, choisissez Choisir la configuration d'infrastructure existante et sélectionnez la configuration d'infrastructure créée dansthe section called “Configuration de l'infrastructure EC2 Image Builder”. Vérifiez que les détails de votre infrastructure sont corrects.
8. Pour Définir les paramètres de distribution, choisissez Créer les paramètres de distribution à l'aide des paramètres de distribution par défaut du service. L'image de sortie doit se trouver dans le même environnement RES Région AWS que celui de votre environnement RES. En utilisant les paramètres par défaut du service, l'image sera créée dans la région où Image Builder est utilisé.
9. Passez en revue les détails du pipeline et choisissez Create pipeline.

Modify an existing Image Builder pipeline

1. Pour utiliser un pipeline existant, modifiez les détails afin d'utiliser la recette créée dansthe section called “Préparez votre recette pour EC2 Image Builder”.
2. Sélectionnez Enregistrer les modifications.

Exécuter le pipeline d'images Image Builder

Pour produire l'image de sortie configurée, vous devez lancer le pipeline d'images. Le processus de création peut prendre jusqu'à une heure selon le nombre de composants contenus dans la recette d'image.

Pour exécuter le pipeline d'images :

1. Dans Pipelines d'images, sélectionnez le pipeline créé dansthe section called “Configurer le pipeline d'images Image Builder”.
2. Dans Actions, sélectionnez Exécuter le pipeline.

Enregistrez une nouvelle pile logicielle dans RES

1. Suivez les instructions the section called “Piles logicielles (AMI)” pour enregistrer une pile logicielle.
2. Pour l'ID AMI, entrez l'ID AMI de l'image de sortie intégréethe section called “Exécuter le pipeline d'images Image Builder”.

Guide de l'administrateur

Ce guide de l'administrateur fournit des instructions supplémentaires à un public technique sur la manière de personnaliser et d'intégrer davantage le studio de recherche et d'ingénierie sur le AWS produit.

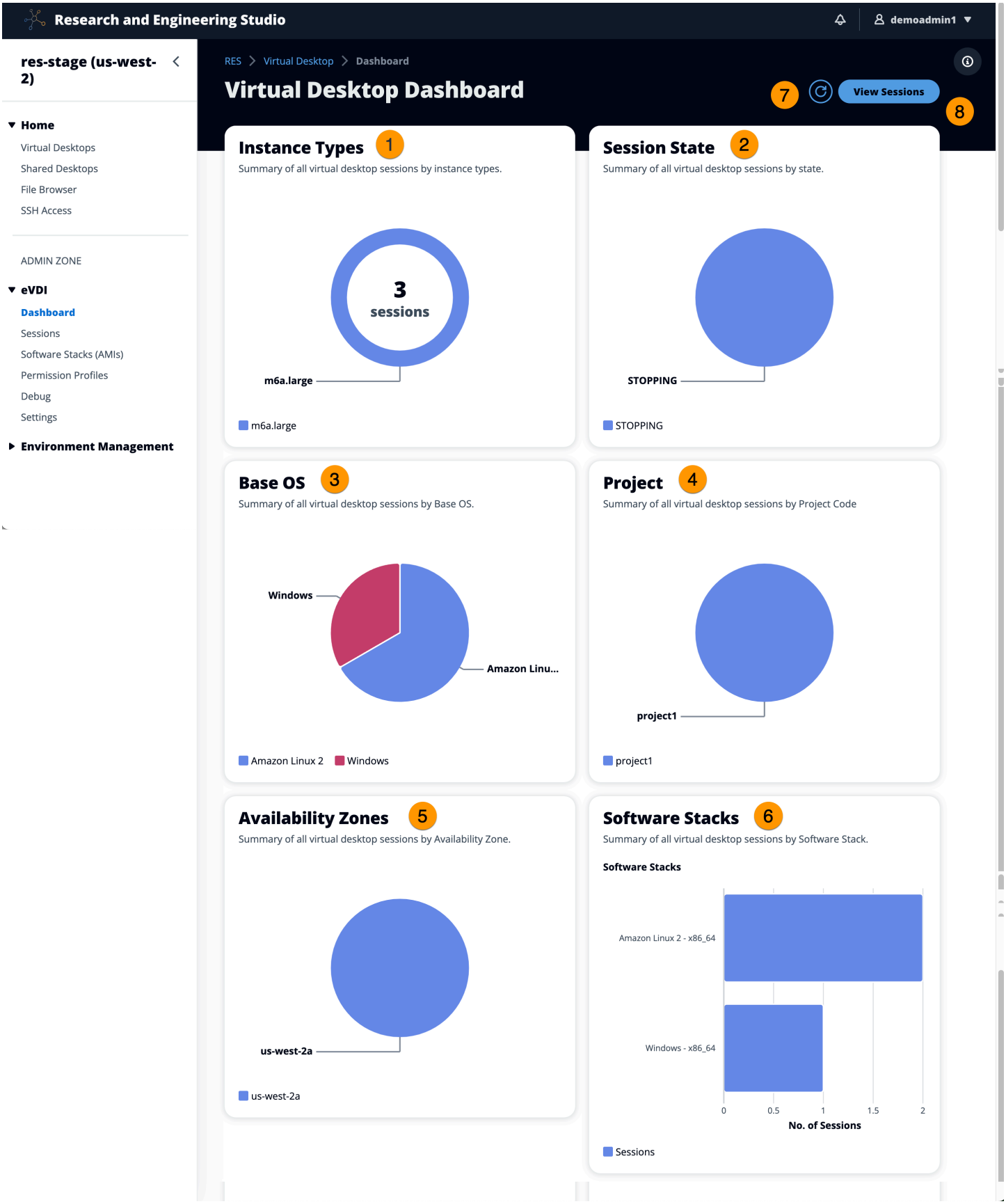
Rubriques

Gestion de session

La gestion des sessions fournit un environnement flexible et interactif pour le développement et le test des sessions. En tant qu'utilisateur administratif, vous pouvez autoriser les utilisateurs à créer et à gérer des sessions interactives au sein de leur environnement de projet.

Rubriques

Tableau de bord



Le tableau de bord de gestion des sessions fournit aux administrateurs un aperçu rapide des éléments suivants :

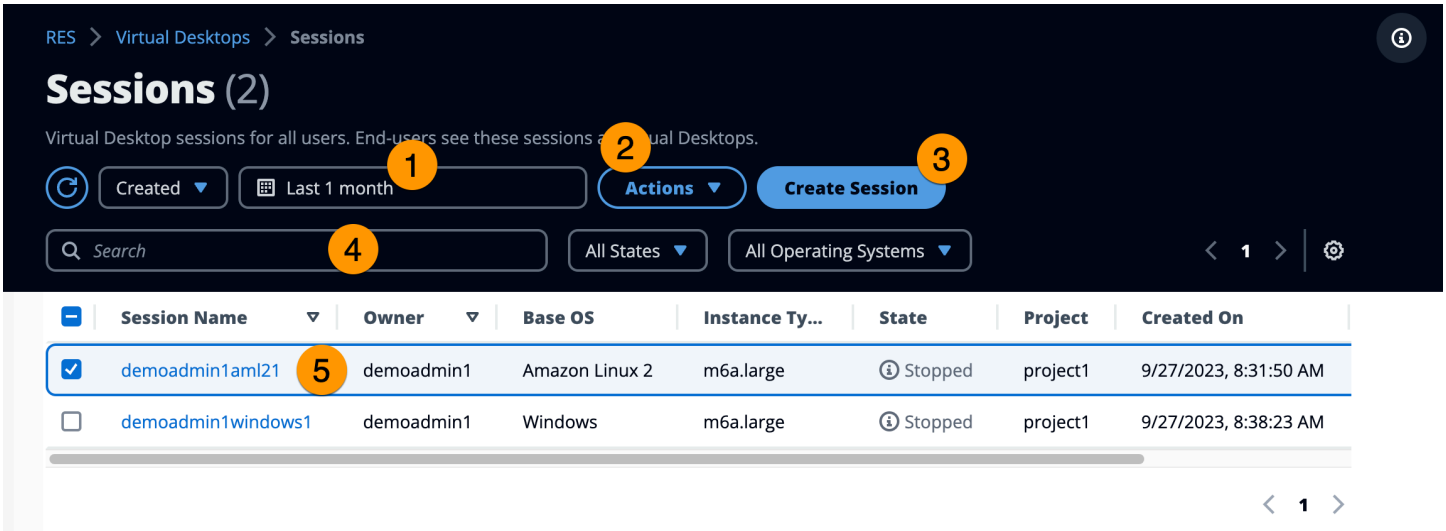
1. Types d'instances
2. États de session
3. Système d'exploitation de base
4. Projets
5. Zones de disponibilité
6. Piles de logiciels

En outre, les administrateurs peuvent :

7. Actualisez le tableau de bord pour mettre à jour les informations.
8. Choisissez Afficher les sessions pour accéder aux sessions.

Séances

Sessions affiche tous les bureaux virtuels créés dans Research and Engineering Studio. Sur la page Sessions, vous pouvez filtrer et afficher les informations de session ou créer une nouvelle session.



1. Utilisez le menu pour filtrer les résultats par sessions créées ou mises à jour au cours d'une période spécifiée.
2. Sélectionnez une session et utilisez le menu Actions pour :
   a. Reprendre une ou plusieurs sessions

b. Arrêter/mettre en veille prolongée une ou plusieurs sessions
c. Session (s) forcée (s) d'arrêt/hibernation
d. Terminer une ou plusieurs sessions
e. Forcer la fermeture d'une ou de plusieurs sessions
f. Séance (s) Santé
g. Créez une pile de logiciels

3. Choisissez Create Session pour créer une nouvelle session.
4. Recherchez une session par nom et filtrez par état et système d'exploitation.
5. Choisissez le nom de la session pour afficher plus de détails.

Création d'une session

1. Choisissez Create Session. Le modal Launch New Virtual Desktop s'ouvre.
2. Entrez les détails de la nouvelle session.
3. (Facultatif.) Activez Afficher les options avancées pour fournir des informations supplémentaires telles que l'ID de sous-réseau et le type de session DCV.
4. Sélectionnez Envoyer.

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

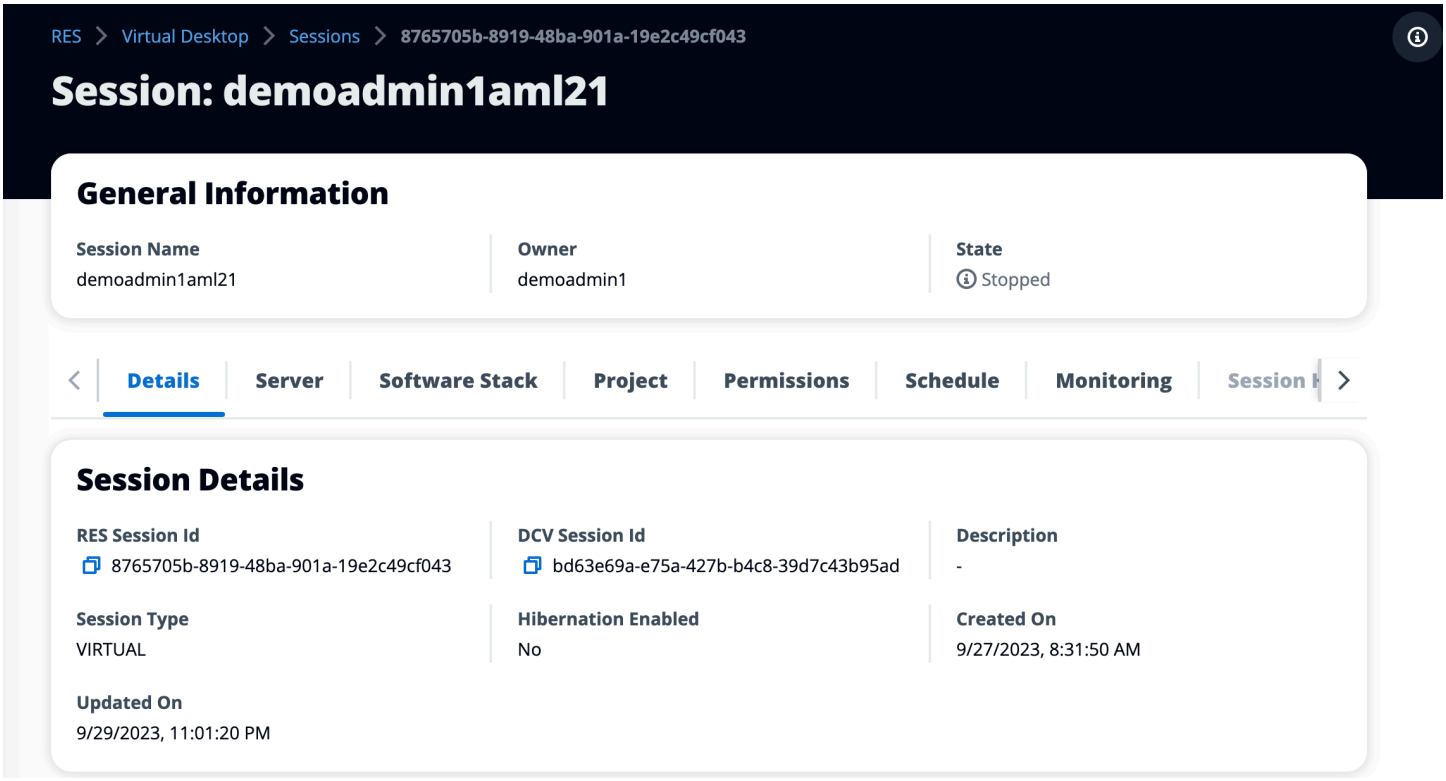
Enable Instance Hibernation
Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

Virtual Desktop Size
Select a virtual desktop instance type

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

Détails de la session

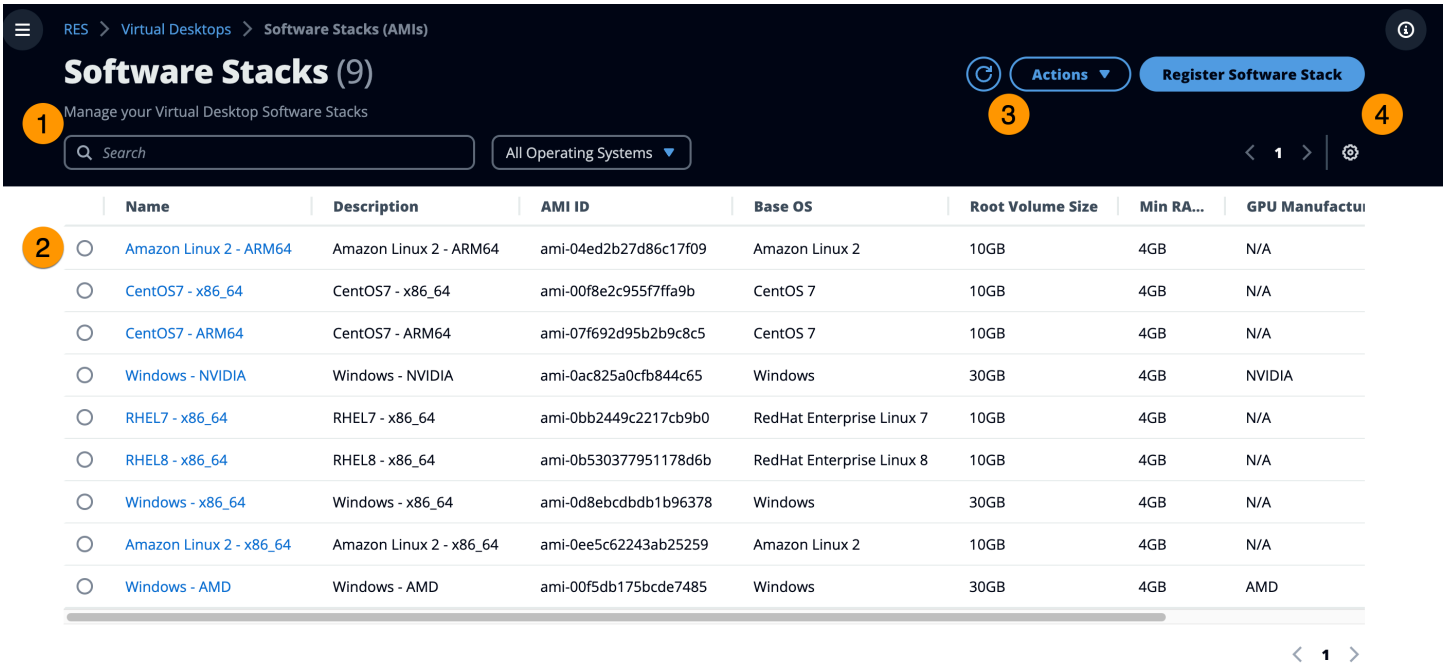
Dans la liste des sessions, choisissez le nom de la session pour afficher les détails de la session.



Piles logicielles (AMI)

Sur la page Software Stacks, vous pouvez configurer Amazon Machine Images (AMI) et gérer les AMI existantes.

> **Note**
>
> Pour exécuter la pile logicielle CentSO7 fournie AWS GovCloud (US), vous devez vous abonner à l'AMI AWS Marketplace en utilisant votre compte standard associé.



1. Recherchez une pile logicielle existante. Utilisez le menu déroulant du système d'exploitation pour filtrer par système d'exploitation.
2. Choisissez le nom d'une pile logicielle pour afficher les détails de la pile.
3. Si vous sélectionnez une pile logicielle, utilisez le menu Actions pour modifier la pile et l'affecter à un projet.
4. Choisissez Register Software Stack pour créer une nouvelle pile.

Enregistrer une pile logicielle

1. Choisissez Register Software Stack.
2. Entrez les détails de la nouvelle pile logicielle.
3. Sélectionnez Envoyer.

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

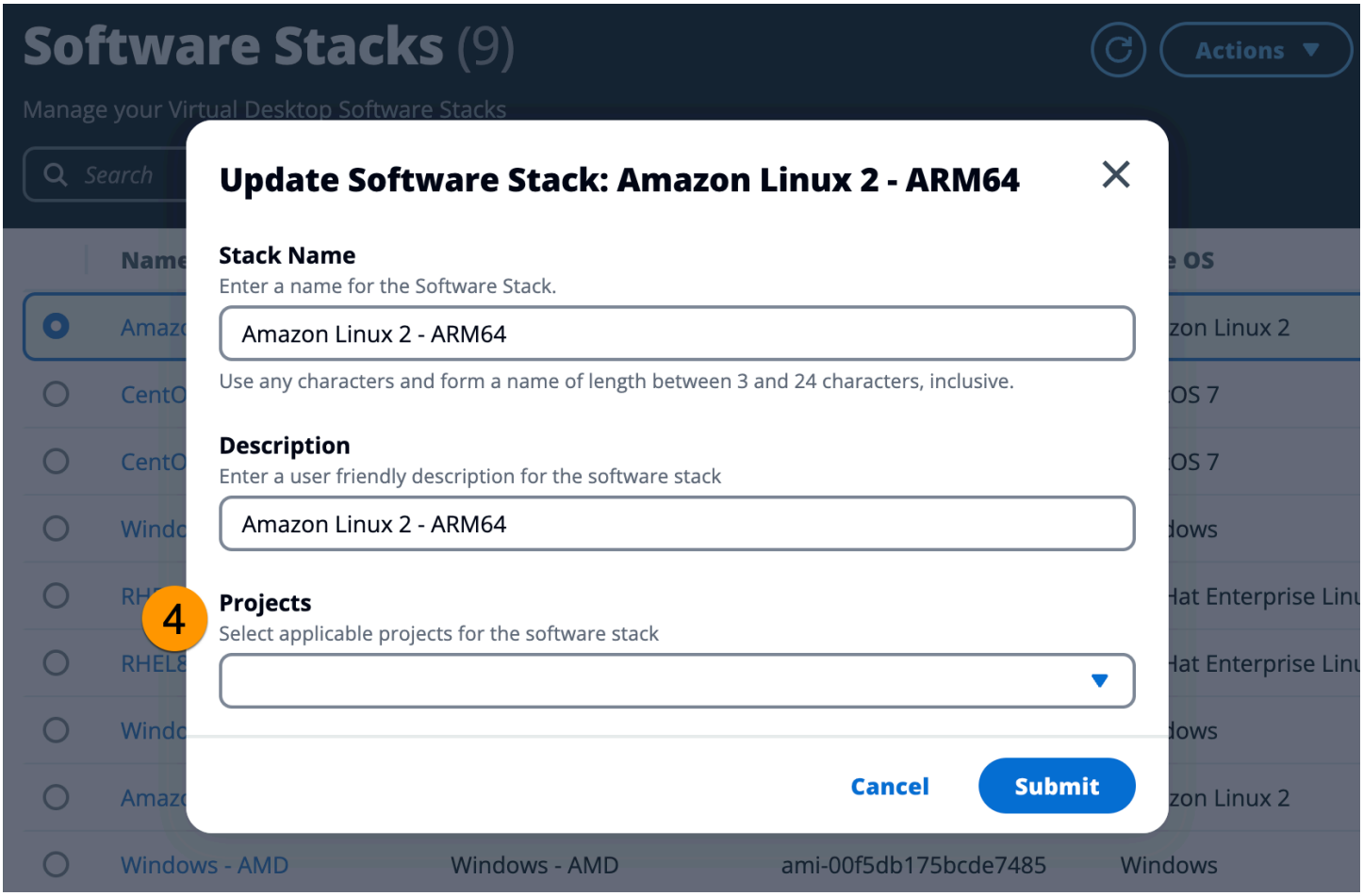
Attribuer une pile logicielle à un projet

Lorsque vous créez une nouvelle pile logicielle, vous pouvez attribuer la pile à des projets. Si vous devez ajouter la pile à un projet après sa création initiale, procédez comme suit :

> **Note**
>
> Vous ne pouvez attribuer des piles de logiciels qu'aux projets dont vous êtes membre.

1. Sélectionnez la pile logicielle que vous devez ajouter à un projet sur la page Software Stacks.
2. Choisissez Actions.
3. Choisissez Modifier.
4. Utilisez le menu déroulant Projets pour sélectionner le projet.
5. Sélectionnez Envoyer.

Vous pouvez également modifier la pile logicielle depuis la page des détails de la pile.

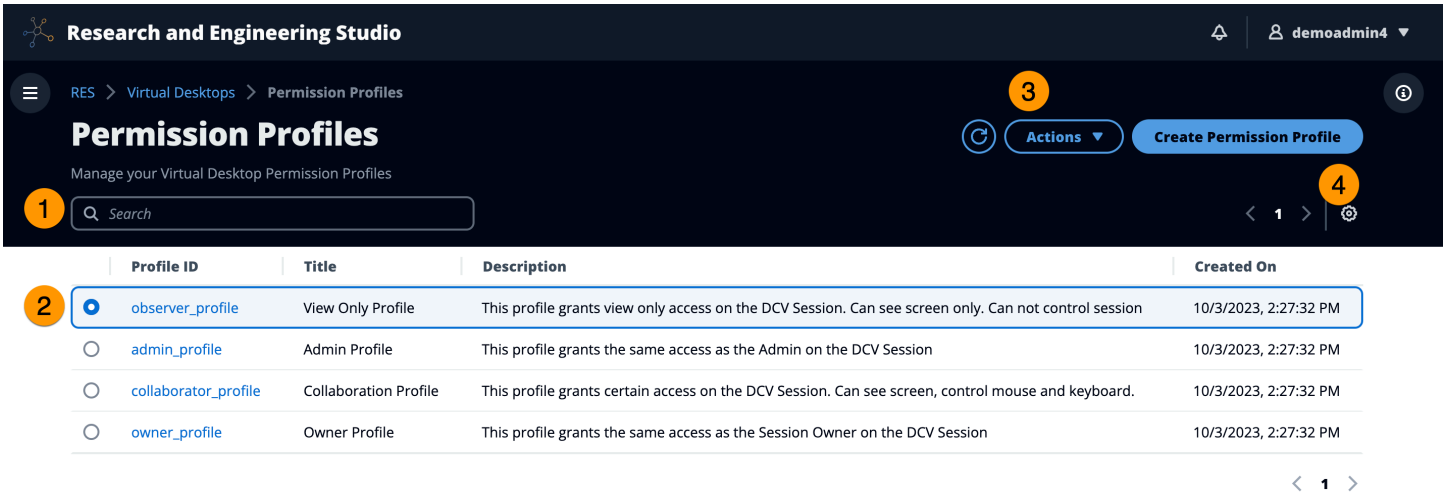


Afficher les détails de la pile logicielle

Dans la liste des piles logicielles, choisissez le nom de la pile logicielle pour afficher les détails. Sur la page de détails, vous pouvez également choisir Modifier pour modifier la pile logicielle.

Profils d'autorisation

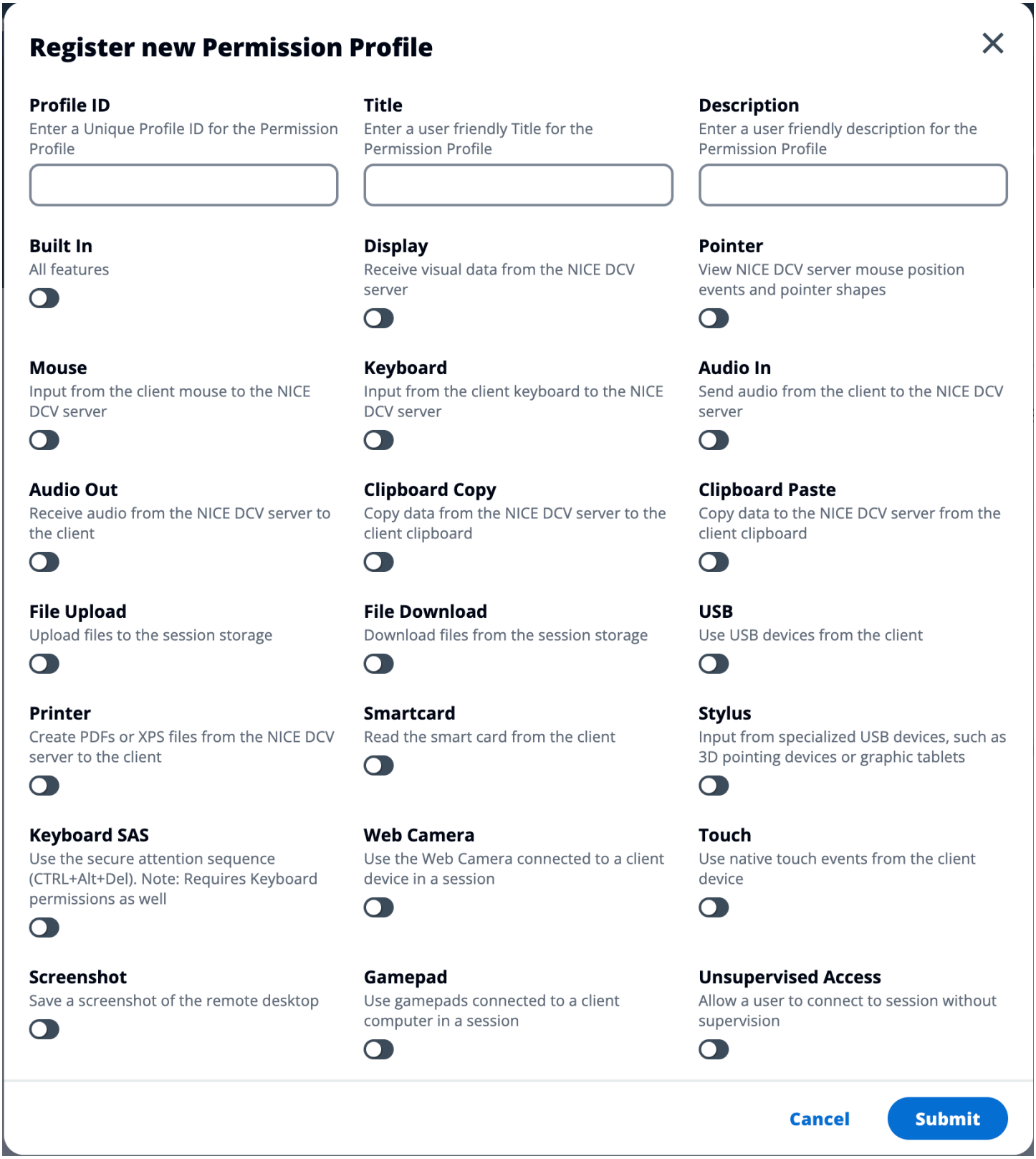
Utilisez les profils d'autorisation pour créer et gérer des profils réutilisables pour les autorisations.



1. Recherchez un profil d'autorisation.
2. Choisissez l'ID du profil pour afficher les détails.
3. Lorsqu'un profil est sélectionné, utilisez le menu Actions pour le modifier.
4. Choisissez Créer un profil d'autorisation pour créer un nouveau profil.

Création d'un profil d'autorisation

1. Choisissez Créer un profil d'autorisation.
2. Entrez les détails du nouveau profil et utilisez les boutons d'autorisation pour sélectionner les autorisations pour le profil.
3. Sélectionnez Envoyer.


Register new Permission Profile
Profile ID
Enter a Unique Profile ID for the Permission Profile
Title
Enter a user friendly Title for the Permission Profile
Description
Enter a user friendly description for the Permission Profile
Built In
All features
Display
Receive visual data from the NICE DCV server
Pointer
View NICE DCV server mouse position events and pointer shapes
Mouse
Input from the client mouse to the NICE DCV server
Keyboard
Input from the client keyboard to the NICE DCV server
Audio In
Send audio from the client to the NICE DCV server
Audio Out
Receive audio from the NICE DCV server to the client
Clipboard Copy
Copy data from the NICE DCV server to the client clipboard
Clipboard Paste
Copy data to the NICE DCV server from the client clipboard
File Upload
Upload files to the session storage
File Download
Download files from the session storage
USB
Use USB devices from the client
Printer
Create PDFs or XPS files from the NICE DCV server to the client
Smartcard
Read the smart card from the client
Stylus
Input from specialized USB devices, such as 3D pointing devices or graphic tablets
Keyboard SAS
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
Web Camera
Use the Web Camera connected to a client device in a session
Touch
Use native touch events from the client device
Screenshot
Save a screenshot of the remote desktop
Gamepad
Use gamepads connected to a client computer in a session
Unsupervised Access
Allow a user to connect to session without supervision
Cancel
Submit

Modifier un profil d'autorisation

1. Sélectionnez le profil d'autorisation que vous devez modifier sur la page Profils d'autorisation.
2. Choisissez Actions.
3. Choisissez Modifier le profil d'autorisation.
4. Modifiez le profil.
5. Sélectionnez Envoyer.

Afficher les détails du profil d'autorisation

Dans la liste des profils d'autorisation, choisissez l'ID du profil pour afficher les détails. Sur la page de détails, vous pouvez également choisir Modifier pour modifier le profil d'autorisation.

Débogage

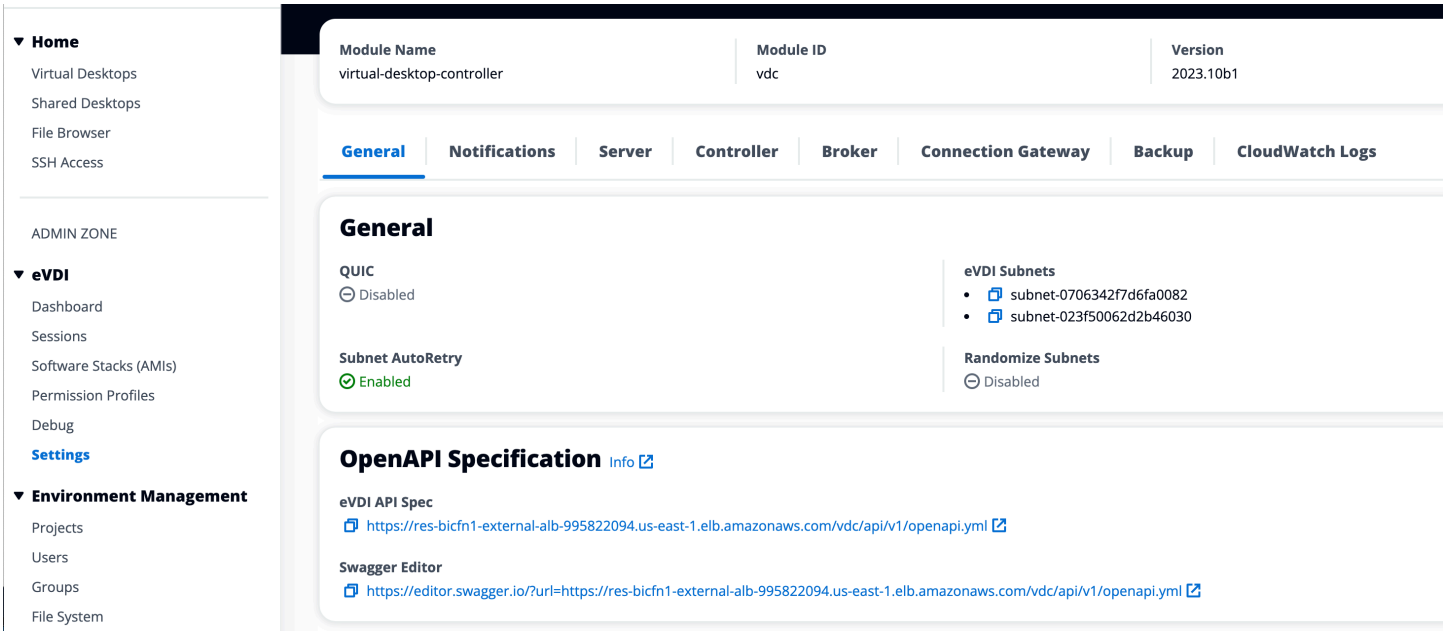
Le panneau de débogage affiche le trafic de messages associé aux bureaux virtuels. Vous pouvez utiliser ce panneau pour observer l'activité entre les hôtes. L'onglet VD Host affiche l'activité spécifique à l'instance, et l'onglet VD Sessions affiche l'activité de session en cours.

Réglages du bureau

Vous pouvez utiliser la page Paramètres du bureau pour configurer les ressources associées aux bureaux virtuels. L'onglet Serveur permet d'accéder à des paramètres tels que :

- Expiration du délai d'inactivité de la session DCV
- Avertissement d'expiration du délai d'inactivité
- Seuil d'utilisation du processeur

- Sessions autorisées par utilisateur



Gestion de l'environnement

Dans la section Gestion de l'environnement de RES, les utilisateurs administratifs peuvent créer et gérer des environnements isolés pour leurs projets de recherche et d'ingénierie. Ces environnements peuvent inclure des ressources informatiques, du stockage et d'autres composants nécessaires, le tout dans un environnement sécurisé. Les utilisateurs peuvent configurer et personnaliser ces environnements pour répondre aux exigences spécifiques de leurs projets, ce qui facilite l'expérimentation, le test et l'itération de leurs solutions sans impact sur les autres projets ou environnements.

Rubriques

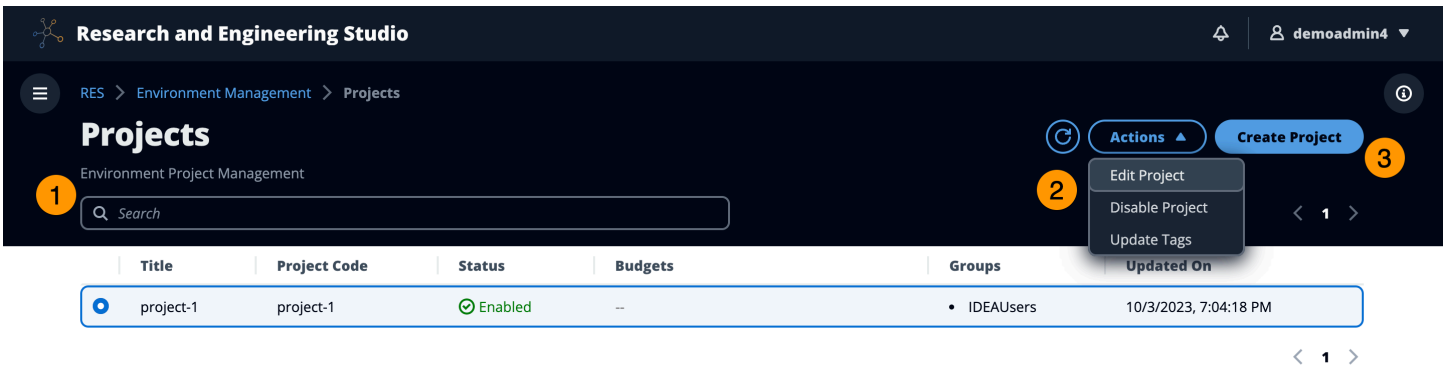
- Projets
- Users
- Groups
- Systèmes de fichiers
- État de l'environnement
- Gestion des snapshots
- Paramètres d'environnement

Projets

Les projets constituent une limite pour les bureaux virtuels, les équipes et les budgets. Lorsque vous créez un projet, vous définissez ses paramètres, tels que le nom, la description et la configuration de l'environnement. Les projets incluent généralement un ou plusieurs environnements, qui peuvent être personnalisés pour répondre aux exigences spécifiques de votre projet, telles que le type et la taille des ressources informatiques, la pile logicielle et la configuration réseau.

Rubriques

Afficher les projets



Le tableau de bord des projets fournit une liste des projets mis à votre disposition. Depuis le tableau de bord des projets, vous pouvez :

1. Vous pouvez utiliser le champ de recherche pour trouver des projets.
2. Lorsqu'un projet est sélectionné, vous pouvez utiliser le menu Actions pour :
   a. Modifier un projet
   b. Activer ou désactiver un projet
   c. Mettre à jour les balises du projet

3. Vous pouvez choisir Create Project pour créer un nouveau projet.

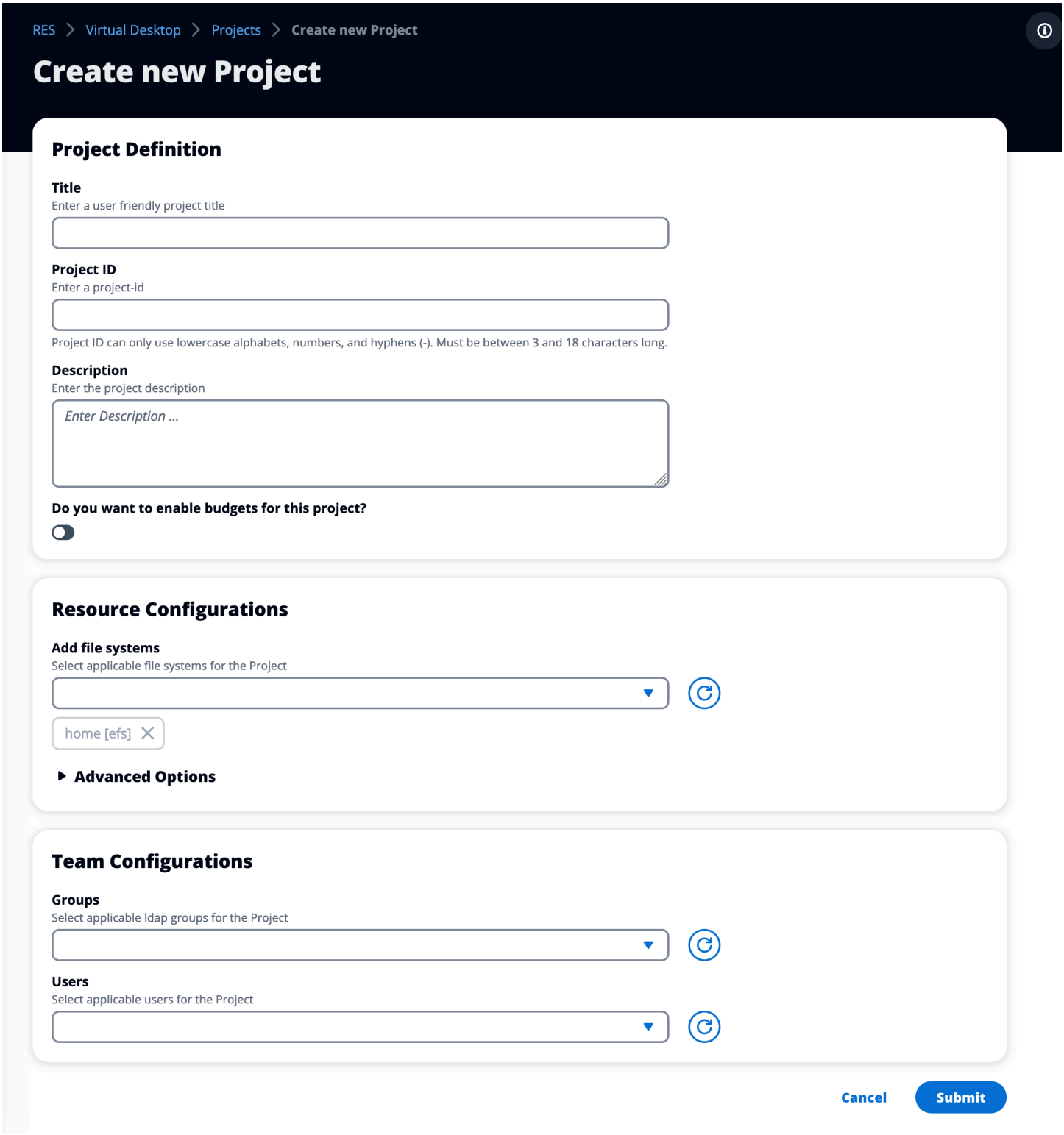
Création d'un projet

1. Choisissez Create Project (Créer un projet).
2. Entrez les détails du projet.

   - L'ID de projet est une balise de ressource qui peut être utilisée pour suivre la répartition des coûts dans AWS Cost Explorer Service. Pour plus d'informations, consultez la section Activation des balises de répartition des coûts définies par l'utilisateur.

     > **Important**
     >
     > L'ID du projet ne peut pas être modifié après sa création.

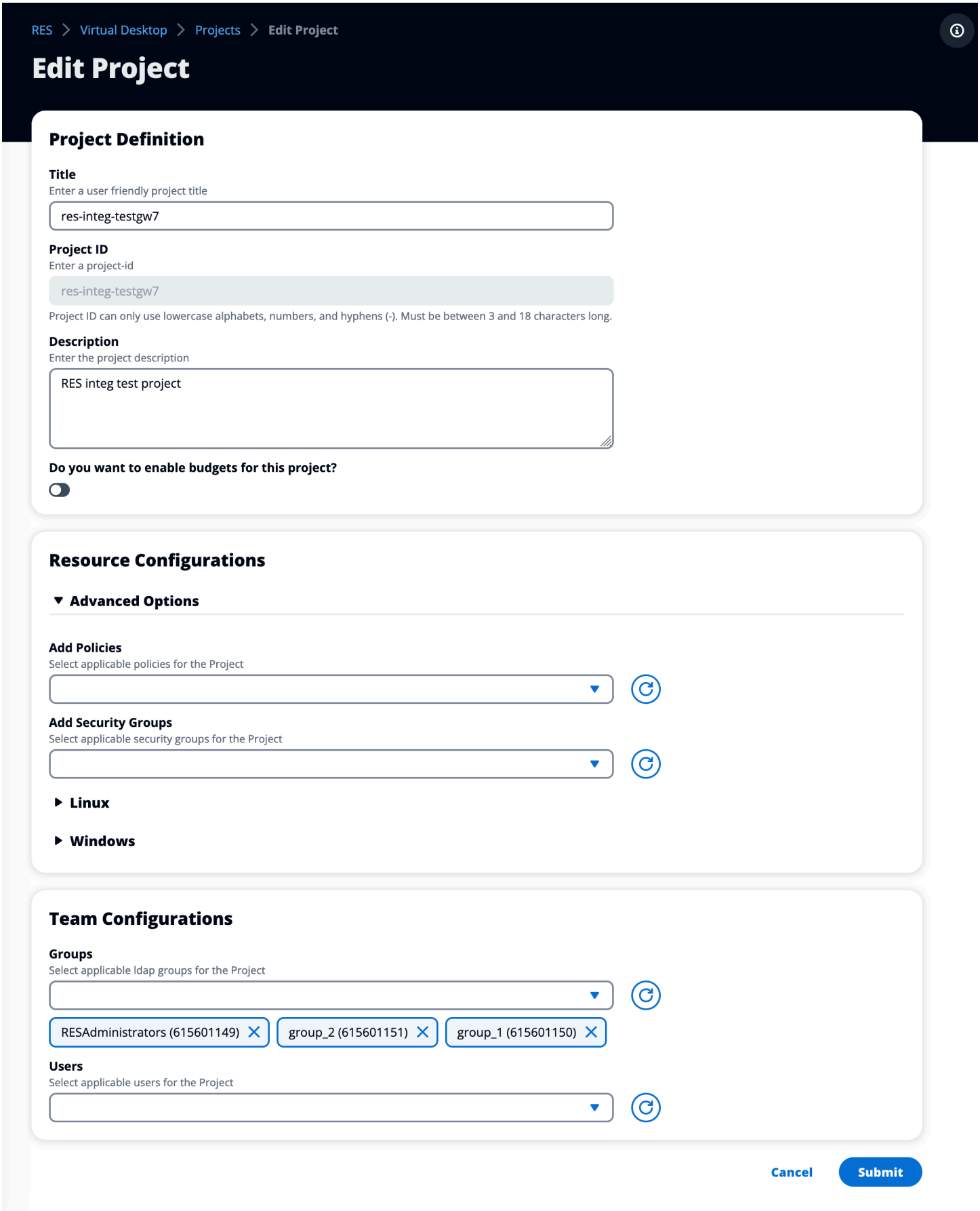
   - Pour plus d'informations sur les options avancées, consultezthe section called "Ajouter un modèle de lancement".
3. (Facultatif) Activez les budgets pour le projet. Pour plus d'informations sur les budgets, voirthe section called "Surveillance et contrôle des coûts".
4. Sélectionnez Envoyer.



Modifier un projet

1. Sélectionnez un projet dans la liste des projets.

2. Dans le menu Actions, choisissez Modifier le projet.
3. Entrez vos mises à jour. Si vous avez l'intention d'activer les budgets, consultez the section called “Surveillance et contrôle des coûts” pour plus d'informations. Pour plus d'informations sur les options avancées, consultezthe section called “Ajouter un modèle de lancement”.
4. Sélectionnez Envoyer.


RES > Virtual Desktop > Projects > Edit Project
Edit Project
Project Definition
Title
Enter a user friendly project title
res-integ-testgw7
Project ID
Enter a project-id
res-integ-testgw7
Project ID can only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long.
Description
Enter the project description
RES integ test project
Do you want to enable budgets for this project?
Resource Configurations
Advanced Options
Add Policies
Select applicable policies for the Project
Add Security Groups
Select applicable security groups for the Project
Linux
Windows
Team Configurations
Groups
Select applicable ldap groups for the Project
RESAdministrators (615601149)
group_2 (615601151)
group_1 (615601150)
Users
Select applicable users for the Project
Cancel
Submit

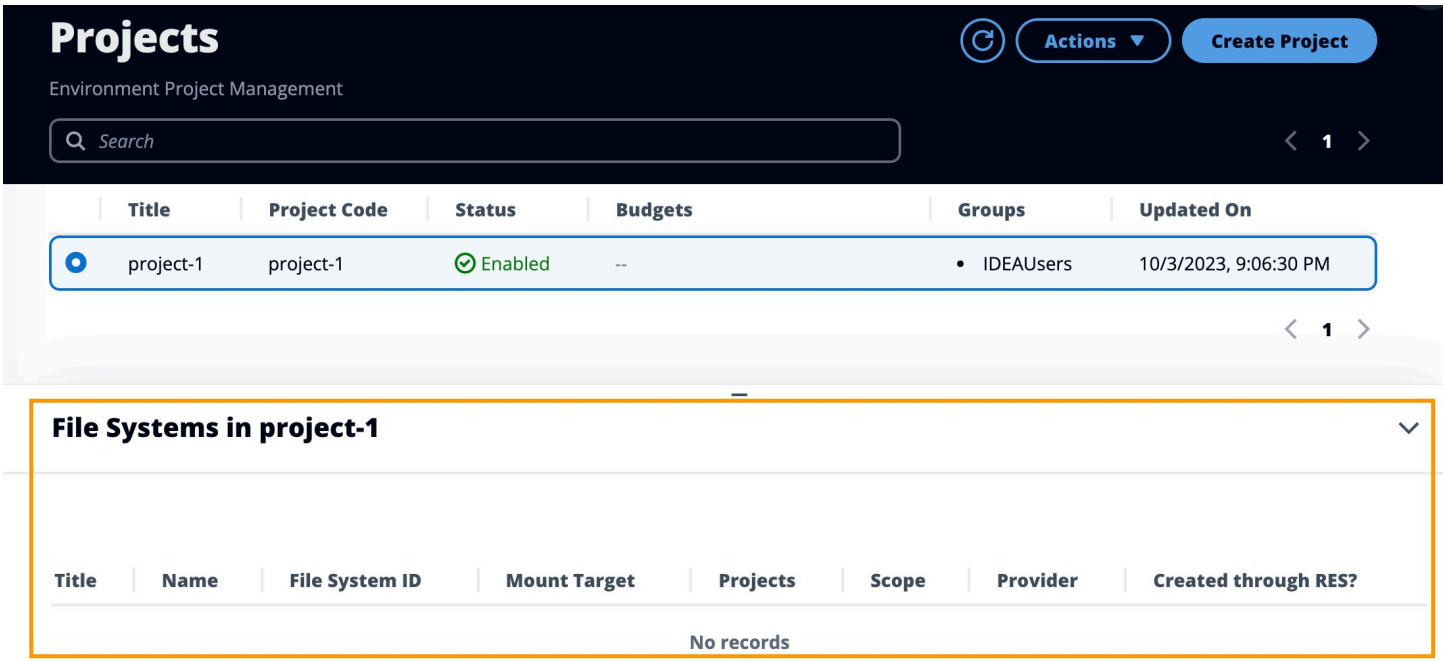
Ajouter ou supprimer des balises dans un projet

Les balises de projet attribueront des balises à toutes les instances créées dans le cadre de ce projet.

1. Sélectionnez un projet dans la liste des projets.
2. Dans le menu Actions, choisissez Mettre à jour les balises.
3. Choisissez Ajouter des balises et entrez une valeur pour Key.
4. Pour supprimer des balises, choisissez Supprimer à côté de la balise que vous souhaitez supprimer.

Afficher les systèmes de fichiers associés à un projet

Lorsqu'un projet est sélectionné, vous pouvez développer le volet Systèmes de fichiers en bas de l'écran pour afficher les systèmes de fichiers associés au projet.



Ajouter un modèle de lancement

Lorsque vous créez ou modifiez un projet, vous pouvez ajouter des modèles de lancement à l'aide des options avancées de la configuration du projet. Les modèles de lancement fournissent des configurations supplémentaires, telles que des groupes de sécurité, des politiques IAM et des scripts de lancement pour toutes les instances VDI du projet.

Ajouter des politiques

Vous pouvez ajouter une politique IAM pour contrôler l'accès VDI pour toutes les instances déployées dans le cadre de votre projet. Pour intégrer une politique, balisez-la avec la paire clé-valeur suivante :

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

Pour plus d'informations sur les rôles IAM, consultez la section Politiques et autorisations dans IAM.

Ajout de groupes de sécurité

Vous pouvez ajouter un groupe de sécurité pour contrôler les données de sortie et d'entrée pour toutes les instances VDI de votre projet. Pour intégrer un groupe de sécurité, balisez-le avec la paire clé-valeur suivante :

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

Pour plus d'informations sur les groupes de sécurité, consultez la section Contrôler le trafic vers vos AWS ressources à l'aide de groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Ajouter des scripts de lancement

Vous pouvez ajouter des scripts de lancement qui seront lancés sur toutes les sessions VDI de votre projet. RES prend en charge l'initiation de scripts pour Linux et Windows. Pour lancer le script, vous pouvez choisir l'une des options suivantes :

Exécuter le script au démarrage du VDI

Cette option lance le script au début d'une instance VDI avant l'exécution de toute configuration ou installation RES.

Exécuter le script lorsque le VDI est configuré

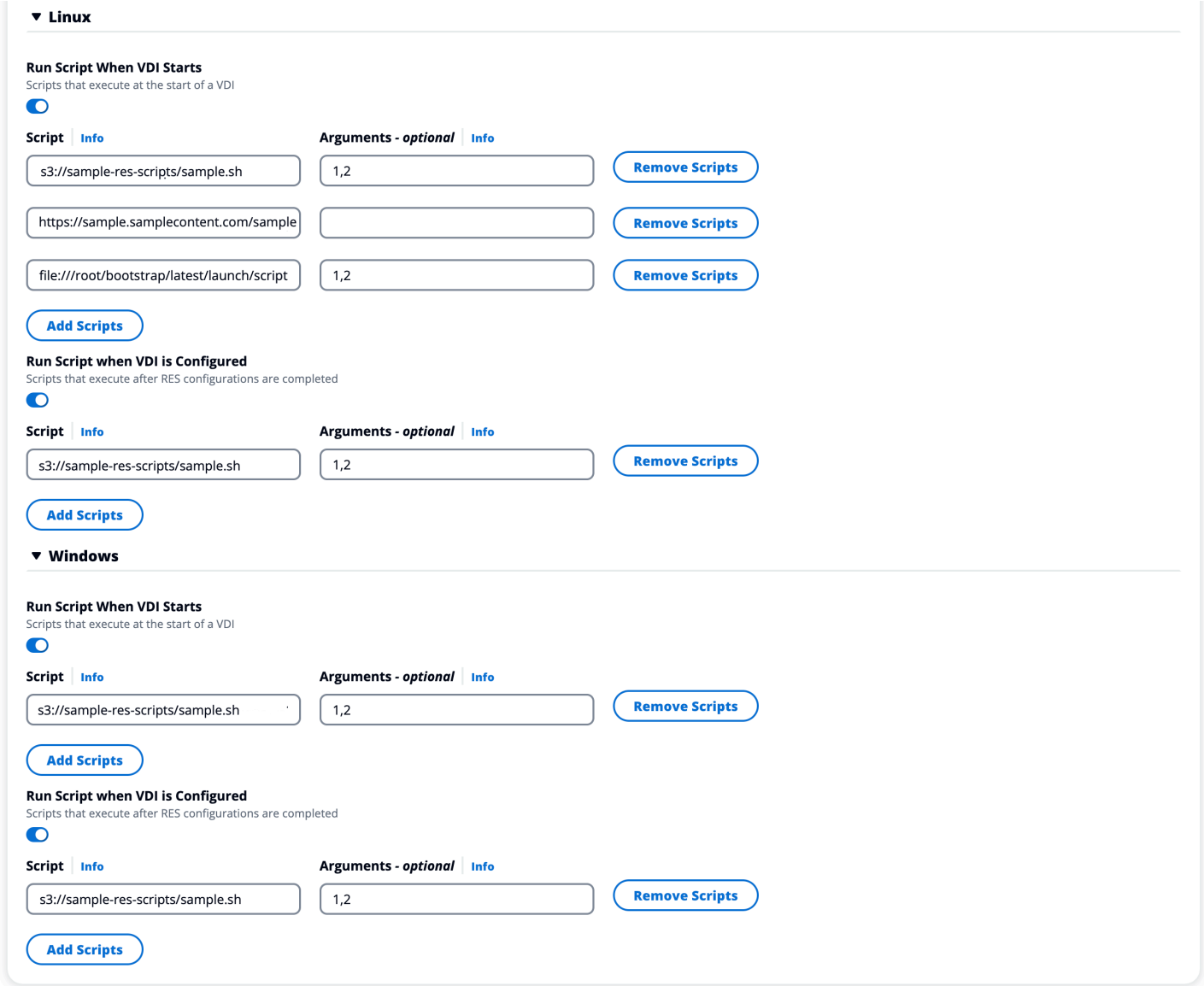
Cette option lance le script une fois les configurations RES terminées.

Les scripts prennent en charge les options suivantes :

Configuration du script	Exemple
URI S3	s3://bucketname/script.sh

Configuration du script	Exemple
URL HTTPS	https://sample.samplecontent.com/sample
Fichier local	fichier : ///user/scripts/example.sh

Pour Arguments, fournissez tous les arguments séparés par une virgule.

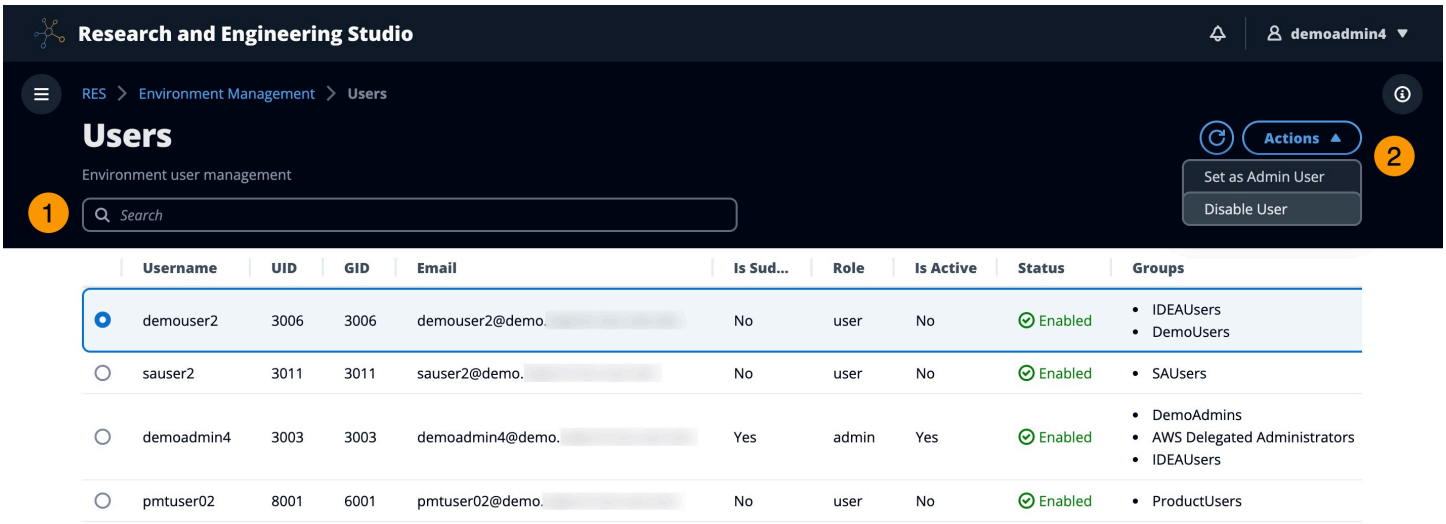


Exemple de configuration de projet

Users

Tous les utilisateurs synchronisés depuis votre Active Directory apparaîtront sur la page Utilisateurs. Les utilisateurs sont synchronisés par l'utilisateur cluster-admin lors de la configuration du produit. Pour plus d'informations sur la configuration utilisateur initiale, consultez leGuide de configuration.

> **Note**
>
> Les administrateurs ne peuvent créer des sessions que pour les utilisateurs actifs. Par défaut, tous les utilisateurs seront inactifs jusqu'à ce qu'ils se connectent à l'environnement du produit. Si un utilisateur est inactif, demandez-lui de se connecter avant de créer une session pour lui.

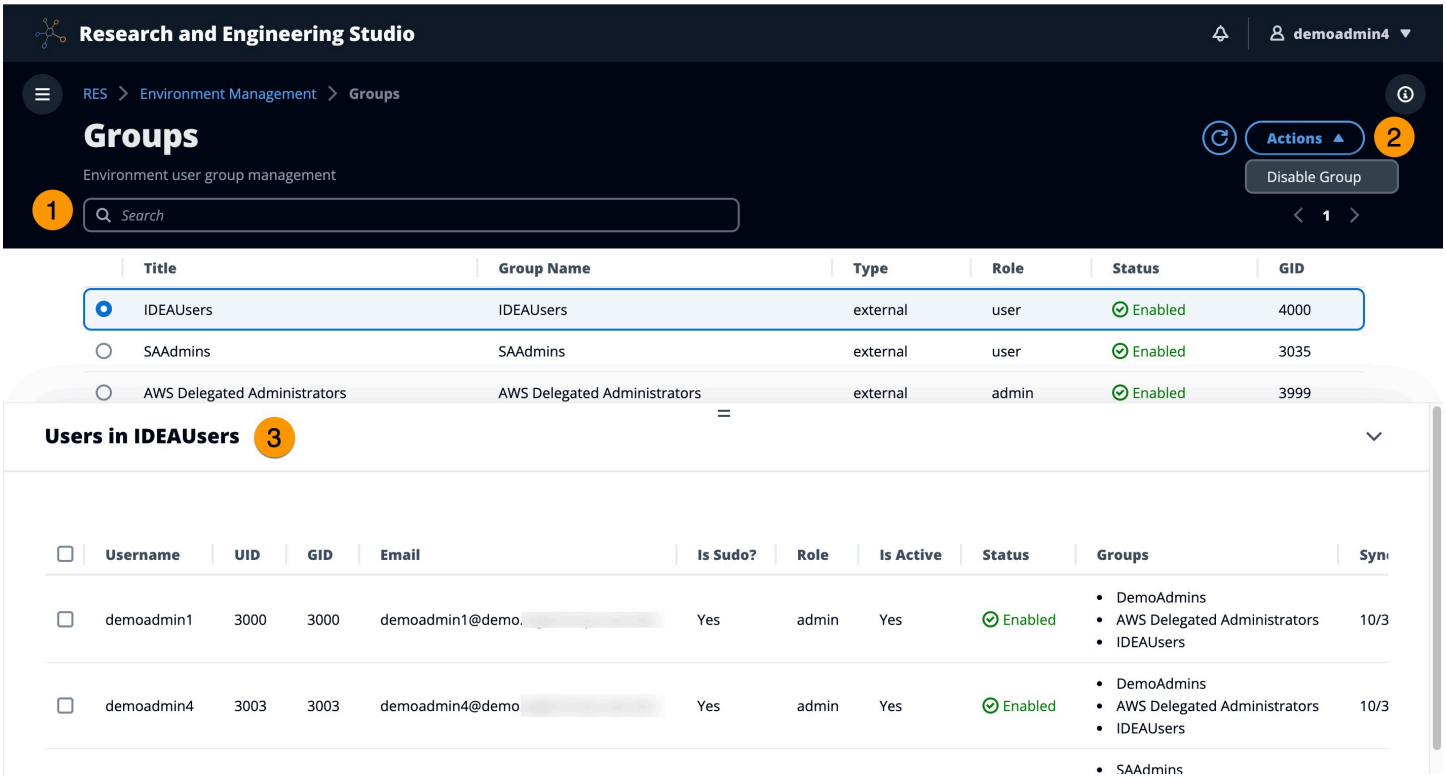


Depuis la page Utilisateurs, vous pouvez :

1. Recherche des utilisateurs.
2. Lorsqu'un nom d'utilisateur est sélectionné, utilisez le menu Actions pour :
    a. Définir en tant qu'utilisateur administrateur
    b. Désactiver l'utilisateur

Groups

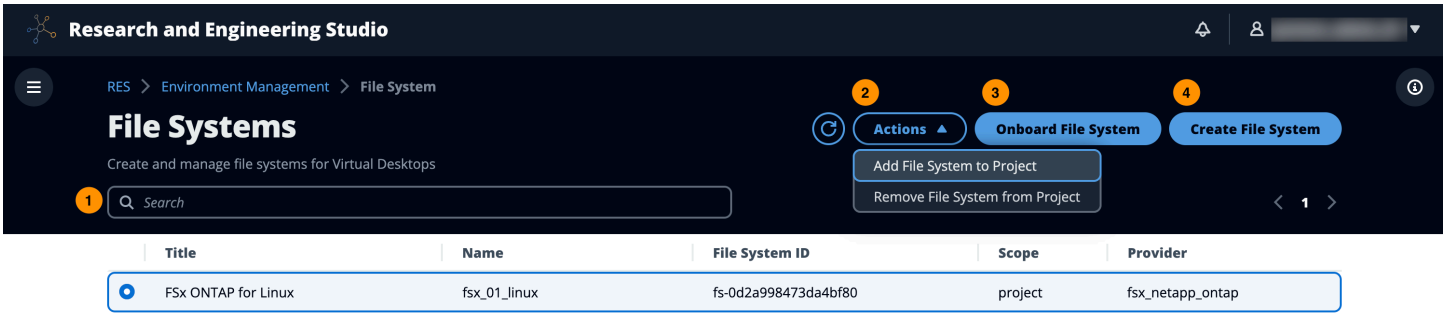
Tous les groupes synchronisés depuis Active Directory apparaissent sur la page Groupes. Pour plus d'informations sur la configuration et la gestion des groupes, consultez leGuide de configuration.



Sur la page Groupes, vous pouvez :

1. Recherchez des groupes d'utilisateurs.
2. Lorsqu'un groupe d'utilisateurs est sélectionné, utilisez le menu Actions pour activer ou désactiver un groupe.
3. Lorsqu'un groupe d'utilisateurs est sélectionné, vous pouvez développer le volet Utilisateurs en bas de l'écran pour afficher les utilisateurs du groupe.

Systèmes de fichiers



Sur la page Systèmes de fichiers, vous pouvez :

1. Recherchez des systèmes de fichiers.
2. Lorsqu'un système de fichiers est sélectionné, utilisez le menu Actions pour :
    a. Ajouter le système de fichiers à un projet
    b. Supprimer le système de fichiers d'un projet
3. Intégrez un nouveau système de fichiers.
4. Créez un système de fichiers.
5. Lorsqu'un système de fichiers est sélectionné, vous pouvez agrandir le volet en bas de l'écran pour afficher les détails du système de fichiers.

Création d'un système de fichiers

1. Sélectionnez Créer un système de fichiers.
2. Entrez les détails du nouveau système de fichiers.
3. Fournissez des ID de sous-réseau à partir du VPC. Vous pouvez trouver les identifiants dans l'onglet Gestion de l'environnement > Paramètres > Réseau.
4. Sélectionnez Envoyer.

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

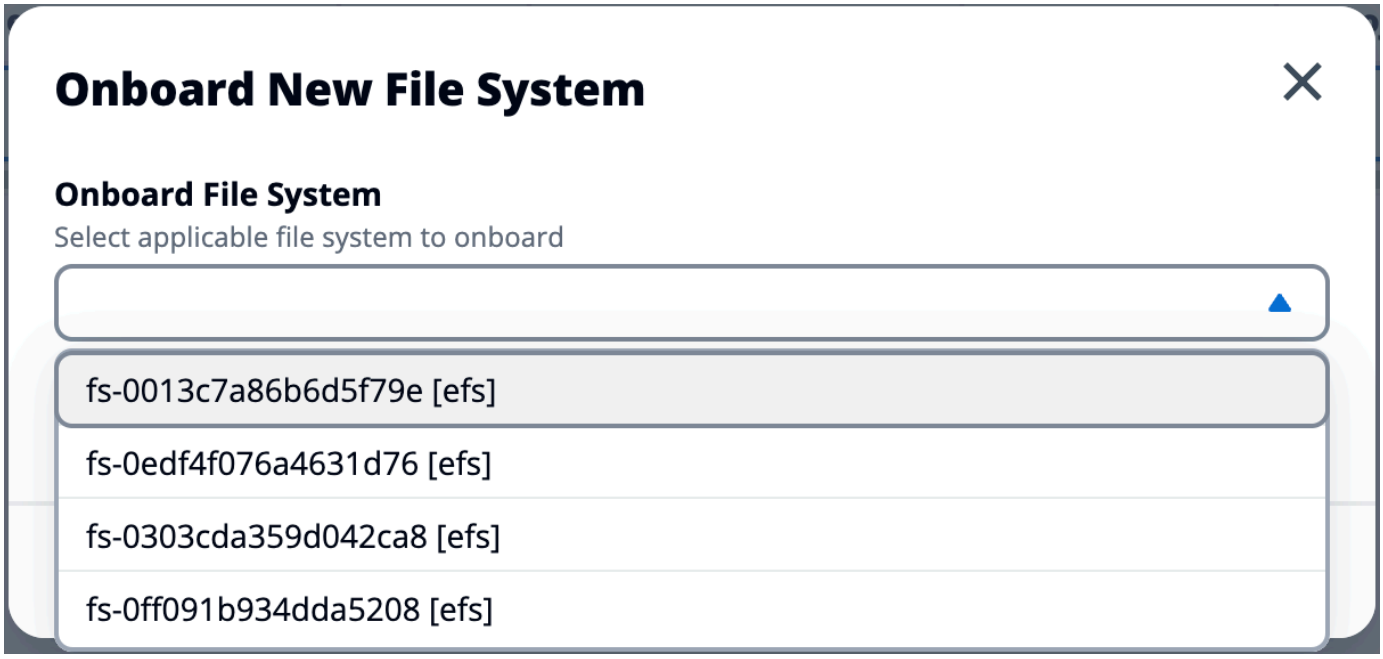
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

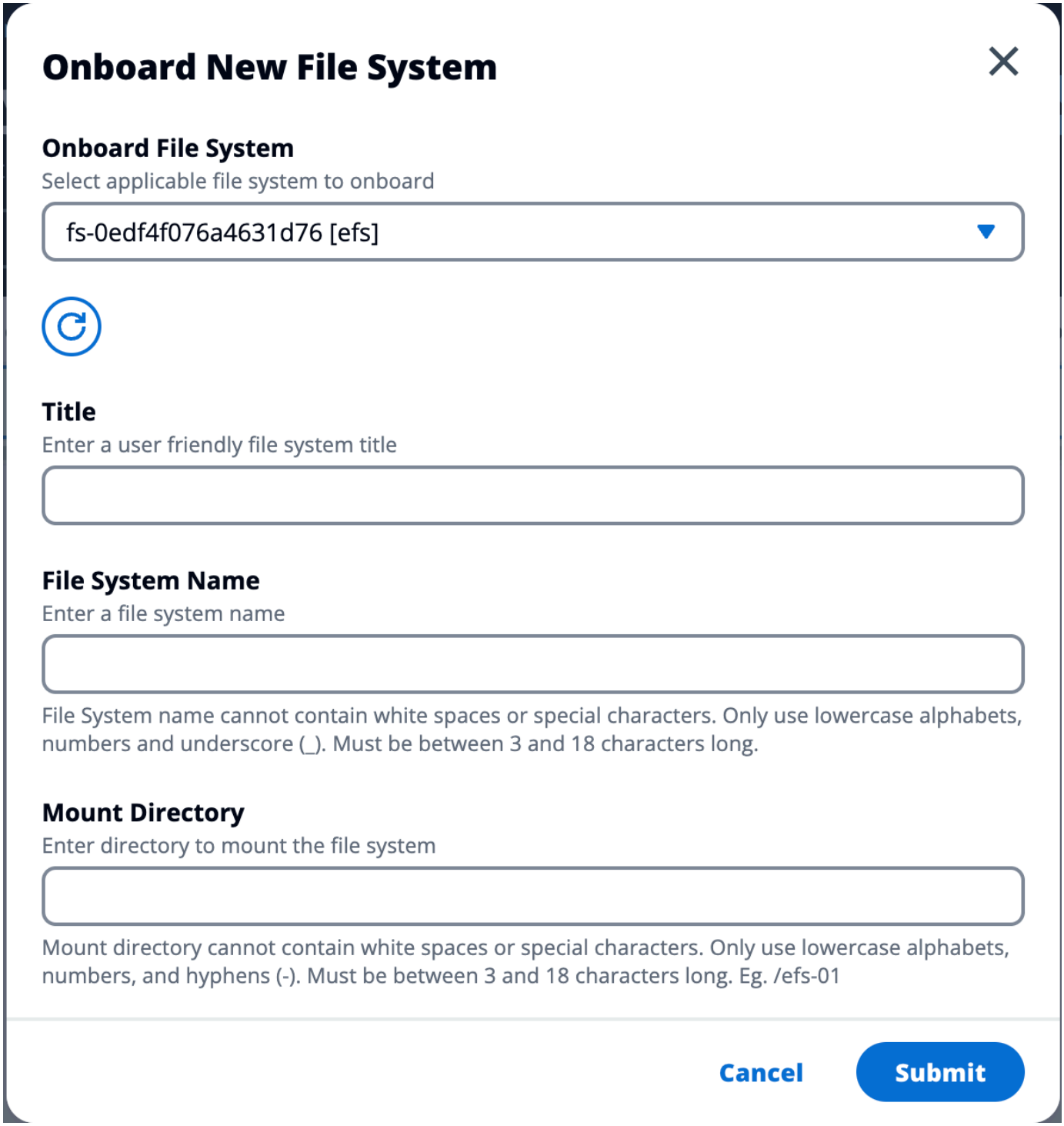
Enter directory to mount the file system

Intégrer un système de fichiers

1. Choisissez le système de fichiers intégré.
2. Sélectionnez un système de fichiers dans le menu déroulant. Le modal s'étendra avec des entrées de détails supplémentaires.

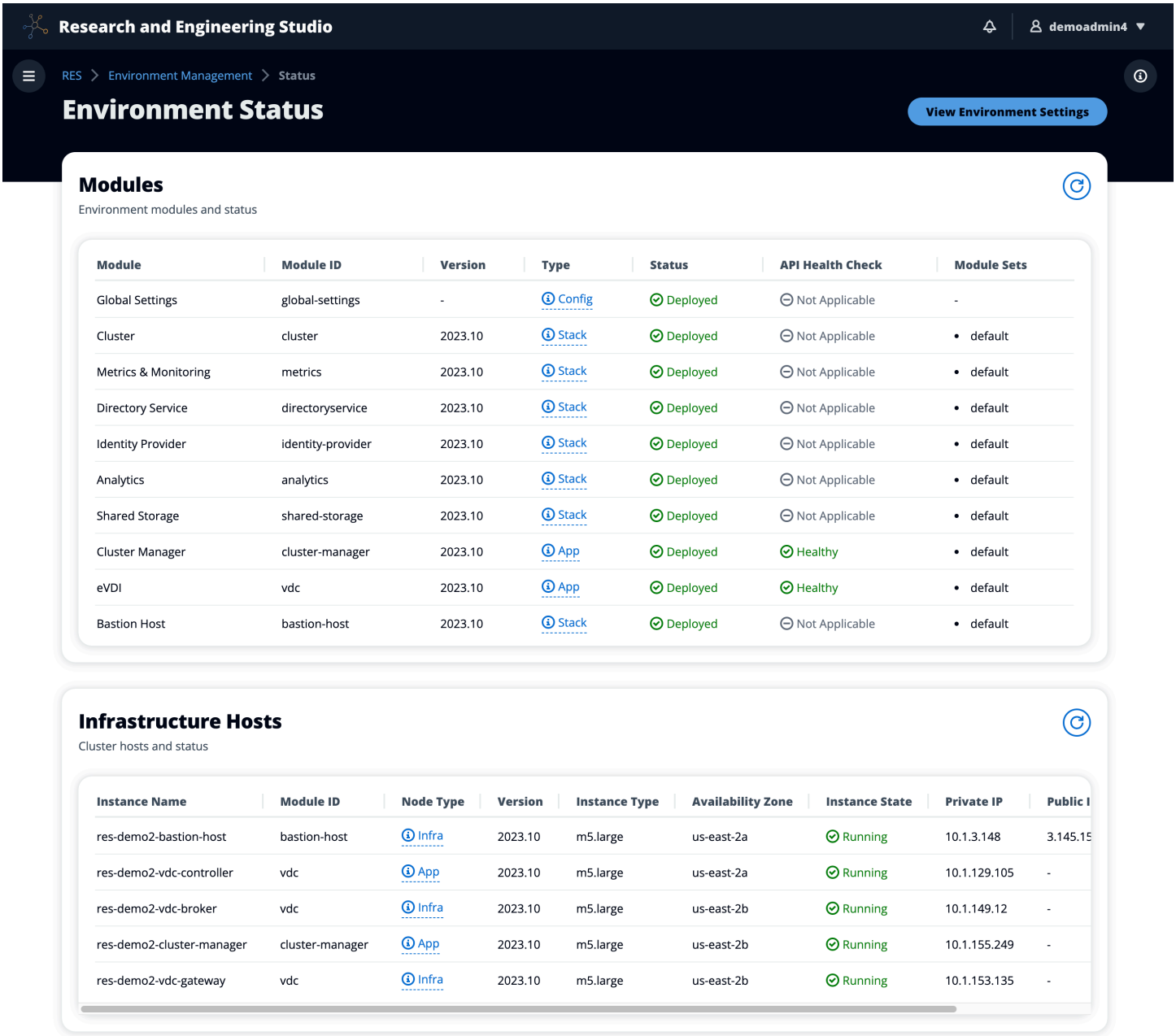


3. Entrez les détails du système de fichiers.
4. Sélectionnez Envoyer.



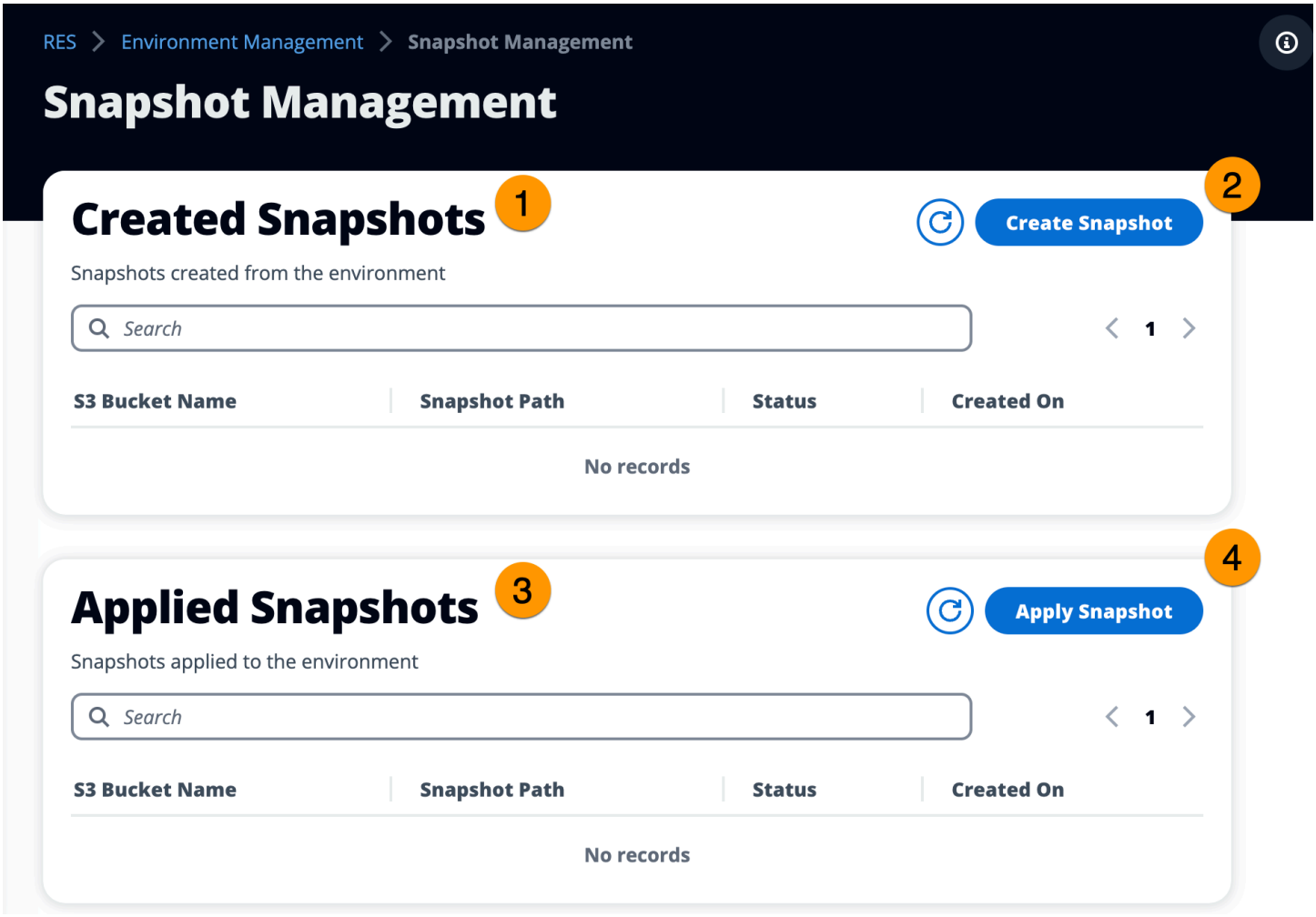
État de l'environnement

La page État de l'environnement affiche le logiciel déployé et les hôtes du produit. Il inclut des informations telles que la version du logiciel, les noms des modules et d'autres informations système.



Gestion des snapshots

La gestion des snapshots simplifie le processus de sauvegarde et de migration des données entre les environnements, garantissant ainsi cohérence et précision. Avec les instantanés, vous pouvez enregistrer l'état de votre environnement et migrer les données vers un nouvel environnement ayant le même état.



Depuis la page de gestion des snapshots, vous pouvez :

1. Affichez tous les instantanés créés et leur statut.
2. Créez un instantané. Avant de créer un instantané, vous devez créer un bucket doté des autorisations appropriées.
3. Affichez tous les instantanés appliqués et leur état.
4. Appliquez un instantané.

Créer un instantané

Avant de créer un instantané, vous devez fournir à un compartiment Amazon S3 les autorisations nécessaires. Pour en savoir plus sur la création d'un compartiment, consultez Créer un compartiment. Nous vous recommandons d'activer la gestion des versions des compartiments et la

journalisation des accès au serveur. Ces paramètres peuvent être activés depuis l'onglet Propriétés du bucket après le provisionnement.

> **Note**
>
> Le cycle de vie de ce compartiment Amazon S3 ne sera pas géré au sein du produit. Vous devrez gérer le cycle de vie du bucket depuis la console.

Pour ajouter des autorisations au bucket, procédez comme suit :

1. Choisissez le compartiment que vous avez créé dans la liste des compartiments.
2. Choisissez l'onglet Permissions (Autorisations).
3. Sous Politique de compartiment, choisissez Modifier.
4. Ajoutez la déclaration suivante à la politique du compartiment. Remplacez les valeurs suivantes par les vôtres :

   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

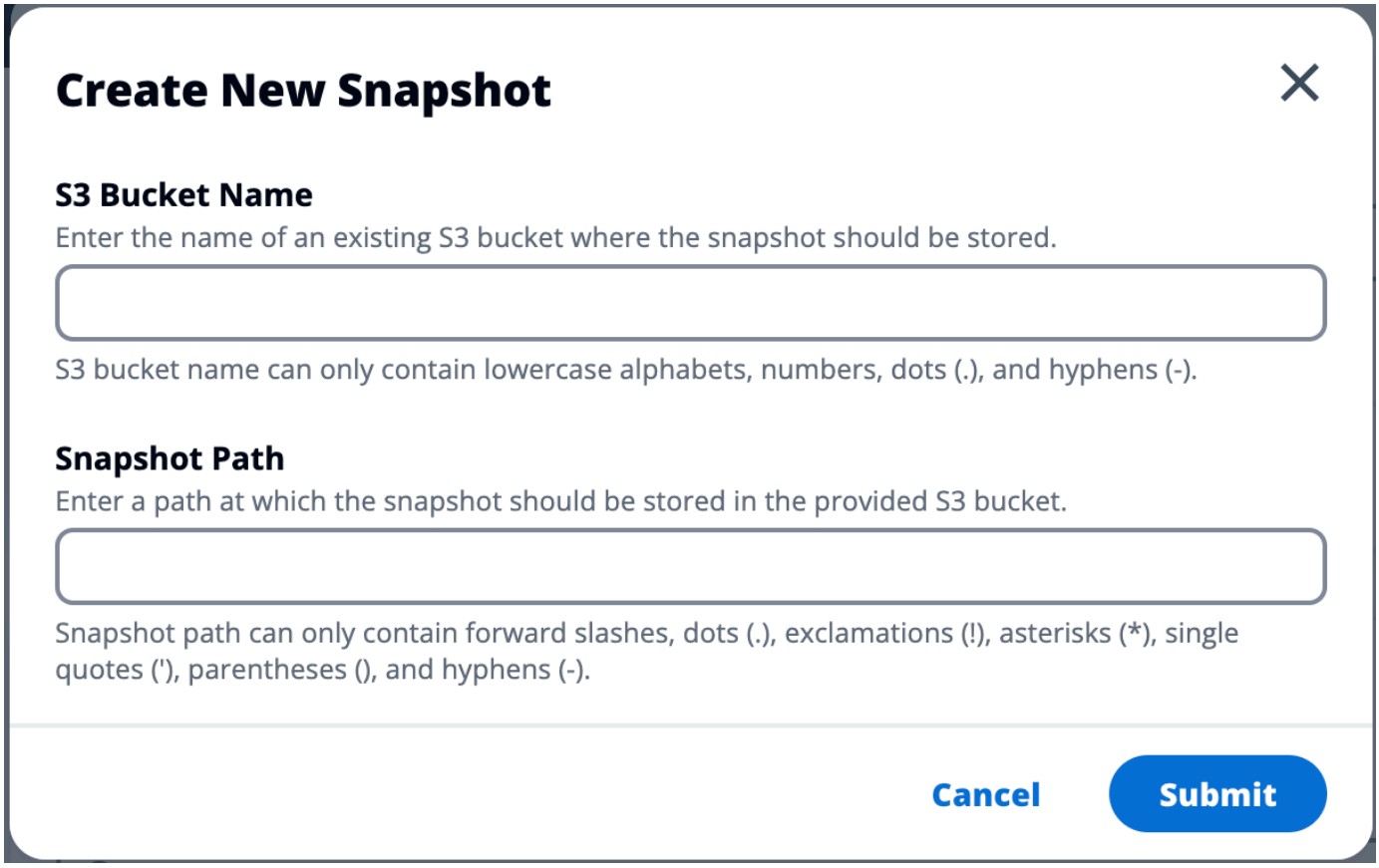
   > **Important**
   >
   > Certaines chaînes de version limitées sont prises en charge par AWS. Pour plus d'informations, consultez https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
```

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

Pour créer l'instantané, procédez comme suit :

1. Choisissez Create Snapshot (Créer un instantané).
2. Entrez le nom du compartiment Amazon S3 que vous avez créé.
3. Entrez le chemin où vous souhaitez que le cliché soit stocké dans le compartiment. Par exemple, **`october2023/23`**.
4. Sélectionnez Envoyer.



5. Après cinq à dix minutes, choisissez Actualiser sur la page Instantanés pour vérifier l'état. Un instantané ne sera pas valide tant que le statut ne passera pas de IN_PROGRESS à COMPLETED.

Appliquer un instantané

Une fois que vous avez créé un instantané d'un environnement, vous pouvez l'appliquer à un nouvel environnement pour faire migrer les données. Vous devrez ajouter une nouvelle politique au compartiment pour permettre à l'environnement de lire l'instantané.

L'application d'un instantané copie des données telles que les autorisations des utilisateurs, les projets, les piles de logiciels, les profils d'autorisation et les systèmes de fichiers avec leurs associations dans un nouvel environnement. Les sessions utilisateur ne seront pas répliquées. Lorsque le cliché est appliqué, il vérifie les informations de base de chaque enregistrement de ressource pour déterminer s'il existe déjà. Pour les enregistrements dupliqués, le snapshot ignore la création de ressources dans le nouvel environnement. Pour les enregistrements similaires, tels que partager un nom ou une clé, mais les autres informations de base sur les ressources varient, il créera un nouvel enregistrement avec un nom et une clé modifiés en utilisant la convention

suivante :`RecordName_SnapshotRESVersion_ApplySnapshotID`. `ApplySnapshotID`Il ressemble à un horodatage et identifie chaque tentative d'application d'un instantané.

Au cours de l'application de capture instantanée, la capture instantanée vérifie la disponibilité des ressources. La ressource non disponible pour le nouvel environnement ne sera pas créée. Pour les ressources dotées d'une ressource dépendante, le cliché vérifie la disponibilité de la ressource dépendante. Si la ressource dépendante n'est pas disponible, elle créera la ressource principale sans la ressource dépendante.

Si le nouvel environnement ne fonctionne pas comme prévu ou échoue, vous pouvez consulter les CloudWatch journaux trouvés dans le groupe de journaux `/res-<env-name>/cluster-manager` pour plus de détails. Chaque journal comportera la balise [apply snapshot]. Une fois que vous avez appliqué un instantané, vous pouvez vérifier son statut the section called “Gestion des snapshots” sur la page.

Pour ajouter des autorisations au bucket, procédez comme suit :

1. Choisissez le compartiment que vous avez créé dans la liste des compartiments.
2. Choisissez l'onglet Permissions (Autorisations).
3. Sous Politique de compartiment, choisissez Modifier.
4. Ajoutez la déclaration suivante à la politique du compartiment. Remplacez les valeurs suivantes par les vôtres :

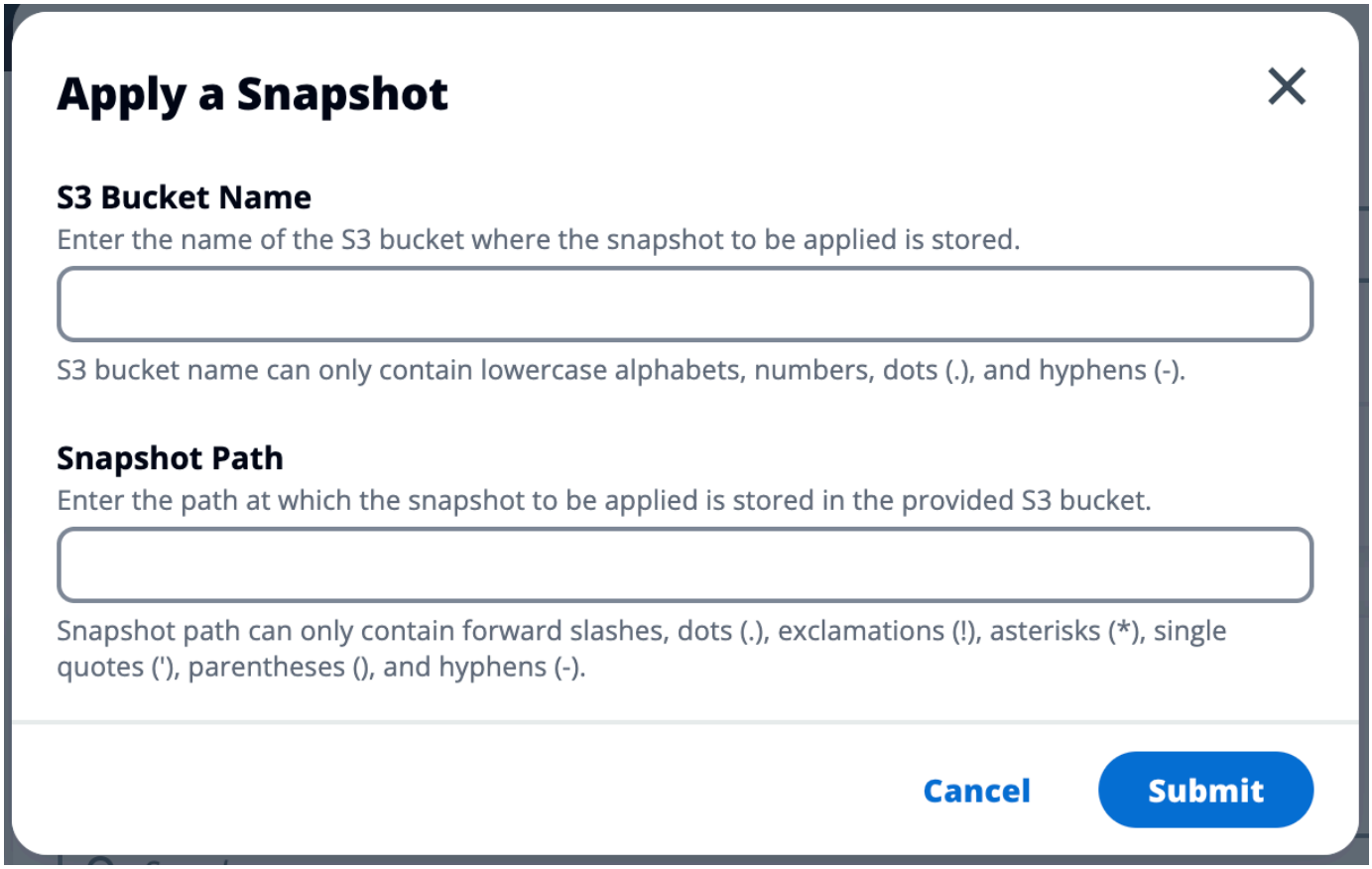
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

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

Pour appliquer un instantané :

1. Choisissez Appliquer un instantané.
2. Entrez le nom du compartiment Amazon S3 contenant le snapshot.
3. Entrez le chemin du fichier vers le snapshot dans le compartiment.
4. Sélectionnez Envoyer.



5. Après cinq à dix minutes, choisissez Actualiser sur la page de gestion des snapshots pour vérifier l'état.

Paramètres d'environnement

Les paramètres d'environnement affichent les détails de configuration du produit, tels que :

- Général

  Affiche des informations telles que le nom d'utilisateur de l'administrateur et l'adresse e-mail de l'utilisateur qui a approvisionné le produit. Vous pouvez modifier le titre du portail Web et le texte du copyright.

- Fournisseur d'identité

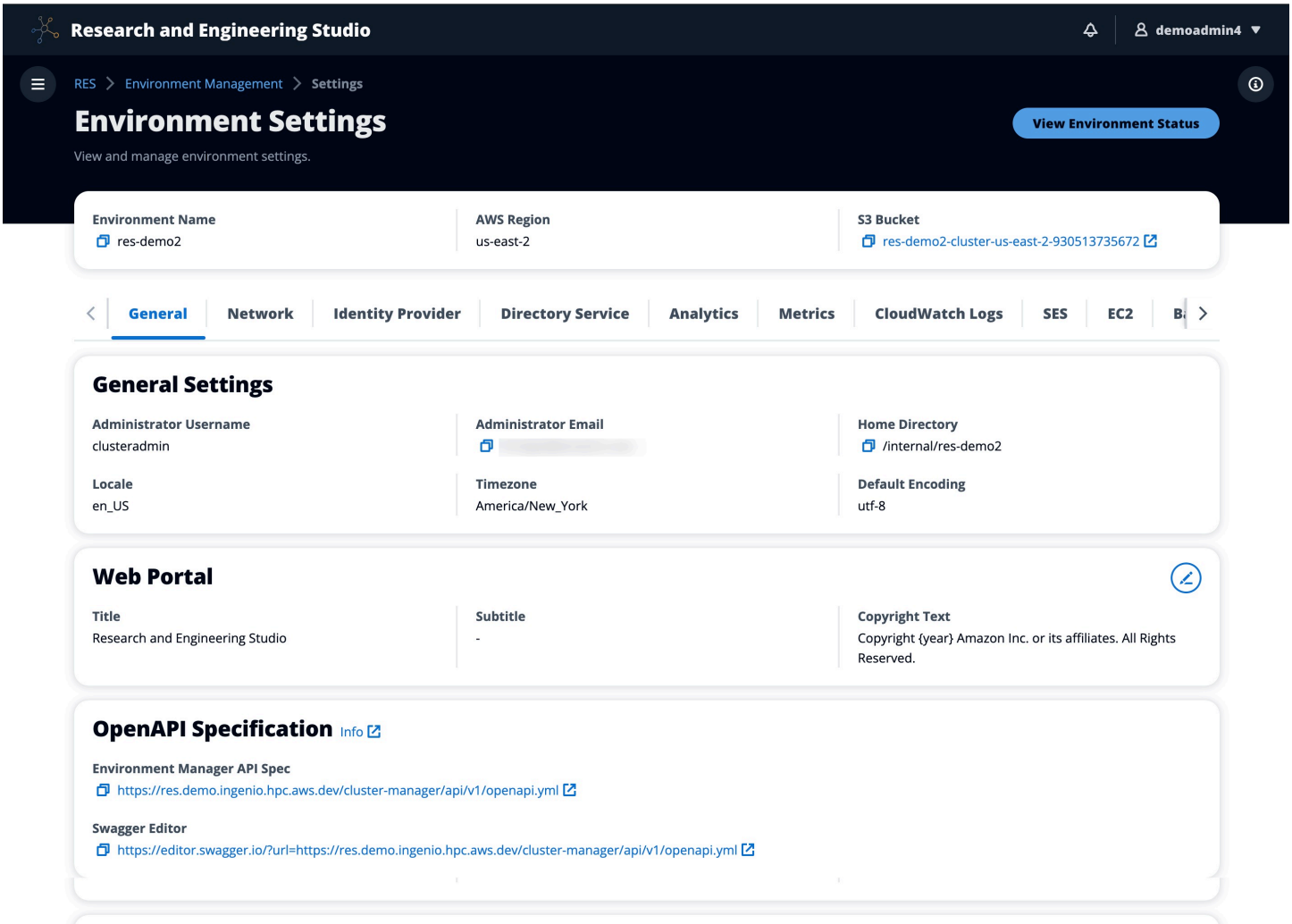
  Affiche des informations telles que l'état de l'authentification unique.

- Réseau

  Affiche l'ID du VPC et les identifiants de la liste de préfixes pour l'accès.

- Directory Service

  Affiche les paramètres Active Directory et l'ARN du gestionnaire de secrets des comptes de service pour le nom d'utilisateur et le mot de passe.



Gestion des secrets

Le studio de recherche et d'ingénierie conserve les secrets suivants en utilisant AWS Secrets Manager. RES crée automatiquement des secrets lors de la création de l'environnement. Les secrets saisis par l'administrateur lors de la création de l'environnement sont saisis en tant que paramètres.

Nom du secret	Description	RES généré	Admin saisi
<envname>- sso-client-secret	Secret du client OAuth2 à authentification unique pour l'environnement	✓	
<envname>- vdc-client-secret	vdc ClientSecret	✓	
<envname>- vdc-client-id	vdc ClientId	✓	
<envname>- vdc-gateway-certificate-private -clé	Clé privée du certificat autosigné pour le domaine	✓	
<envname>- vdc-gateway-certificate-certificate	Certificat auto-signé pour le domaine	✓	
<envname>- cluster-manager-client-secret	gestionnaire de clusters ClientSecret	✓	
<envname>- cluster-manager-client-id	gestionnaire de clusters ClientId	✓	
<envname>- external-private-key	Clé privée du certificat autosigné pour le domaine	✓	
<envname>-certificat externe	Certificat auto-signé pour le domaine	✓	
<envname>- internal-private-key	Clé privée du certificat autosigné pour le domaine	✓	

Nom du secret	Description	RES généré	Admin saisi
<envname>-certificat interne	Certificat auto-signé pour le domaine	✓	
<envname>-service d'annuaire - ServiceAccountUsername			✓
<envname>-service d'annuaire - ServiceAccountPassword			✓

Les valeurs ARN secrètes suivantes figurent dans la <envname>table -cluster-settings de DynamoDB :

Clé	Source
fournisseur d'identité.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	pile
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	pile
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	pile
directoryservice.root_username_secret_arn	
vdc.client_secret	pile
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	pile
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	pile

Clé	Source
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	pile
cluster-manager.client_secret	

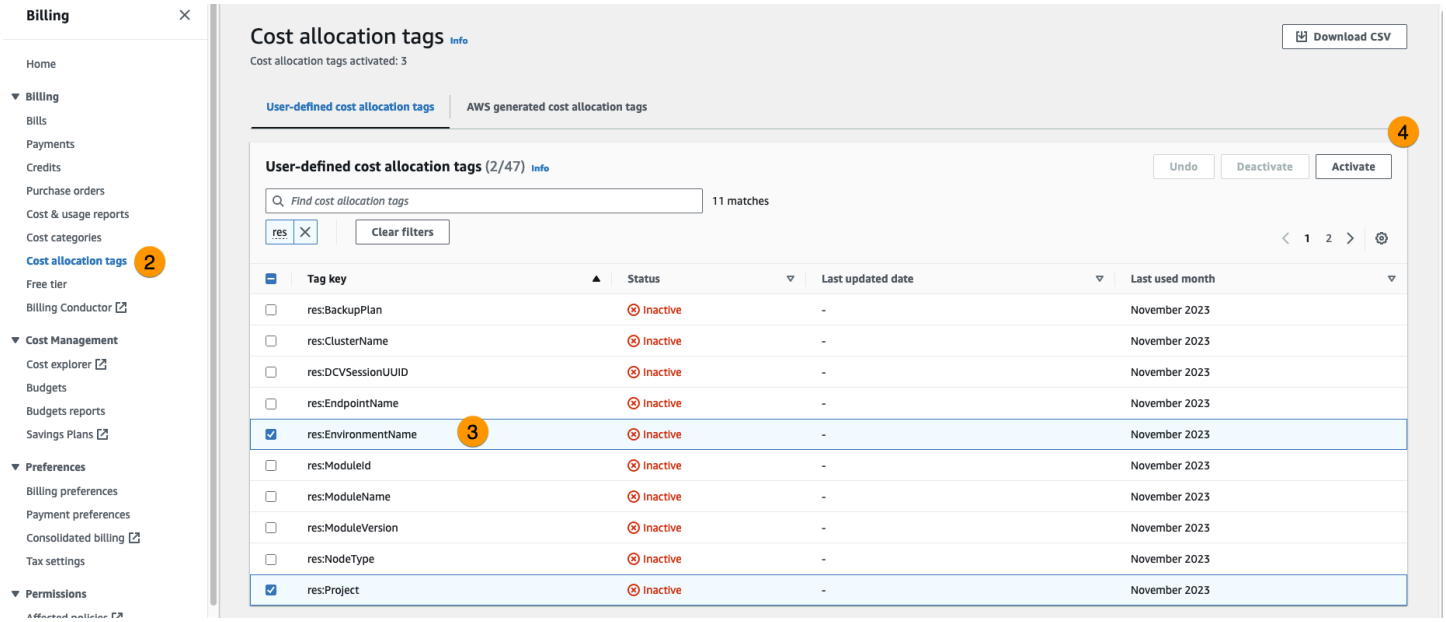
Surveillance et contrôle des coûts

> **Note**
>
> L'association de projets de studios de recherche et d'ingénierie à des projets n' AWS Budgets est pas prise en charge dans AWS GovCloud (US).

Nous vous recommandons de créer un budget via AWS Cost Explorer pour faciliter la gestion des coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chacun desthe section called "AWSservices inclus dans ce produit".

Pour faciliter le suivi des coûts, vous pouvez associer des projets RES aux budgets créés dans ce cadre AWS Budgets. Vous devez d'abord activer les balises d'environnement dans les balises de répartition des coûts de facturation.

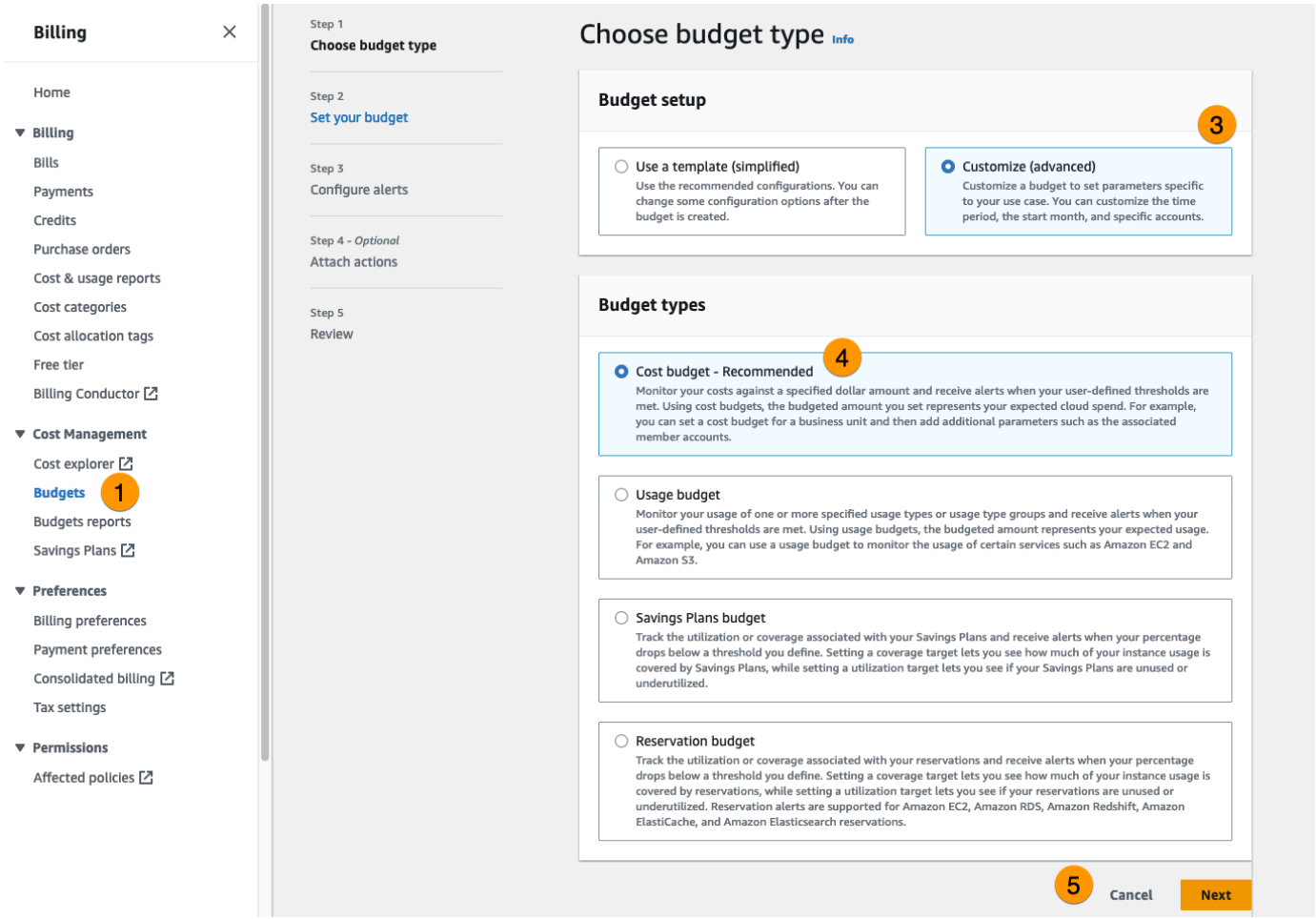
1. Connectez-vous à la AWS Billing console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/billing/.
2. Choisissez les balises de répartition des coûts.
3. Recherchez et sélectionnez les `res:EnvironmentName` balises `res:Project` et.
4. Choisissez Activer.



> **Note**
>
> L'affichage des balises RES après le déploiement peut prendre jusqu'à un jour.

Pour créer un budget pour les ressources RES :

1. Dans la console de facturation, sélectionnez Budgets.
2. Choisissez Créer un budget.
3. Sous Configuration du budget, choisissez Personnaliser (avancé).
4. Sous Types de budget, sélectionnez Budget des coûts - Recommandé.
5. Choisissez Suivant.

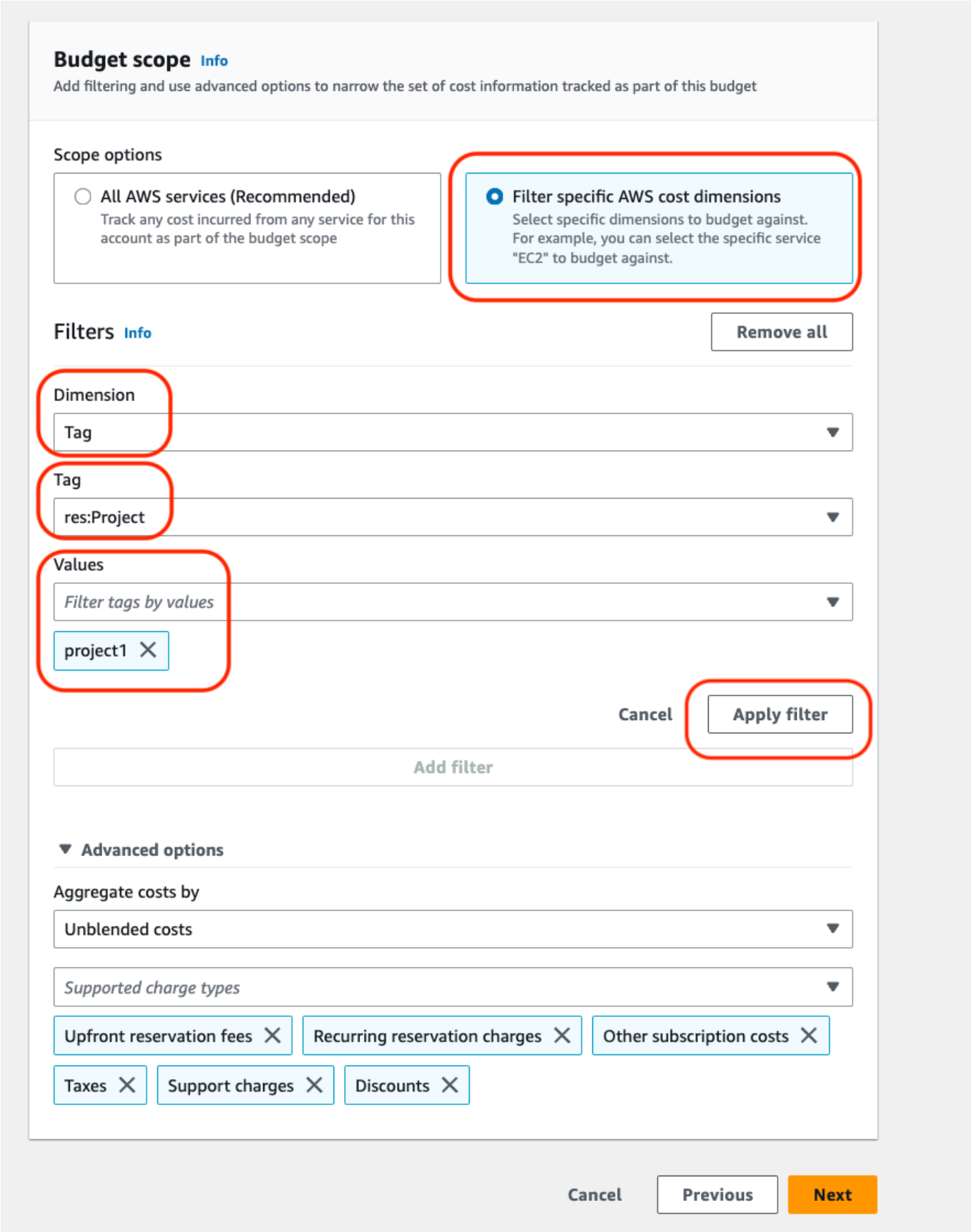


6. Sous Détails, saisissez un nom de budget significatif pour votre budget afin de le distinguer des autres budgets de votre compte. Par exemple, [EnvironmentName] - [ProjectName] - [BudgetName].
7. Sous Définir le montant du budget, entrez le montant budgétisé pour votre projet.
8. Sous Étendue du budget, choisissez Filtrer les dimensions de AWS coût spécifiques.
9. Choisissez Add filter.
10. Sous Dimension, choisissez Tag.
11. Sous Tag, sélectionnez RES:Project.

> **Note**
>
> La disponibilité des balises et des valeurs peut prendre jusqu'à deux jours. Vous pouvez créer un budget une fois que le nom du projet sera disponible.

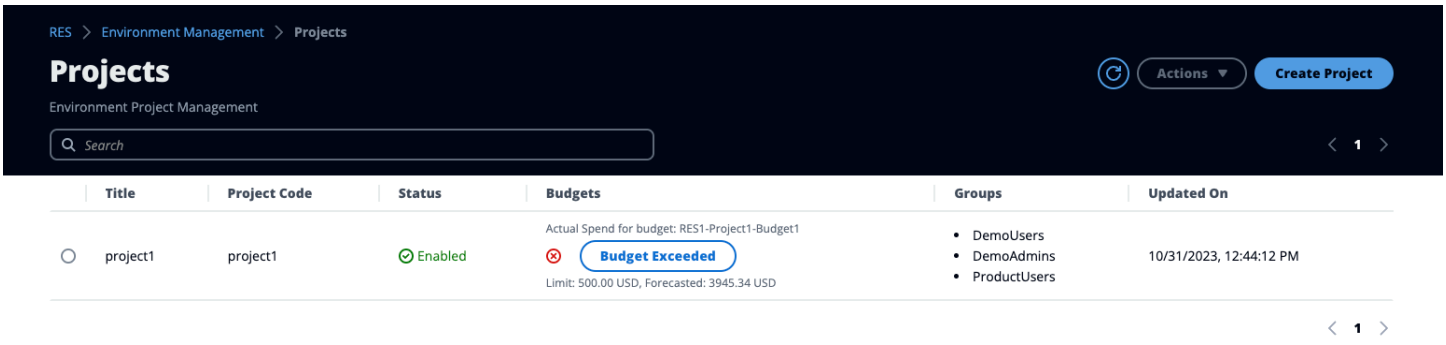
12. Sous Valeurs, sélectionnez le nom du projet.

13. Choisissez Appliquer le filtre pour associer le filtre de projet au budget.
14. Choisissez Suivant.


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. (Facultatif.) Ajoutez un seuil d'alerte.
16. Choisissez Suivant.
17. (Facultatif.) Si une alerte a été configurée, utilisez Attacher des actions pour configurer les actions souhaitées avec l'alerte.
18. Choisissez Suivant.
19. Vérifiez la configuration du budget et confirmez que la balise correcte a été définie sous Paramètres budgétaires supplémentaires.
20. Choisissez Créer un budget.

Maintenant que le budget a été créé, vous pouvez activer le budget pour les projets. Pour activer les budgets d'un projet, voirthe section called "Modifier un projet". Le lancement des bureaux virtuels sera bloqué en cas de dépassement du budget. Si le budget est dépassé lors du lancement d'un ordinateur de bureau, celui-ci continuera à fonctionner.



Si vous devez modifier votre budget, revenez à la console pour modifier le montant du budget. La prise en compte de la modification dans RES peut prendre jusqu'à quinze minutes. Vous pouvez également modifier un projet pour désactiver un budget.

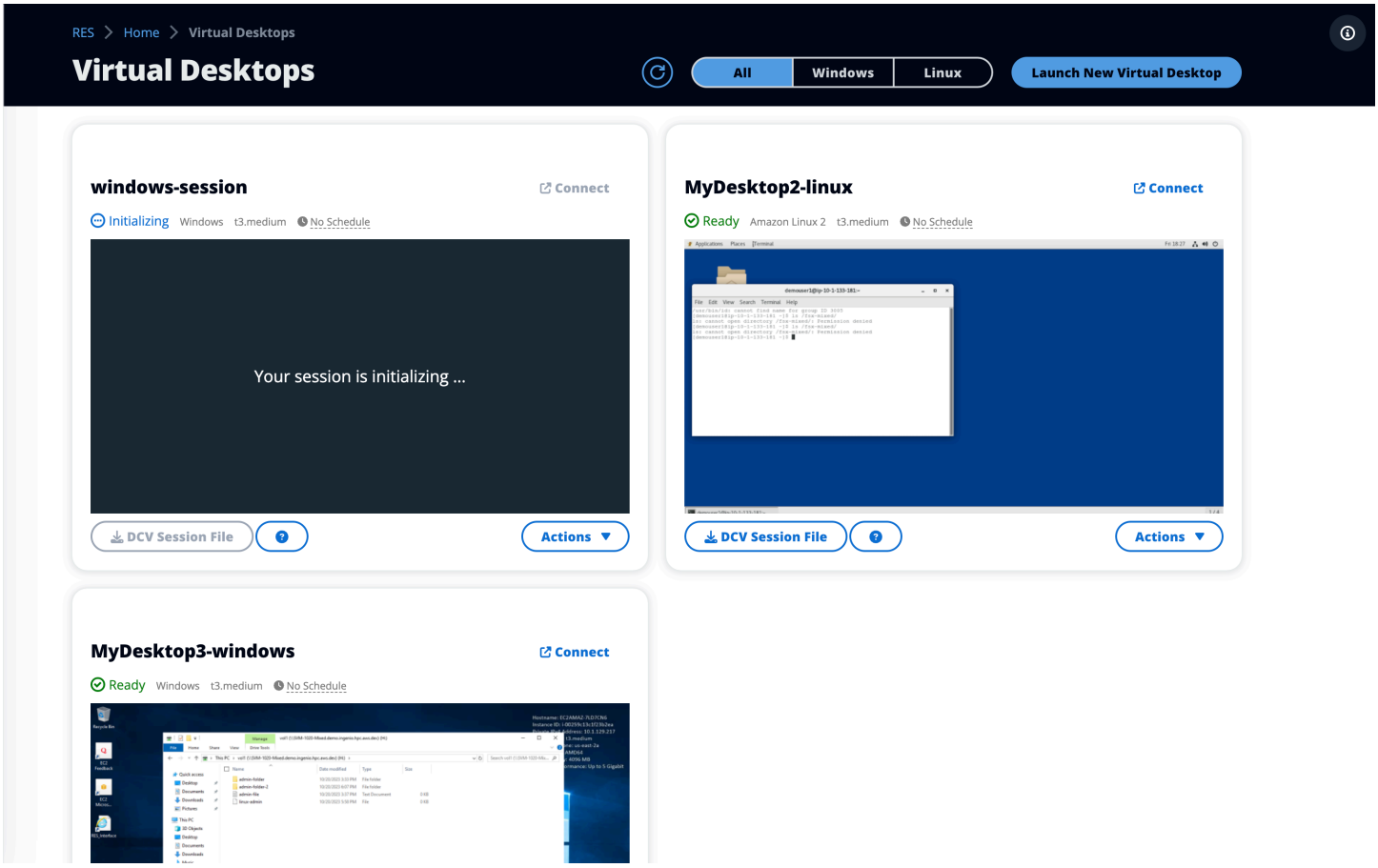
Utiliser le produit

Cette section fournit des conseils aux utilisateurs sur l'utilisation de bureaux virtuels pour collaborer avec d'autres utilisateurs.

Rubriques

Bureaux virtuels

Le module d'interface de bureau virtuel (VDI) permet aux utilisateurs de créer et de gérer des bureaux virtuels Windows ou Linux sur. AWS Les utilisateurs peuvent lancer des instances Amazon EC2 avec leurs outils et applications préférés préinstallés et configurés.



Lancer un nouvel ordinateur

1. Dans le menu, choisissez My Virtual Desktops.
2. Choisissez Lancer un nouveau bureau virtuel.
3. Entrez les informations relatives à votre nouvel ordinateur de bureau.
4. Sélectionnez Envoyer.

Une nouvelle carte contenant les informations de votre bureau apparaît instantanément, et votre bureau sera prêt à être utilisé dans les 10 à 15 minutes. Le temps de démarrage dépend de l'image sélectionnée. RES détecte les instances de GPU et installe les pilotes appropriés.

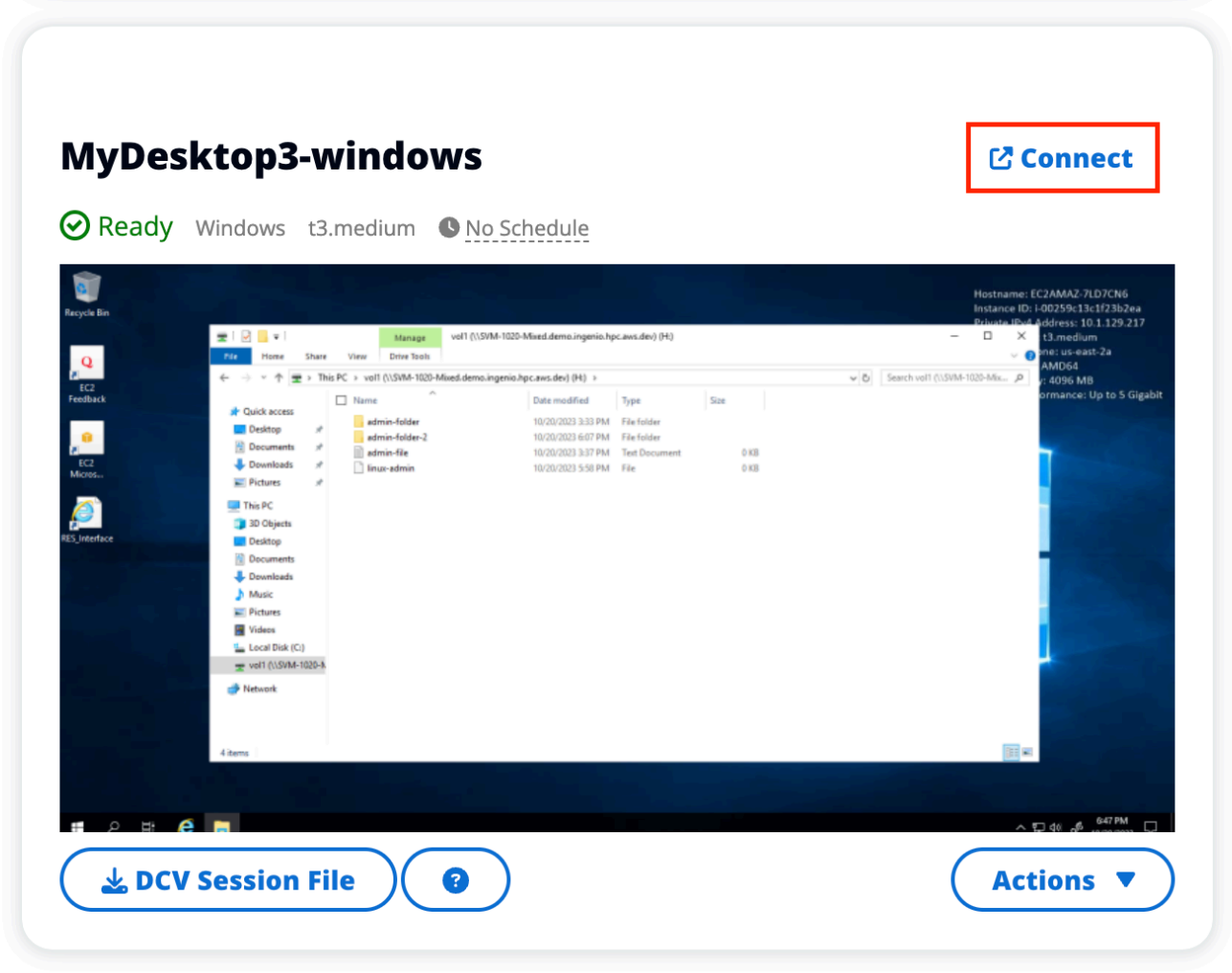
Accédez à votre bureau

Pour accéder à un bureau virtuel, choisissez la carte correspondant au poste de travail et connectez-vous à l'aide d'un client Web ou DCV.

Web connection

L'accès à votre bureau via le navigateur Web est la méthode de connexion la plus simple.

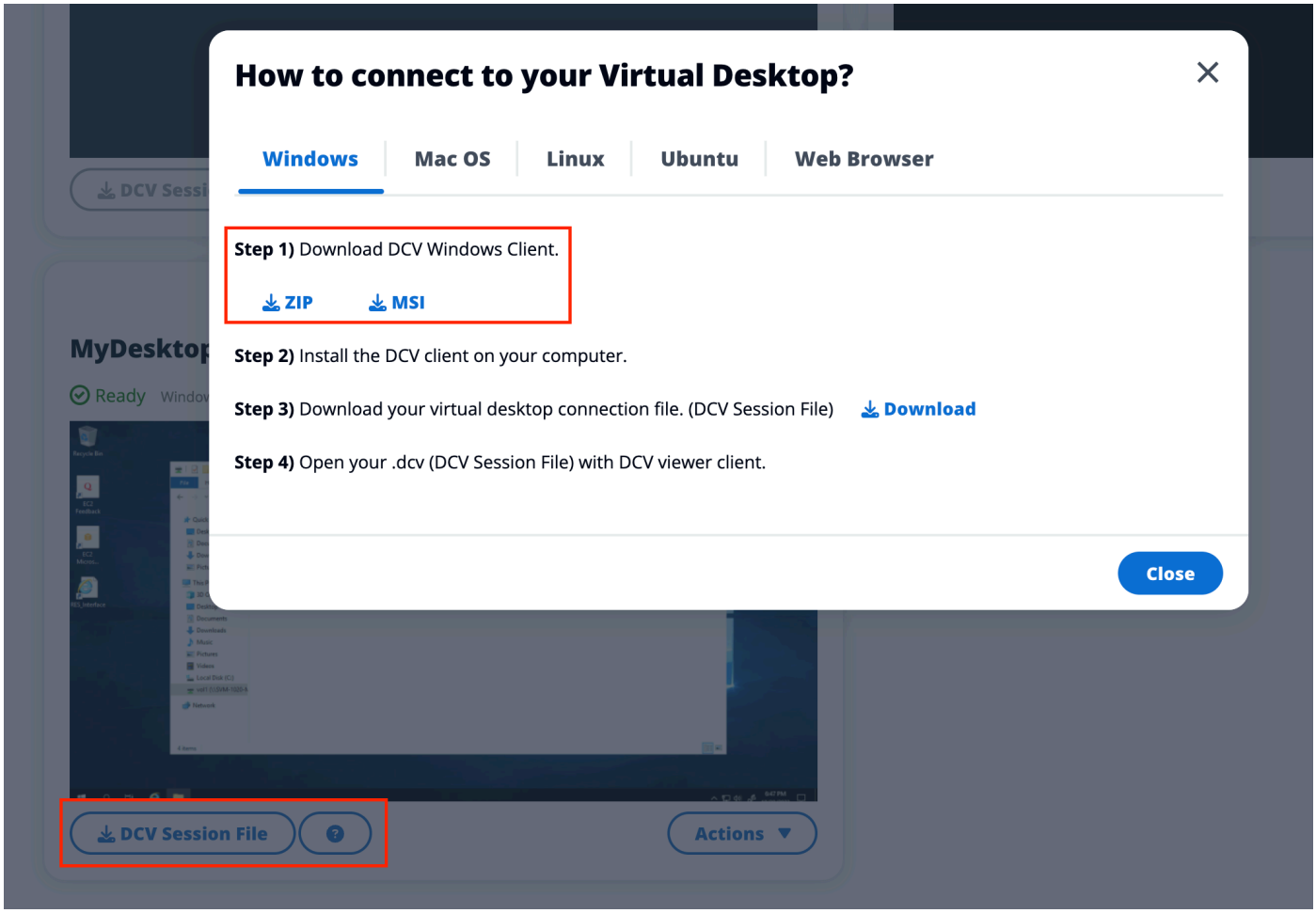
- Choisissez Connect ou choisissez la miniature pour accéder à votre bureau directement via votre navigateur.



DCV connection

L'accès à votre bureau par le biais d'un client DCV offre les meilleures performances. Pour y accéder via DCV :

1. Choisissez le fichier de session DCV pour télécharger le. `dcv`fichier. Vous aurez besoin d'un client DCV installé sur votre système.
2. Pour les instructions d'installation, choisissez le ? icône.



Contrôlez l'état de votre bureau

Pour contrôler l'état de votre ordinateur de bureau :

1. Choisissez Actions.
2. Choisissez Virtual Desktop State. Vous avez le choix entre quatre états :

   - Arrêter

     Une session arrêtée ne subira aucune perte de données, et vous pouvez redémarrer une session arrêtée à tout moment.

   - Redémarrer

     Redémarre la session en cours.

   - Résilier

Met définitivement fin à une session. La fin d'une session peut entraîner une perte de données si vous utilisez un stockage éphémère. Vous devez sauvegarder vos données sur le système de fichiers RES avant de terminer.

- Hiberner

  L'état de votre bureau sera enregistré en mémoire. Lorsque vous redémarrez le bureau, vos applications reprennent, mais les connexions à distance risquent d'être perdues. Toutes les instances ne prennent pas en charge l'hibernation, et l'option n'est disponible que si elle a été activée lors de la création de l'instance. Pour vérifier si votre instance prend en charge cet état, consultez la section Conditions préalables à l'hibernation.

Modifier un bureau virtuel

Vous pouvez mettre à jour le matériel de votre bureau virtuel ou modifier le nom de session.

1. Avant de modifier la taille de l'instance, vous devez arrêter la session :
   a. Choisissez Actions.
   b. Choisissez Virtual Desktop State.
   c. Choisissez Arrêter.

> **Note**
>
> Vous ne pouvez pas mettre à jour la taille du bureau pour les sessions en veille prolongée.

2. Une fois que vous avez confirmé l'arrêt du bureau, choisissez Actions, puis choisissez Mettre à jour la session.
3. Modifiez le nom de la session ou choisissez la taille de bureau que vous souhaitez.
4. Sélectionnez Envoyer.
5. Une fois vos instances mises à jour, redémarrez votre bureau :
   a. Choisissez Actions.
   b. Choisissez Virtual Desktop State.
   c. Sélectionnez Démarrer.

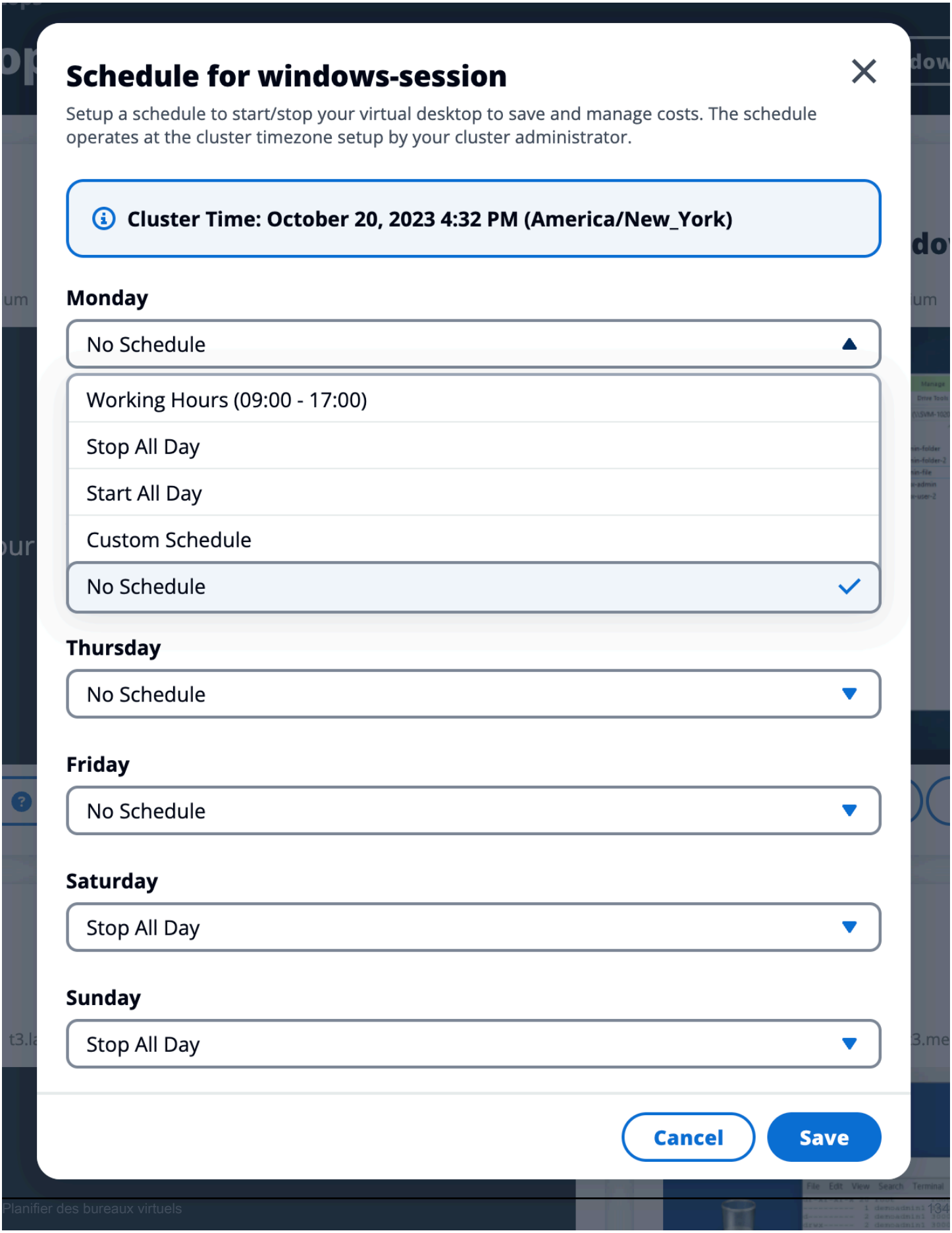
Récupérer les informations de session

1. Choisissez Actions.
2. Choisissez Afficher les informations.

Planifier des bureaux virtuels

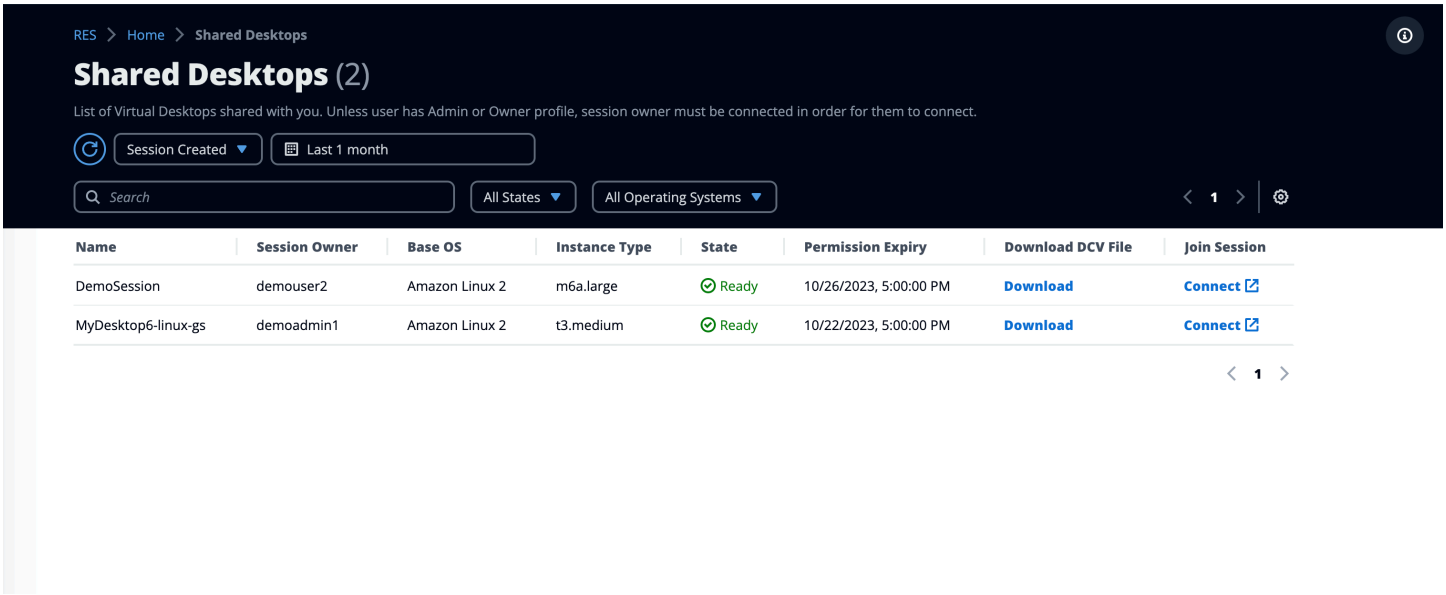
Par défaut, les bureaux virtuels n'ont pas de calendrier et restent actifs jusqu'à ce que vous arrêtiez ou mettiez fin à la session. Les ordinateurs de bureau s'arrêtent également en cas d'inactivité pour éviter les arrêts accidentels. Un état d'inactivité est déterminé par l'absence de connexion active et par une utilisation du processeur inférieure à 15 % pendant au moins 15 minutes. Vous pouvez configurer un calendrier pour démarrer et arrêter automatiquement votre bureau.

1. Choisissez Actions.
2. Sélectionnez Programme.
3. Définissez votre emploi du temps pour chaque jour.
4. Choisissez Enregistrer.


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

Bureaux partagés

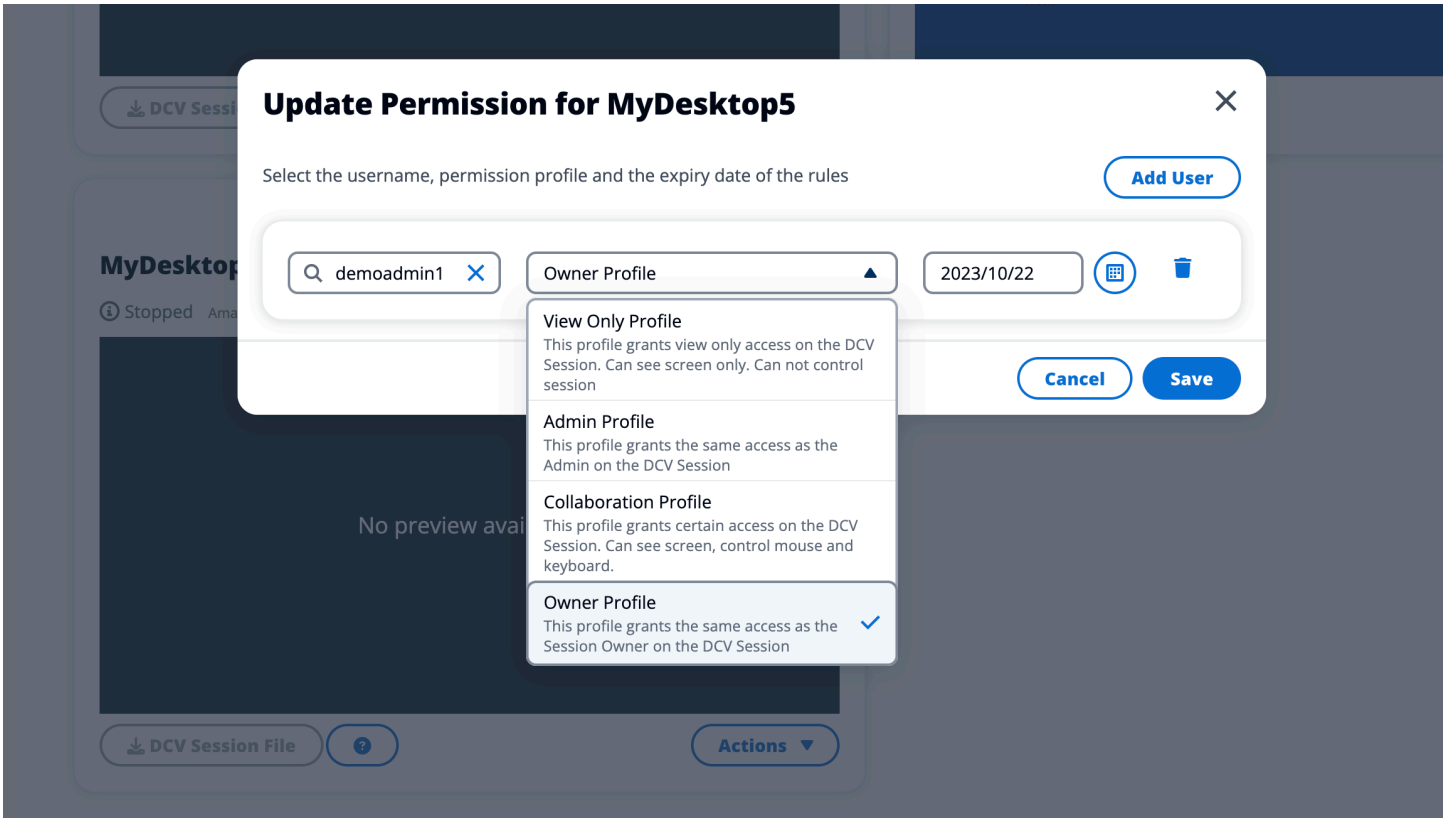
Sur les bureaux partagés, vous pouvez voir les bureaux qui ont été partagés avec vous. Pour se connecter à un poste de travail, le propriétaire de la session doit également être connecté, sauf si vous êtes administrateur ou propriétaire.



Lorsque vous partagez une session, vous pouvez configurer les autorisations pour vos collaborateurs. Par exemple, vous pouvez accorder un accès en lecture seule à un coéquipier avec lequel vous collaborez.

Partage d'un ordinateur

1. Dans votre session de bureau, choisissez Actions.
2. Choisissez Autorisations de session.
3. Choisissez l'utilisateur et le niveau d'autorisation. Vous pouvez également définir une date d'expiration.
4. Choisissez Enregistrer.



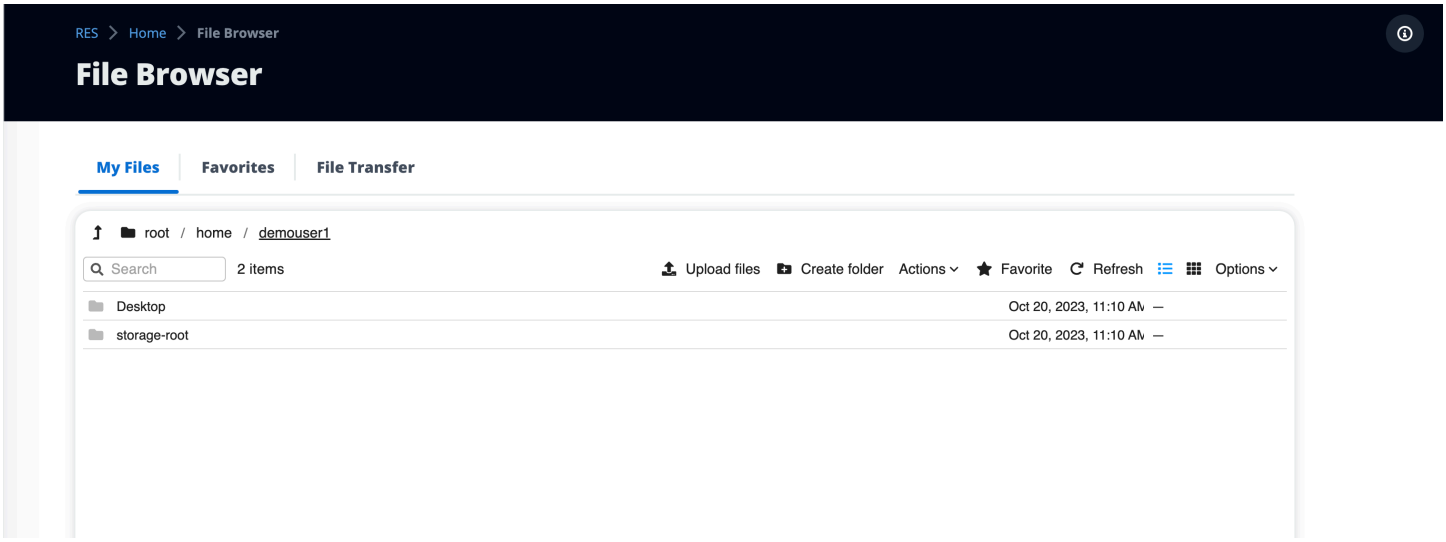
Pour plus d'informations sur les autorisations, consultezthe section called “Profils d'autorisation”.

Accédez à un bureau partagé

Dans Bureaux partagés, vous pouvez afficher les bureaux partagés avec vous et vous connecter à une instance. Vous pouvez vous inscrire par navigateur Web ou par DCV. Pour vous connecter, suivez les instructions indiquées dansthe section called “Accédez à votre bureau”.

Navigateur de fichiers

Le navigateur de fichiers vous permet d'accéder aux systèmes de fichiers via le portail Web. Vous pouvez gérer tous les fichiers disponibles auxquels vous êtes autorisé à accéder sur le système de fichiers sous-jacent. Le stockage principal (Amazon EFS) est disponible pour tous les nœuds Linux. Pour les nœuds Linux et Windows, FSx for ONTAP est disponible. La mise à jour de fichiers sur votre bureau virtuel est identique à la mise à jour d'un fichier via le terminal ou un navigateur de fichiers basé sur le Web.



Téléversez un ou plusieurs fichiers

1. Choisissez Charger un fichier.
2. Déposez des fichiers ou recherchez les fichiers à télécharger.
3. Choisissez Upload (n) files.

Supprimer le (s) fichier (s)

1. Sélectionnez le ou les fichiers que vous souhaitez supprimer.
2. Choisissez Actions.
3. Choisissez Supprimer les fichiers.

Vous pouvez également cliquer avec le bouton droit sur un fichier ou un dossier et sélectionner Supprimer les fichiers.

Gérer les favoris

Pour épingler des fichiers et des dossiers importants, vous pouvez les ajouter aux favoris.

1. Sélectionnez un fichier ou un dossier.
2. Choisissez Favori.

Vous pouvez également cliquer avec le bouton droit sur un fichier ou un dossier et sélectionner Favoris.

> **Note**
>
> Les favoris sont enregistrés dans le navigateur local. Si vous changez de navigateur ou si vous videz le cache, vous devrez réépingler vos favoris.

Modifier des fichiers

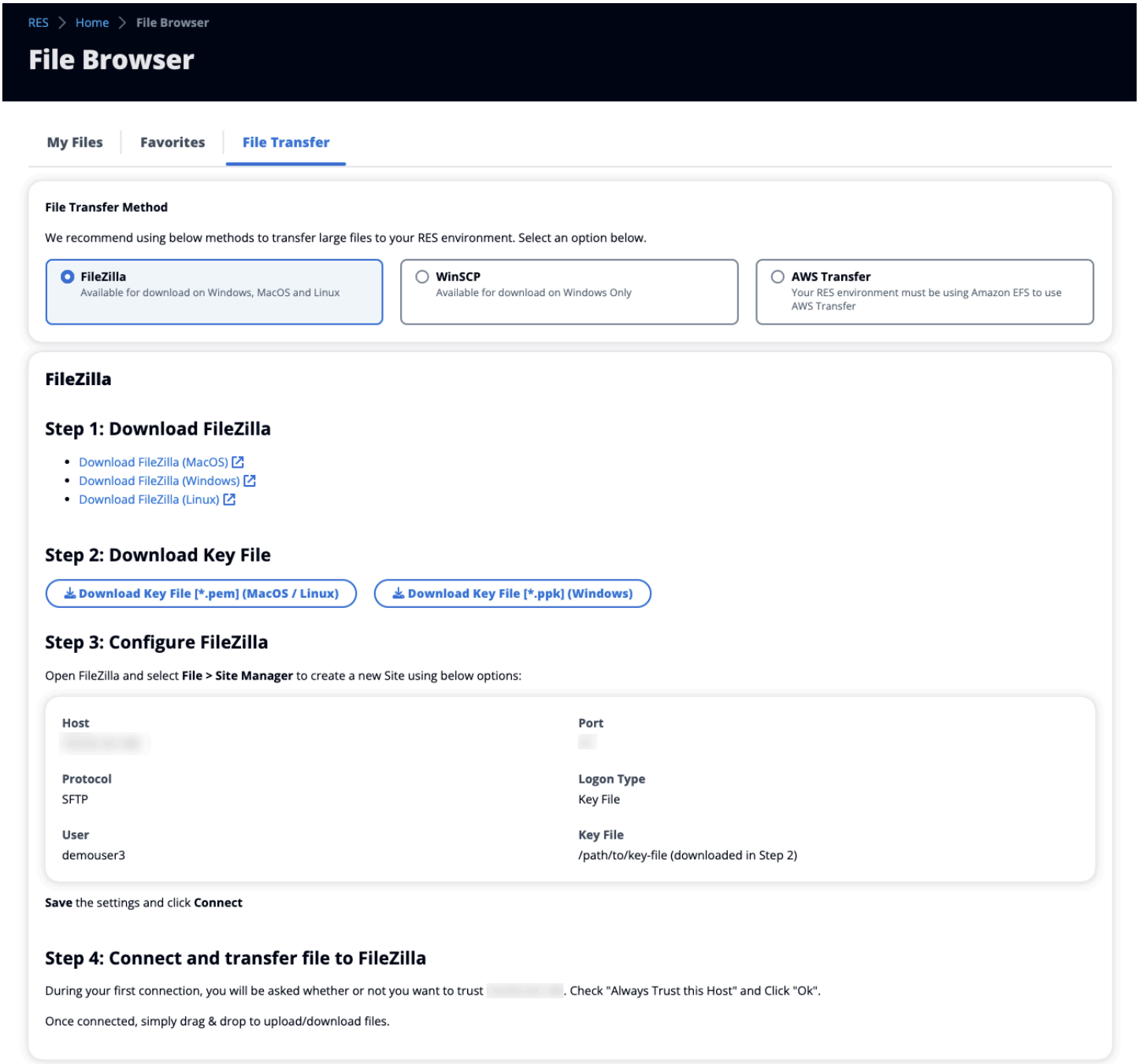
Vous pouvez modifier le contenu des fichiers texte dans le portail Web.

1. Choisissez le fichier que vous souhaitez mettre à jour. Un modal s'ouvre avec le contenu du fichier.
2. Effectuez vos mises à jour et choisissez Enregistrer.

Transférer des fichiers

Utilisez le transfert de fichiers pour utiliser des applications de transfert de fichiers externes pour transférer des fichiers. Vous pouvez sélectionner l'une des applications suivantes et suivre les instructions affichées à l'écran pour transférer des fichiers.

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



Accès SSH

Pour utiliser SSH pour accéder à l'hôte du bastion, procédez comme suit :

1. Dans le menu RES, choisissez SSH access.
2. Suivez les instructions à l'écran pour utiliser SSH ou PuTTY pour y accéder.

Résolution des problèmes

Ce document contient des informations sur la façon de surveiller le système et de résoudre les problèmes spécifiques qui peuvent survenir. Si vous ne trouvez pas de solution à un problème, vous trouverez peut-être d'autres rubriques de résolution des problèmes sur GitHub.

Rubriques

Problèmes d'installation

Rubriques

AWS CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»

Pour identifier le problème, examinez le groupe de CloudWatch journaux Amazon nommé`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. S'il existe plusieurs groupes de journaux portant le même nom, examinez le premier groupe disponible. Un message d'erreur dans les journaux fournira plus d'informations sur le problème.

> **Note**
>
> Vérifiez que les valeurs des paramètres ne comportent pas d'espaces.

Notification par e-mail non reçue après la création AWS CloudFormation réussie des piles

Si aucune invitation par e-mail n'a été reçue après la AWS CloudFormation création réussie, vérifiez les points suivants :

1. Vérifiez que le paramètre d'adresse e-mail a été correctement saisi.

   Si l'adresse e-mail est incorrecte ou n'est pas accessible, supprimez et redéployez l'environnement Research and Engineering Studio.
2. Consultez la console Amazon EC2 pour trouver des preuves de l'existence d'instances cycliques.

   S'il existe des instances Amazon EC2 dont le `<envname>` préfixe apparaît comme terminé et qu'elles sont ensuite remplacées par une nouvelle instance, il se peut qu'il y ait un problème avec le réseau ou la configuration d'Active Directory.
3. Si vous avez déployé les recettes AWS High Performance Compute pour créer vos ressources externes, vérifiez que le VPC, les sous-réseaux privés et publics et les autres paramètres sélectionnés ont été créés par la pile.

   Si l'un des paramètres est incorrect, vous devrez peut-être supprimer et redéployer l'environnement RES. Pour plus d'informations, consultez Désinstallez le produit.
4. Si vous avez déployé le produit avec vos propres ressources externes, vérifiez que le réseau et Active Directory correspondent à la configuration attendue.

   Il est essentiel de confirmer que les instances d'infrastructure ont rejoint avec succès Active Directory. Essayez les étapes ci-dessous the section called "Instances en cycle ou contrôleur VDC en état d'échec" pour résoudre le problème.

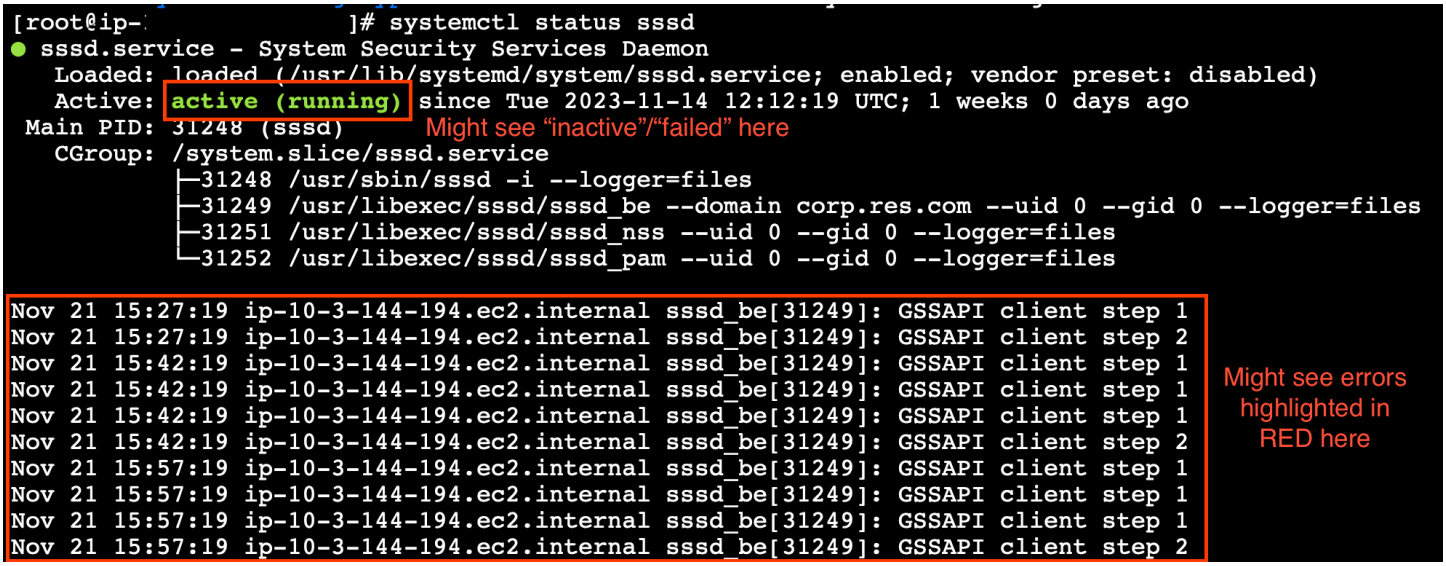
Instances en cycle ou contrôleur VDC en état d'échec

La cause la plus probable de ce problème est l'incapacité des ressources à se connecter ou à rejoindre Active Directory.

Pour vérifier le problème, procédez comme suit :

1. À partir de la ligne de commande, démarrez une session avec SSM sur l'instance en cours d'exécution du vdc-controller.
2. Exécutez `sudo su -`.
3. Exécutez `systemctl status sssd`.

Si le statut est inactif, en échec ou si des erreurs apparaissent dans les journaux, cela signifie que l'instance n'a pas pu rejoindre Active Directory.



Journal des erreurs SSM

Pour résoudre le problème, procédez comme suit :

- À partir de la même instance de ligne de commande, exécutez `cat /root/bootstrap/logs/userdata.log` pour examiner les journaux.

Le problème pourrait être l'une des trois causes profondes possibles.

Cause première 1 : informations de connexion LDAP saisies incorrectes

Passez en revue les journaux. Si le message suivant se répète plusieurs fois, cela signifie que l'instance n'a pas pu rejoindre Active Directory.

```
+ local AD_AUTHORIZATION_ENTRY=
```

```
+ [[ -z '' ]]
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))
```

1. Vérifiez que les valeurs des paramètres suivants ont été saisies correctement lors de la création de la pile RES.

   - directoryservice.ldap_connection_uri
   - directoryservice.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - directoryservice.name

2. Mettez à jour les valeurs incorrectes dans la table DynamoDB. La table se trouve dans la console DynamoDB sous Tables. Le nom de la table doit être**`[stack name].cluster-settings`**.
3. Après avoir mis à jour la table, supprimez le gestionnaire de clusters et le contrôleur vdc qui exécutent actuellement les instances de l'environnement. Auto Scaling démarrera de nouvelles instances en utilisant les dernières valeurs de la table DynamoDB.

Cause première 2 : ServiceAccount nom d'utilisateur saisi incorrect

Si les journaux sont renvoyés`Insufficient permissions to modify computer account`, le ServiceAccount nom saisi lors de la création de la pile est peut-être incorrect.

1. Depuis la AWS console, ouvrez Secrets Manager.
2. Recherchez `directoryserviceServiceAccountUsername`. Le secret devrait être**`[stack name]`**`-directoryservice-ServiceAccountUsername`.

3. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis Texte en clair.
4. Si la valeur a été mise à jour, supprimez les instances de cluster-manager et vdc-controller en cours d'exécution de l'environnement. Auto Scaling démarrera de nouvelles instances en utilisant la dernière valeur de Secrets Manager.

Cause première 3 : ServiceAccount mot de passe saisi incorrect

Si les journaux s'affichent`Invalid credentials`, le ServiceAccount mot de passe saisi lors de la création de la pile est peut-être incorrect.

1. Depuis la AWS console, ouvrez Secrets Manager.
2. Recherchez `directoryserviceServiceAccountPassword`. Le secret devrait être**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
3. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis Texte en clair.
4. Si vous avez oublié le mot de passe ou si vous n'êtes pas certain que le mot de passe saisi est correct, vous pouvez le réinitialiser dans Active Directory et Secrets Manager.
    a. Pour réinitialiser le mot de passe dans AWS Managed Microsoft AD :
        i. Ouvrez la AWS console et accédez à AWS Directory Service.
        ii. Sélectionnez l'ID de répertoire pour votre répertoire RES, puis choisissez Actions.
        iii. Choisissez Réinitialiser le mot de passe utilisateur.
        iv. Entrez le ServiceAccount nom d'utilisateur.
        v. Entrez un nouveau mot de passe, puis choisissez Réinitialiser le mot de passe.
    b. Pour réinitialiser le mot de passe dans Secrets Manager, procédez comme suit :
        i. Ouvrez la AWS console et accédez à Secrets Manager.
        ii. Recherchez `directoryserviceServiceAccountPassword`. Le secret devrait être**`[stack name]`**`-directoryservice-ServiceAccountPassword`.
        iii. Ouvrez le secret pour afficher la page de détails. Sous Valeur secrète, choisissez Récupérer la valeur secrète, puis Texte en clair.
        iv. Choisissez Modifier.

v. Définissez un nouveau mot de passe pour l' ServiceAccount utilisateur et choisissez Enregistrer.

5. Si la valeur a été mise à jour, supprimez les instances de cluster-manager et vdc-controller en cours d'exécution de l'environnement. La mise à l'échelle automatique démarrera les nouvelles instances en utilisant la dernière valeur.

La CloudFormation pile d'environnements ne parvient pas à être supprimée en raison d'une erreur d'objet dépendant

Si la suppression de la **`[env-name]`**`-vdc` CloudFormation pile échoue en raison d'une erreur d'objet dépendant telle que la`vdcdcvhostsecuritygroup`, cela peut être dû à une instance Amazon EC2 lancée dans un sous-réseau ou un groupe de sécurité créé par RES à l'aide de la console. AWS

Pour résoudre le problème, recherchez et mettez fin à toutes les instances Amazon EC2 lancées de cette manière. Vous pouvez ensuite reprendre la suppression de l'environnement.

Erreur rencontrée pour le paramètre de bloc CIDR lors de la création de l'environnement

Lors de la création d'un environnement, une erreur apparaît pour le paramètre de bloc CIDR avec un statut de réponse de [FAILED].

Exemple d'erreur :

```
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.
```

Pour résoudre le problème, le format attendu est x.x.x.0/24 ou x.x.x.0/32.

CloudFormation échec de création de pile lors de la création de l'environnement

La création d'un environnement implique une série d'opérations de création de ressources. Dans certaines régions, un problème de capacité peut survenir et entraîner l'échec de la création d'une CloudFormation pile.

Dans ce cas, supprimez l'environnement et réessayez de le créer. Vous pouvez également réessayer la création dans une autre région.

La création d'une pile de ressources externes (démo) échoue avec AdDomainAdminNode CREATE_FAILED

Si la création de la pile d'environnement de démonstration échoue avec l'erreur suivante, cela peut être dû au fait que l'application de correctifs Amazon EC2 s'est produite de manière inattendue lors du provisionnement après le lancement de l'instance.

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

Pour déterminer la cause de l'échec, procédez comme suit :

1. Dans le gestionnaire d'état SSM, vérifiez si les correctifs sont configurés et s'ils sont configurés pour toutes les instances.
2. Dans l'historique d'exécution de RunCommand SSM/Automation, vérifiez si l'exécution d'un document SSM lié à l'application de correctifs coïncide avec le lancement d'une instance.
3. Dans les fichiers journaux des instances Amazon EC2 de l'environnement, consultez la journalisation des instances locales pour déterminer si l'instance a redémarré pendant le provisionnement.

Si le problème est dû à l'application de correctifs, retardez l'application des correctifs pour les instances RES au moins 15 minutes après le lancement.

Problèmes liés à la gestion des identités

La plupart des problèmes liés à l'authentification unique (SSO) et à la gestion des identités sont dus à une mauvaise configuration. Pour plus d'informations sur la configuration de votre configuration SSO, voir :

- the section called “Configuration du SSO avec IAM Identity Center”
- the section called “Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)”

Pour résoudre d'autres problèmes liés à la gestion des identités, consultez les rubriques de résolution des problèmes suivantes :

Rubriques

Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion

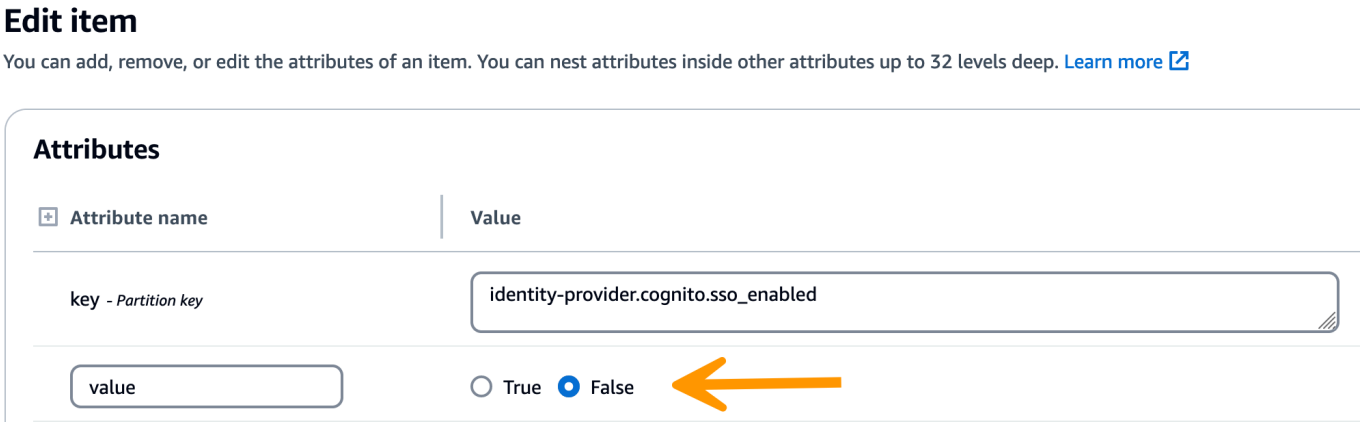
Ce problème se produit lorsque votre intégration SSO est mal configurée. Pour déterminer le problème, consultez les journaux de l'instance du contrôleur et vérifiez que les paramètres de configuration ne contiennent pas d'erreurs.

Pour consulter les journaux, procédez comme suit :

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans Groupes de journaux, recherchez le groupe nommé/*<environment-name>*/cluster-manager.
3. Ouvrez le groupe de journaux pour rechercher d'éventuelles erreurs dans les flux de journaux.

Pour vérifier les paramètres de configuration, procédez comme suit :

1. Ouvrez la console DynamoDB à l'adresse https://console.aws.amazon.com/dynamodb/.
2. Dans Tables, recherchez la table nommée*<environment-name>*.cluster-settings.
3. Ouvrez le tableau et choisissez Explorer les éléments du tableau.
4. Développez la section des filtres et entrez les variables suivantes :
   - Nom de l'attribut — clé
   - État — contient
   - Valeur — SSO
5. Cliquez sur Exécuter.
6. Dans la chaîne renvoyée, vérifiez que les valeurs de configuration SSO sont correctes. S'ils sont incorrects, remplacez la valeur de la clé sso_enabled par False.



7. Retournez à l'interface utilisateur RES pour reconfigurer le SSO.

Erreur « Utilisateur introuvable » lors de la tentative de connexion

Si vous recevez le message d'erreur « Utilisateur introuvable » lorsque vous vous connectez à l'interface RES, cela signifie que l'utilisateur est présent dans Active Directory, mais pas dans RES. Si vous avez récemment ajouté l'utilisateur à AD, il est possible qu'il ne soit pas synchronisé avec RES. RES se synchronise toutes les heures, vous devrez donc peut-être attendre et vérifier que l'utilisateur a été ajouté après la prochaine synchronisation. Pour synchroniser immédiatement, suivez les étapes décrites dansthe section called “Utilisateur ajouté dans Active Directory, mais absent de RES”.

Si l'utilisateur est présent dans RES :

1. Assurez-vous que le mappage des attributs est correctement configuré. Pour de plus amples informations, veuillez consulter the section called “Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)”.
2. Assurez-vous que l'objet et l'e-mail SAML correspondent tous deux à l'adresse e-mail de l'utilisateur.

Utilisateur ajouté dans Active Directory, mais absent de RES

Si vous avez ajouté un utilisateur à Active Directory mais qu'il est absent de RES, la synchronisation AD doit être déclenchée. La synchronisation AD est effectuée toutes les heures par une fonction Lambda pour importer des entrées AD dans l'environnement RES. Parfois, il y a un délai avant l'exécution du prochain processus de synchronisation après l'ajout de nouveaux utilisateurs ou groupes. Vous pouvez lancer la synchronisation manuellement depuis le service Amazon Simple Queue.

Lancez le processus de synchronisation manuellement :

1. Ouvrez la console Amazon SQS à l'adresse https://console.aws.amazon.com/sqs/.
2. Dans Files d'attente, sélectionnez`<environment-name>-cluster-manager-tasks.fifo`.
3. Choisissez Envoyer et recevoir des messages.
4. Dans le champ Corps du message, entrez :

   `{ "name": "adsync.sync-from-ad", "payload": {} }`
5. Pour l'ID du groupe de messages, entrez : **`adsync.sync-from-ad`**
6. Pour l'ID de déduplication des messages, entrez une chaîne alphanumérique aléatoire. Cette entrée doit être différente de tous les appels effectués dans les cinq minutes, sinon la demande sera ignorée.

Utilisateur non disponible lors de la création d'une session

Si vous êtes un administrateur qui crée une session, mais que vous constatez qu'un utilisateur figurant dans Active Directory n'est pas disponible lors de la création d'une session, il se peut que l'utilisateur doive se connecter pour la première fois. Les sessions ne peuvent être créées que pour les utilisateurs actifs. Les utilisateurs actifs doivent se connecter à l'environnement au moins une fois.

Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters

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

Si vous recevez cette erreur dans le journal du CloudWatch gestionnaire de clusters, la recherche LDAP a peut-être renvoyé trop d'enregistrements utilisateur. Pour résoudre ce problème, augmentez la limite de résultats de recherche LDAP de votre fournisseur de services Internet.

Avis

Chaque instance Amazon EC2 est fournie avec deux licences Remote Desktop Services (Terminal Services) à des fins d'administration. Ces informations sont disponibles pour vous aider à fournir ces licences à vos administrateurs. Vous pouvez également utiliser AWS Systems Manager Session Manager, qui permet d'accéder à distance à des instances Amazon EC2 sans RDP et sans avoir besoin de licences RDP. Si des licences Remote Desktop Services supplémentaires sont nécessaires, les CAL utilisateur de Remote Desktop doivent être achetées auprès de Microsoft ou d'un revendeur de licences Microsoft. Les utilisateurs de Remote Desktop (CAL) dotés d'une assurance logicielle active bénéficient des avantages liés à la mobilité des licences et peuvent être transférés vers des environnements locataires (partagés) AWS par défaut. Pour plus d'informations sur l'acquisition de licences sans les avantages liés à l'assurance logicielle ou à la mobilité des licences, consultez cette section de la FAQ.

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques AWS actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. AWS les responsabilités et les obligations envers ses clients sont régies par des AWS accords, et ce document ne fait partie ni ne modifie aucun accord entre AWS et ses clients.

Research and Engineering Studio on AWS est licencié selon les termes de la licence Apache version 2.0 disponible auprès de l'Apache Software Foundation.

Révisions

Pour plus d'informations, consultez le fichier ChangeLog.md dans le référentiel. GitHub

Date	Modification
Novembre 2023	Première version
Décembre 2023	GovCloud instructions et modèles ajoutés
Janvier 2024	Version de sortie 2024.01
Février 2024	Version de publication 2024.01.01 — modèle de déploiement mis à jour
Mars 2024	Rubriques de résolution des problèmes supplémentaires, conservation CloudWatch des journaux, désinstallation des versions mineures
Avril 2024	Version de publication 2024.04 — AMI compatibles RES et modèles de lancement de projet

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.