



Guide de l'utilisateur

Studio de recherche et d'ingénierie



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

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Présentation	1
Fonctionnalités et avantages	2
Concepts et définitions	3
Présentation de l'architecture	5
Diagramme d'architecture	5
AWS services inclus dans ce produit	6
Environnement de démonstration	10
Créez une pile de démonstration en un clic	10
Prérequis	10
Création de ressources et de paramètres d'entrée	11
Étapes après le déploiement	13
Planifiez votre déploiement	14
Coût	14
Sécurité	14
Rôles IAM	14
Groupes de sécurité	15
Chiffrement des données	15
Quotas	15
Quotas pour AWS les services inclus dans ce produit	15
AWS CloudFormation quotas	16
Planification de la résilience	16
Soutenu Régions AWS	16
Déployez le produit	19
Prérequis	19
Créez un Compte AWS avec un utilisateur administratif	20
Création d'une paire de clés Amazon EC2 SSH	20
Augmenter les quotas de service	20
Création d'un domaine public (facultatif)	21
Créer un domaine (GovCloud uniquement)	21
Fournir des ressources externes	22
Configurer LDAPS dans votre environnement (facultatif)	23
Configuration d'un VPC privé (facultatif)	24
Création de ressources externes	36
Étape 1 : Lancez le produit	42

Étape 2 : Connectez-vous pour la première fois	51
Mettre à jour le produit	53
Mises à jour majeures des versions	53
Mises à jour mineures des versions	53
Désinstallez le produit	55
À l'aide du AWS Management Console	55
En utilisant AWS Command Line Interface	55
Suppression du shared-storage-security-group	55
Suppression des compartiments Amazon S3	56
Guide de configuration	57
Gestion des utilisateurs et des groupes	57
Configuration du SSO avec IAM Identity Center	57
Configuration de votre fournisseur d'identité pour l'authentification unique (SSO)	61
Définition de mots de passe pour les utilisateurs	72
Création de sous-domaines	72
Création d'un certificat ACM	73
Amazon CloudWatch Logs	74
Définition de limites d'autorisation personnalisées	75
Configurez Res Ready AMIs	80
Préparer le rôle IAM pour accéder à l'environnement RES	80
Créer un composant EC2 Image Builder	82
Préparez votre recette EC2 Image Builder	86
Configuration de l'infrastructure EC2 Image Builder	88
Configurer le pipeline d'images Image Builder	89
Exécuter le pipeline d'images Image Builder	90
Enregistrez une nouvelle pile logicielle dans RES	90
Guide de l'administrateur	91
Gestion de session	91
Tableau de bord	92
Séances	93
Piles de logiciels () AMIs	96
Débogage	100
Paramètres du bureau	101
Gestion de l'environnement	102
Projets	103
Users	109

Groups	110
Profils d'autorisation	111
Systèmes de fichiers	120
État de l'environnement	124
Gestion des instantanés	125
Réglages d'environnement	132
Compartiments Amazon S3	133
Gestion des secrets	147
Surveillance et contrôle des coûts	150
Utiliser le produit	156
Bureaux virtuels	156
Systèmes d'exploitation pris en charge	157
Lancer un nouvel ordinateur de bureau	157
Accédez à votre bureau	157
Contrôlez l'état de votre bureau	159
Modifier un bureau virtuel	160
Récupérer les informations de session	161
Planifier des bureaux virtuels	161
Bureaux partagés	163
Partage d'un ordinateur	163
Accédez à un bureau partagé	164
Navigateur de fichiers	164
Téléversez un ou plusieurs fichiers	165
Supprimer le (s) fichier (s)	165
Gérer les favoris	165
Modifier des fichiers	166
Transférer des fichiers	166
Accès SSH	167
Résolution des problèmes	168
Débogage et surveillance généraux	171
Sources d'informations utiles sur les journaux et les événements	172
Apparence typique de EC2 la console Amazon	176
Débogage de Windows DCV	178
Trouvez des informations sur la version DCV de NICE	179
Problème RunBooks	179
Problèmes d'installation	181

Problèmes de gestion des identités	188
Stockage	193
Instantanés	198
Infrastructure	199
Lancement de bureaux virtuels	200
Composant de bureau virtuel	205
Suppression d'environnements	212
Environnement de démonstration	219
Problèmes connus	220
Problèmes connus 2024.x	221
Avis	237
Révisions	238
.....	ccxl

Présentation

Important

Cette version du guide de l'utilisateur couvre la version 2024.08 de Research and Engineering Studio sur AWS. Pour la version actuelle, consultez le [guide de l' AWS utilisateur du studio de recherche et d'ingénierie](#).

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 (AMIs) 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 ordinateurs de bureau Linux et Amazon FSx for NetApp 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 du projet (souvent appelées ensembles de données). Il fournit une solution de stockage dans les limites d'un projet et améliore la collaboration et le contrôle d'accès aux données.

Administrateur global

Délégué administratif ayant accès aux ressources RES partagées dans un environnement RES. Le champ d'application et les autorisations s'étendent sur plusieurs projets. Ils peuvent créer ou modifier des projets et désigner des propriétaires de projets. Ils peuvent déléguer ou attribuer des autorisations aux propriétaires de projets et aux membres du projet. Parfois, la même personne agit en tant qu'administrateur RES en fonction de la taille de l'organisation.

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 VDI s'il n'a pas obtenu d'adhésion.

Membre du projet

Utilisateur final des ressources RES (VDI, stockage, etc.) La portée et les autorisations sont limitées aux projets auxquels elles sont attribuées. Ils ne peuvent ni déléguer ni attribuer d'autorisations.

Propriétaire du projet

Délégué administratif ayant accès à un projet spécifique et en étant le propriétaire. La portée et les autorisations sont limitées au (x) projet (s) dont ils sont propriétaires. Ils peuvent attribuer des autorisations aux membres du projet dans les projets dont ils sont propriétaires.

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 votre Compte AWS.

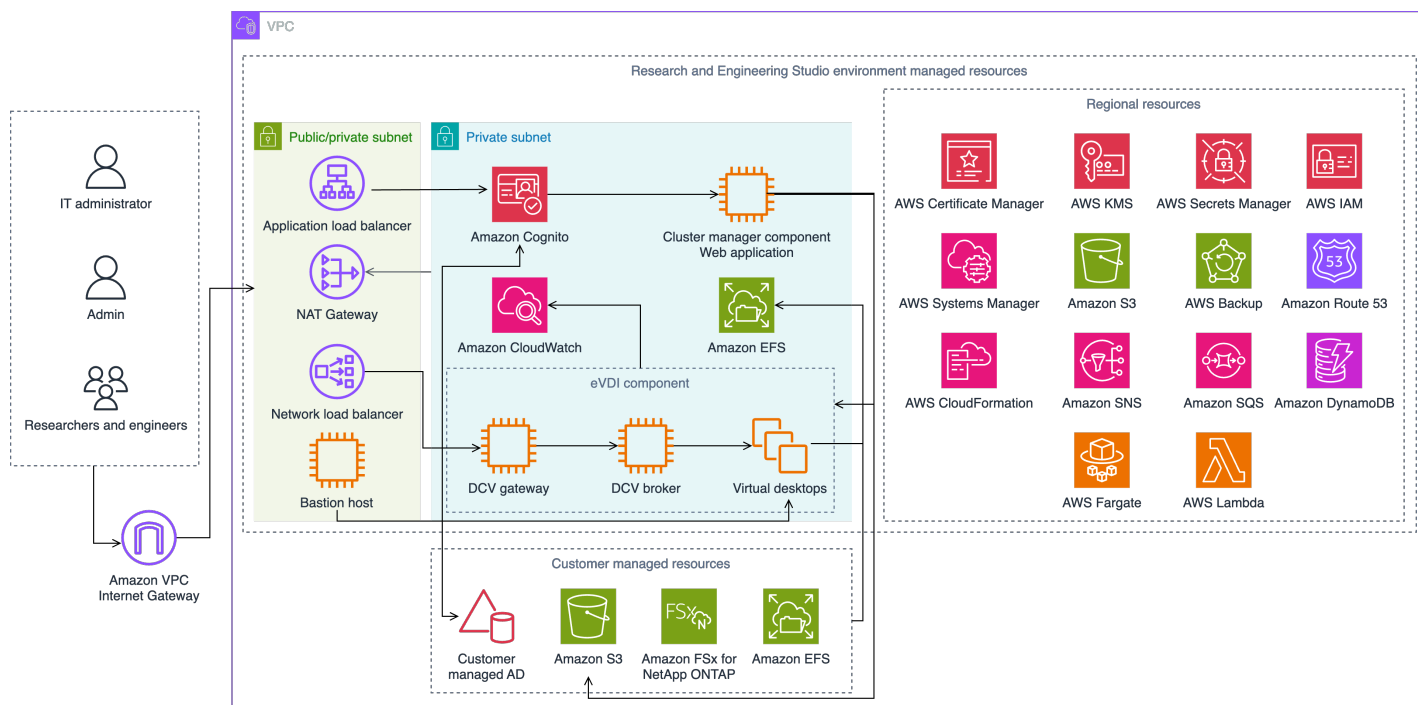


Figure 1 : Studio de recherche et d'ingénierie sur AWS l'architecture

Note

AWS CloudFormation les 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.

AWS services inclus dans ce produit

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

AWS service	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 configuration 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.

AWS service	Description
AWS Lambda	Noyau. Prend en charge les fonctionnalités du produit telles que la mise à jour des paramètres 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 statistiques et des journaux d'activité pour tous les EC2 hôtes Amazon et les fonctions Lambda.
Amazon Simple Storage Service	Soutenir. Stocke les fichiers binaires des applications pour le démarrage et la configuration 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 du compte de service dans Active Directory et les certificats auto-signés pour VDI.
AWS CloudFormation	Soutenir. Fournit un mécanisme de déploiement 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 d'attente de tâches pour prendre en charge les exécutions asynchrones.

AWS service	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 FSx de fichiers Amazon	Facultatif. Fournit un système de fichiers partagé externe.
Amazon FSx pour NetApp ONTAP	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 EC2 hôtes Amazon, les systèmes de fichiers et DynamoDB.

Création d'un environnement de démonstration

Suivez les étapes décrites dans cette section pour essayer Research and Engineering Studio sur AWS. Cette démonstration déploie un environnement hors production avec un ensemble minimal de paramètres à l'aide du modèle de [pile d'environnement de AWS démonstration du studio de recherche et d'ingénierie](#). Il utilise un serveur Keycloak pour le SSO.

Notez qu'après avoir déployé la pile, vous devez suivre les étapes [Étapes après le déploiement](#) ci-dessous pour configurer les utilisateurs dans l'environnement avant de vous connecter.

Créez une pile de démonstration en un clic

Cette AWS CloudFormation pile crée tous les composants requis par le studio de recherche et d'ingénierie.

Temps de déploiement : ~90 minutes

Prérequis

Rubriques

- [Créez un Compte AWS avec un utilisateur administratif](#)
- [Création d'une paire de clés Amazon EC2 SSH](#)
- [Augmenter les quotas de service](#)

Créez un Compte AWS avec un utilisateur administratif

Vous devez avoir Compte AWS un utilisateur administratif :

1. Ouvrez l'<https://portal.aws.amazon.com/billing/inscription>.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 AWS est créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un

utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

Création d'une paire de clés Amazon EC2 SSH

Si vous ne possédez pas de paire de clés Amazon EC2 SSH, vous devrez en créer une. Pour plus d'informations, consultez la section [Créer une paire de clés à l'aide d'Amazon EC2](#) dans le guide de EC2 l'utilisateur Amazon.

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](#)
 - Augmentez le EC2 -VPC Elastic IPs 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 de plus amples informations, veuillez consulter [the section called “Quotas pour AWS les services inclus dans ce produit”](#).

Création de ressources et de paramètres d'entrée

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.
3. Sous Paramètres, passez en revue les paramètres de ce modèle de produit et modifiez-les si nécessaire.

Paramètre	Par défaut	Description
EnvironmentName	<i><res-demo></i>	Nom unique attribué à votre environnement RES, commençant par res- et ne dépassant pas 11 caractères.
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.
KeyPair		La paire de clés utilisée pour se connecter aux hôtes de l'infrastructure.
ClientIPCIDR	<0.0.0.0/0>	Filtre d'adresse IP qui limite la connexion au système. Vous pouvez le mettre à jour ClientIPCIDR après le déploiement.
InboundPrefixList		(Facultatif) Fournissez une liste de préfixes gérés pour IP autoriser l'accès direct à l'interface utilisateur Web et au protocole SSH sur l'hôte Bastion.

Étapes après le déploiement

1. Réinitialisez les mots de passe des utilisateurs AWS Directory Service — La pile de démonstration crée quatre utilisateurs avec des noms d'utilisateur que vous pouvez utiliser : `admin1user1`, `admin2`, `etuser2`.
 - a. Accédez à la console Directory Service.
 - b. Sélectionnez l'ID de répertoire pour votre environnement. Vous pouvez obtenir l'identifiant du répertoire à partir de la sortie de `<StackName>*DirectoryService*` stack.
 - c. Dans le menu déroulant Action en haut à droite, sélectionnez Réinitialiser le mot de passe utilisateur.
 - d. Pour tous les utilisateurs que vous souhaitez utiliser, saisissez le nom d'utilisateur et le mot de passe que vous souhaitez avoir, puis sélectionnez Réinitialiser le mot de passe.
2. Une fois que vous avez réinitialisé les mots de passe des utilisateurs, vous devez attendre que Research and Engineering Studio synchronise les utilisateurs dans l'environnement. Le studio de recherche et d'ingénierie synchronise les utilisateurs toutes les heures à xx.00. Vous pouvez soit attendre que cela se produise, soit suivre les étapes répertoriées [Utilisateur ajouté dans Active Directory, mais absent de RES](#) pour synchroniser immédiatement les utilisateurs.

Votre déploiement est maintenant prêt. Utilisez celle EnvironmentUrl que vous avez reçue dans votre e-mail pour accéder à l'interface utilisateur, ou vous pouvez également obtenir la même URL à partir de la sortie de la pile déployée. Vous pouvez désormais vous connecter à l'environnement du studio de recherche et d'ingénierie avec l'utilisateur et le mot de passe pour lesquels vous avez réinitialisé le mot de passe dans Active Directory.

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 de plus amples informations, veuillez consulter [AWS services 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 Explorer](#) pour 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 EC2 instances Amazon 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 EC2 instances, 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 client restantes 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.

Quotas

Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre 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 plus d'informations, consultez [Quotas de service 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' EC2instances Amazon 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 bénéficier 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 EC2 console Amazon à <https://console.aws.amazon.com/ec2/> l'adresse. Le produit en crée quatre ASGs par défaut, chaque nom se terminant par -asg. 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 ASGs, consultez la section [Scale the size of your Auto Scaling group](#) dans le manuel Amazon EC2 Auto Scaling User Guide.

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 AWS est soutenu dans les domaines suivants Régions AWS :

Nom de la région	Région	Versions 2024.06 et antérieures	Version 2024.08
USA Est (Virginie du Nord)	us-east-1	oui	oui
USA Est (Ohio)	us-east-2	oui	oui
USA Ouest (Californie du Nord)	us-west-1	oui	oui
USA Ouest (Oregon)	us-west-2	oui	oui
Asie-Pacifique (Tokyo)	ap-northeast-1	oui	oui
Asie-Pacifique (Séoul)	ap-northeast-2	oui	oui
Asie-Pacifique (Mumbai)	ap-south-1	oui	oui
Asie-Pacifique (Singapour)	ap-southeast-1	oui	oui
Asie-Pacifique (Sydney)	ap-southeast-2	oui	oui
Canada (Centre)	ca-central-1	oui	oui
Europe (Francfort)	eu-central-1	oui	oui
Europe (Milan)	eu-south-1	oui	oui
Europe (Irlande)	eu-west-1	oui	oui
Europe (Londres)	eu-west-2	oui	oui
Europe (Paris)	eu-west-3	oui	oui
Europe (Stockholm)	eu-north-1	non	oui

Nom de la région	Région	Versions 2024.06 et antérieures	Version 2024.08
Israël (Tel Aviv)	il-central-1	oui	oui
AWS GovCloud (US-Ouest)	us-gov-west-1	oui	non

Déployez le produit

Note

Ce produit utilise des [AWS CloudFormation modèles et des piles](#) pour automatiser son déploiement. Les CloudFormation modèles décrivent les AWS ressources incluses dans ce produit et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans 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](#)
- [Création de ressources externes](#)
- [Étape 1 : Lancez le produit](#)
- [Étape 2 : Connectez-vous pour la première fois](#)

Prérequis

Rubriques

- [Créez un Compte AWS avec un utilisateur administratif](#)
- [Création d'une paire de clés Amazon EC2 SSH](#)
- [Augmenter les quotas de service](#)
- [Création d'un domaine public \(facultatif\)](#)
- [Créer un domaine \(GovCloud uniquement\)](#)
- [Fournir des ressources externes](#)
- [Configurer LDAPS dans votre environnement \(facultatif\)](#)
- [Configuration d'un VPC privé \(facultatif\)](#)

Créez un Compte AWS avec un utilisateur administratif

Vous devez avoir Compte AWS un utilisateur administratif :

1. Ouvrez l'<https://portal.aws.amazon.com/billing/inscription>.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 AWS est créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

Création d'une paire de clés Amazon EC2 SSH

Si vous ne possédez pas de paire de clés Amazon EC2 SSH, vous devrez en créer une. Pour plus d'informations, consultez la section [Créer une paire de clés à l'aide d'Amazon EC2](#) dans le guide de EC2 l'utilisateur Amazon.

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](#)
 - Augmentez le EC2 -VPC Elastic IPs 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 de plus amples informations, veuillez consulter [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, puis 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 effectuez un déploiement 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 etPrivateKeySecretARN.

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

Research and Engineering Studio s' AWS attend à ce que les ressources externes suivantes existent lors de son déploiement.

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

C'est ici que vous exécuterez les EC2 instances utilisées pour héberger l'environnement RES, 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 dans l'environnement RES.

- Un secret contenant le mot de passe du compte de service

Research and Engineering Studio accède aux [secrets](#) que vous fournissez, y compris le mot de passe du compte de service, en utilisant [AWS Secrets Manager](#).

 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 les ressources externes. Consultez la section suivante pour déployer des ressources dans votre compte. [Création de ressources externes](#)

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 en tant que `DomainTLSCertificateSecretARN` paramètre dans [the 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 l'accès à Internet pour installer les dépendances. Pour installer RES dans un VPC privé, vous devez satisfaire aux conditions préalables suivantes :

Rubriques

- [Préparer Amazon Machine Images \(AMIs\)](#)
- [Configuration des points de terminaison VPC](#)
- [Connectez-vous aux services sans points de terminaison VPC](#)
- [Définir les paramètres de déploiement d'un VPC privé](#)

Préparer Amazon Machine Images (AMIs)

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 et choisissez Suivant.
 - d. Dans Ajouter des autorisations, sélectionnez les politiques d'autorisation suivantes, puis cliquez sur Suivant :
 - Amazon S3 ReadOnlyAccess
 - Amazon SSMManaged InstanceCore
 - EC2InstanceProfileForImageBuilder
 - e. Ajoutez un nom et une description du rôle, puis choisissez Créer un rôle.

3. Créez le composant du générateur d' EC2 images :

- a. Ouvrez la console EC2 Image Builder à l'adresse <https://console.aws.amazon.com/imagebuilder>.
- 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 : <i><research-and-engineering-studio-infrastructure></i>
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. Chargez 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 }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
            {{ AWSRegion }}.elb.amazonaws.com,s3.
            {{ AWSRegion }}.amazonaws.com,s3.dualstack.
            {{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
            {{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
            {{ AWSRegion }}.amazonaws.com,ssmmessages.
            {{ AWSRegion }}.amazonaws.com,kms.
            {{ AWSRegion }}.amazonaws.com,secretsmanager.
            {{ AWSRegion }}.amazonaws.com,sqs.
            {{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
            {{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
            {{ AWSRegion }}.amazonaws.com,logs.
            {{ AWSRegion }}.api.aws,elasticfilesystem.
            {{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
            {{ AWSRegion }}.amazonaws.com,api.ecr.
            {{ AWSRegion }}.amazonaws.com,.dkr.ecr.
            {{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
            kinesis.{{ AWSRegion }}.amazonaws.com,.control-
            kinesis.{{ AWSRegion }}.amazonaws.com,events.

```

```

{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com
" > /etc/environment

```

- e. 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-x86.
	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.

Section	Paramètre	Entrée utilisateur
Configuration de l'instance	–	Conservez tout dans les paramètres par défaut et assurez-vous que l'option Supprimer l'agent SSM après l'exécution du pipeline n'est pas sélectionnée.
Répertoire de travail	Chemin du répertoire de travail	/root/bootstrap/ressources_dépendances
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 • Vous êtes propriétaire : EC2 composant Amazon créé précédemment. Entrez votre Compte AWS identifiant et votre actuelle Région AWS dans les champs.
	Composants de test	Recherchez et sélectionnez : • 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.

Section	Paramètre	Entrée utilisateur
	VPC, sous-réseau et groupes de sécurité	Sélectionnez une option qui autorise l'accès à Internet et au compartiment Amazon S3. Si vous devez créer un groupe de sécurité, vous pouvez en créer un depuis la EC2 console Amazon avec les entrées suivantes : • VPC : sélectionnez le même VPC que celui utilisé pour la configuration de l'infrastructure. 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 dans [the 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 les points de terminaison n'ont pas encore été configurés, 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 Autoscaling	com.amazonaws. <i>region</i> .mise à l'échelle automatique de l'application
AWS CloudFormation	com.amazonaws. <i>region</i> .formation sur le cloud
Amazon CloudWatch	com.amazonaws. <i>region</i> .surveillance
Amazon CloudWatch Logs	com.amazonaws. <i>region</i> .journaux
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb (nécessite un point de terminaison de passerelle)
Amazon EC2	com.amazonaws. <i>region</i> .ec2
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr .dkr
Amazon Elastic File System	com.amazonaws. <i>region</i> système de fichiers .elastic
Elastic Load Balancing	com.amazonaws. <i>region</i> . équilibrage de charge élastique
Amazon EventBridge	com.amazonaws. <i>region</i> .événements
Amazon FSx	com.amazonaws. <i>region</i> .fsx
AWS Key Management Service	com.amazonaws. <i>region</i> .km
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-streams
Amazon S3	com.amazonaws. <i>region</i> .s3 (Nécessite un point de terminaison de passerelle créé par défaut dans RES.)
AWS Secrets Manager	com.amazonaws. <i>region</i> .secretsmanager
Amazon SES	com.amazonaws. <i>region</i> .email-smtp (Non pris en charge dans les zones de disponibilité suivantes : use-1-

Service AWS	Nom du service
	az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 et cac1-az4.)
AWS Security Token Service	com.amazonaws. <i>region</i> .sts
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
AWS Systems Manager	com.amazonaws. <i>region</i> Messages .ec2
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> Messages .ssm

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 permettre à toutes les connexions entrantes d'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 VDI Infrastructure/.
 4. Modifiez le groupe de sécurité de l' EC2 instance 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

Dans [the section called “Étape 1 : Lancez le produit”](#), vous êtes censé 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 dans the section called “Préparer Amazon Machine Images (AMIs)” .
IsLoadBalancerInternetFacing	Réglé sur false.
LoadBalancerSubnets	Choisissez des sous-réseaux privés sans accès à Internet.
InfrastructureHostSubnets	Choisissez des sous-réseaux privés sans accès à Internet.

Paramètre	Entrée
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 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

Paramètre	Par défaut	Description
		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 sera préfixé DomainName et par le paramètre fourni. Le nom de domaine Active Directory fourni deviendra un sous-domaine.

Paramètre	Par défaut	Description
AdminPassword		Le mot de passe de l'administrateur Active Directory (nom d'utilisateurAdmin). Cet utilisateur est créé dans le répertoire actif pour la phase d'amorçage initiale et n'est plus utilisé par la suite. Important : le format de ce champ peut être (1) un mot de passe en texte brut ou (2) l'ARN d'un AWS secret formaté par key/value paire{"password": "somepassword"} . 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
ServiceAccountPassword		Mot de passe utilisé pour créer un compte de service (ReadOnlyUser). Ce compte est utilisé pour la synchronisation. Important : le format de ce champ peut être (1) un mot de passe en texte brut ou (2) l'ARN d'un AWS secret formaté par key/value paire{"password": "somepassword"} . Remarque : Le mot de passe de cet utilisateur doit répondre aux exigences de complexité du mot de passe d'Active Directory.
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.

Paramètre	Par défaut	Description
LDIFS3Chemin	<code>aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif</code>	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 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
ClientIpCidr		Adresse IP à partir de laquelle vous allez accéder au site. Par exemple, vous pouvez sélectionner votre adresse IP et l'utiliser <code>[IPADDRESS]/32</code> 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.

Paramètre	Par défaut	Description
EnvironmentName	res- <i>[environment name]</i>	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.
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.

- 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 du tout. 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	<i><res-demo></i>	Nom unique attribué à votre environnement RES, commençant par res- et ne dépassant pas 11 caractères.
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- <i>[numbers or letters only]</i>	(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 de plus amples informations, veuillez consulter Configurez Res Ready AMIs .
SSHKeyPair		La paire de clés utilisée pour se connecter aux hôtes de l'infrastructure.

Paramètre	Par défaut	Description
ClientIP	<code>x.x.x.0/24</code> ou <code>.0/32 x.x.x.x</code>	Filtre d'adresse IP qui limite la connexion au système. Vous pouvez le mettre à jour ClientIpCidr après le déploiement.
ClientPrefixList		(Facultatif) Fournissez une liste de préfixes gérés pour IPs autoriser l'accès direct à l'interface utilisateur Web et au protocole SSH sur l'hôte Bastion.
IAMPermissionLimite		(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 de plus amples informations, veuillez consulter Définition de limites d'autorisation personnalisées .
VpcId		IP du VPC où les instances seront lancées.

Paramètre	Par défaut	Description
IsLoadBalancerInternetFacing		Sélectionnez true pour déployer un équilibreur de charge connecté à Internet (nécessite des sous-réseaux publics pour l'équilibreur de charge). Pour les déploiements nécessitant un accès Internet restreint, sélectionnez false.
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.

Paramètre	Par défaut	Description
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.
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	<i>corp.res.com</i>	Domaine de l'Active Directory. Il n'est pas nécessaire qu'il corresponde au nom de domaine du portail.
ADShortNom	<i>corp</i>	Nom abrégé de l'Active Directory. Ce nom est également appelé le nom NetBIOS.
Base LDAP	<i>DC=corp,DC=res,DC=com</i>	Un chemin LDAP vers la base au sein de la hiérarchie LDAP.

Paramètre	Par défaut	Description
LDAPConnectionURI		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.
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.
ServiceAccountPasswordSecretArn		Fournissez un ARN secret contenant le mot de passe en texte brut pour le ServiceAccount.
Utilisateur Sou		Unité organisationnelle au sein d'AD pour les utilisateurs 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.

Paramètre	Par défaut	Description
SudoersGroupName	RESAdministrators	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.
Domaine : TLSCertificateSecretArn		(Facultatif) Fournissez un ARN secret de certificat TLS de domaine pour permettre la communication TLS avec AD.
EnableLdapIDMapping		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. Dans la plupart des cas, ce paramètre doit être défini sur True.

Paramètre	Par défaut	Description
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.
CustomDomainNameforWebApp		(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.

Paramètre	Par défaut	Description
ACMCertificateARNforWebApp		(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 ressources 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, consultez Guide de configuration .
CertificateSecretARNforVDI		(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.

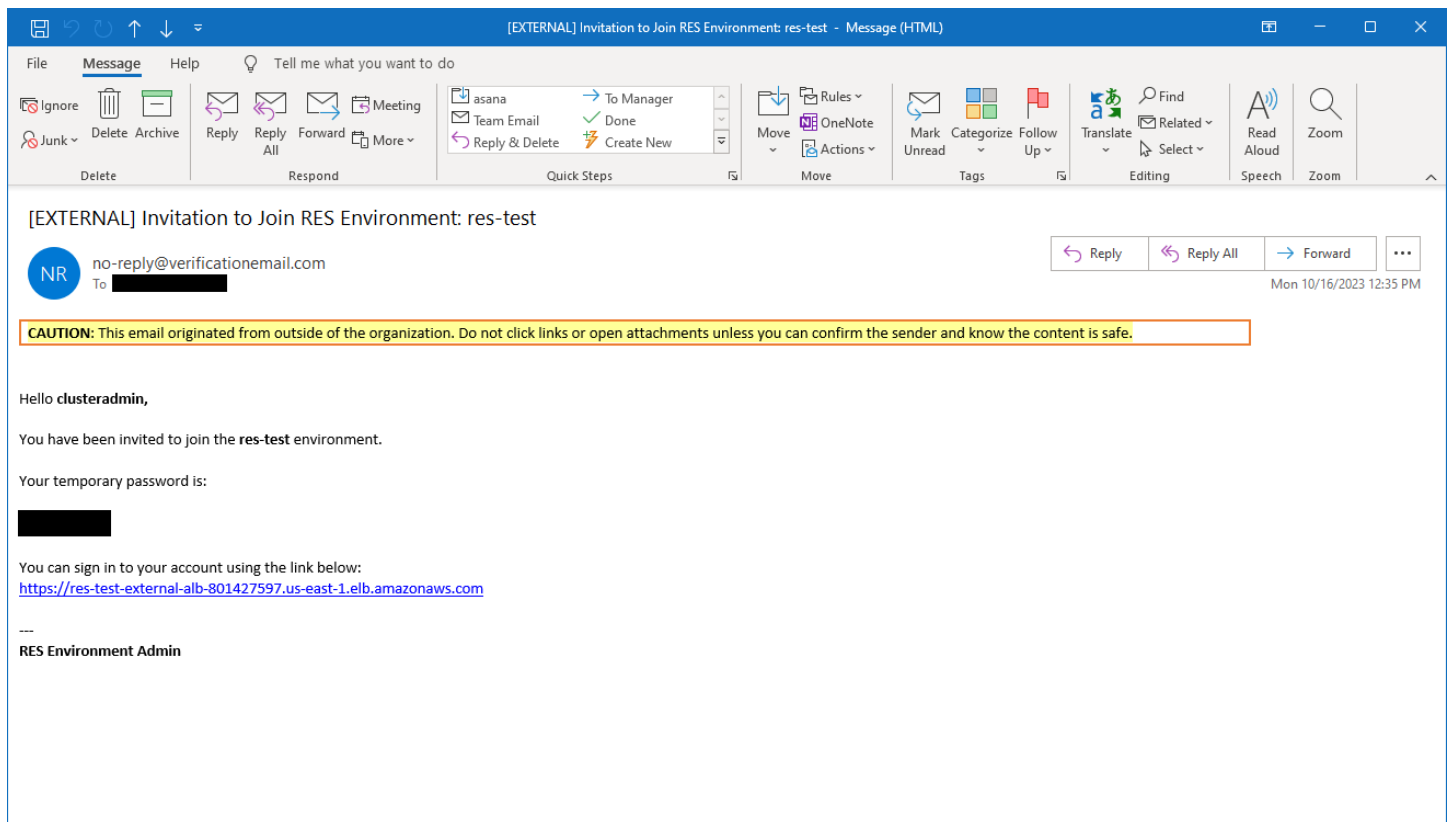
Paramètre	Par défaut	Description
PrivateKeySecretARNforVDI		(Facultatif) Ce secret ARN stocke la clé privée du certificat de votre portail Web. Si vous définissez un nom de domaine de portail pour vos ressources externes automatisées, vous pouvez trouver cette valeur sous l'onglet Outputs de la pile 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 le [Guide de configuration](#). Notez qu'il `clusteradmin` s'agit d'un compte révolutionnaire : vous pouvez l'utiliser pour créer des projets et attribuer des membres d'utilisateurs ou de groupes à ces projets ; il ne peut pas attribuer de piles logicielles ni déployer un bureau pour lui-même.

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](#)
- [Mises à jour mineures des versions](#)

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. Consultez [the section called “Créer un instantané”](#).
2. Redéployez RES avec la nouvelle version. Consultez [the section called “Étape 1 : Lancez le produit”](#).
3. Appliquez l'instantané à votre environnement mis à jour. Consultez [the section called “Appliquer un instantané”](#).
4. Vérifiez que toutes les données ont bien migré vers le nouvel environnement.

Mises à jour mineures des versions

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 en [the 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 EC2 console Amazon 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](#)
- [Création de sous-domaines](#)
- [Création d'un certificat ACM](#)
- [Amazon CloudWatch Logs](#)
- [Définition de limites d'autorisation personnalisées](#)
- [Configurez Res Ready AMIs](#)

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, consultez [Configuration de l'authentification unique \(SSO\) avec IAM Identity Center](#). Si vous avez votre propre fournisseur d'identité conforme à la norme SAML 2.0, consultez [Configuration de votre fournisseur d'identité pour l'authentification unique \(SSO\)](#).

Rubriques

- [Configuration de l'authentification unique \(SSO\) avec IAM Identity Center](#)
- [Configuration de votre fournisseur d'identité pour l'authentification unique \(SSO\)](#)
- [Définition de mots de passe pour les utilisateurs](#)

Configuration de l'authentification unique (SSO) avec IAM Identity Center

Si aucun centre d'identité n'est déjà connecté à l'Active Directory géré, commencez par [Étape 1 : configurer un centre d'identité](#). Si vous avez déjà un centre d'identité connecté à l'Active Directory géré, commencez par [Étape 2 : Se connecter 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 IAM

1. Connectez-vous à la [console AWS Identity and Access Management](#).
2. Ouvrez le Identity Center.
3. Sélectionnez Activer.
4. Sélectionnez Activer avec AWS Organizations.
5. Sélectionnez Continuer.

 Note

Assurez-vous que vous vous trouvez dans la même région que celle dans laquelle vous gérez Active Directory.

Connexion d'IAM Identity Center à un Active Directory géré

Après avoir activé IAM Identity Center, suivez les étapes de configuration recommandées ci-dessous :

1. Dans le volet de navigation, sélectionnez Paramètres.
2. Sous Source d'identité, sélectionnez Actions, puis choisissez Modifier la source d'identité.
3. Sous Répertoires existants, sélectionnez votre répertoire.
4. Sélectionnez Suivant.
5. Passez en revue vos modifications et entrez **ACCEPT** dans le champ de confirmation.
6. Sélectionnez Modifier la source d'identité.

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

Une fois les modifications [Connexion d'IAM Identity Center à un Active Directory géré](#) effectuées, une bannière de confirmation verte apparaît.

1. Dans le bandeau de confirmation, sélectionnez Démarrer la configuration guidée.
2. Dans Configurer les mappages d'attributs, sélectionnez Suivant.
3. Dans la section Utilisateur, entrez les utilisateurs que vous souhaitez synchroniser.
4. Sélectionnez Ajouter.
5. Sélectionnez Suivant.
6. Passez en revue vos modifications, puis sélectionnez 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, sélectionnez Reprendre la synchronisation.

Activation des utilisateurs

1. Dans le menu, sélectionnez Utilisateurs.
2. Choisissez le ou les utilisateurs auxquels vous souhaitez autoriser l'accès.
3. Sélectionnez Activer l'accès utilisateur.

Étape 2 : Se connecter à un centre d'identité

Configuration de l'application dans IAM Identity Center

1. Ouvrez la [console IAM Identity Center](#).
2. Sélectionnez Applications.
3. Sélectionnez Ajouter une application.
4. Dans les préférences de configuration, sélectionnez J'ai une application que je souhaite configurer.
5. Sous Type d'application, sélectionnez SAML 2.0.
6. Sélectionnez 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 lors de la configuration d'IAM Identity Center 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. Sous l'onglet Fournisseur d'identité, recherchez 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. Après avoir saisi l'URN Amazon Cognito, sélectionnez Soumettre.

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. Sélectionnez Actions, puis sélectionnez Modifier les mappages d'attributs.
3. Dans le champ Objet, entrez `${user:email}`.
4. Sous Format, sélectionnez Adresse e-mail.
5. Sélectionnez Ajouter un nouveau mappage d'attributs.
6. Sous Attribut utilisateur dans l'application, entrez « e-mail ».
7. Sous Correspond à cette valeur de chaîne ou à cet attribut utilisateur dans IAM Identity Center, entrez `${user:email}`.
8. Dans Format, saisissez « non spécifié ».
9. Sélectionnez Enregistrer les modifications.

Ajouter des utilisateurs à l'application dans IAM Identity Center

1. Dans le Identity Center, ouvrez Utilisateurs assignés pour l'application que vous avez créée et choisissez Attribuer des utilisateurs.
2. Choisissez les utilisateurs auxquels vous souhaitez attribuer l'accès à l'application.
3. Sélectionnez Attribuer des utilisateurs.

Configuration de l'IAM Identity Center dans l'environnement RES

1. Dans l'environnement du studio de recherche et d'ingénierie, sous Gestion de l'environnement, ouvrez les paramètres généraux.
2. Ouvrez l'onglet Fournisseur d'identité.
3. Sous Authentification unique, sélectionnez Modifier (à côté de Statut).
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 lors de la copie [Configuration de l'application dans IAM 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, consultez [the 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](#)
- [Configurez RES pour utiliser votre fournisseur d'identité](#)
- [Configuration de votre fournisseur d'identité dans un environnement hors production](#)
- [Débogage des problèmes liés à l'IdP SAML](#)

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 être fields/claims définie comme suit sur l'adresse e-mail de l'utilisateur :
- Sujet ou NameID SAML
 - Courrier électronique SAML

4. Votre IdP ajoute des éléments fields/claims 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— Régulé sur `urn:amazon:cognito:sp: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 — Régulé InResponseTo sur `https://user-pool-domain/saml2/idpresponse`. 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— Régulé 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 afin d'établir un lien de 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.

Cognito user pool sign-in [Info](#)
Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.
Cognito user pool sign-in options
User name
Email

User name requirements
User names are not case sensitive

Federated identity provider sign-in (1) [Info](#)  [Delete](#) [Add identity provider](#) [View signing certificate](#)
Your app users can sign-in through external social identity providers like Facebook, Google, Amazon, or Apple, and through your on-prem directories via SAML or Open ID Connect.

Identity provider	Identity provider type	Created time	Last updated time
 idc	SAML	2 weeks ago	3 hours ago

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.

- 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

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

Environment Settings

View and manage environment settings.

[View Environment Status](#)

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

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

Identity Provider

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

Single Sign-On

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

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.

Single Sign On Configuration

Identity Provider

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

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

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

Provider Name

Name used for the provider in cognito

Metadata Document Source

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

☒ Upload metadata document

☐ Enter metadata document endpoint URL

Metadata document

Provider Email Attribute

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

Refresh Token Expiration (hours)

Must be between 1 and 87600 (10 years)

Cancel

Submit

- Pour le fournisseur d'identité, choisissez SAML.
- 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 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 souhaitez 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.

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

View, add, and edit attribute mappings between SAML and your user pool.

< 1 >
⚙

User pool attribute	SAML attribute
email	email

Metadata document [Info](#)
Replace metadata

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

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

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.

▼ Scan or query items

☒ Scan

☐ Query

Select a table or index

Table - res-jan19.cluster-settings

Select attribute projection

All attributes

▼ Filters

Attribute name

Type

Condition

Value

key

String

Equal to

identity-provider

Remove

Add filter

Run

Reset

Completed. Read capacity units consumed: 13

Items returned (1)

key (String)

identity-provider.cognito.ss

email

Enter any string value.

Cancel

Save

Actions

Create item

8

< 1 >

version

1

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](#), choisissez le répertoire de la pile créée.
2. Dans le menu Actions, sélectionnez Réinitialiser le mot de passe utilisateur.
3. Choisissez l'utilisateur et entrez un nouveau mot de passe.
4. Sélectionnez 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. Ouvrez la [console Route 53](#).
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 Créer des enregistrements.
7. Pour créer un enregistrement pour le VDC, récupérez l'adresse NLB.
 - a. Ouvrez la [AWS CloudFormation console](#).

- b. Sélectionnez `<environment-name>-vdc`.
 - c. Choisissez Ressources et ouvrez `<environmentname>-vdc-external-nlb`.
 - d. Copiez le nom DNS depuis le NLB.
8. Ouvrez la [console Route 53](#).
 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 SSL/TLS certificat 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 SSL/TLS canal 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 externes [Création de ressources externes](#).

Pour créer un certificat pour des domaines personnalisés :

1. Depuis la console, ouvrez [AWS Certificate Manager](#) pour 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 en tant que paramètre pourACMCertificateARNforWebApp.

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](#) 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 paramètre IAMPermission Boundary. 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:*"
  ]
}
```

Configurez Res Ready AMIs

Avec RES Ready AMIs, vous pouvez préinstaller les dépendances RES pour les instances de bureau virtuel (VDIs) sur votre compte personnalisé. AMIs L'utilisation de RES Ready AMIs améliore les temps de démarrage des instances VDI à l'aide des images préconfigurées. À l'aide EC2 d'Image Builder, vous pouvez créer et enregistrer vos piles de logiciels AMIs en tant que nouvelles. 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](#)
- [Créer un composant EC2 Image Builder](#)
- [Préparez votre recette EC2 Image Builder](#)
- [Configuration de l'infrastructure EC2 Image Builder](#)
- [Configurer le pipeline d'images Image Builder](#)
- [Exécuter le pipeline d'images Image Builder](#)
- [Enregistrez une nouvelle pile logicielle dans RES](#)

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- EC2InstanceProfileForImageBuilder. 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 EC2 service Amazon
- Amazon SSMManaged InstanceCore et ses EC2 InstanceProfileForImageBuilder politiques
- 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": "RES DynamoDB Access",
      "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": "RESS3 Access",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-Account-ID}/idea/vdc/res-ready-install-script-packages/*"
    }
  ]
}
```

}

Créer 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_{{ RESEnvReleaseVersion }}.tar.gz'
            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 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)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Ouvrez la console EC2 Image Builder à l'adresse <https://console.aws.amazon.com/imagebuilder>.
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 EC2 instances pour Linux](#)

- [Installation et désinstallation manuelles de l'agent SSM sur les EC2 instances 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 obligatoires : AWSAccount ID, RESEnv Nom, RESEnv Région 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 obligatoires : AWSAccount ID, RESEnv Nom, RESEnv Région 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' EC2 infrastructure Amazon utilisée par Image Builder 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' EC2 instances Amazon](#).
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 qu' AMIsil soit prêt pour 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'adresse<https://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 dans[the section called "Préparez votre recette 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 dans[the 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 dans [the section called “Préparez votre recette 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 dans [the 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 de logiciels \(\) AMIs”](#) pour enregistrer une pile logicielle.
2. Pour l'ID AMI, entrez l'ID AMI de l'image de sortie intégrée [the 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](#)
- [Gestion de l'environnement](#)
- [Gestion des secrets](#)
- [Surveillance et contrôle des coûts](#)

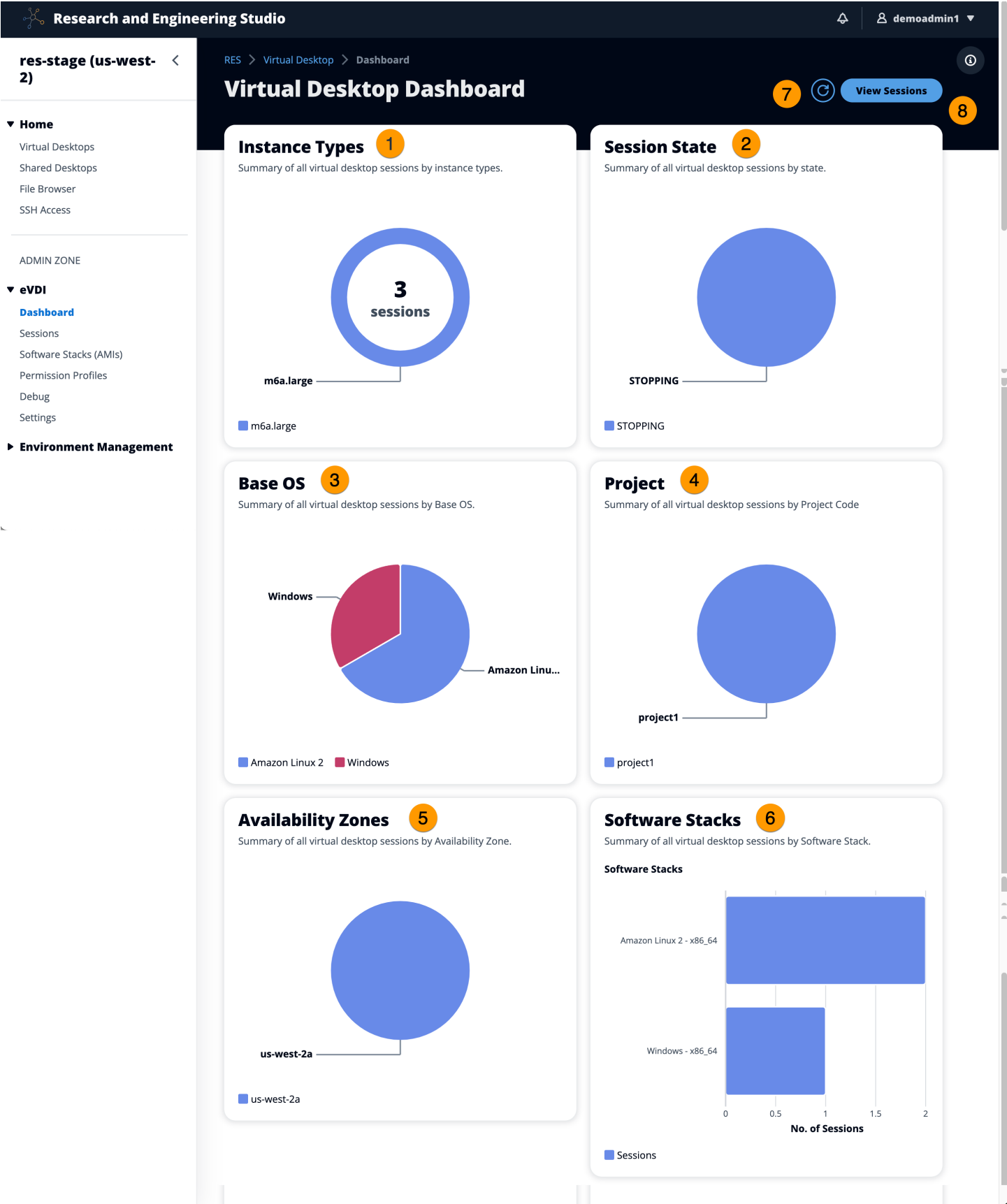
Gestion de session

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](#)
- [Séances](#)
- [Piles de logiciels \(\) AMIs](#)
- [Débogage](#)
- [Paramètres du bureau](#)

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.

RES > Virtual Desktops > Sessions

Sessions (2)

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

Created ▾ Last 1 month Actions ▾ Create Session

Search All States All Operating Systems < 1 > ⚙

	Session Name ▾	Owner ▾	Base OS	Instance Ty...	State	Project	Created On
☒	demoadmin1aml21	demoadmin1	Amazon Linux 2	m6a.large	Stopped ⓘ	project1	9/27/2023, 8:31:50 AM
☐	demoadmin1windows1	demoadmin1	Windows	m6a.large	Stopped ⓘ	project1	9/27/2023, 8:38:23 AM

< 1 >

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. Stop/Hibernate Séance (s)
 - c. Stop/Hibernate Séance (s) forcée (s)
 - d. Terminer une ou plusieurs sessions
 - e. Forcer la fermeture d'une ou de plusieurs sessions
 - f. Séance (s) Santé
 - g. Création d'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 Créer une 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

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.

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

Session: demoadmin1aml21

General Information

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

< Details Server Software Stack Project Permissions Schedule Monitoring Session >

Session Details

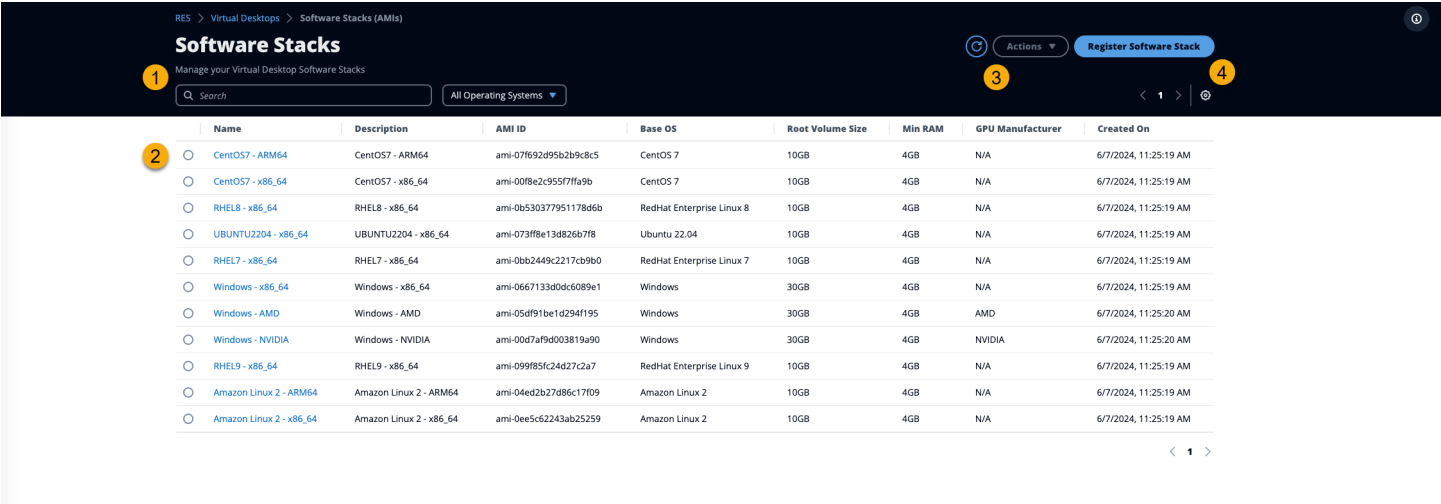
RES Session Id 8765705b-8919-48ba-901a-19e2c49cf043	DCV Session Id bd63e69a-e75a-427b-b4c8-39d7c43b95ad	Description -
Session Type VIRTUAL	Hibernation Enabled No	Created On 9/27/2023, 8:31:50 AM
Updated On 9/29/2023, 11:01:20 PM		

Piles de logiciels () AMIs

Note

Pour exécuter le stack SO7 logiciel Cent fourni AWS GovCloud (US), vous devez vous abonner à l'AMI en AWS Marketplace utilisant votre [compte standard associé](#).

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



1. Pour rechercher 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. Une fois que vous avez sélectionné une pile logicielle, utilisez le menu Actions pour modifier la pile et l'attribuer à un projet.
4. Le bouton Register Software Stack vous permet de créer une nouvelle pile :
 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

GPU Manufacturer

Select the GPU Manufacturer for the software stack

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

Projects

Select applicable projects for the software stack

Attribuer une pile logicielle à un projet

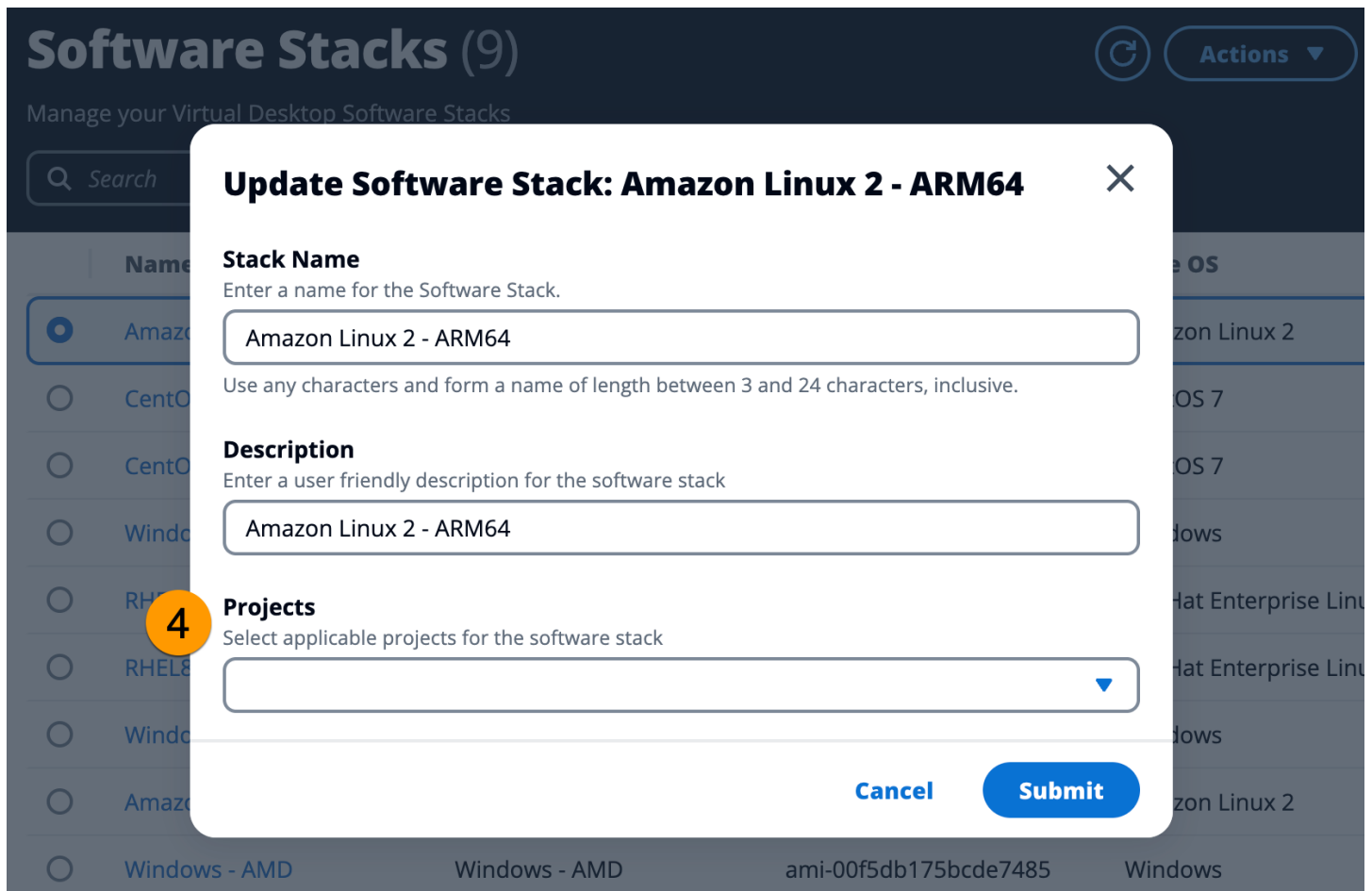
Lorsque vous créez une nouvelle pile logicielle, vous pouvez attribuer la pile à des projets. Si vous devez ajouter la pile à un projet après sa création initiale, procédez comme suit :

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.

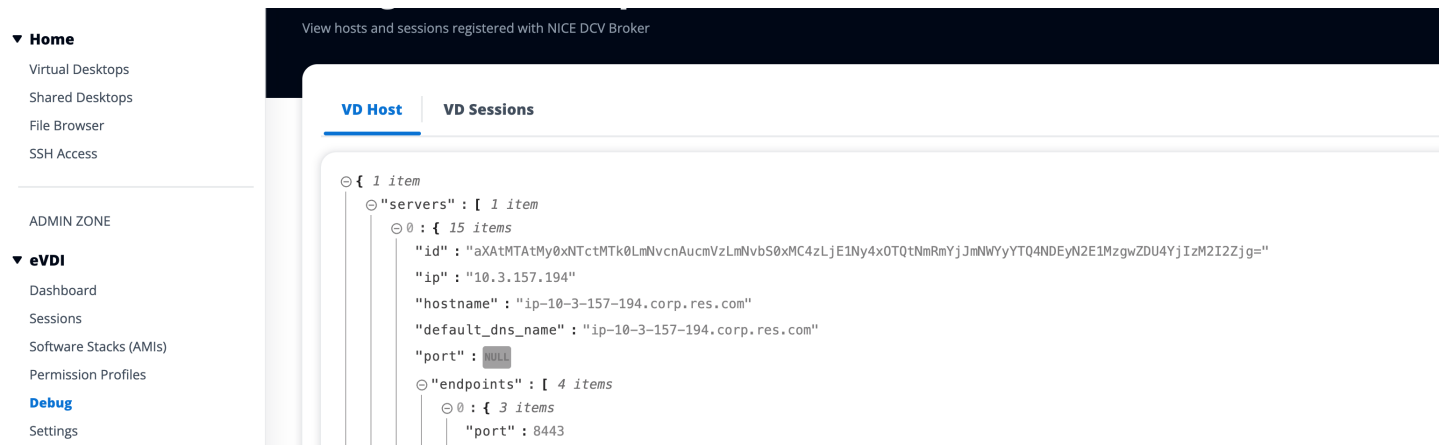


Afficher les détails de la pile logicielle

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.

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.



Paramètres 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

Durée après laquelle la session DCV sera automatiquement déconnectée. Cela ne change pas l'état de la session de bureau, cela ferme uniquement la session à partir du client DCV ou du navigateur Web.

Avertissement d'expiration du délai d'inactivité

Durée après laquelle un avertissement d'inactivité sera envoyé au client.

Seuil d'utilisation du processeur

L'utilisation du processeur doit être considérée comme inactive.

Sessions autorisées par utilisateur

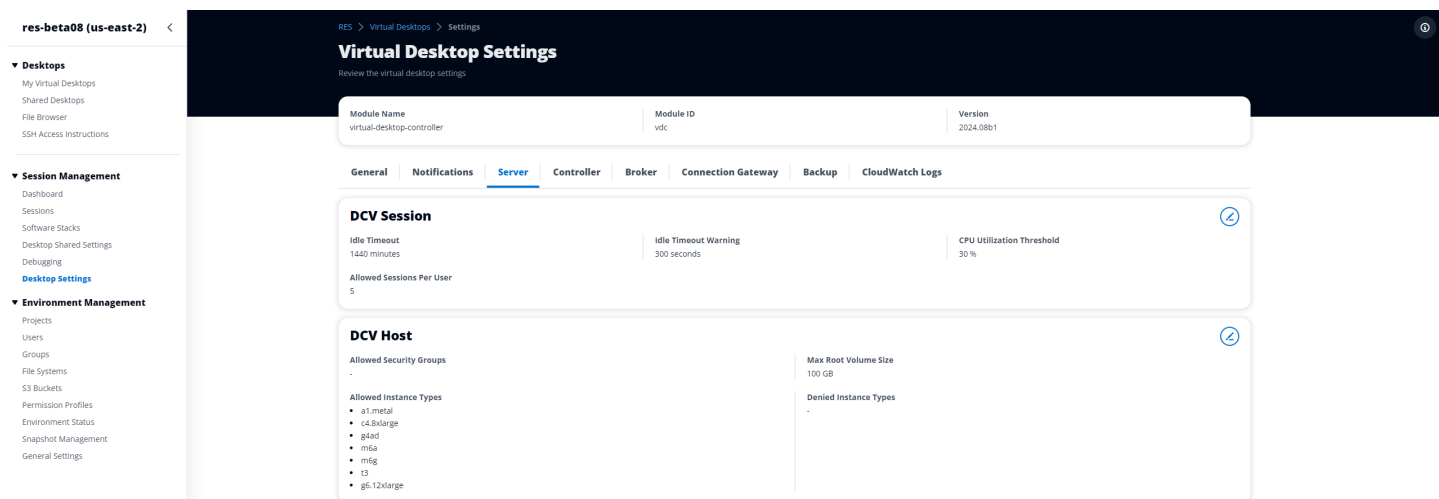
Le nombre de sessions VDI qu'un utilisateur individuel peut avoir à un moment donné. Si un utilisateur atteint ou dépasse cette valeur, cela l'empêchera de lancer de nouvelles sessions depuis la page Mes bureaux virtuels. La possibilité de lancer des sessions via la page Sessions n'est pas affectée par cette valeur.

Taille maximale du volume racine

Taille par défaut du volume racine sur les sessions de bureau virtuel.

Types d'instances autorisés

Liste des familles et tailles d'instances pouvant être lancées pour cet environnement RES. Les combinaisons de familles et de tailles d'instances sont toutes deux acceptées. Par exemple, si vous spécifiez « m7a », toutes les tailles de la famille m7a pourront être lancées sous forme de sessions VDI. Si vous spécifiez « m7a.24xlarge », seul m7a.24xlarge pourra être lancé en tant que session VDI. Cette liste concerne tous les projets dans l'environnement.



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](#)
- [Profils d'autorisation](#)
- [Systèmes de fichiers](#)

- [État de l'environnement](#)
- [Gestion des instantanés](#)
- [Réglages d'environnement](#)
- [Compartiments Amazon S3](#)

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](#)
- [Création d'un projet](#)
- [Modifier un projet](#)
- [Ajouter ou supprimer des balises dans un projet](#)
- [Afficher les systèmes de fichiers associés à un projet](#)
- [Ajouter un modèle de lancement](#)

Afficher les projets

Research and Engineering Studio

RES > Environment Management > Projects

Projects

Environment Project Management

1 Search

2 Actions

3 Create Project

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUUsers	10/3/2023, 7:04:18 PM

< 1 >

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, consultez [Ajouter un modèle de lancement](#).

3. (Facultatif) Activez les budgets pour le projet. Pour plus d'informations sur les budgets, voir [Surveillance et contrôle des coûts](#).
4. Attribuez aux and/or groupes d'utilisateurs le rôle approprié (« Membre du projet » ou « Propriétaire du projet »). Découvrez [Profils d'autorisations par défaut](#) les actions que chaque rôle peut entreprendre.
5. Sélectionnez Envoyer.

Create new Project

Project Definition

Title

Enter a user friendly project title

Project ID

Enter a project-id

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

Description

Enter the project description

Do you want to enable budgets for this project?

☐

Resource Configurations

Add file systems

Select applicable file systems for the Project



home [efs] X

► Advanced Options

Team Configurations

Groups

Select applicable ldap groups for the Project

Add group

Role

Choose a role for the group

Remove group

Users

Select applicable users for the Project

Add user

Role

Choose a role for the user

Remove user

Cancel

Submit

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 [Surveillance et contrôle des coûts](#) pour plus d'informations. Pour plus d'informations sur les options avancées, consultez [Ajouter un modèle de lancement](#).
4. Sélectionnez Envoyer.

Edit Project

Project Definition

Title

Enter a user friendly project title

Project1

Project ID

Enter a project-id

100

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

Description

Enter the project description

Enter Description ...

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 Idap groups for the Project

group_1

Add group

Role

Choose a role for the group

Project Member

Remove group

Users

Select applicable users for the Project

user1

Add user

Role

Choose a role for the user

Project Member

Remove user

Cancel

Submit

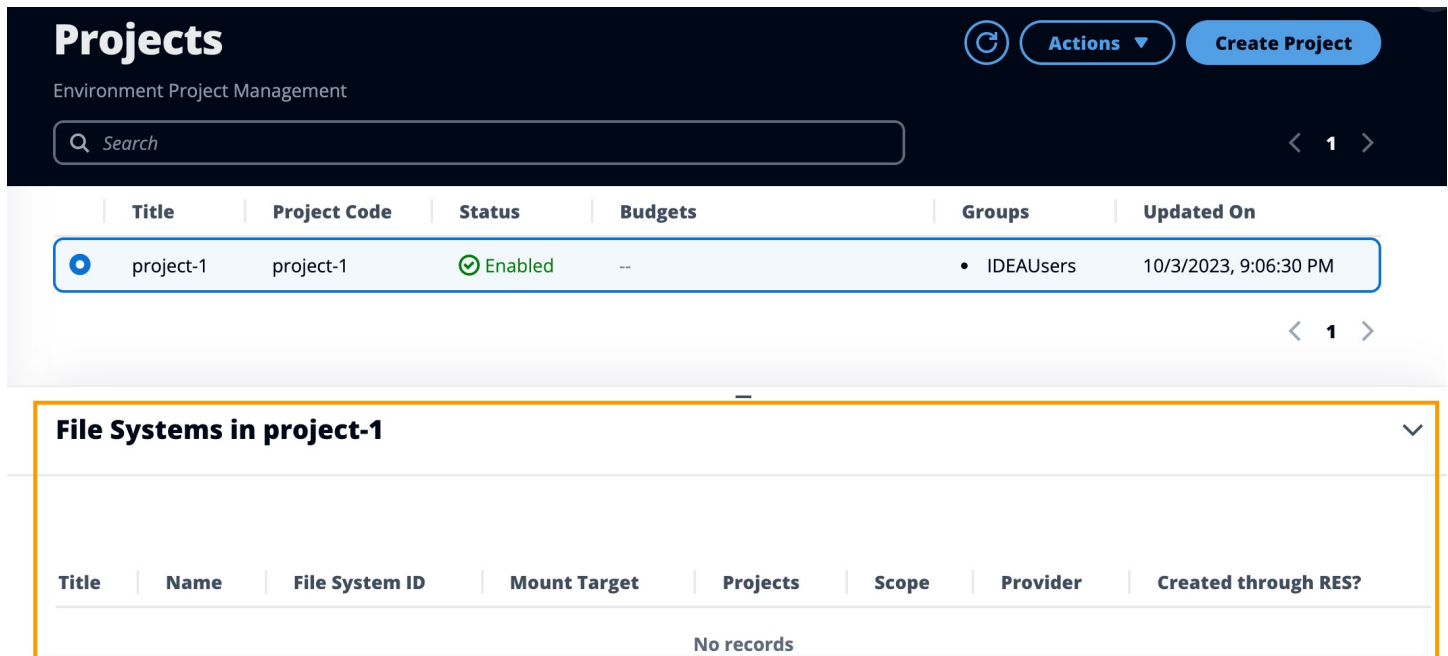
Ajouter ou supprimer des balises dans un projet

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.



The screenshot shows the 'Projects' management interface. At the top, there's a header with 'Projects' and 'Environment Project Management'. Below this is a search bar and a table of projects. The first project, 'project-1', is selected. Below the table, a section titled 'File Systems in project-1' is expanded, showing a table with columns: Title, Name, File System ID, Mount Target, Projects, Scope, Provider, and Created through RES?. The table currently shows 'No records'.

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

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

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
URL HTTPS	https://sample.samplecontent.com/échantillon
Fichier local	fichier :///.sh user/scripts/example

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

▼ Linux

Run Script When VDI Starts

Scripts that execute at the start of a VDI

☒

Script

Info

Arguments - optional

Info

s3://sample-res-scripts/sample.sh

1,2

Remove Scripts

https://sample.samplecontent.com/sample

Remove Scripts

file:///root/bootstrap/latest/launch/script

1,2

Remove Scripts

Add Scripts

Run Script when VDI is Configured

Scripts that execute after RES configurations are completed

☒

Script

Info

Arguments - optional

Info

s3://sample-res-scripts/sample.sh

1,2

Remove Scripts

Add Scripts

▼ Windows

Run Script When VDI Starts

Scripts that execute at the start of a VDI

☒

Script

Info

Arguments - optional

Info

s3://sample-res-scripts/sample.sh

1,2

Remove Scripts

Add Scripts

Run Script when VDI is Configured

Scripts that execute after RES configurations are completed

☒

Script

Info

Arguments - optional

Info

s3://sample-res-scripts/sample.sh

1,2

Remove Scripts

Add Scripts

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 le [Guide 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.

Research and Engineering Studio

RES > Environment Management > Users

Users

Environment user management

1

2 **Actions**

- Set as Admin User
- Disable User

	Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
☒	demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	- IDEAUsers - DemoUsers
☐	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	SAUsers
☐	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	- DemoAdmins - AWS Delegated Administrators - IDEAUsers
☐	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	ProductUsers

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 le [Guide de configuration](#).

Research and Engineering Studio

RES > Environment Management > Groups

Groups

Environment user group management

1 Search

2 Actions

Disable Group

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

Users in IDEAUsers 3

☐	Username	UID	GID	Email	Is Sudo?	Role	Is Active	Status	Groups	Syn
☐	demoadmin1	3000	3000	demoadmin1@demo.	Yes	admin	Yes	Enabled	- DemoAdmins - AWS Delegated Administrators - IDEAUsers	10/3
☐	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	- DemoAdmins - AWS Delegated Administrators - IDEAUsers - SAAAdmins	10/3

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 désactiver ou activer 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.

Profils d'autorisation

Présentation

Research and Engineering Studio (RES) permet à un utilisateur administratif de créer des profils d'autorisation personnalisés qui accordent aux utilisateurs sélectionnés des autorisations supplémentaires pour gérer le projet auquel ils participent. Chaque projet est fourni avec deux [profils d'autorisation par défaut](#), « Membre du projet » et « Propriétaire du projet », qui peuvent être personnalisés après le déploiement.

À l'heure actuelle, les administrateurs peuvent accorder deux ensembles d'autorisations à l'aide d'un profil d'autorisation :

1. Les autorisations de gestion de projet consistent à « mettre à jour l'adhésion au projet », qui permet à un utilisateur désigné d'ajouter d'autres utilisateurs et groupes à un projet ou de les en retirer, et à « mettre à jour le statut du projet », qui permet à un utilisateur désigné d'activer ou de désactiver un projet.
2. Les autorisations de gestion de session VDI consistent en « Créer une session » qui permet à un utilisateur désigné de créer une session VDI dans son projet, et « Créer/mettre fin à la session d'un autre utilisateur » qui permet à un utilisateur désigné de créer ou de terminer les sessions d'autres utilisateurs au sein d'un projet.

De cette façon, les administrateurs peuvent déléguer des autorisations basées sur des projets à des non-administrateurs de leur environnement.

Autorisations de gestion de projet

Mettre à jour l'adhésion au projet

Cette autorisation permet aux utilisateurs non administrateurs qui l'ont accordée d'ajouter et de supprimer des utilisateurs ou des groupes d'un projet. Cela leur permet également de définir le profil d'autorisation et de décider du niveau d'accès pour tous les autres utilisateurs et groupes associés à ce projet.

Team Configurations

Groups Info

group_1

Permission profile Info

Project Owner

Remove

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

group_2

Project Member

Remove

Add group

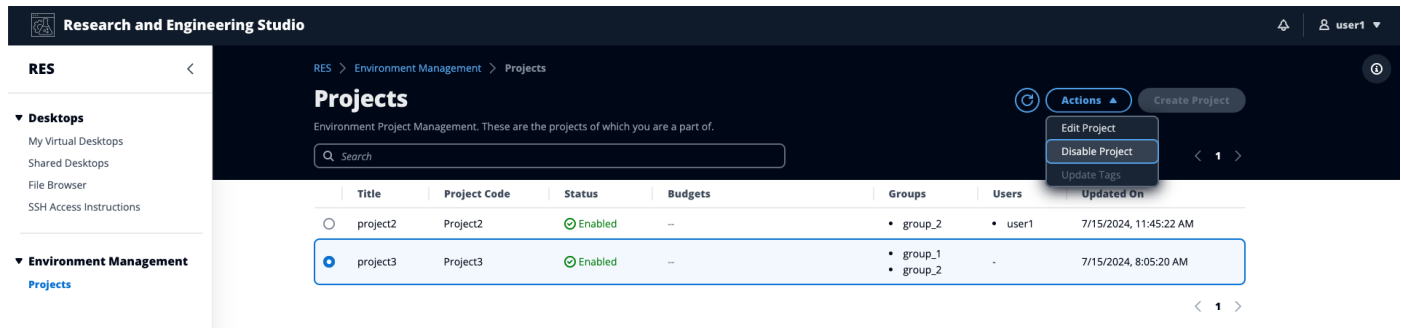
No users attached. Click 'Add user' below to get started.

Add user

Cancel Submit

Mettre à jour le statut du projet

Cette autorisation permet aux utilisateurs non administrateurs qui l'ont accordée d'activer ou de désactiver un projet à l'aide du bouton Actions de la page Projets.

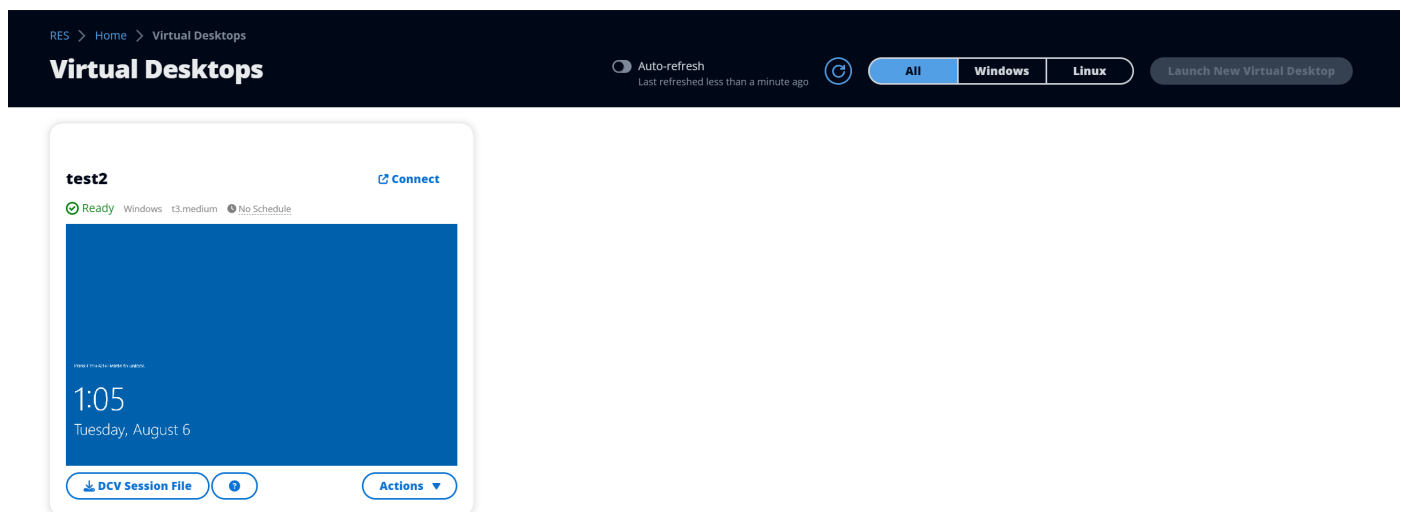


Autorisations de gestion des sessions VDI

Création d'une session

Contrôle si un utilisateur est autorisé ou non à lancer sa propre session VDI depuis la page Mes bureaux virtuels. Désactivez cette option pour empêcher les utilisateurs non administrateurs de lancer leurs propres sessions VDI. Les utilisateurs peuvent toujours arrêter et terminer leurs propres sessions VDI.

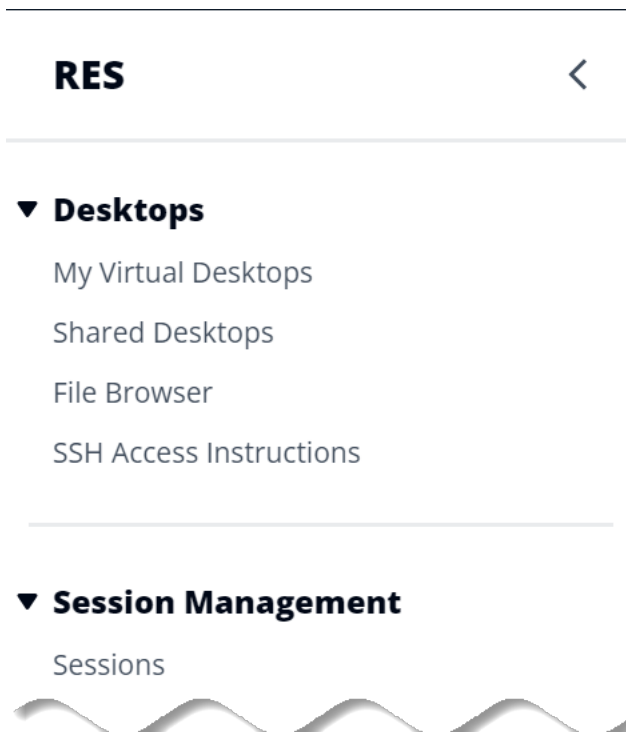
Si un utilisateur non administrateur n'est pas autorisé à créer une session, le bouton Lancer un nouveau bureau virtuel sera désactivé pour lui, comme indiqué ici :



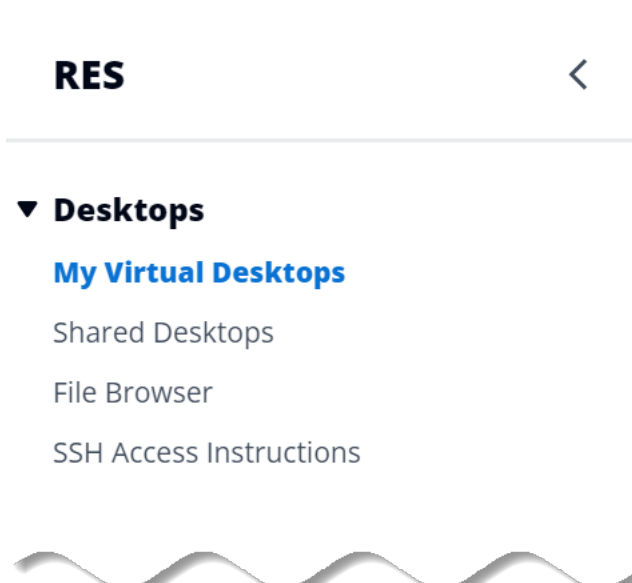
Créer ou mettre fin aux sessions des autres

Permet aux utilisateurs non administrateurs d'accéder à la page Sessions depuis le volet de navigation de gauche. Ces utilisateurs pourront lancer des sessions VDI pour d'autres utilisateurs des projets pour lesquels cette autorisation leur a été accordée.

Si un utilisateur non administrateur est autorisé à lancer des sessions pour d'autres utilisateurs, son volet de navigation de gauche affiche le lien Sessions sous Gestion des sessions, comme indiqué ici :



Si un utilisateur non administrateur n'est pas autorisé à créer des sessions pour d'autres utilisateurs, son volet de navigation de gauche n'affichera pas la gestion des sessions, comme indiqué ici :

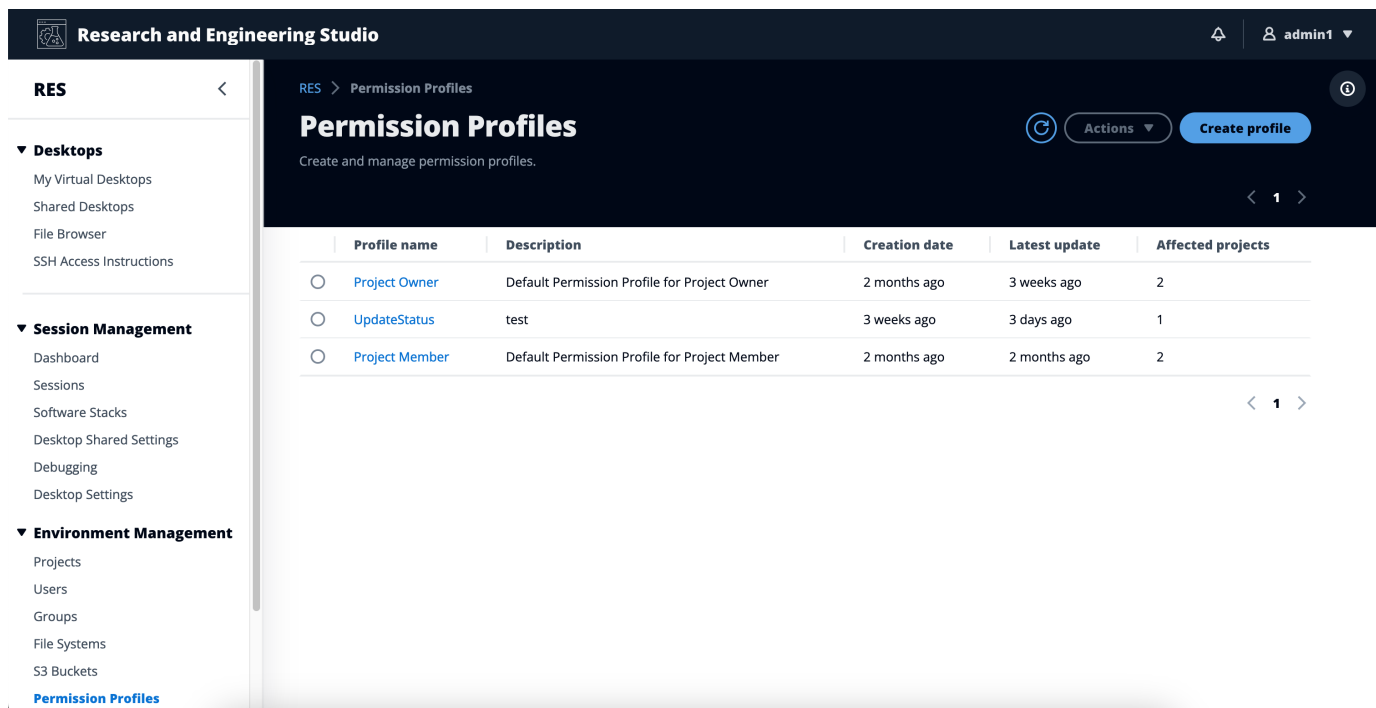


Gestion des profils d'autorisation

En tant qu'administrateur RES, vous pouvez effectuer les actions suivantes pour gérer les profils d'autorisation.

Lister les profils d'autorisation

- Sur la page de console Research and Engineering Studio, sélectionnez Permission Profiles dans le volet de navigation de gauche. À partir de cette page, vous pouvez créer, mettre à jour, répertorier, afficher et supprimer des profils d'autorisation.



The screenshot displays the 'Permission Profiles' management interface in Research and Engineering Studio. The left-hand navigation pane is expanded, showing the 'Permission Profiles' link under the 'RES' section. The main content area features a header with the title 'Permission Profiles' and a subtitle 'Create and manage permission profiles.' Below this is a table listing the existing profiles.

	Profile name	Description	Creation date	Latest update	Affected projects
☐	Project Owner	Default Permission Profile for Project Owner	2 months ago	3 weeks ago	2
☐	UpdateStatus	test	3 weeks ago	3 days ago	1
☐	Project Member	Default Permission Profile for Project Member	2 months ago	2 months ago	2

Afficher les profils d'autorisation

- Sur la page principale des profils d'autorisation, sélectionnez le nom du profil d'autorisation que vous souhaitez consulter. Sur cette page, vous pouvez modifier ou supprimer le profil d'autorisation sélectionné.

RES > Permission Profiles > Project Owner

Project Owner

EditDelete

General Settings

Profile ID

project_owner

Description

Default Permission Profile for Project Owner

Creation date

3 weeks ago

Latest update

3 weeks ago

Permissions

Affected projects

Permissions (4)

Permissions granted to this permission profile.

Project management permissions (selected 2/2)

Update project membership

Update users and groups associated with a project.

Enabled

Update project status

Enable or disable a project.

Enabled

VDI session management permissions (selected 2/2)

Create session

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

Enabled

Create/Terminate other's session

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

Enabled

2. Sélectionnez l'onglet Projets concernés pour afficher les projets qui utilisent actuellement le profil d'autorisation.

RES > Permission Profiles > Project Owner

Project Owner

EditDelete

General Settings

Profile ID

project_owner

Description

Default Permission Profile for Project Owner

Creation date

2 months ago

Latest update

4 hours ago

Permissions

Affected projects

Affected projects (2)

List of projects using this permission profile.

Project name	Groups	Users
Project1	1	2
Project3	2	0

Création de profils d'autorisation

1. Sur la page principale des profils d'autorisation, sélectionnez Créer un profil pour créer un profil d'autorisation.
2. Entrez le nom et la description du profil d'autorisation, puis choisissez les autorisations à accorder aux utilisateurs ou aux groupes que vous attribuez à ce profil.

The screenshot shows the 'Create permission profile' form. At the top, there is a breadcrumb trail: 'RES > Permission Profiles > Create Profile'. Below this is the title 'Create permission profile'. The form is divided into two main sections: 'Permission profile definition' and 'Permissions'.

Permission profile definition

Profile name
Assign a name to the profile

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

Profile description
Optionally add more details to describe the specific profile

Permissions
Permissions granted to this permission profile.

Project management permissions

Update project membership Update users and groups associated with a project. ☐	Update project status Enable or disable a project. ☐
--	--

VDI session management permissions

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

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

Modifier les profils d'autorisation

- Sur la page principale des profils d'autorisation, choisissez un profil en cliquant sur le cercle à côté de celui-ci, sélectionnez Actions, puis choisissez Modifier le profil pour mettre à jour ce profil d'autorisation.

RES > Permission Profiles > Project Member > Edit

Edit Project Member

Permission profile definition

Profile name

Assign a name to the profile

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

Profile description

Optionally add more details to describe the specific profile

Permissions

Permissions granted to this permission profile.

Project management permissions

Update project membership

Update users and groups associated with a project.

**Update project status**

Enable or disable a project.



VDI session management permissions

Create session

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

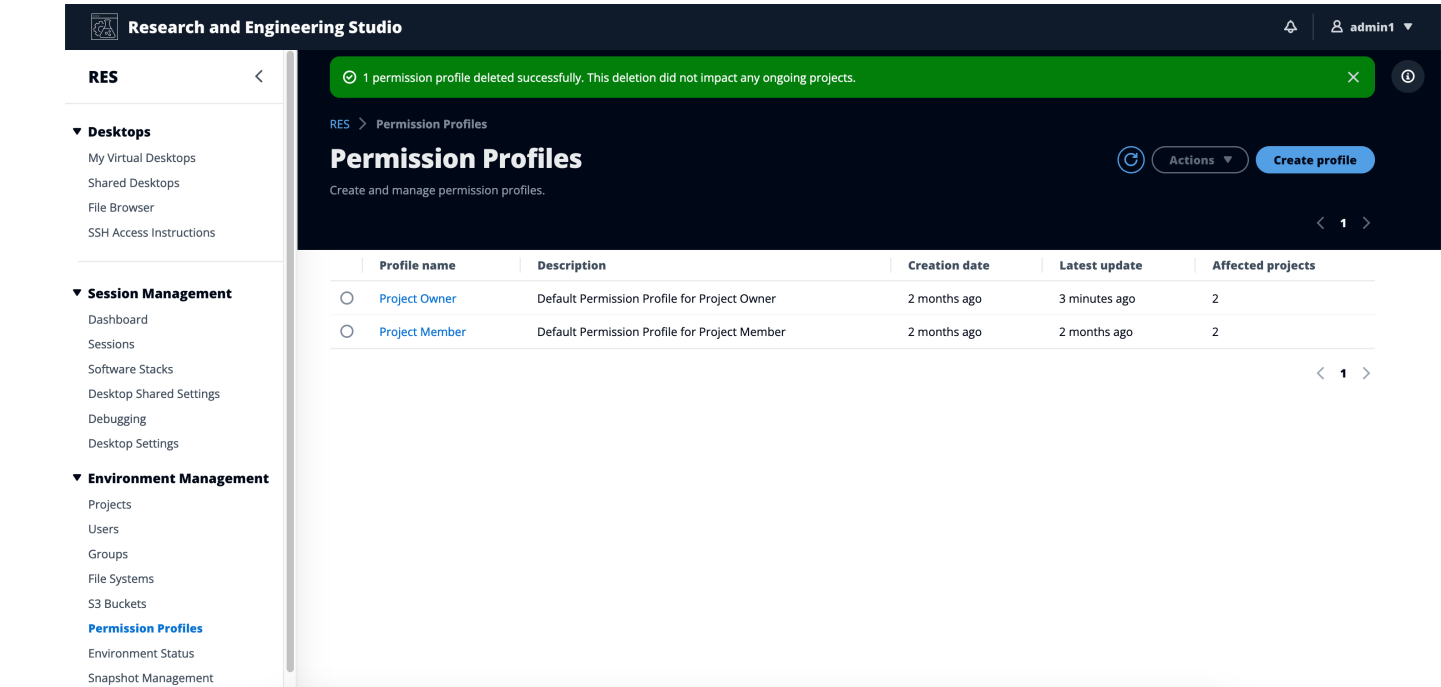
**Create/Terminate other's session**

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

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

Supprimer les profils d'autorisation

- Sur la page principale des profils d'autorisation, choisissez un profil en cliquant sur le cercle à côté de celui-ci, sélectionnez Actions, puis sélectionnez Supprimer le profil. Vous ne pouvez pas supprimer un profil d'autorisation utilisé par un projet existant.



Profils d'autorisations par défaut

Chaque projet RES est fourni avec deux profils d'autorisation par défaut que les administrateurs globaux peuvent configurer. (En outre, les administrateurs globaux peuvent créer et modifier de nouveaux profils d'autorisation pour un projet.) Le tableau suivant indique les autorisations autorisées pour les profils d'autorisation par défaut, « Membre du projet » et « Propriétaire du projet ». Les profils d'autorisation, et les autorisations qu'ils accordent pour sélectionner les utilisateurs d'un projet, ne s'appliquent qu'au projet auquel ils appartiennent ; les administrateurs globaux sont des super utilisateurs qui disposent de toutes les autorisations ci-dessous pour tous les projets.

Autorisations	Description	Membre du projet	Propriétaire du projet	
Créer une session	Créez votre propre session. Les utilisateurs peuvent toujours arrêter et terminer leurs propres sessions avec ou sans	X	X	

Autorisations	Description	Membre du projet	Propriétaire du projet	
	cette autorisation.			
Créer/terminer les sessions des autres	Créez ou mettez fin à la session d'un autre utilisateur dans un projet.		X	
Mettre à jour l'adhésion au projet	Mettez à jour les utilisateurs et les groupes associés à un projet.		X	
Mettre à jour le statut du projet	Activez ou désactivez un projet.		X	

Systèmes de fichiers

Research and Engineering Studio

RES > Environment Management > File System

File Systems

Create and manage file systems for Virtual Desktops

1 Search

2 Actions

3 Onboard File System

4 Create File System

Add File System to Project

Remove File System from Project

Title	Name	File System ID	Scope	Provider
FSx ONTAP for Linux	fsx_01_linux	fs-0d2a998473da4bf80	project	fsx_netapp_ontap

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 un sous-réseau IDs à partir du VPC. Vous pouvez les trouver IDs 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

Projects

Select applicable project



Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

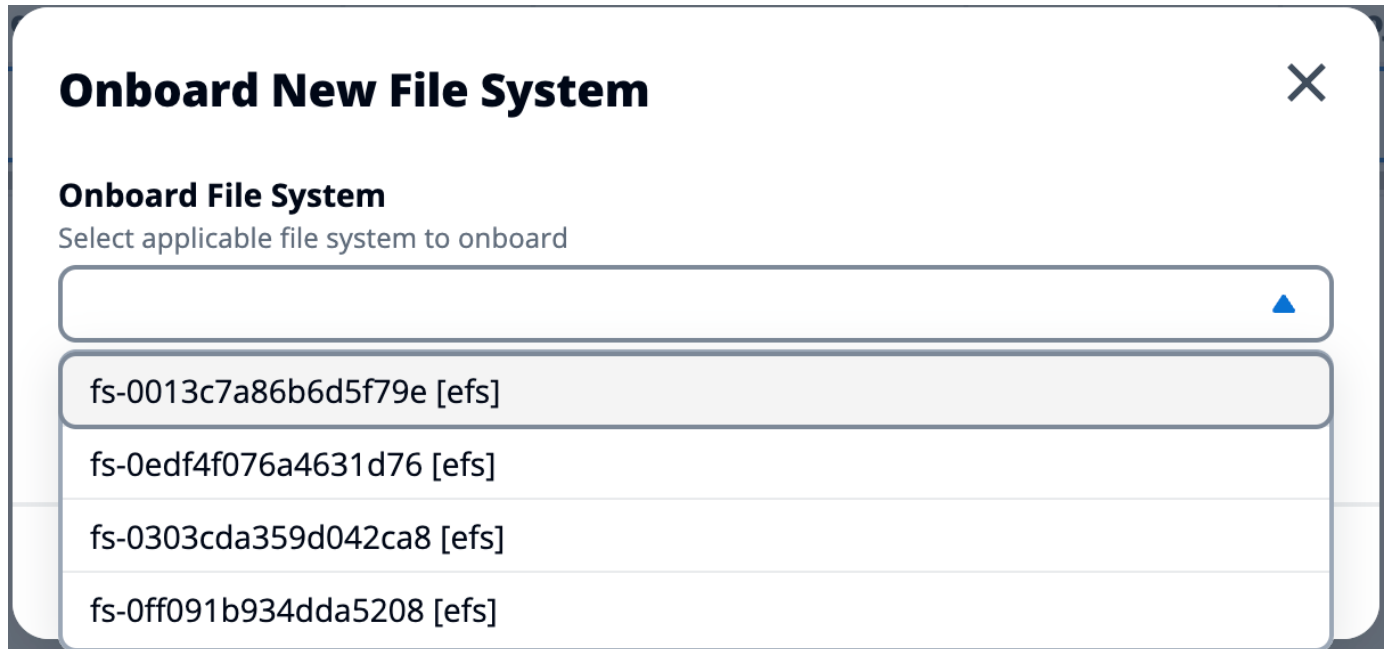
Subnet ID 1 and Subnet ID 2 should be in two different AZs

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 détaillées supplémentaires.



Onboard New File System ✕

Onboard File System
Select applicable file system to onboard

- fs-0013c7a86b6d5f79e [efs]
- fs-0edf4f076a4631d76 [efs]
- fs-0303cda359d042ca8 [efs]
- fs-0ff091b934dda5208 [efs]

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

Onboard New File System ✕

Onboard File System

Select applicable file system to onboard

fs-0edf4f076a4631d76 [efs] ▼



Title

Enter a user friendly file system title

File System Name

Enter a file system name

File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

Mount Directory

Enter directory to mount the file system

Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01

Cancel Submit

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.

Research and Engineering Studio

RES > Environment Management > Status

Environment Status

View Environment Settings

Modules

Environment modules and status

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

Infrastructure Hosts

Cluster hosts and status

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

Gestion des instantanés

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.

RES > Environment Management > Snapshot Management



Snapshot Management

Created Snapshots

1



Create Snapshot

2

Snapshots created from the environment

< 1 >

S3 Bucket Name

Snapshot Path

Status

Created On

No records

Applied Snapshots

3



Apply Snapshot

4

Snapshots applied to the environment

< 1 >

S3 Bucket Name

Snapshot Path

Status

Created On

No records

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 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 :

1. Choisissez le compartiment que vous avez créé dans la liste des compartiments.
2. Sélectionnez l'onglet 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 de plus amples informations, consultez https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html.

JSON

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

```

    "Principal": {
      "AWS":
        "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
        role-{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.

Create New Snapshot

S3 Bucket Name

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

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

Snapshot Path

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

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

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

5. 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. ApplySnapshotIDII 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 instantanés"](#) sur la page.

Pour ajouter des autorisations au bucket :

1. Choisissez le compartiment que vous avez créé dans la liste des compartiments.
2. Sélectionnez l'onglet 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

JSON

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

```

        "Principal": {
            "AWS":
                "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
                role-{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, procédez comme suit :

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.

Apply a Snapshot ✕

S3 Bucket Name

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

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

Snapshot Path

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

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

Cancel Submit

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

Réglages 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 VPC et la liste IDs des 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.

Compartiments Amazon S3

Rubriques

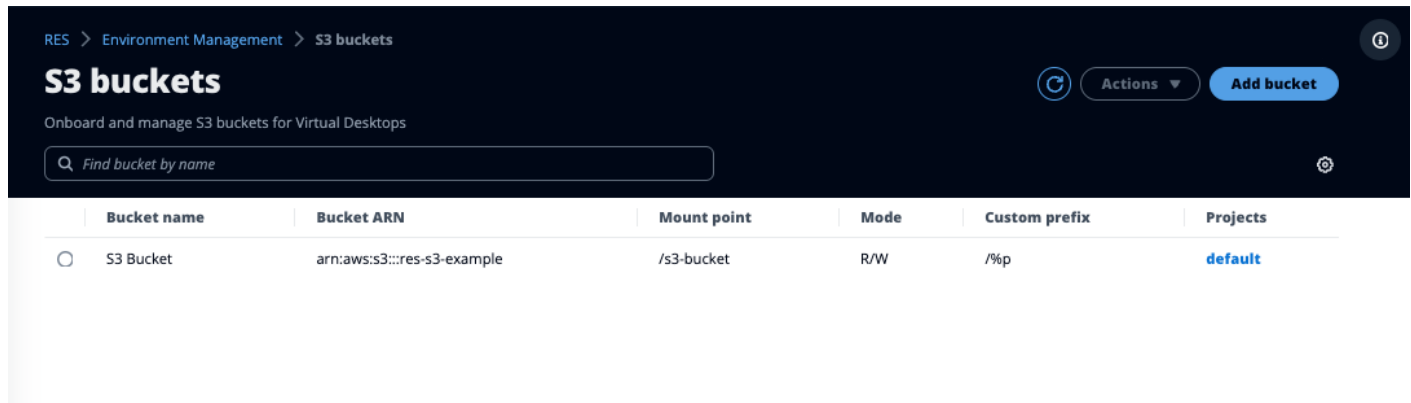
- [Monter un compartiment Amazon S3](#)
- [Ajouter un compartiment Amazon S3](#)
- [Modifier un compartiment Amazon S3](#)
- [Supprimer un compartiment Amazon S3](#)
- [Isolation des données](#)
- [Accès au bucket entre comptes](#)
- [Empêcher l'exfiltration de données dans un VPC privé](#)
- [Résolution des problèmes](#)
- [Activant CloudTrail](#)

Monter un compartiment Amazon S3

Research and Engineering Studio (RES) prend en charge le montage de buckets Amazon S3 sur des instances VDI (Virtual Desktop Infrastructure) Linux. Les administrateurs RES peuvent intégrer des compartiments S3 à RES, les associer à des projets, modifier leur configuration et supprimer des compartiments dans l'onglet Compartiments S3 sous Gestion de l'environnement.

Le tableau de bord des compartiments S3 fournit une liste des compartiments S3 intégrés mis à votre disposition. Depuis le tableau de bord des compartiments S3, vous pouvez :

1. Utilisez Ajouter un compartiment pour intégrer un compartiment S3 à RES.
2. Sélectionnez un compartiment S3 et utilisez le menu Actions pour :
 - Modifier un bucket
 - Supprimer un seau
3. Utilisez le champ de recherche pour effectuer une recherche par nom de compartiment et trouver des compartiments S3 intégrés.



Ajouter un compartiment Amazon S3

Pour ajouter un compartiment S3 à votre environnement RES :

1. Choisissez Add bucket (Ajouter un compartiment).
2. Entrez les détails du bucket tels que le nom du bucket, l'ARN et le point de montage.

Important

- L'ARN du bucket, le point de montage et le mode fournis ne peuvent pas être modifiés après la création.
- L'ARN du bucket peut contenir un préfixe qui isolera le bucket S3 intégré par rapport à ce préfixe.

3. Sélectionnez le mode dans lequel vous souhaitez embarquer votre bucket.

Important

- Voir [Isolation des données](#) pour plus d'informations sur l'isolation des données avec des modes spécifiques.

4. Sous Options avancées, vous pouvez fournir un ARN de rôle IAM pour monter les buckets pour l'accès entre comptes. Suivez les étapes décrites [Accès au bucket entre comptes](#) pour créer le rôle IAM requis pour l'accès entre comptes.

5. (Facultatif) Associez le bucket à des projets, qui peuvent être modifiés ultérieurement. Toutefois, un compartiment S3 ne peut pas être monté sur les sessions VDI existantes d'un projet. Seules les sessions lancées une fois que le projet a été associé au bucket monteront le bucket.
6. Sélectionnez Envoyer.

RES > Environment Management > S3 buckets > Add bucket

Add bucket

Currently only available for Linux desktops

Bucket setup

Bucket display name
Type a user friendly name to display

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

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

Mode

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

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

Custom prefix
Enable the system to create a prefix automatically

No custom prefix

▼ Advanced settings - optional

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

Project association

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



Modifier un compartiment Amazon S3

1. Sélectionnez un compartiment S3 dans la liste des compartiments S3.
2. Dans le menu Actions, choisissez Modifier.
3. Entrez vos mises à jour.

⚠ Important

- L'association d'un projet à un compartiment S3 ne montera pas le compartiment sur les instances d'infrastructure de bureau virtuel (VDI) existantes de ce projet. Le bucket ne sera monté sur les sessions VDI lancées dans un projet qu'une fois le bucket associé à ce projet.
- La dissociation d'un projet d'un compartiment S3 n'aura aucun impact sur les données contenues dans le compartiment S3, mais les utilisateurs d'ordinateurs de bureau perdront l'accès à ces données.

4. Choisissez Enregistrer la configuration du bucket.

The screenshot shows the 'Edit S3 Bucket' configuration page. At the top, there is a breadcrumb trail: 'RES > Environment Management > S3 buckets > Edit bucket'. The page title is 'Edit S3 Bucket'. Below the title, there are two main sections: 'Bucket setup' and 'Project association'. In the 'Bucket setup' section, there is a 'Bucket display name' field with the placeholder text 'Type a user friendly name to display'. The current value in the field is 'S3 Bucket'. In the 'Project association' section, there is a 'Projects - optional' dropdown menu with the placeholder text 'Choose the projects to associate to the bucket'. The dropdown is currently empty. Below the dropdown, there is a 'default' button with a close icon. At the bottom right of the page, there are two buttons: 'Cancel' and 'Save bucket setup'.

Supprimer un compartiment Amazon S3

1. Sélectionnez un compartiment S3 dans la liste des compartiments S3.
2. Dans le menu Actions, choisissez Supprimer.

⚠ Important

- Vous devez d'abord supprimer toutes les associations de projets du compartiment.
- L'opération de suppression n'a aucun impact sur les données du compartiment S3. Il supprime uniquement l'association du compartiment S3 avec RES.

- La suppression d'un compartiment entraîne la perte de l'accès des sessions VDI existantes au contenu de ce compartiment à l'expiration des informations d'identification de cette session (environ 1 heure).

Isolation des données

Lorsque vous ajoutez un compartiment S3 à RES, vous avez la possibilité d'isoler les données qu'il contient pour des projets et des utilisateurs spécifiques. Sur la page Ajouter un compartiment, vous pouvez choisir un mode Read Only (R) ou Read and Write (R/W).

Lecture seule

Si Read Only (R) cette option est sélectionnée, l'isolation des données est appliquée en fonction du préfixe de l'ARN du bucket (Amazon Resource Name). Par exemple, si un administrateur ajoute un bucket à RES à l'aide de l'ARN `arn:aws:s3:::bucket-name/example-data/` et associe ce bucket au projet A et au projet B, les utilisateurs qui lancent VDIs depuis le projet A et le projet B ne peuvent lire que les données situées *bucket-name* sous le chemin */example-data*. Ils n'auront pas accès aux données en dehors de ce chemin. Si aucun préfixe n'est ajouté à l'ARN du bucket, l'intégralité du bucket sera mise à la disposition de tous les projets qui lui sont associés.

Lisez et écrivez

Si Read and Write (R/W) cette option est sélectionnée, l'isolation des données est toujours appliquée en fonction du préfixe de l'ARN du bucket, comme décrit ci-dessus. Ce mode comporte des options supplémentaires permettant aux administrateurs de fournir un préfixe basé sur des variables pour le compartiment S3. Lorsque cette option Read and Write (R/W) est sélectionnée, une section Préfixe personnalisé devient disponible et propose un menu déroulant avec les options suivantes :

- Aucun préfixe personnalisé
- `/p`
- `/p/u`

RES > Environment Management > S3 buckets > Add bucket

Add bucket

Currently only available for Linux desktops

Bucket setup

Bucket display name
Type a user friendly name to display

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

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

Mode

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

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

Custom prefix
Enable the system to create a prefix automatically

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

Aucune isolation personnalisée des données

Lorsque `No custom prefix` le préfixe personnalisé est sélectionné, le bucket est ajouté sans aucune isolation de données personnalisée. Cela permet à tous les projets associés au bucket d'avoir un accès en lecture et en écriture. Par exemple, si un administrateur ajoute un bucket à RES en utilisant l'ARN `arn:aws:s3:::bucket-name` avec `No custom prefix` selected et associe ce bucket au projet A et au projet B, les utilisateurs qui lancent VDI depuis le projet A et le projet B auront un accès illimité en lecture et en écriture au bucket.

Isolation des données au niveau du projet

Lorsque `/%p` le préfixe personnalisé est sélectionné, les données du compartiment sont isolées pour chaque projet spécifique qui lui est associé. La `%p` variable représente le code du projet. Par exemple, si un administrateur ajoute un bucket à RES en utilisant l'ARN `arn:aws:s3:::bucket-name` avec `/%p` selected et un point de montage de `/bucket`, et qu'il associe ce bucket aux projets A et B, l'utilisateur A du projet A peut y écrire un fichier `/bucket`. L'utilisateur B du projet A peut également voir le fichier dans lequel l'utilisateur A a écrit `/bucket`. Toutefois, si l'utilisateur B lance un VDI dans le projet B et y jette un `/bucket` œil, il

ne verra pas le fichier écrit par l'utilisateur A, car les données sont isolées par projet. Le fichier écrit par l'utilisateur A se trouve dans le compartiment S3 sous le préfixe, /ProjectA tandis que l'utilisateur B ne peut y accéder que /ProjectB s'il utilise le fichier VDI depuis le projet B.

Isolation des données au niveau du projet et de l'utilisateur

Lorsque le préfixe personnalisé **/p/u** est sélectionné, les données du compartiment sont isolées pour chaque projet spécifique et pour chaque utilisateur associé à ce projet. La **%p** variable représente le code du projet et **%u** le nom d'utilisateur. Par exemple, un administrateur ajoute un bucket à RES en utilisant l'ARN `arn:aws:s3:::bucket-name` dont le point de montage est **/p/u** sélectionné et le point de montage est égal à **/bucket**. Ce compartiment est associé au projet A et au projet B. L'utilisateur A du projet A peut y écrire un fichier **/bucket**. Contrairement au scénario précédent avec uniquement **%p** l'isolation, l'utilisateur B ne verra pas dans ce cas le fichier écrit par l'utilisateur A dans le projet A **/bucket**, car les données sont isolées à la fois par le projet et par l'utilisateur. Le fichier écrit par l'utilisateur A se trouve dans le compartiment S3 sous le préfixe, /ProjectA/UserA tandis que l'utilisateur B ne peut y accéder que /ProjectA/UserB s'il l'utilise VDI dans le projet A.

Accès au bucket entre comptes

RES est capable de monter des buckets à partir d'autres AWS comptes, à condition que ces buckets disposent des autorisations appropriées. Dans le scénario suivant, un environnement RES du compte A souhaite monter un compartiment S3 dans le compte B.

Étape 1 : Créez un rôle IAM dans le compte dans lequel RES est déployé (ce rôle sera appelé compte A) :

1. Connectez-vous à la console AWS de gestion du compte RES qui doit accéder au compartiment S3 (compte A).
2. Ouvrez la console IAM :
 - a. Accédez au tableau de bord IAM.
 - b. Dans le panneau de navigation, sélectionnez Stratégies.
3. Créez une politique :
 - a. Sélectionnez Create Policy (Créer une politique).
 - b. Choisissez l'onglet JSON.

- c. Collez la politique JSON suivante (<BUCKET-NAME>remplacez-la par le nom du compartiment S3 situé dans le compte B) :

JSON

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

- d. Sélectionnez Suivant.
4. Passez en revue et créez la politique :
- Donnez un nom à la politique (par exemple, AccessPolicy « S3 »).
 - Ajoutez une description facultative pour expliquer l'objectif de la politique.
 - Passez en revue la politique et sélectionnez Créer une politique.
5. Ouvrez la console IAM :
- Accédez au tableau de bord IAM.
 - Dans le volet de navigation, sélectionnez Rôles.
6. Créez un rôle :
- Sélectionnez Créer le rôle.
 - Choisissez Politique de confiance personnalisée comme type d'entité de confiance.

- c. Collez la politique JSON suivante (<ACCOUNT_ID>remplacez-la par l'ID de compte réel du compte A, <ENVIRONMENT_NAME> par le nom de l'environnement du déploiement de RES et <REGION> par la AWS région dans laquelle RES est déployé) :

JSON

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

- d. Sélectionnez « Suivant ».
7. Joindre des politiques d'autorisation :
- Recherchez et sélectionnez la politique que vous avez créée précédemment.
 - Sélectionnez « Suivant ».
8. Marquez, révisiez et créez le rôle :
- Entrez un nom de rôle (par exemple, AccessRole « S3 »).
 - À l'étape 3, sélectionnez Ajouter une étiquette, puis entrez la clé et la valeur suivantes :
 - Clé : res:Resource
 - Valeur : s3-bucket-iam-role
 - Vérifiez le rôle et sélectionnez Créer un rôle.
9. Utilisez le rôle IAM dans RES :
- Copiez l'ARN du rôle IAM que vous avez créé.
 - Connectez-vous à la console RES.

- c. Dans le volet de navigation de gauche, sélectionnez S3 Bucket.
- d. Sélectionnez Ajouter un compartiment et remplissez le formulaire avec l'ARN du compartiment S3 multi-comptes.
- e. Sélectionnez le menu déroulant Paramètres avancés - facultatif.
- f. Entrez l'ARN du rôle dans le champ ARN du rôle IAM.
- g. Sélectionnez Ajouter un compartiment.

Étape 2 : Modifier la politique de compartiment dans le compte B

1. Connectez-vous à la console AWS de gestion du compte B.
2. Ouvrez la console S3 :
 - a. Accédez au tableau de bord S3.
 - b. Sélectionnez le bucket auquel vous souhaitez accorder l'accès.
3. Modifiez la politique relative aux compartiments :
 - a. Choisissez l'onglet Permissions, puis sélectionnez Bucket Policy.
 - b. Ajoutez la politique suivante pour accorder au rôle IAM depuis le compte A l'accès au compartiment (remplacez-le `<AccountA_ID>` par l'ID de compte réel du compte A et `<BUCKET-NAME>` par le nom du compartiment S3) :

JSON

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

```
    ],  
    "Resource": [  
        "arn:aws:s3:::<BUCKET-NAME>",  
        "arn:aws:s3:::<BUCKET-NAME>/*"  
    ]  
  }  
]  
}
```

- c. Sélectionnez Save.

Empêcher l'exfiltration de données dans un VPC privé

Pour empêcher les utilisateurs d'exfiltrer les données des compartiments S3 sécurisés vers leurs propres compartiments S3 de leur compte, vous pouvez associer un point de terminaison VPC pour sécuriser votre VPC privé. Les étapes suivantes montrent comment créer un point de terminaison VPC pour le service S3 qui prend en charge l'accès aux compartiments S3 au sein de votre compte, ainsi qu'à tout compte supplémentaire doté de compartiments multicomptes.

1. Ouvrez la console Amazon VPC :
 - a. Connectez-vous à la console AWS de gestion.
 - b. Ouvrez la console Amazon VPC à l'adresse. <https://console.aws.amazon.com/vpc/>
2. Créez un point de terminaison VPC pour S3 :
 - a. Dans le volet de navigation de gauche, sélectionnez Endpoints.
 - b. Sélectionnez Create Endpoint (Créer un point de terminaison).
 - c. Pour Catégorie de service, assurez-vous que l'option services AWS est sélectionnée.
 - d. Dans le champ Nom du service, entrez `com.amazonaws.<region>.s3` (remplacez `<region>` par votre AWS région) ou recherchez « S3 ».
 - e. Sélectionnez le service S3 dans la liste.
3. Configurer les paramètres du point de terminaison :
 - a. Pour le VPC, sélectionnez le VPC dans lequel vous souhaitez créer le point de terminaison.
 - b. Pour les sous-réseaux, sélectionnez les deux sous-réseaux privés utilisés pour les sous-réseaux VDI lors du déploiement.
 - c. Pour Activer le nom DNS, assurez-vous que l'option est cochée. Cela permet de résoudre le nom d'hôte DNS privé sur les interfaces réseau du point de terminaison.

4. Configurez la politique pour restreindre l'accès :

- a. Sous Politique, sélectionnez Personnaliser.
- b. Dans l'éditeur de règles, entrez une politique qui restreint l'accès aux ressources de votre compte ou d'un compte spécifique. Voici un exemple de politique (remplacez-le *mybucket* par le nom de votre compartiment S3 *111122223333* et *444455556666* par le AWS compte approprié IDs auquel vous souhaitez avoir accès) :

JSON

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

5. Créez le point de terminaison :

- a. Vérifiez vos paramètres.
- b. Sélectionnez Créer un point de terminaison.

6. Vérifiez le point de terminaison :

- a. Une fois le point de terminaison créé, accédez à la section Points de terminaison de la console VPC.

- b. Sélectionnez le point de terminaison nouvellement créé.
- c. Vérifiez que l'état est disponible.

En suivant ces étapes, vous créez un point de terminaison VPC qui autorise un accès S3 limité aux ressources de votre compte ou à un ID de compte spécifié.

Résolution des problèmes

Comment vérifier si un bucket ne parvient pas à être monté sur un VDI

Si un bucket ne parvient pas à être monté sur un VDI, vous pouvez vérifier les erreurs à certains endroits. Suivez les étapes ci-dessous.

1. Vérifiez les journaux VDI :

- a. Connectez-vous à la console AWS de gestion.
- b. Ouvrez la EC2 console et accédez à Instances.
- c. Sélectionnez l'instance VDI que vous avez lancée.
- d. Connectez-vous au VDI via le gestionnaire de session.
- e. Exécutez les commandes suivantes :

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

Vous trouverez ici les journaux de bootstrap. Les détails de toute défaillance figureront dans le `configure.log.{time}` fichier.

Consultez également le `/etc/message journal` pour plus de détails.

2. Vérifiez les journaux CloudWatch Lambda de Custom Credential Broker :

- a. Connectez-vous à la console AWS de gestion.
- b. Ouvrez la CloudWatch console et accédez à Log groups.
- c. Recherchez le groupe de journaux `/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.
- d. Examinez le premier groupe de journaux disponible et repérez les éventuelles erreurs dans les journaux. Ces journaux contiendront des détails concernant les problèmes potentiels liés

à la fourniture d'informations d'identification personnalisées temporaires pour le montage de compartiments S3.

3. Vérifiez les CloudWatch journaux personnalisés de Credential Broker API Gateway :
 - a. Connectez-vous à la console AWS de gestion.
 - b. Ouvrez la CloudWatch console et accédez à Log groups.
 - c. Recherchez le groupe de journaux `<stack-name>-vdc-custom-credential-broker-lambda-vdc-custom-credential-broker-api-gateway-access-logs<nonce>`.
 - d. Examinez le premier groupe de journaux disponible et repérez les éventuelles erreurs dans les journaux. Ces journaux contiendront des détails concernant toutes les demandes et réponses adressées à l'API Gateway concernant les informations d'identification personnalisées nécessaires au montage des compartiments S3.

Comment modifier la configuration du rôle IAM d'un bucket après l'intégration

1. Connectez-vous à la console [AWS DynamoDB](#).
2. Sélectionnez le tableau :
 - a. Dans le volet de navigation de gauche, sélectionnez Tables.
 - b. Recherchez et sélectionnez `<stack-name>.cluster-settings`.
3. Scannez le tableau :
 - a. Sélectionnez Explorer les éléments de table.
 - b. Assurez-vous que Scan est sélectionné.
4. Ajoutez un filtre :
 - a. Sélectionnez Filtres pour ouvrir la section de saisie des filtres.
 - b. Réglez le filtre pour qu'il corresponde à votre clé-
 - Attribut : Entrez la clé.
 - État : Choisissez Commence par.
 - Valeur : entrez « `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` remplacement `<filesystem_id>` » par la valeur du système de fichiers à modifier.
5. Exécutez le scan :

Sélectionnez Exécuter pour exécuter le scan avec le filtre.

6. Vérifiez la valeur :

Si l'entrée existe, assurez-vous que la valeur est correctement définie avec le bon ARN du rôle IAM.

Si l'entrée n'existe pas :

- a. Sélectionnez Créer un article.
- b. Entrez les détails de l'article :
 - Pour l'attribut clé, entrez `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
 - Ajoutez le bon ARN du rôle IAM.
- c. Sélectionnez Enregistrer pour ajouter l'article.

7. Redémarrez les instances VDI :

Redémarrez l'instance pour vous assurer VDI que les ARN affectés par le rôle IAM incorrect sont à nouveau montés.

Activant CloudTrail

Pour l'activer CloudTrail dans votre compte à l'aide de la CloudTrail console, suivez les instructions fournies dans la [section Création d'un historique avec la CloudTrail console](#) dans le guide de AWS CloudTrail l'utilisateur. CloudTrail enregistrera l'accès aux compartiments S3 en enregistrant le rôle IAM qui y a accédé. Cela peut être lié à un ID d'instance, qui est lié à un projet ou à un utilisateur.

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	Administrateur entré
<envname>- sso-client-secret	Secret du OAuth2 client Single Sign-On 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	✓	
<envname>-certificat interne	Certificat auto-signé pour le domaine	✓	

Nom du secret	Description	RES généré	Administrateur entré
<envname>- service d'annuaire - ServiceAccountUser name			✓
<envname>- service d'annuaire - ServiceAccountPass word			✓

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
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	

Clé	Source
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 des [the section called "AWS services 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 and Cost Management console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/costmanagement/>.
2. Choisissez les balises de répartition des coûts.
3. Recherchez et sélectionnez les `res:EnvironmentName` balises `res:Project` et.
4. Choisissez Activer.

Billing

Home

▼ Billing

Bills

Payments

Credits

Purchase orders

Cost & usage reports

Cost categories

Cost allocation tags 2

Free tier

Billing Conductor

▼ Cost Management

Cost explorer

Budgets

Budgets reports

Savings Plans

▼ Preferences

Billing preferences

Payment preferences

Consolidated billing

Tax settings

▼ Permissions

Cost allocation tags info

Cost allocation tags activated: 3

Download CSV

User-defined cost allocation tags

AWS generated cost allocation tags

User-defined cost allocation tags (2/47) info

Undo Deactivate Activate

Find cost allocation tags 11 matches

res Clear filters

Tag key	Status	Last updated date	Last used month
☐ res:BackupPlan	Inactive	-	November 2023
☐ res:ClusterName	Inactive	-	November 2023
☐ res:DCVSessionUUID	Inactive	-	November 2023
☐ res:EndpointName	Inactive	-	November 2023
☒ res:EnvironmentName 3	Inactive	-	November 2023
☐ res:ModuleId	Inactive	-	November 2023
☐ res:ModuleName	Inactive	-	November 2023
☐ res:ModuleVersion	Inactive	-	November 2023
☐ res:NodeType	Inactive	-	November 2023
☒ res:Project	Inactive	-	November 2023

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.

Billing ×

- Home
- ▼ **Billing**
 - Bills
 - Payments
 - Credits
 - Purchase orders
 - Cost & usage reports
 - Cost categories
 - Cost allocation tags
 - Free tier
 - Billing Conductor [↗](#)
- ▼ **Cost Management**
 - Cost explorer [↗](#)
 - Budgets** 1
 - Budgets reports
 - Savings Plans [↗](#)
- ▼ **Preferences**
 - Billing preferences
 - Payment preferences
 - Consolidated billing [↗](#)
 - Tax settings
- ▼ **Permissions**
 - Affected policies [↗](#)

Step 1
Choose budget type

Step 2
[Set your budget](#)

Step 3
Configure alerts

Step 4 - Optional
Attach actions

Step 5
Review

Choose budget type [Info](#)

Budget setup

3

☐ Use a template (simplified)
Use the recommended configurations. You can change some configuration options after the budget is created.

☒ **Customize (advanced)**
Customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific accounts.

Budget types

4

☒ **Cost budget - Recommended**
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met. Using cost budgets, the budgeted amount you set represents your expected cloud spend. For example, you can set a cost budget for a business unit and then add additional parameters such as the associated member accounts.

☐ Usage budget
Monitor your usage of one or more specified usage types or usage type groups and receive alerts when your user-defined thresholds are met. Using usage budgets, the budgeted amount represents your expected usage. For example, you can use a usage budget to monitor the usage of certain services such as Amazon EC2 and Amazon S3.

☐ Savings Plans budget
Track the utilization or coverage associated with your Savings Plans and receive alerts when your percentage drops below a threshold you define. Setting a coverage target lets you see how much of your instance usage is covered by Savings Plans, while setting a utilization target lets you see if your Savings Plans are unused or underutilized.

☐ Reservation budget
Track the utilization or coverage associated with your reservations and receive alerts when your percentage drops below a threshold you define. Setting a coverage target lets you see how much of your instance usage is covered by reservations, while setting a utilization target lets you see if your reservations are unused or underutilized. Reservation alerts are supported for Amazon EC2, Amazon RDS, Amazon Redshift, Amazon ElastiCache, and Amazon Elasticsearch reservations.

5 Cancel **Next**

- 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].
- Sous Définir le montant du budget, entrez le montant budgétisé pour votre projet.
- Sous Étendue du budget, choisissez Filtrer les dimensions de AWS coût spécifiques.
- Choisissez Add filter.
- Sous Dimension, choisissez Tag.
- 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.

- 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 X

[Cancel](#)

[Apply filter](#)

[Add filter](#)

▼ Advanced options

Aggregate costs by

Unblended costs

Supported charge types

Upfront reservation fees X

Recurring reservation charges X

Other subscription costs X

Taxes X

Support charges X

Discounts X

[Cancel](#)

[Previous](#)

[Next](#)

15. (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, voir [the section called “Modifier un projet”](#). Le lancement des bureaux virtuels sera bloqué si le budget est dépassé. Si le budget est dépassé lors du lancement d'un ordinateur de bureau, celui-ci continuera à fonctionner.

RES > Environment Management > Projects

Projects

Environment Project Management

⌂

Actions ▾

Create Project

Title	Project Code	Status	Budgets	Groups	Updated On
☐ project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 ⊗ Budget Exceeded Limit: 500.00 USD, Forecasted: 3945.34 USD	- DemoUsers - DemoAdmins - ProductUsers	10/31/2023, 12:44:12 PM

< 1 >

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

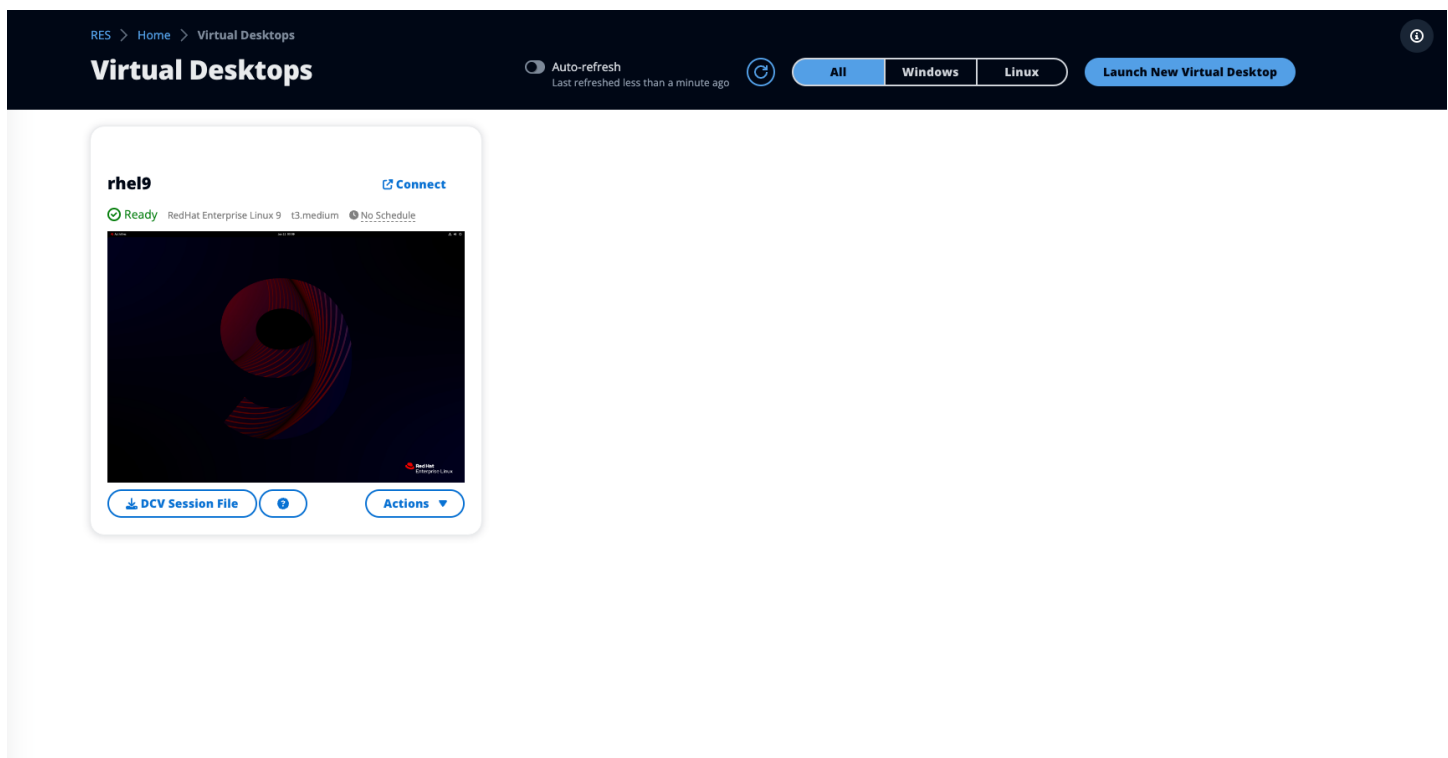
Cette section fournit des conseils aux utilisateurs sur l'utilisation de bureaux virtuels pour collaborer avec d'autres utilisateurs.

Rubriques

- [Bureaux virtuels](#)
- [Bureaux partagés](#)
- [Navigateur de fichiers](#)
- [Accès SSH](#)

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 EC2 des instances Amazon avec leurs outils et applications préférés préinstallés et configurés.



Systèmes d'exploitation pris en charge

RES prend actuellement en charge le lancement de bureaux virtuels à l'aide des systèmes d'exploitation suivants :

- Amazon Linux 2 (x86 et ARM64)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Lancer un nouvel ordinateur de bureau

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

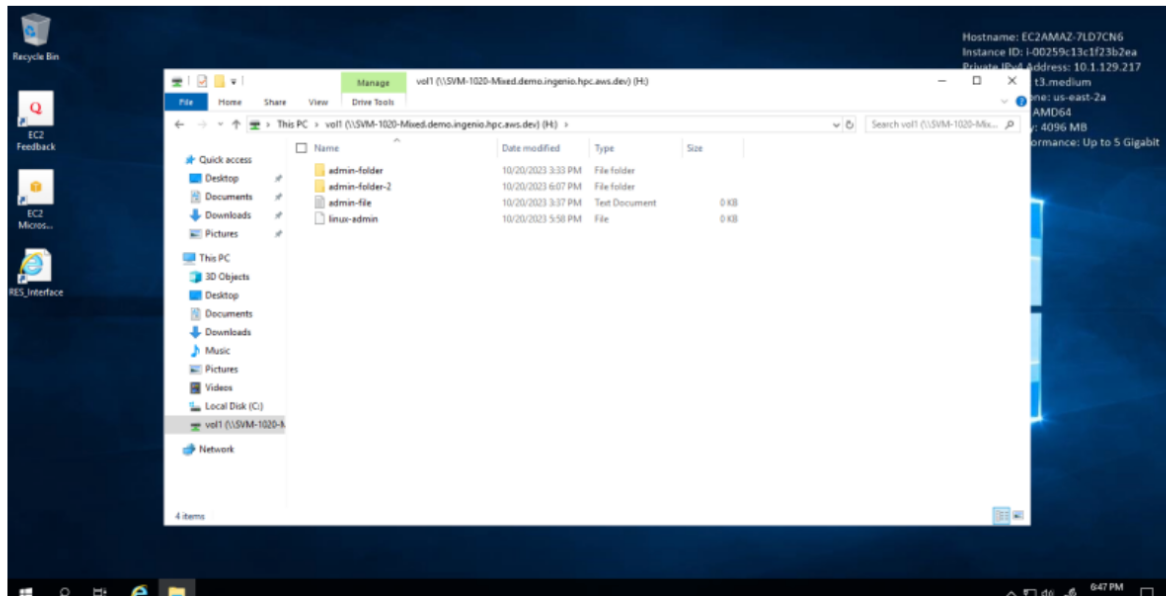
L'accès à votre bureau via le navigateur Web est la méthode de connexion la plus simple.

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

MyDesktop3-windows

[Connect](#)

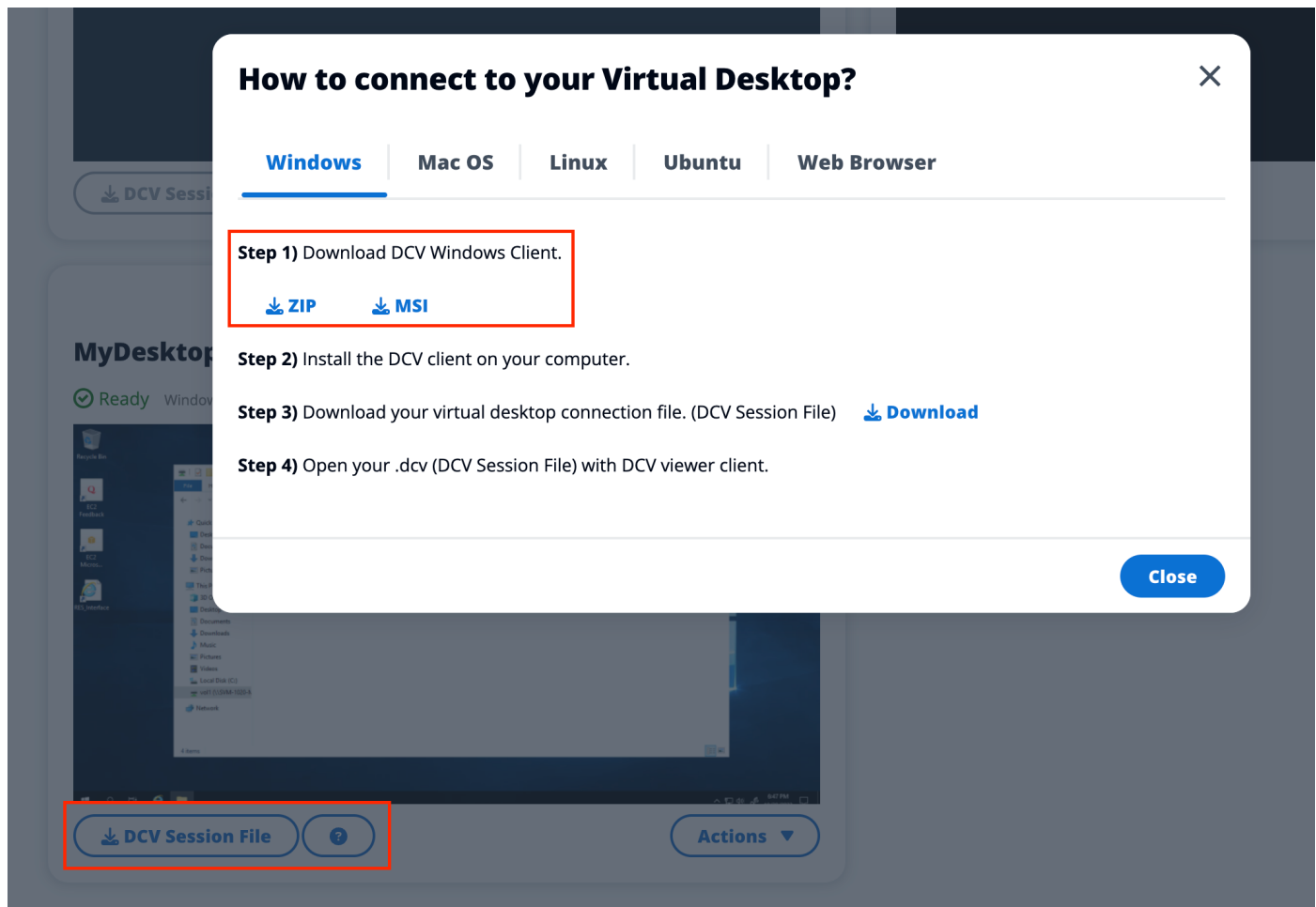
✓ Ready Windows t3.medium ⌚ No Schedule

[DCV Session File](#)[Actions](#)

DCV connection

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

1. Choisissez le fichier de session DCV pour télécharger le .dcvfichier. 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 que le bureau s'est arrêté, 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 arrêtez 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

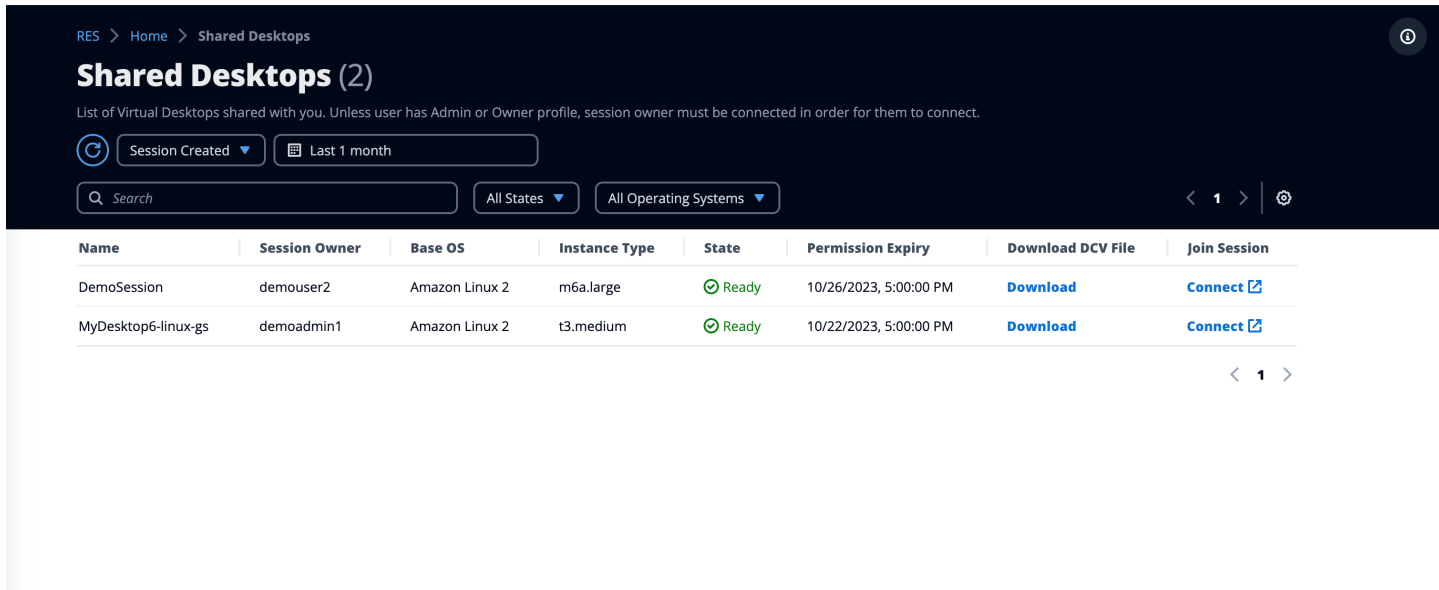
Stop All Day 

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.



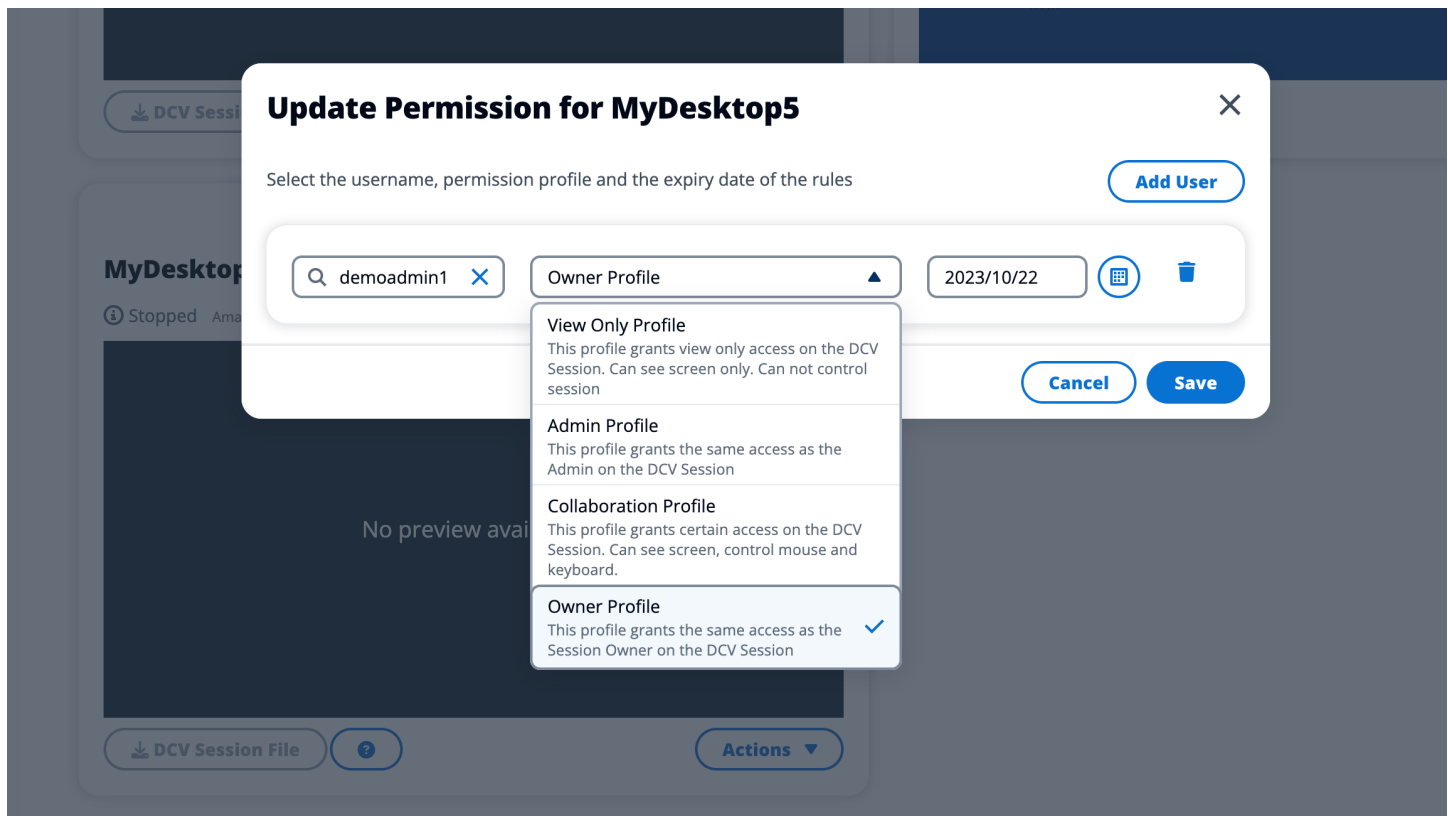
The screenshot shows the 'Shared Desktops' page in a web application. At the top, there's a breadcrumb trail: 'RES > Home > Shared Desktops'. The main heading is 'Shared Desktops (2)'. Below it, a note states: 'List of Virtual Desktops shared with you. Unless user has Admin or Owner profile, session owner must be connected in order for them to connect.' There are filters for 'Session Created' (dropdown) and 'Last 1 month' (calendar icon). A search bar with the placeholder 'Search' is present, along with filters for 'All States' and 'All Operating Systems'. The main content is a table with two rows of shared desktops. The table has columns: Name, Session Owner, Base OS, Instance Type, State, Permission Expiry, Download DCV File, and Join Session. The first row is 'DemoSession' owned by 'demouser2' on 'Amazon Linux 2' with instance type 'm6a.large', state 'Ready', and expiry '10/26/2023, 5:00:00 PM'. The second row is 'MyDesktop6-linux-gs' owned by 'demoadmin1' on 'Amazon Linux 2' with instance type 't3.medium', state 'Ready', and expiry '10/22/2023, 5:00:00 PM'. Both rows have 'Download' and 'Connect' links. A pagination control at the bottom right shows '< 1 >'.

Name	Session Owner	Base OS	Instance Type	State	Permission Expiry	Download DCV File	Join Session
DemoSession	demouser2	Amazon Linux 2	m6a.large	Ready	10/26/2023, 5:00:00 PM	Download	Connect
MyDesktop6-linux-gs	demoadmin1	Amazon Linux 2	t3.medium	Ready	10/22/2023, 5:00:00 PM	Download	Connect

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.



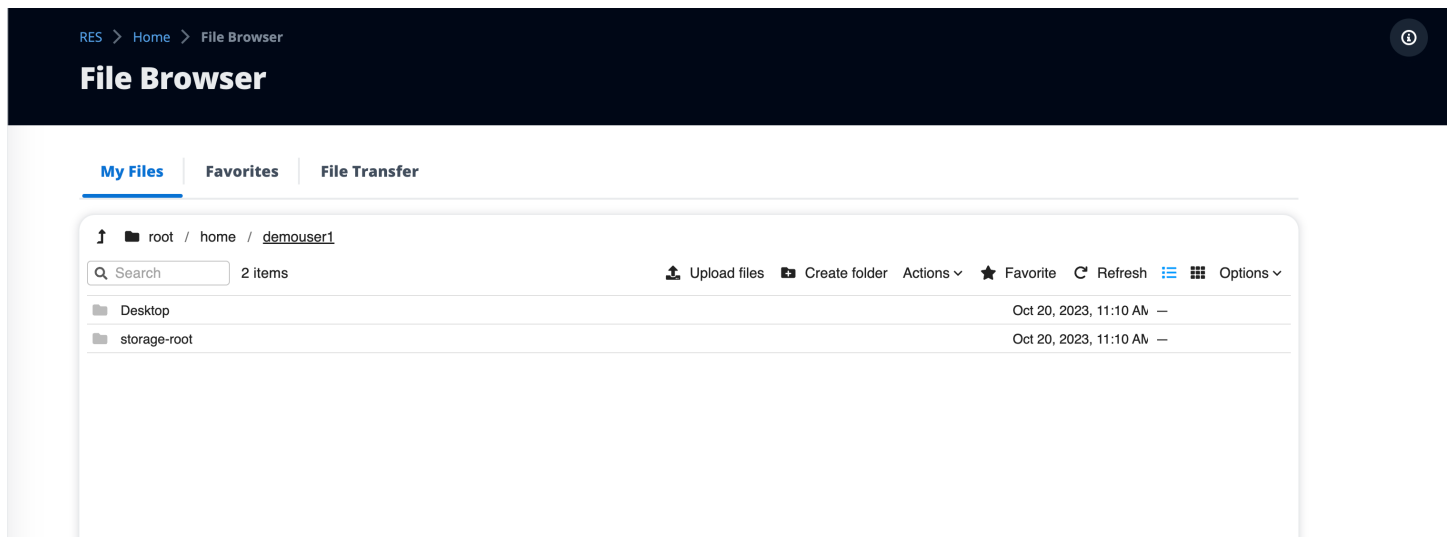
Pour plus d'informations sur les autorisations, consultez [the section called "Profils d'autorisation"](#).

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 dans [the 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 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)

RES > Home > File Browser

File Browser

My Files | **Favorites** | **File Transfer**

File Transfer Method

We recommend using below methods to transfer large files to your RES environment. Select an option below.

☒ **FileZilla**

Available for download on Windows, MacOS and Linux

☐ **WinSCP**

Available for download on Windows Only

☐ **AWS Transfer**

Your RES environment must be using Amazon EFS to use AWS Transfer

FileZilla

Step 1: Download FileZilla

- [Download FileZilla \(MacOS\)](#)
- [Download FileZilla \(Windows\)](#)
- [Download FileZilla \(Linux\)](#)

Step 2: Download Key File

[Download Key File \[*.pem\] \(MacOS / Linux\)](#)[Download Key File \[*.ppk\] \(Windows\)](#)

Step 3: Configure FileZilla

Open FileZilla and select **File > Site Manager** to create a new Site using below options:

Host [Redacted]	Port [Redacted]
Protocol SFTP	Logon Type Key File
User demouser3	Key File /path/to/key-file (downloaded in Step 2)

Save the settings and click **Connect**

Step 4: Connect and transfer file to FileZilla

During your first connection, you will be asked whether or not you want to trust [Redacted]. Check "Always Trust this Host" and Click "Ok".

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

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

Cette section contient des informations sur la façon de surveiller le système et de résoudre les problèmes spécifiques susceptibles de survenir.

Rubriques

- [Débogage et surveillance généraux](#)
- [Problème RunBooks](#)
- [Problèmes connus](#)

Contenu détaillé :

- [Débogage et surveillance généraux](#)
 - [Sources d'informations utiles sur les journaux et les événements](#)
 - [Fichiers journaux sur les EC2 instances Amazon de l'environnement](#)
 - [CloudFormation Piles](#)
 - [Défaillances du système dues à un problème et reflétées par l'activité du groupe Amazon EC2 Auto Scaling](#)
 - [Apparence typique de EC2 la console Amazon](#)
 - [Hôtes d'infrastructure](#)
 - [Hôtes d'infrastructure et bureaux virtuels](#)
 - [Hôtes en état de terminaison](#)
 - [Commandes utiles liées à Active Directory \(AD\) à titre de référence](#)
 - [Débogage de Windows DCV](#)
 - [Trouvez des informations sur la version DCV de NICE](#)
- [Problème RunBooks](#)
 - [Problèmes d'installation](#)
 - [AWS CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»](#)
 - [Notification par e-mail non reçue après la création AWS CloudFormation réussie des piles](#)
 - [Instances en cycle ou contrôleur VDC en état d'échec](#)

- [La CloudFormation pile d'environnements ne parvient pas à être supprimée en raison d'une erreur d'objet dépendant](#)
- [Erreur rencontrée pour le paramètre de bloc CIDR lors de la création de l'environnement](#)
- [CloudFormation échec de création de pile lors de la création de l'environnement](#)
- [La création d'une pile de ressources externes \(démon\) échoue avec AdDomainAdminNode CREATE_FAILED](#)
- [Problèmes de gestion des identités](#)
 - [Je ne suis pas autorisé à effectuer iam : PassRole](#)
 - [Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources](#)
 - [Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion](#)
 - [Erreur « Utilisateur introuvable » lors de la tentative de connexion](#)
 - [Utilisateur ajouté dans Active Directory, mais absent de RES](#)
 - [Utilisateur non disponible lors de la création d'une session](#)
 - [Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters](#)
- [Stockage](#)
 - [J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
 - [J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
 - [Je ne parviens pas à read/write le faire à partir d'hôtes VDI](#)
 - [Exemples de cas d'utilisation relatifs à la gestion des autorisations](#)
 - [J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine](#)
- [Instantanés](#)
 - [Un instantané a le statut Echoué](#)
 - [Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.](#)
- [Infrastructure](#)
 - [Groupes cibles d'équilibreur de charge dépourvus d'instances saines](#)
- [Lancement de bureaux virtuels](#)
 - [Un bureau virtuel qui fonctionnait auparavant ne peut plus se connecter correctement](#)

- [Je ne peux lancer que 5 bureaux virtuels](#)
- [Les tentatives de connexion Windows pour ordinateur de bureau échouent avec le message « La connexion a été fermée ». Erreur de transport »](#)
- [VDIs bloqué dans l'état de provisionnement](#)
- [VDIs passer à l'état d'erreur après le lancement](#)
- [Composant de bureau virtuel](#)
 - [L' EC2 instance Amazon s'affiche à plusieurs reprises comme terminée dans la console](#)
 - [L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API](#)
 - [Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter](#)
 - [Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init < > le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » \(où le compte est un nom d'utilisateur\)](#)
 - [Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »](#)
 - [Problèmes liés aux options DHCP avec la configuration d' external/customer AD](#)
 - [Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)
- [Suppression d'environnements](#)
 - [res-xxx-cluster pile dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement en raison de l'erreur « Le rôle n'est pas valide ou ne peut pas être assumé »](#)
 - [Collecte de journaux](#)
 - [Téléchargement des journaux VDI](#)
 - [Téléchargement de journaux depuis des EC2 instances Linux](#)
 - [Téléchargement de journaux à partir d' EC2 instances Windows](#)
 - [Collecte des journaux ECS pour l' WaitCondition erreur](#)
- [Environnement de démonstration](#)
 - [Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité](#)
- [Problèmes connus 2024.x](#)
 - [Problèmes connus 2024.x](#)

- [\(2024.06\) L'application d'un instantané échoue lorsque le nom du groupe AD contient des espaces](#)
- [\(2024.04-2024.04.02\) La limite d'autorisation IAM fournie n'est pas attachée au rôle des instances VDI](#)
- [\(2024.04.02 et versions antérieures\) Les instances Windows NVIDIA dans ap-southeast-2 \(Sydney\) ne démarrent pas](#)
- [\(2024.04 et 2024.04.01\) Échec de la suppression RES dans GovCloud](#)
- [\(2024.04 - 2024.04.02\) Le bureau virtuel Linux peut être bloqué à l'état « REPRISE » au redémarrage](#)
- [\(2024.04.02 et versions antérieures\) Impossible de synchroniser les utilisateurs AD dont l'attribut SAMAccount Name inclut des majuscules ou des caractères spéciaux](#)
- [\(2024.04.02 et versions antérieures\) La clé privée pour accéder à l'hôte Bastion n'est pas valide](#)
- [\(2024.06 et versions antérieures\) Les membres du groupe ne sont pas synchronisés avec RES lors de la synchronisation AD](#)
- [\(2024.06 et versions antérieures\) CVE-2024-6387, Regre, vulnérabilité de sécurité dans et Ubuntu SSHion RHEL9 VDIs](#)

Débogage et surveillance généraux

Cette section contient des informations sur l'endroit où les informations peuvent être trouvées dans RES.

- [Sources d'informations utiles sur les journaux et les événements](#)
 - [Fichiers journaux sur les EC2 instances Amazon de l'environnement](#)
 - [CloudFormation Piles](#)
 - [Défaillances du système dues à un problème et reflétées par l'activité du groupe Amazon EC2 Auto Scaling](#)
- [Apparence typique de EC2 la console Amazon](#)
 - [Hôtes d'infrastructure](#)
 - [Hôtes d'infrastructure et bureaux virtuels](#)
 - [Hôtes en état de terminaison](#)
- [Commandes utiles liées à Active Directory \(AD\) à titre de référence](#)

- [Débogage de Windows DCV](#)
- [Trouvez des informations sur la version DCV de NICE](#)

Sources d'informations utiles sur les journaux et les événements

Diverses sources d'informations conservées peuvent être référencées à des fins de dépannage et de surveillance.

Fichiers journaux sur les EC2 instances Amazon de l'environnement

Les fichiers journaux existent sur les EC2 instances Amazon utilisées par RES. Le gestionnaire de session SSM peut être utilisé pour ouvrir une session sur l'instance afin d'examiner ces fichiers.

Sur les instances d'infrastructure telles que le gestionnaire de clusters et le contrôleur vdc, les journaux d'applications et autres se trouvent aux emplacements suivants.

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

Sur un bureau virtuel Linux, les fichiers suivants contiennent des fichiers journaux utiles

- /var/log/dcv/
- /root/bootstrap/logs/userdata.journal
- /var/log/messages

Sur Windows, les journaux des instances de bureau virtuel se trouvent à l'adresse

- PS C : \ ProgramData \ n ice \ dcv \ log
- PS C : \ ProgramData \ n nice \ DCVSession ManagerAgent \ log

Sous Windows, la journalisation de certaines applications se trouve à l'adresse suivante :

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

Sous Windows, les fichiers du certificat DCV NICE se trouvent dans :

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

Groupes Amazon CloudWatch Log

Amazon EC2 et les ressources de AWS Lambda calcul enregistrent les informations dans Amazon CloudWatch Log Groups. Les entrées du journal qu'ils contiennent peuvent fournir des informations utiles pour résoudre des problèmes potentiels ou pour obtenir des informations générales.

Ces groupes sont nommés comme suit :

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

Lorsque vous examinez des groupes de journaux, il peut être utile de les filtrer à l'aide de chaînes majuscules et minuscules telles que les suivantes. Cela ne produira que les messages contenant les chaînes notées.

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

Une autre méthode de surveillance des problèmes consiste à créer des CloudWatch tableaux de bord Amazon contenant des widgets affichant les données qui vous intéressent.

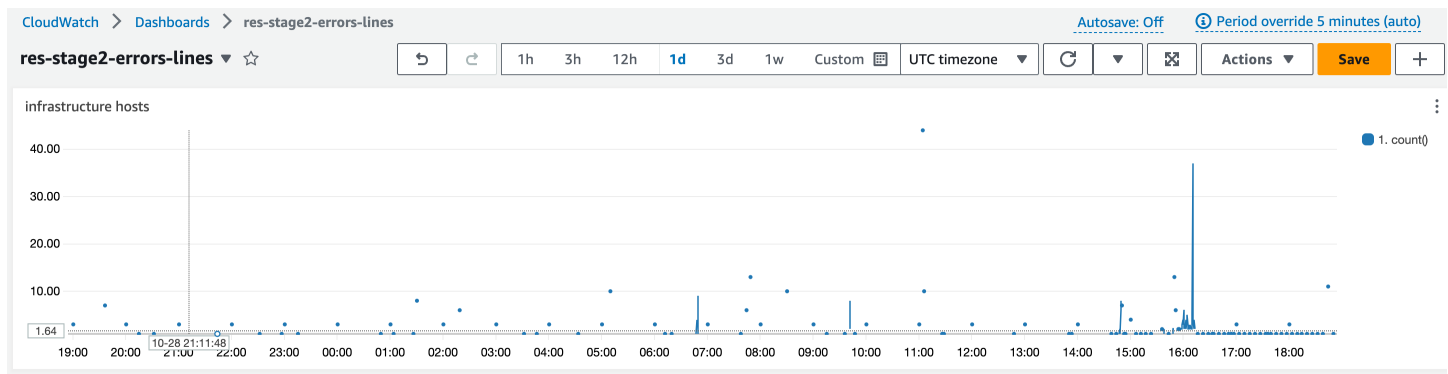
Un exemple consiste à créer un widget qui compte l'occurrence des chaînes error et ERROR et à les représenter graphiquement sous forme de lignes. Cette méthode permet de détecter plus facilement

l'apparition de problèmes ou de tendances potentiels indiquant qu'un changement de modèle s'est produit.

Voici un exemple de cela pour les hôtes d'infrastructure. Pour l'utiliser, concaténez les lignes de requête et remplacez les <region> attributs <envname> et par les valeurs appropriées.

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

Un exemple de tableau de bord peut apparaître comme suit :



CloudFormation Piles

Les CloudFormation piles créées lors de la création de l'environnement contiennent des informations sur les ressources, les événements et les sorties associées à la configuration de l'environnement.

Pour chacune des piles, l'onglet Événements, ressources et sorties peut être consulté pour obtenir des informations sur les piles.

piles RES :

- <envname>-sangle
- <envname>-grappe
- <envname>-métriques
- <envname>- service d'annuaire
- <envname>-fournisseur d'identité
- <envname>-stockage partagé
- <envname>-gestionnaire de clusters
- <envname>-vdc
- <envname>-bastion-hôte

Suite d'environnements de démonstration (si vous déployez un environnement de démonstration et que vous ne disposez pas de ces ressources externes, vous pouvez utiliser des recettes de calcul à AWS haute performance pour générer des ressources pour un environnement de démonstration.)

- <envname>
- <envname>-Réseautage
- <envname>- DirectoryService
- <envname>-Rangement
- <envname>- WindowsManagementHost

Défaillances du système dues à un problème et reflétées par l'activité du groupe Amazon EC2 Auto Scaling

Si le RES UIs indique des erreurs de serveur, cela peut être dû à un logiciel d'application ou à un autre problème.

Chacun des groupes d'autoscaling d' EC2 instance Amazon d'infrastructure (ASGs) contient un onglet **Activité** qui peut être utile pour détecter l'activité de dimensionnement des instances. Si les pages de l'interface utilisateur indiquent des erreurs ou ne sont pas accessibles, vérifiez la présence de plusieurs instances résiliées sur la EC2 console Amazon et consultez l'onglet **Auto Scaling Group Activity** pour l'ASG correspondant afin de déterminer si les EC2 instances Amazon sont cycliques.

Dans ce cas, utilisez le groupe de CloudWatch journaux Amazon associé à l'instance afin de déterminer si des erreurs susceptibles d'indiquer la cause du problème sont enregistrées. Il peut également être possible d'utiliser la console de session SSM pour ouvrir une session sur une instance en cours d'exécution de ce type et examiner les fichiers journaux de l'instance afin d'en déterminer la cause avant que l'instance ne soit marquée comme défectueuse et interrompue par l'ASG.

La console ASG peut afficher une activité similaire à celle qui suit si ce problème se produit.

The screenshot displays the Amazon EC2 console interface for an Auto Scaling Group (ASG) named **res-bicfn3-web-portal-e2958adc**. The left sidebar shows the navigation menu with categories like **Instances**, **Images**, **Elastic Block Store**, **Network & Security**, **Load Balancing**, and **Auto Scaling**. The **Load Balancing** section is highlighted, and the **Load Balancers** link is selected. The main content area shows the details of the ASG, including its ARN, target type (Instance), protocol (HTTPS), and port (8443). The **Health** section indicates that the ASG is **Healthy** with 1 healthy instance and 0 unhealthy instances. The **Registered targets** table shows one target with Instance ID **i-0ba5d508631f20043** and Name **res-bicfn3-cluster-manager**, which is in a **healthy** state.

Apparence typique de EC2 la console Amazon

Cette section contient des captures d'écran du système fonctionnant dans différents états.

Hôtes d'infrastructure

Lorsqu'aucun ordinateur de bureau n'est en cours d'exécution, la EC2 console Amazon ressemble généralement à ce qui suit. Les instances présentées sont l'infrastructure RES EC2 hébergée par Amazon. Le préfixe d'un nom d'instance est le nom de l'environnement RES.

Instances (5) Info

Find Instance by attribute or tag (case-sensitive)

res-stage2 Instance state = running Clear filters

☐	Name	Instance ID	Instance state	Instance type
☐	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
☐	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
☐	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
☐	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
☐	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

Hôtes d'infrastructure et bureaux virtuels

Dans la EC2 console Amazon, lorsque des bureaux virtuels sont en cours d'exécution, ils ressemblent à ce qui suit. Dans ce cas, les bureaux virtuels sont indiqués en rouge. Le suffixe du nom de l'instance est l'utilisateur qui a créé le poste de travail. Le nom au centre est le nom de session défini au moment du lancement. Il s'agit soit du « MyDesktop » par défaut, soit du nom défini par l'utilisateur.

Instances (7) Info

Find Instance by attribute or tag (case-sensitive)

res-stage2 Instance state = running Clear filters

☐	Name	Instance ID	Instance state	Instance type
☐	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
☐	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
☐	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
☐	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
☐	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
☐	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
☐	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

Hôtes en état de terminaison

Lorsque la EC2 console Amazon affiche des instances résiliées, il s'agit généralement d'hôtes de bureau qui ont été résiliés. Si la console inclut des hôtes d'infrastructure en état d'arrêt, en particulier s'il en existe plusieurs du même type, cela peut indiquer qu'un problème système est en cours.

L'image suivante montre les instances de bureau qui ont été mises hors service.

EC2 Dashboard

EC2 Global View

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

EC2 Block Store

Instances (10) Info

Find Instance by attribute or tag (case-sensitive)

res-stage2 Clear filters

☐	Name	Instance ID	Instance state		Instance type
☐	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running		m5.large
☐	res-stage2-vdc-broker	i-041867308771e71d3	Running		m5.large
☐	res-stage2-vdc-controller	i-08800976c757717e6	Running		m5.large
☐	res-stage2-windows1-demoadmin4	i-092cdf6a7e52e9b9a	Terminated		m6a.large
☐	res-stage2-rhel91-demoadmin4	i-0b3d134f606a53636	Terminated		m6a.large
☐	res-stage2-bastion-host	i-0523e5480f434581a	Running		m5.large
☐	res-stage2-aml21-demoadmin4	i-023844b29c12b9393	Terminated		m6a.large
☐	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running		m6a.large
☐	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running		m6a.large
☐	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running		m5.large

Commandes utiles liées à Active Directory (AD) à titre de référence

Vous trouverez ci-dessous des exemples de commandes liées au protocole LDAP qui peuvent être saisies sur les hôtes d'infrastructure pour afficher les informations relatives à la configuration AD. Le domaine et les autres paramètres utilisés doivent refléter ceux saisis au moment de la création de l'environnement.

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

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

Débogage de Windows DCV

Sur un poste de travail Windows, vous pouvez répertorier la session qui lui est associée à l'aide de ce qui suit :

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

Trouvez des informations sur la version DCV de NICE

NICE DCV est utilisé pour les sessions de bureau virtuel. [AWS JOLI DCV](#). Les exemples suivants montrent comment déterminer la version du logiciel DCV installée.

Linux

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

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

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

Windows

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

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

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

Problème RunBooks

La section suivante décrit les problèmes susceptibles de survenir, explique comment les détecter et propose des suggestions pour les résoudre.

- [Problèmes d'installation](#)
 - [AWS CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»](#)
 - [Notification par e-mail non reçue après la création AWS CloudFormation réussie des piles](#)
 - [Instances en cycle ou contrôleur VDC en état d'échec](#)

- [La CloudFormation pile d'environnements ne parvient pas à être supprimée en raison d'une erreur d'objet dépendant](#)
- [Erreur rencontrée pour le paramètre de bloc CIDR lors de la création de l'environnement](#)
- [CloudFormation échec de création de pile lors de la création de l'environnement](#)
- [La création d'une pile de ressources externes \(démon\) échoue avec AdDomainAdminNode CREATE_FAILED](#)
- [Problèmes de gestion des identités](#)
 - [Je ne suis pas autorisé à effectuer iam : PassRole](#)
 - [Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources](#)
 - [Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion](#)
 - [Erreur « Utilisateur introuvable » lors de la tentative de connexion](#)
 - [Utilisateur ajouté dans Active Directory, mais absent de RES](#)
 - [Utilisateur non disponible lors de la création d'une session](#)
 - [Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters](#)
- [Stockage](#)
 - [J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
 - [J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
 - [Je ne parviens pas à read/write le faire à partir d'hôtes VDI](#)
 - [Exemples de cas d'utilisation relatifs à la gestion des autorisations](#)
 - [J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine](#)
- [Instantanés](#)
 - [Un instantané a le statut Echoué](#)
 - [Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.](#)
- [Infrastructure](#)
 - [Groupes cibles d'équilibreur de charge dépourvus d'instances saines](#)
- [Lancement de bureaux virtuels](#)
 - [Un bureau virtuel qui fonctionnait auparavant ne peut plus se connecter correctement](#)
- [Je ne peux lancer que 5 bureaux virtuels](#)

- [Les tentatives de connexion Windows pour ordinateur de bureau échouent avec le message « La connexion a été fermée ». Erreur de transport »](#)
- [VDIs bloqué dans l'état de provisionnement](#)
- [VDIs passer à l'état d'erreur après le lancement](#)
- [Composant de bureau virtuel](#)
 - [L' EC2 instance Amazon s'affiche à plusieurs reprises comme terminée dans la console](#)
 - [L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API](#)
 - [Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter](#)
 - [Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init < > le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » \(où le compte est un nom d'utilisateur\)](#)
 - [Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »](#)
 - [Problèmes liés aux options DHCP avec la configuration d' external/customer AD](#)
 - [Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)
- [Suppression d'environnements](#)
 - [res-xxx-cluster pile dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement en raison de l'erreur « Le rôle n'est pas valide ou ne peut pas être assumé »](#)
 - [Collecte de journaux](#)
 - [Téléchargement des journaux VDI](#)
 - [Téléchargement de journaux depuis des EC2 instances Linux](#)
 - [Téléchargement de journaux à partir d' EC2 instances Windows](#)
 - [Collecte des journaux ECS pour l' WaitCondition erreur](#)
- [Environnement de démonstration](#)
 - [Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité](#)

Problèmes d'installation

- [AWS CloudFormation la pile ne parvient pas à être créée avec le message « message d'échec WaitCondition reçu ». Erreur : États. TaskFailed»](#)
- [Notification par e-mail non reçue après la création AWS CloudFormation réussie des piles](#)
- [Instances en cycle ou contrôleur VDC en état d'échec](#)
- [La CloudFormation pile d'environnements ne parvient pas à être supprimée en raison d'une erreur d'objet dépendant](#)
- [Erreur rencontrée pour le paramètre de bloc CIDR lors de la création de l'environnement](#)
- [CloudFormation échec de création de pile lors de la création de l'environnement](#)
- [La création d'une pile de ressources externes \(démon\) échoue avec AdDomainAdminNode CREATE_FAILED](#)

.....

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 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 création réussie des AWS CloudFormation piles, 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 EC2 console Amazon pour trouver des preuves de l'existence d'instances cycliques.

Si certaines EC2 instances Amazon avec le <envname> préfixe apparaissent comme terminées puis sont 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 de plus amples informations, veuillez consulter [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 bien rejoint 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 :

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.

```
[root@ip-10-3-144-194 ~]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
     Main PID: 31248 (sss)
    CGroup: /system.slice/sss.service
            └─31248 /usr/sbin/sss -i --logger=files
              └─31249 /usr/libexec/sss/sss_be --domain corp.res.com --uid 0 --gid 0 --logger=files
                └─31251 /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger=files
                  └─31252 /usr/libexec/sss/sss_pam --uid 0 --gid 0 --logger=files

Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
```

Might see "inactive"/"failed" here

Might see errors highlighted in RED here

Journal des erreurs SSM

Pour résoudre le problème :

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

Le problème peut avoir 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. Le dimensionnement automatique 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, sélectionnez Récupérer la valeur secrète et choisissez Texte en clair.
 - iv. Tâche de sélection Modifier.
 - v. Définissez un nouveau mot de passe pour l' ServiceAccount utilisateur et sélectionnez Enregistrer.
5. Si vous avez mis à jour la valeur, 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 `lavdcvhostsecuritygroup`, cela peut être dû à une EC2 instance Amazon lancée dans un sous-réseau ou un groupe de sécurité créé par RES à l'aide de la AWS console.

Pour résoudre le problème, recherchez et mettez fin à toutes les EC2 instances Amazon 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 (démon) 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 EC2 correctifs Amazon 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 :

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 RunCommand/Automation d'exécution du SSM, vérifiez si l'exécution d'un document SSM lié aux correctifs coïncide avec le lancement d'une instance.
3. Dans les fichiers journaux des EC2 instances Amazon 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 de 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

- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources](#)
- [Lorsque je me connecte à l'environnement, je reviens immédiatement à la page de connexion](#)
- [Erreur « Utilisateur introuvable » lors de la tentative de connexion](#)
- [Utilisateur ajouté dans Active Directory, mais absent de RES](#)
- [Utilisateur non disponible lors de la création d'une session](#)
- [Erreur de dépassement de la limite de taille dans le journal du gestionnaire de CloudWatch clusters](#)

.....

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à exécuter l'PassRole action iam :, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à RES.

Certains AWS services vous permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé marymajor essaie d'utiliser la console pour effectuer une action dans RES. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'effectuer l'PassRole action iam :. Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

.....

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mon studio de recherche et d'ingénierie sur les AWS ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir comment fournir un accès à vos ressources sur les AWS comptes que vous possédez, consultez la section [Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez](#) dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section [Fournir un accès aux AWS comptes détenus par des tiers](#) dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section [Fournir un accès aux utilisateurs authentifiés de manière externe \(fédération d'identité\)](#) dans le guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En [quoi les rôles IAM diffèrent des politiques basées sur les ressources dans le Guide de](#) l'utilisateur IAM.

.....

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 :

1. Ouvrez la [CloudWatch console](#).
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 :

1. Ouvrez la console [DynamoDB](#)
2. Dans Tables, recherchez la table nommée `<environment-name>.cluster-settings`.
3. Ouvrez le tableau et sélectionnez 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. Sélectionnez 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`.

Edit item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#)

Attribute name	Value
key - Partition key	identity-provider.cognito.sso_enabled

value ☐ True ☒ False

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

.....

Erreur « Utilisateur introuvable » lors de la tentative de connexion

Si un utilisateur reçoit le message d'erreur « Utilisateur introuvable » lorsqu'il essaie de se connecter à l'interface RES, alors que l'utilisateur est présent dans Active Directory :

- Si l'utilisateur n'est pas présent dans RES et que vous l'avez récemment ajouté à AD
 - Il est possible que l'utilisateur ne soit pas encore 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 dans [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 [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 qui importe 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](#).
2. Dans Files d'attente, sélectionnez `<environment-name>-cluster-manager-tasks.fifo`.
3. Sélectionnez 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 au cours des cinq minutes précédentes, 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.

.....

Stockage

Rubriques

- [J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
- [J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI](#)
- [Je ne parviens pas à read/write le faire à partir d'hôtes VDI](#)
- [J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine](#)

.....

J'ai créé le système de fichiers via RES mais il ne se monte pas sur les hôtes VDI

Les systèmes de fichiers doivent être dans l'état « Disponible » avant de pouvoir être montés par des hôtes VDI. Suivez les étapes ci-dessous pour vérifier que le système de fichiers est dans l'état requis.

Amazon EFS

1. Accédez à la [console Amazon EFS](#).
2. Vérifiez que l'état du système de fichiers est disponible.
3. Si l'état du système de fichiers n'est pas disponible, attendez avant de lancer les hôtes VDI.

1. Accédez à la [FSx console Amazon](#).
2. Vérifiez que le statut est disponible.
3. Si le statut n'est pas disponible, attendez avant de lancer les hôtes VDI.

.....

J'ai intégré un système de fichiers via RES mais il ne se monte pas sur les hôtes VDI

Les systèmes de fichiers intégrés à RES doivent avoir les règles de groupe de sécurité requises configurées pour permettre aux hôtes VDI de monter les systèmes de fichiers. Ces systèmes de fichiers étant créés en externe à RES, RES ne gère pas les règles de groupe de sécurité associées.

Le groupe de sécurité associé aux systèmes de fichiers intégrés doit autoriser le trafic entrant suivant :

- Trafic NFS (port : 2049) depuis les hôtes Linux VDC
- Trafic SMB (port : 445) depuis les hôtes Windows VDC

.....

Je ne parviens pas à read/write le faire à partir d'hôtes VDI

ONTAP prend en charge les styles de sécurité UNIX, NTFS et MIXED pour les volumes. Les styles de sécurité déterminent le type d'autorisations qu'ONTAP utilise pour contrôler l'accès aux données et le type de client qui peut modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole d'ONTAP. ONTAP utilise toutefois des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Exemples de cas d'utilisation relatifs à la gestion des autorisations

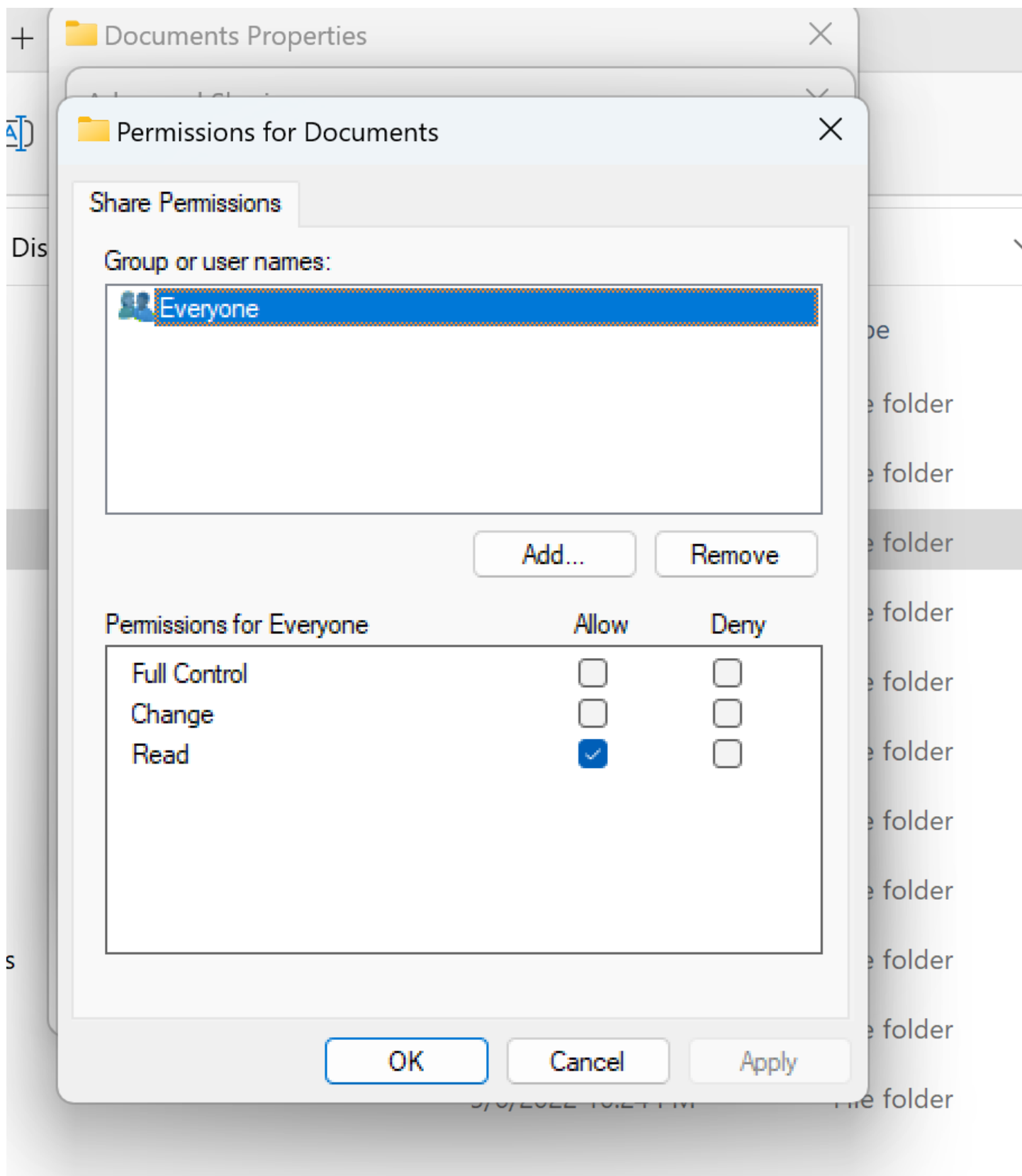
Utilisation d'un volume de style UNIX avec des charges de travail Linux

Les autorisations peuvent être configurées par le sudoer pour les autres utilisateurs. Par exemple, ce qui suit accorderait à tous les membres des read/write autorisations <group-ID> complètes sur le /<project-name> répertoire :

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

Utilisation d'un volume de style NTFS avec des charges de travail Linux et Windows

Les autorisations de partage peuvent être configurées à l'aide des propriétés de partage d'un dossier spécifique. Par exemple, pour un utilisateur user_01 et un dossier myfolder, vous pouvez définir des autorisations de Full ControlChange, ou Read pour Allow ou Deny :



Si le volume doit être utilisé à la fois par des clients Linux et Windows, nous devons configurer un mappage de noms sur la SVM qui associera tout nom d'utilisateur Linux au même nom d'utilisateur au format de nom de domaine NetBIOS de domaine \ nom d'utilisateur. Cela est nécessaire pour traduire entre les utilisateurs de Linux et de Windows. Pour référence, voir [Activation des charges de travail multiprotocoles avec Amazon FSx pour NetApp ONTAP](#).

.....

J'ai créé Amazon FSx pour NetApp ONTAP à partir de RES, mais il n'a pas rejoint mon domaine

Actuellement, lorsque vous créez Amazon FSx pour NetApp ONTAP à partir de la console RES, le système de fichiers est provisionné mais il ne rejoint pas le domaine. Pour associer la SVM du système de fichiers ONTAP créée à votre domaine, consultez [Joindre SVMs à un Microsoft Active Directory](#) et suivez les étapes indiquées sur la console [Amazon FSx](#). Assurez-vous que [les autorisations requises sont déléguées au compte Amazon FSx Service](#) dans AD. Une fois que la SVM a rejoint le domaine avec succès, allez dans Résumé de la SVM > Points de terminaison > Nom DNS SMB et copiez le nom DNS car vous en aurez besoin ultérieurement.

Une fois qu'elle est jointe au domaine, modifiez la clé de configuration DNS SMB dans le tableau DynamoDB des paramètres du cluster :

1. Accédez à la console [Amazon DynamoDB](#).
2. Sélectionnez Tables, puis choisissez <stack-name>-cluster-settings.
3. Sous Explorer les éléments du tableau, développez les filtres et entrez le filtre suivant :
 - Nom de l'attribut - clé
 - État : égal à
 - Valeur - shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns
4. Sélectionnez l'article renvoyé, puis Actions, Modifier l'article.
5. Mettez à jour la valeur avec le nom DNS SMB que vous avez copié précédemment.
6. Sélectionnez Enregistrer et fermez.

En outre, assurez-vous que le groupe de sécurité associé au système de fichiers autorise le trafic conformément aux recommandations de la section [Contrôle d'accès au système de fichiers avec Amazon VPC](#). Les nouveaux hôtes VDI utilisant le système de fichiers pourront désormais monter la SVM et le système de fichiers joints au domaine.

Vous pouvez également intégrer un système de fichiers existant déjà joint à votre domaine à l'aide de la fonctionnalité RES Onboard File System : dans Gestion de l'environnement, sélectionnez Systèmes de fichiers, Système de fichiers intégré.

.....

Instantanés

Rubriques

- [Un instantané a le statut Echoué](#)
 - [Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.](#)
-

Un instantané a le statut Echoué

Sur la page RES Snapshots, si un instantané a le statut Echec, vous pouvez en déterminer la cause en accédant au groupe de CloudWatch journaux Amazon du gestionnaire de clusters au moment où l'erreur s'est produite.

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

.....

Un instantané ne s'applique pas avec des journaux indiquant que les tables n'ont pas pu être importées.

Si un instantané pris à partir d'un environnement précédent ne s'applique pas dans un nouvel environnement, consultez les CloudWatch journaux du gestionnaire de clusters pour identifier le problème. Si le problème indique que les tables requises ne peuvent pas être importées, vérifiez que l'instantané est dans un état valide.

1. Téléchargez le fichier metadata.json et vérifiez que le ExportStatus statut des différentes tables est COMPLETED. Assurez-vous que le ExportManifest champ est défini dans les différentes tables. Si les champs ci-dessus ne sont pas définis, l'état de l'instantané n'est pas valide et ne peut pas être utilisé avec la fonctionnalité d'application d'un instantané.
2. Après avoir lancé la création d'un instantané, assurez-vous que le statut de l'instantané passe à TERMINÉ dans RES. Le processus de création d'un instantané prend de 5 à 10 minutes. Rechargez ou revisitez la page de gestion des instantanés pour vous assurer que le cliché a été créé avec succès. Cela garantira que l'instantané créé est dans un état valide.

.....

Infrastructure

Rubriques

- [Groupe cible d'équilibreur de charge dépourvu d'instances saines](#)

.....

Groupe cible d'équilibreur de charge dépourvu d'instances saines

Si des problèmes tels que des messages d'erreur du serveur apparaissent dans l'interface utilisateur ou si les sessions de bureau ne peuvent pas se connecter, cela peut indiquer un problème dans l'infrastructure EC2 des instances Amazon.

Les méthodes permettant de déterminer la source du problème consistent à vérifier d'abord dans la EC2 console Amazon la présence d' EC2 instances Amazon qui semblent se terminer à plusieurs reprises et être remplacées par de nouvelles instances. Si tel est le cas, la vérification des CloudWatch journaux Amazon peut en déterminer la cause.

Une autre méthode consiste à vérifier les équilibreurs de charge du système. Cela indique qu'il peut y avoir des problèmes avec le système si les équilibreurs de charge, trouvés sur la EC2 console Amazon, n'affichent aucune instance saine enregistrée.

Voici un exemple d'apparence normale :

The screenshot displays the AWS Management Console interface for a target group. The breadcrumb navigation at the top shows the path: EC2 > Target groups > res-bicfn3-web-portal-e2958adc. The main header identifies the target group as 'res-bicfn3-web-portal-e2958adc'. Below this, the 'Details' section provides information about the target group, including its type (Instance), protocol (HTTPS), port (8443), and VPC. A summary row shows the status of targets: Total targets (1), Healthy (1), Unhealthy (0), Unused (0), Initial (0), and Draining (0). The 'Distribution of targets by Availability Zone (AZ)' section is also visible. At the bottom, the 'Registered targets' table lists one target with the instance ID 'i-Oba5d508631f20043', name 'res-bicfn3-cluster-manager', port '8443', zone 'eu-central-1c', and a 'healthy' status.

Si l'entrée Healthy est 0, cela indique qu'aucune EC2 instance Amazon n'est disponible pour traiter les demandes.

Si l'entrée Unhealthy n'est pas égale à 0, cela indique qu'une EC2 instance Amazon est peut-être en cours de cycle. Cela peut être dû au fait que le logiciel d'application installé ne passe pas les tests de santé.

Si les entrées saines et malsaines sont toutes deux égales à 0, cela indique une erreur de configuration potentielle du réseau. Par exemple, les sous-réseaux public et privé peuvent ne pas avoir de correspondance AZs. Dans ce cas, un texte supplémentaire peut apparaître sur la console indiquant que l'état du réseau existe.

.....

Lancement de bureaux virtuels

Rubriques

- [Un bureau virtuel qui fonctionnait auparavant ne peut plus se connecter correctement](#)
- [Je ne peux lancer que 5 bureaux virtuels](#)
- [Les tentatives de connexion Windows pour ordinateur de bureau échouent avec le message « La connexion a été fermée ». Erreur de transport »](#)
- [VDIs bloqué dans l'état de provisionnement](#)

- [VDIs passer à l'état d'erreur après le lancement](#)

.....

Un bureau virtuel qui fonctionnait auparavant ne peut plus se connecter correctement

Si une connexion de bureau se ferme ou si vous ne pouvez plus vous y connecter, le problème peut être dû à la défaillance de l' EC2 instance Amazon sous-jacente ou à la résiliation ou à l'arrêt de l' EC2 instance Amazon en dehors de l'environnement RES. L'état de l'interface utilisateur d'administration peut continuer à indiquer qu'il est prêt, mais les tentatives de connexion échouent.

La EC2 console Amazon doit être utilisée pour déterminer si l'instance a été résiliée ou arrêtée. En cas d'arrêt, essayez de le redémarrer. Si l'état est résilié, un autre bureau devra être créé. Toutes les données stockées dans le répertoire personnel de l'utilisateur doivent toujours être disponibles au démarrage de la nouvelle instance.

Si l'instance qui a échoué précédemment apparaît toujours dans l'interface utilisateur d'administration, il peut être nécessaire de la fermer à l'aide de l'interface utilisateur d'administration.

.....

Je ne peux lancer que 5 bureaux virtuels

La limite par défaut du nombre de bureaux virtuels qu'un utilisateur peut lancer est de 5. Cela peut être modifié par un administrateur à l'aide de l'interface utilisateur d'administration comme suit :

- Accédez aux paramètres du bureau.
- Sélectionnez l'onglet Serveur.
- Dans le panneau DCV Session, cliquez sur l'icône d'édition à droite.
- Modifiez la valeur du champ Sessions autorisées par utilisateur à la nouvelle valeur souhaitée.
- Sélectionnez Submit (Envoyer).
- Actualisez la page pour confirmer que le nouveau paramètre est en place.

.....

Les tentatives de connexion Windows pour ordinateur de bureau échouent avec le message « La connexion a été fermée ». Erreur de transport »

Si une connexion de bureau Windows échoue avec le message d'erreur « La connexion a été fermée » s'affiche dans l'interface utilisateur. « Erreur de transport », la cause peut être due à un problème dans le logiciel du serveur DCV lié à la création de certificats sur l'instance Windows.

Le groupe de CloudWatch log Amazon <envname>/vdc/dcv-connection-gateway peut enregistrer l'erreur de tentative de connexion avec des messages similaires aux suivants :

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

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

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

Dans ce cas, une solution peut être d'utiliser le gestionnaire de session SSM pour ouvrir une connexion à l'instance Windows et supprimer les 2 fichiers relatifs aux certificats suivants :

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

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

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

Les fichiers doivent être automatiquement recréés et une tentative de connexion ultérieure peut réussir.

Si cette méthode résout le problème et si les nouveaux lancements de postes de travail Windows produisent la même erreur, utilisez la fonction Create Software Stack pour créer une nouvelle pile logicielle Windows de l'instance fixe avec les fichiers de certificat régénérés. Cela peut produire une pile logicielle Windows qui peut être utilisée pour des lancements et des connexions réussis.

.....

VDIs bloqué dans l'état de provisionnement

Si le lancement d'un poste de travail reste en état de provisionnement dans l'interface utilisateur d'administration, cela peut être dû à plusieurs raisons.

Pour en déterminer la cause, examinez les fichiers journaux de l'instance de bureau et recherchez les erreurs susceptibles d'être à l'origine du problème. Ce document contient une liste de fichiers journaux et de groupes de CloudWatch journaux Amazon contenant des informations pertinentes dans la section intitulée Sources d'informations utiles sur les journaux et les événements.

Les causes potentielles de ce problème sont les suivantes.

- L'identifiant AMI utilisé a été enregistré en tant que pile logicielle mais n'est pas pris en charge par RES.

Le script de provisionnement bootstrap n'a pas pu se terminer car l'AMI ne dispose pas de la configuration attendue ou de l'outillage requis. Les fichiers journaux de l'instance, par exemple `/root/bootstrap/logs/` sur une instance Linux, peuvent contenir des informations utiles à ce sujet. AMIs les identifiants extraits du AWS Marketplace peuvent ne pas fonctionner pour les instances de bureau RES. Ils doivent être testés pour confirmer s'ils sont pris en charge.

- Les scripts de données utilisateur ne sont pas exécutés lorsque l'instance de bureau virtuel Windows est lancée à partir d'une AMI personnalisée.

Par défaut, les scripts de données utilisateur s'exécutent une seule fois lors du lancement d'une EC2 instance Amazon. Si vous créez une AMI à partir d'une instance de bureau virtuel existante, puis que vous enregistrez une pile logicielle auprès de l'AMI et que vous essayez de lancer un autre bureau virtuel avec cette pile logicielle, les scripts de données utilisateur ne s'exécuteront pas sur la nouvelle instance de bureau virtuel.

Pour résoudre le problème, ouvrez une fenêtre de PowerShell commande en tant qu'administrateur sur l'instance de bureau virtuel d'origine que vous avez utilisée pour créer l'AMI, puis exécutez la commande suivante :

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

Créez ensuite une nouvelle AMI à partir de l'instance. Vous pouvez utiliser la nouvelle AMI pour enregistrer des piles de logiciels et lancer de nouveaux bureaux virtuels par la suite. Notez que vous pouvez également exécuter la même commande sur l'instance qui reste dans l'état de provisionnement et redémarrer l'instance pour corriger la session de bureau virtuel, mais vous rencontrerez à nouveau le même problème lors du lancement d'un autre bureau virtuel à partir de l'AMI mal configurée.

.....

VDIs passer à l'état d'erreur après le lancement

Problème possible 1 : le système de fichiers personnel possède un répertoire pour l'utilisateur avec différentes autorisations POSIX.

C'est peut-être le problème que vous rencontrez si les scénarios suivants sont vrais :

1. La version RES déployée est 2024.01 ou supérieure.
2. Lors du déploiement de la pile RES, l'attribut `EnableLdapIDMapping` a été défini sur `True`.
3. Le système de fichiers home spécifié lors du déploiement de la pile RES était utilisé dans une version antérieure à RES 2024.01 ou dans un environnement précédent avec `EnableLdapIDMapping` une valeur définie sur `False`

Étapes de résolution : supprimez les répertoires utilisateur du système de fichiers.

1. SSM vers l'hôte du gestionnaire de clusters.
2. `cd /home`.
3. `ls`- doit répertorier les répertoires dont les noms de répertoire correspondent aux noms d'utilisateur, tels `queadmin1`, `admin2`.. et ainsi de suite.
4. Supprimez les répertoires, `sudo rm -r 'dir_name'`. Ne supprimez pas les répertoires `ssm-user` et `ec2-user`.

5. Si les utilisateurs sont déjà synchronisés avec le nouvel environnement, supprimez ceux de l'utilisateur de la table DDB de l'utilisateur (sauf clusteradmin).
6. Lancez la synchronisation AD : `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` exécutez-la dans le gestionnaire de clusters Amazon. EC2
7. Redémarrez l'instance VDI dans l'Error état indiqué sur la page Web RES. Vérifiez que le VDI passe à l'Ready état en 20 minutes environ.

Composant de bureau virtuel

Rubriques

- [L' EC2 instance Amazon s'affiche à plusieurs reprises comme terminée dans la console](#)
- [L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API](#)
- [Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter](#)
- [Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init < > le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » \(où le compte est un nom d'utilisateur\)](#)
- [Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »](#)
- [Problèmes liés aux options DHCP avec la configuration d' external/customer AD](#)
- [Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING](#)

L' EC2 instance Amazon s'affiche à plusieurs reprises comme terminée dans la console

Si une instance d'infrastructure apparaît à plusieurs reprises comme étant terminée dans la EC2 console Amazon, la cause peut être liée à sa configuration et dépendre du type d'instance d'infrastructure. Les méthodes suivantes permettent d'en déterminer la cause.

Si l'instance vdc-controller affiche des états de terminaison répétés dans la EC2 console Amazon, cela peut être dû à une balise secrète incorrecte. Les secrets conservés par RES comportent

des balises utilisées dans le cadre des politiques de contrôle d'accès IAM associées aux EC2 instances Amazon de l'infrastructure. Si le contrôleur vdc fonctionne en cycle et que l'erreur suivante apparaît dans le groupe de CloudWatch journaux, cela peut être dû au fait qu'un secret n'a pas été correctement étiqueté. Notez que le secret doit être marqué comme suit :

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

Le message du CloudWatch journal Amazon correspondant à cette erreur s'affichera comme suit :

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

Vérifiez les balises de l' EC2 instance Amazon et confirmez qu'elles correspondent à la liste ci-dessus.

.....

L'instance vdc-controller est en cours de cycle car le module AD/eVDI ne parvient pas à rejoindre le module AD/eVDI et affiche un échec du contrôle de santé de l'API

Si le module eVDI échoue lors de son contrôle de santé, il affichera ce qui suit dans la section État de l'environnement.

Modules

Environment modules and status



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

Dans ce cas, le chemin général pour le débogage consiste à consulter les journaux du gestionnaire de clusters [CloudWatch](#). (Recherchez le groupe de journaux nommé <env-name>/cluster-manager.)

Problèmes possibles :

- Si les journaux contiennent le texte `Insufficient permissions`, assurez-vous que le ServiceAccount nom d'utilisateur indiqué lors de la création de la pile res est correctement orthographié.

Exemple de ligne de journal :

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

- Vous pouvez accéder au ServiceAccount nom d'utilisateur fourni lors du déploiement de RES depuis la [SecretsManager console](#). Trouvez le secret correspondant dans le gestionnaire de secrets et sélectionnez Récupérer le texte brut. Si le nom d'utilisateur est incorrect, sélectionnez

Modifier pour mettre à jour la valeur secrète. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances apparaîtront dans un état stable.

- Le nom d'utilisateur doit être ServiceAccount « » si vous utilisez les ressources créées par la [pile de ressources externes](#) fournie. Si le DisableADJoin paramètre a été défini sur False lors de votre déploiement de RES, assurez-vous que l'utilisateur ServiceAccount « » est autorisé à créer des objets informatiques dans l'AD.
- Si le nom d'utilisateur utilisé est correct, mais que les journaux contiennent le texteInvalid credentials, le mot de passe que vous avez saisi est peut-être erroné ou a expiré.

Exemple de ligne de journal :

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

- Vous pouvez lire le mot de passe que vous avez saisi lors de la création de l'environnement en accédant au secret qui stocke le mot de passe dans la [console Secrets Manager](#). Sélectionnez le secret (par exemple<env_name>directoryserviceServiceAccountPassword), puis sélectionnez Récupérer du texte brut.
- Si le mot de passe indiqué dans le secret est incorrect, sélectionnez Modifier pour mettre à jour sa valeur dans le secret. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances utiliseront le mot de passe mis à jour et apparaîtront dans un état stable.
- Si le mot de passe est correct, il se peut qu'il ait expiré dans l'Active Directory connecté. Vous devez d'abord réinitialiser le mot de passe dans Active Directory, puis mettre à jour le secret. Vous pouvez réinitialiser le mot de passe de l'utilisateur dans Active Directory à partir de la [console Directory Service](#) :
 1. Choisissez l'ID de répertoire approprié
 2. Sélectionnez Actions, Réinitialiser le mot de passe utilisateur, puis remplissez le formulaire avec le nom d'utilisateur (par exemple, ServiceAccount « ») et le nouveau mot de passe.
 3. Si le nouveau mot de passe est différent du mot de passe précédent, mettez-le à jour dans le secret Secret Manager correspondant (par exemple,<env_name>directoryserviceServiceAccountPassword.
 4. Arrêtez les instances actuelles de cluster-manager et de vdc-controller. Les nouvelles instances apparaîtront dans un état stable.

.....

Le projet n'apparaît pas dans le menu déroulant lorsque vous modifiez la Suite logicielle pour l'ajouter

Ce problème peut être lié au problème suivant associé à la synchronisation du compte utilisateur avec AD. Si ce problème apparaît, vérifiez la présence de l'erreur `<user-home-init> account not available yet. waiting for user to be synced` « » dans le groupe de journaux CloudWatch Amazon du gestionnaire de clusters afin de déterminer si la cause est identique ou liée.

.....

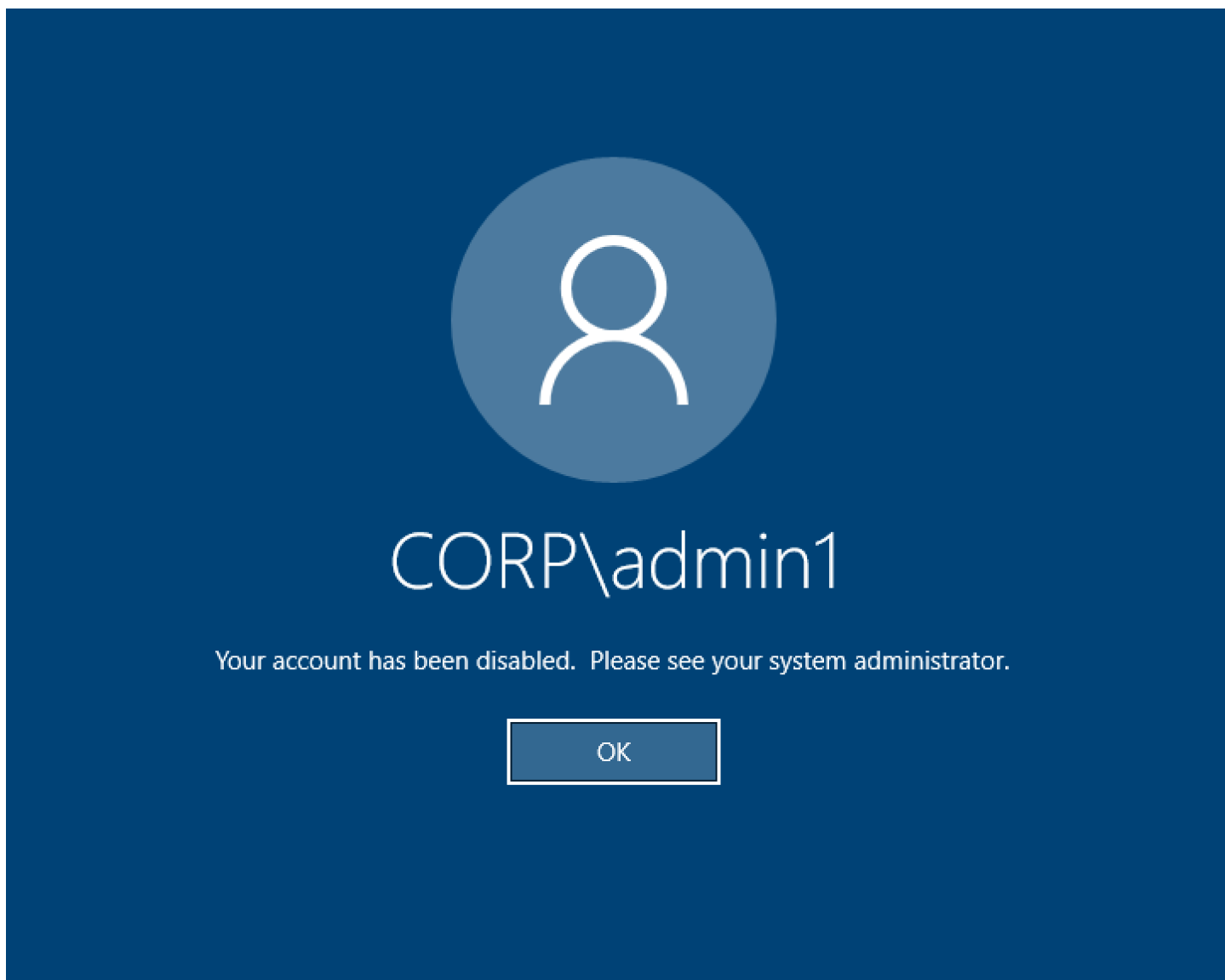
Le journal CloudWatch Amazon du gestionnaire de clusters indique que « user-home-init < > le compte n'est pas encore disponible. En attente de synchronisation de l'utilisateur » (où le compte est un nom d'utilisateur)

L'abonné SQS est occupé et bloqué dans une boucle infinie car il ne peut pas accéder au compte utilisateur. Ce code est déclenché lorsque vous essayez de créer un système de fichiers personnel pour un utilisateur lors de la synchronisation utilisateur.

La raison pour laquelle il ne parvient pas à accéder au compte utilisateur peut être que RES n'a pas été configuré correctement pour l'AD utilisé. Par exemple, le `ServiceAccountUsername` paramètre utilisé lors de la création de BI/RES l'environnement n'était pas la bonne valeur, par exemple en utilisant « `ServiceAccount` » au lieu de « `Admin` ».

.....

Lors de la tentative de connexion, Windows Desktop indique « Votre compte a été désactivé. Veuillez consulter votre administrateur. »



Si l'utilisateur ne parvient pas à se reconnecter à un écran verrouillé, cela peut indiquer qu'il a été désactivé dans l'AD configuré pour RES après s'être connecté avec succès via SSO.

La connexion SSO devrait échouer si le compte utilisateur a été désactivé dans AD.

.....

Problèmes liés aux options DHCP avec la configuration d' external/customer AD

Si vous rencontrez un message d'erreur indiquant que "The connection has been closed. Transport error" vous utilisez les bureaux virtuels Windows lorsque vous utilisez RES avec

vosre propre Active Directory, consultez le CloudWatch journal dcv-connection-gateway Amazon pour trouver un résultat similaire à ce qui suit :

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

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

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

Si vous utilisez un contrôleur de domaine AD pour vos options DHCP pour votre propre VPC, vous devez :

1. Ajoutez le AmazonProvided DNS aux deux contrôleurs de domaine IPs.
2. Définissez le nom de domaine sur ec2.internal.

Un exemple est présenté ici. Sans cette configuration, le bureau Windows vous donnera une erreur de transport, car il RES/DCV recherche le nom d'hôte ip-10-0-x-xx.ec2.internal.

Domain name

 ec2.internal

Domain name servers

 10.0.2.168, 10.0.3.228,
AmazonProvidedDNS

.....

Erreur Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Lorsque vous utilisez le navigateur Web Firefox, le message d'erreur de type MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING peut s'afficher lorsque vous essayez de vous connecter à un bureau virtuel.

[Cela est dû au fait que le serveur Web RES est configuré avec TLS + Stapling On mais ne répond pas à la validation par agrafage \(voir https://support.mozilla.org/en-US/questions/1372483\).](https://support.mozilla.org/en-US/questions/1372483)

Vous pouvez résoudre ce problème en suivant les instructions disponibles sur : https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing.

.....

Suppression d'environnements

Rubriques

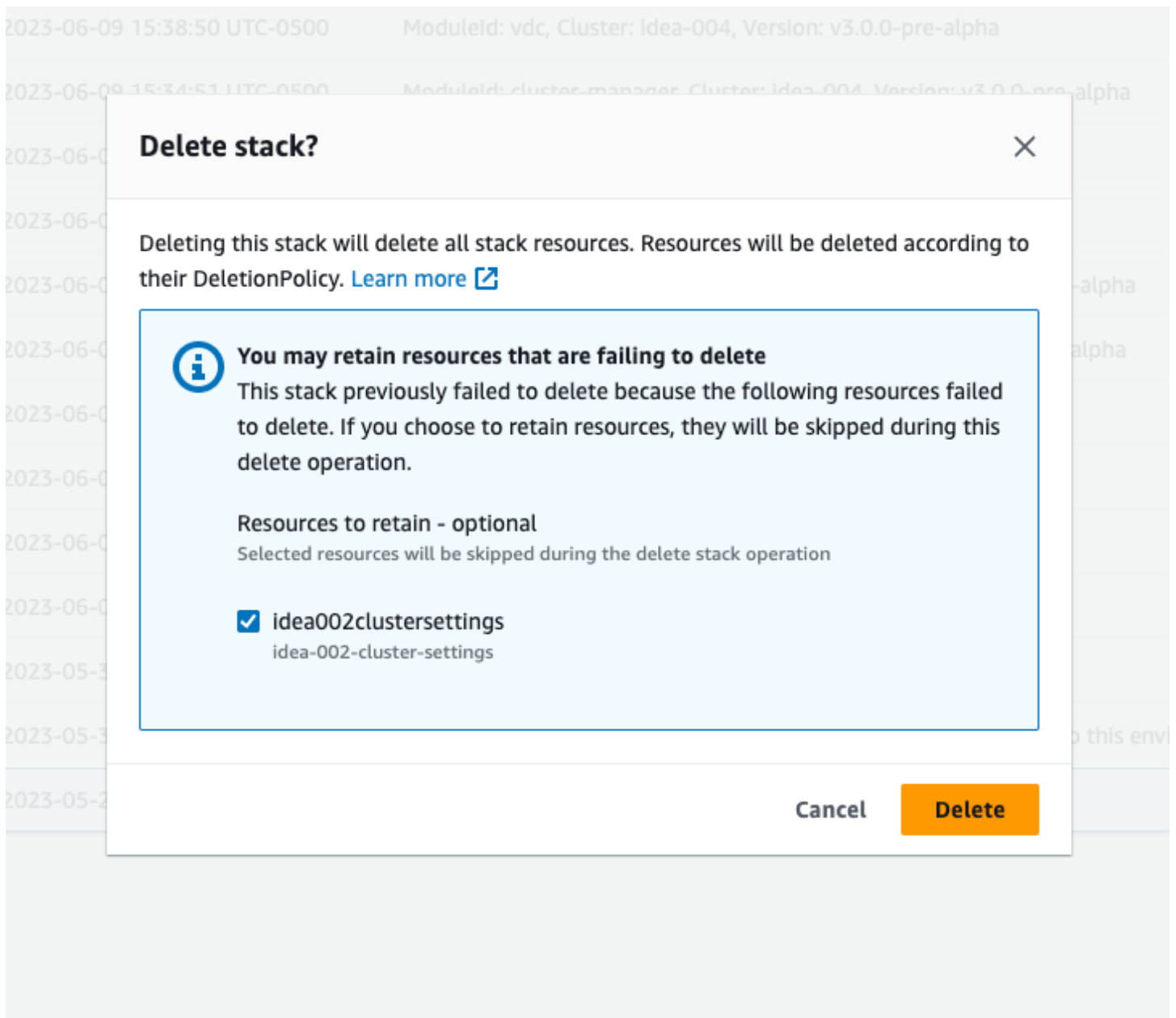
- [res-xxx-cluster pile dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement en raison de l'erreur « Le rôle n'est pas valide ou ne peut pas être assumé »](#)
- [Collecte de journaux](#)
- [Téléchargement des journaux VDI](#)
- [Téléchargement de journaux depuis des EC2 instances Linux](#)
- [Téléchargement de journaux à partir d' EC2 instances Windows](#)
- [Collecte des journaux ECS pour l' WaitCondition erreur](#)

.....

res-xxx-cluster pile dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement en raison de l'erreur « Le rôle n'est pas valide ou ne peut pas être assumé »

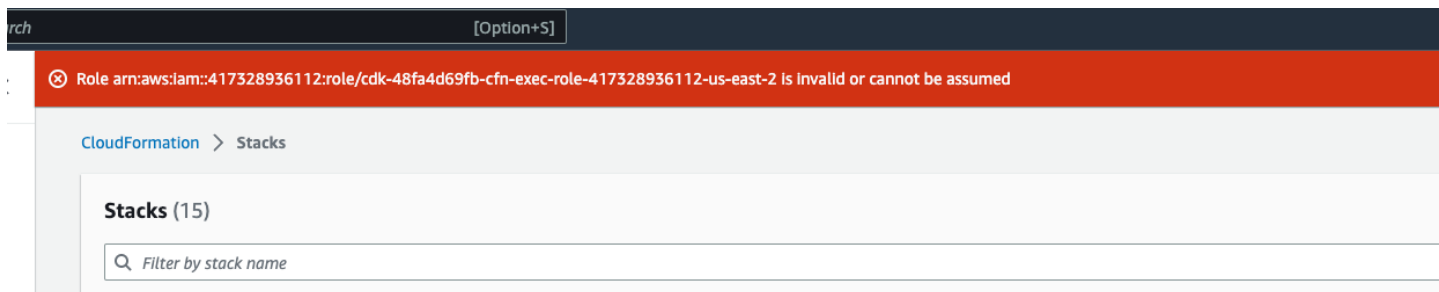
Si vous remarquez que la pile « res-xxx-cluster » est dans l'état « DELETE_FAILED » et ne peut pas être supprimée manuellement, vous pouvez effectuer les étapes suivantes pour la supprimer.

Si vous voyez la pile dans un état « DELETE_FAILED », essayez d'abord de la supprimer manuellement. Une boîte de dialogue confirmant Delete Stack peut s'afficher. Sélectionnez Delete (Supprimer).



Parfois, même si vous supprimez toutes les ressources de pile requises, vous pouvez toujours voir le message vous demandant de sélectionner les ressources à conserver. Dans ce cas, sélectionnez toutes les ressources comme « ressources à conserver » et sélectionnez Supprimer.

Vous pouvez voir un message d'erreur qui ressemble à `Role: arn:aws:iam:... is Invalid or cannot be assumed`



Cela signifie que le rôle requis pour supprimer la pile a été supprimé avant la pile. Pour contourner ce problème, copiez le nom du rôle. Accédez à la console IAM et créez un rôle portant ce nom à l'aide des paramètres indiqués ici, à savoir :

- Pour Type d'entité de confiance, sélectionnez AWS service.
- Pour Cas d'utilisation, sous Use cases for other AWS services Choisir CloudFormation.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allow users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

- ☐ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **Lambda**
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

CloudFormation

- ☒ **CloudFormation**
Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

Cancel Next

Sélectionnez Suivant. Assurez-vous d'accorder les autorisations aux rôles `AWSCloudFormationFullAccess` et `AdministratorAccess`. Votre page d'évaluation doit ressembler à ceci :

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

cdk-48fa4d69b-cfn-exec-role-417328936112-us-east-2

Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters.

Description

Add a short explanation for this role.

Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Step 1: Select trusted entities

Edit

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "",
6-       "Effect": "Allow",
7-       "Principal": {
8-         "Service": "cloudformation.amazonaws.com"
9-       },
10-      "Action": "sts:AssumeRole"
11-     }
12-   ]
13- }
```

Step 2: Add permissions

Edit

Permissions policy summary		
Policy name ?	Type	Attached as
AWSCloudFormationFullAccess	AWS managed	Permissions policy
AdministratorAccess	AWS managed - job function	Permissions policy

Tags

Retournez ensuite sur la CloudFormation console et supprimez la pile. Vous devriez maintenant être en mesure de le supprimer depuis que vous avez créé le rôle. Enfin, accédez à la console IAM et supprimez le rôle que vous avez créé.

Collecte de journaux

Connexion à une EC2 instance depuis la EC2 console

- Suivez [ces instructions](#) pour vous connecter à votre EC2 instance Linux.
- Suivez [ces instructions](#) pour vous connecter à votre EC2 instance Windows. Ouvrez ensuite Windows PowerShell pour exécuter n'importe quelle commande.

Collecte des journaux des hôtes de l'infrastructure

1. Cluster-manager : récupérez les journaux du gestionnaire de cluster aux emplacements suivants et joignez-les au ticket.
 - a. Tous les journaux du groupe de CloudWatch journaux<env-name>/cluster-manager.
 - b. Tous les journaux situés dans le /root/bootstrap/logs répertoire de l'<env-name>-cluster-manager EC2 instance. Suivez les instructions liées à la section « Connexion à une

EC2 instance depuis la EC2 console » au début de cette section pour vous connecter à votre instance.

2. Contrôleur VDC : récupérez les journaux du contrôleur VDC aux emplacements suivants et joignez-les au ticket.
 - a. Tous les journaux du groupe de CloudWatch journaux<env-name>/vdc-controller.
 - b. Tous les journaux situés dans le /root/bootstrap/logs répertoire de l'<env-name>-vdc-controller EC2 instance. Suivez les instructions liées à la section « Connexion à une EC2 instance depuis la EC2 console » au début de cette section pour vous connecter à votre instance.

L'un des moyens d'obtenir facilement les journaux est de suivre les instructions de la [Téléchargement de journaux depuis des EC2 instances Linux](#) section. Le nom du module serait le nom de l'instance.

Collecte des journaux VDI

Identifiez l' EC2 instance Amazon correspondante

Si un utilisateur lançait un VDI avec un nom de session VDI1, le nom correspondant de l'instance sur la EC2 console Amazon serait <env-name>-VDI1-<user name>.

Collectez les journaux VDI Linux

Connectez-vous à l' EC2 instance Amazon correspondante depuis la EC2 console Amazon en suivant les instructions indiquées dans la section « Connexion à une EC2 instance depuis la EC2 console » au début de cette section. Accédez à tous les journaux dans les /var/log/dcv/ répertoires /root/bootstrap/logs et de l' EC2 instance Amazon VDI.

L'un des moyens d'obtenir les journaux serait de les télécharger sur s3, puis de les télécharger à partir de là. Pour cela, vous pouvez suivre ces étapes pour obtenir tous les journaux dans un répertoire, puis les télécharger :

1. Procédez comme suit pour copier les journaux DCV dans le /root/bootstrap/logs répertoire :

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

2. Maintenant, suivez les étapes répertoriées dans la section suivante [Téléchargement des journaux VDI](#) pour télécharger les journaux.

Collectez les journaux Windows VDI

Connectez-vous à l' EC2 instance Amazon correspondante depuis la EC2 console Amazon en suivant les instructions indiquées dans la section « Connexion à une EC2 instance depuis la EC2 console » au début de cette section. Obtenez tous les journaux dans le `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` répertoire de l' EC2 instance VDI.

L'un des moyens d'obtenir les journaux serait de les télécharger sur S3, puis de les télécharger à partir de là. Pour ce faire, suivez les étapes répertoriées dans la section suivante-[Téléchargement des journaux VDI](#).

.....

Téléchargement des journaux VDI

1. Mettez à jour le rôle IAM de l' EC2 instance VDI pour autoriser l'accès à S3.
2. Accédez à la EC2 console et sélectionnez votre instance VDI.
3. Sélectionnez le rôle IAM qu'il utilise.
4. Dans la section Politiques d'autorisation du menu déroulant Ajouter des autorisations, sélectionnez Joindre des politiques, puis choisissez la politique AmazonS3 FullAccess.
5. Sélectionnez Ajouter des autorisations pour joindre cette politique.
6. Ensuite, suivez les étapes ci-dessous en fonction de votre type de VDI pour télécharger les journaux. Le nom du module serait le nom de l'instance.
 - a. [Téléchargement de journaux depuis des EC2 instances Linux](#) pour Linux.
 - b. [Téléchargement de journaux à partir d' EC2 instances Windows](#) pour Windows.
7. Enfin, modifiez le rôle pour supprimer la AmazonS3FullAccess politique.

Note

Ils VDI utilisent tous le même rôle IAM qui est `<env-name>-vdc-host-role-<region>`

.....

Téléchargement de journaux depuis des EC2 instances Linux

Connectez-vous à l' EC2 instance à partir de laquelle vous souhaitez télécharger les journaux et exécutez les commandes suivantes pour télécharger tous les journaux dans un compartiment s3 :

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

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

Ensuite, accédez à la console S3, sélectionnez le bucket avec son nom `<environment_name>-cluster-<region>-<aws_account_number>` et téléchargez le `<module_name>_logs.tar.gz` fichier précédemment téléchargé.

.....

Téléchargement de journaux à partir d' EC2 instances Windows

Connectez-vous à l' EC2 instance à partir de laquelle vous souhaitez télécharger les journaux et exécutez les commandes suivantes pour télécharger tous les journaux dans un compartiment S3 :

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

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

Ensuite, accédez à la console S3, sélectionnez le bucket avec son nom `<environment_name>-cluster-<region>-<aws_account_number>` et téléchargez le `<module_name>_logs.zip` fichier précédemment téléchargé.

.....

Collecte des journaux ECS pour l' WaitCondition erreur

1. Accédez à la pile déployée et choisissez l'onglet Ressources.
2. Développez Deploy ResearchAndEngineeringStudio → → Installer → Tâches CreateTaskDef → CreateContainer → → LogGroup, puis sélectionnez le groupe de journaux pour ouvrir CloudWatch les journaux.
3. Récupérez le dernier journal de ce groupe de journaux.

.....

Environnement de démonstration

Rubriques

- [Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité](#)

.....

Erreur de connexion à l'environnement de démonstration lors du traitement de la demande d'authentification auprès du fournisseur d'identité

Problème

Si vous essayez de vous connecter et que vous recevez une « erreur inattendue lors du traitement de la demande d'authentification auprès du fournisseur d'identité », vos mots de passe ont peut-être expiré. Il peut s'agir du mot de passe de l'utilisateur sous lequel vous essayez de vous connecter ou de votre compte Active Directory Service.

Mitigation

1. Réinitialisez les mots de passe de l'utilisateur et du compte de service dans la [console du service d'annuaire](#).

2. Mettez à jour les mots de passe des comptes de service dans [Secrets Manager](#) pour qu'ils correspondent au nouveau mot de passe que vous avez saisi ci-dessus :
 - pour la pile Keycloak : -... PasswordSecret - RESExternal-... - DirectoryService-... avec description : mot de passe pour Microsoft Active Directory
 - pour RES : res- ServiceAccountPassword -... avec description : mot de passe du compte Active Directory Service
 3. Accédez à la [EC2 console](#) et mettez fin à l'instance du gestionnaire de clusters. Les règles Auto Scaling déclencheront automatiquement le déploiement d'une nouvelle instance.
-

Problèmes connus

- [Problèmes connus 2024.x](#)
 - [\(2024.06\) L'application d'un instantané échoue lorsque le nom du groupe AD contient des espaces](#)
 - [\(2024.04-2024.04.02\) La limite d'autorisation IAM fournie n'est pas attachée au rôle des instances VDI](#)
 - [\(2024.04.02 et versions antérieures\) Les instances Windows NVIDIA dans ap-southeast-2 \(Sydney\) ne démarrent pas](#)
 - [\(2024.04 et 2024.04.01\) Échec de la suppression RES dans GovCloud](#)
 - [\(2024.04 - 2024.04.02\) Le bureau virtuel Linux peut être bloqué à l'état « REPRISE » au redémarrage](#)
 - [\(2024.04.02 et versions antérieures\) Impossible de synchroniser les utilisateurs AD dont l'attribut SAMAccount Name inclut des majuscules ou des caractères spéciaux](#)
 - [\(2024.04.02 et versions antérieures\) La clé privée pour accéder à l'hôte Bastion n'est pas valide](#)
 - [\(2024.06 et versions antérieures\) Les membres du groupe ne sont pas synchronisés avec RES lors de la synchronisation AD](#)
 - [\(2024.06 et versions antérieures\) CVE-2024-6387, Regre, vulnérabilité de sécurité dans et Ubuntu SSHion RHEL9 VDIs](#)

Problèmes connus 2024.x

.....

(2024.06) L'application d'un instantané échoue lorsque le nom du groupe AD contient des espaces

Problème

RES 2024.06 ne parvient pas à appliquer les instantanés des versions précédentes si les noms des groupes AD contiennent des espaces.

Les journaux du gestionnaire de clusters (sous le <environment-name>/cluster-manager groupe de CloudWatch journaux) incluront l'erreur suivante lors de la synchronisation AD :

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

L'erreur est due au fait que RES n'accepte que les noms de groupes répondant aux exigences suivantes :

- Il ne peut contenir que des lettres ASCII minuscules et majuscules, des chiffres, un tiret (-), un point (.) et un trait de soulignement (_)
- Le tiret (-) n'est pas autorisé comme premier caractère
- Il ne doit pas contenir d'espace.

Versions concernées

2024,06

Mitigation

1. Pour télécharger le script de correctif et le fichier de correctif ([patch.py](#) et [groupname_regex.patch](#)), exécutez la commande suivante, en les <output-directory> remplaçant par le répertoire dans lequel vous souhaitez placer les fichiers et par le nom de votre environnement <environment-name> RES :
 - a. Le correctif ne s'applique qu'à RES 2024.06

- b. [Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.](#)
- c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES :

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

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

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante :

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

3. Pour redémarrer l'instance de Cluster Manager pour votre environnement, exécutez les commandes suivantes : Vous pouvez également mettre fin à l'instance depuis Amazon EC2 Management Console.

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

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

Note

Le correctif permet aux noms de groupes AD de contenir des lettres ASCII minuscules et majuscules, des chiffres, des tirets (-), des points (.), des traits de soulignement (_) et des espaces d'une longueur totale comprise entre 1 et 30 inclus.

(2024.04-2024.04.02) La limite d'autorisation IAM fournie n'est pas attachée au rôle des instances VDI

Le problème

Les sessions de bureau virtuel n'héritent pas correctement de la configuration des limites d'autorisation de leur projet. Cela est dû au fait que la limite d'autorisations définie par le paramètre IAMPermission Boundary n'a pas été correctement attribuée à un projet lors de sa création.

Versions concernées

2024,04 - 2024,04.02

Mitigation

Suivez ces étapes pour VDIs hériter correctement de la limite d'autorisations attribuée à un projet :

1. Pour télécharger le script de correctif et le fichier de correctif ([patch.py](#) et [vdi_host_role_permission_boundary.patch](#)), exécutez la commande suivante, en les remplaçant par le répertoire local dans lequel vous souhaitez placer les fichiers : `<output-directory>`
 - a. Le correctif ne s'applique qu'à RES 2024.04.02. Si vous utilisez la version 2024.04 ou 2024.04.01, vous pouvez suivre les [étapes répertoriées dans le document public pour les mises à jour de version mineures afin de mettre à jour votre environnement vers la version 2024.04.02](#).
 - b. [Le script de correctif nécessite AWS CLI \(v2\), Python 3.9.16 ou supérieur et Boto3](#).
 - c. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

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

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

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

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES :

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

3. Redémarrez l'instance de cluster-manager dans votre environnement en exécutant cette commande, en la `<environment-name>` remplaçant par le nom de votre environnement RES. Vous pouvez également mettre fin à l'instance depuis l'Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

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

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

.....

(2024.04.02 et versions antérieures) Les instances Windows NVIDIA dans ap-southeast-2 (Sydney) ne démarrent pas

Le problème

Les Amazon Machine Images (AMIs) sont utilisées pour créer des bureaux virtuels (VDIs) dans RES avec des configurations spécifiques. Chaque AMI possède un identifiant associé qui diffère selon les régions. L'ID AMI configuré dans RES pour lancer des instances Windows Nvidia dans ap-southeast-2 (Sydney) est actuellement incorrect.

L'AMI-ID `ami-0e190f8939a996caf` pour ce type de configuration d'instance n'est pas correctement répertorié dans ap-southeast-2 (Sydney). L'ID AMI `ami-027cf6e71e2e442f4` doit être utilisé à la place.

Les utilisateurs obtiendront le message d'erreur suivant lorsqu'ils essaieront de lancer une instance avec l'`ami-0e190f8939a996caf` AMI par défaut.

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

Étapes pour reproduire le bogue, y compris un exemple de fichier de configuration :

- Déployez RES dans la région ap-southeast-2.
- Lancez une instance à l'aide de la pile logicielle par défaut Windows-NVIDIA (ID `ami-0e190f8939a996caf` AMI).

Versions concernées

Toutes les versions de RES 2024.04.02 ou antérieures sont concernées

Mitigation

Les mesures d'atténuation suivantes ont été testées sur la version RES 2024.01.01 :

- Enregistrez une nouvelle pile logicielle avec les paramètres suivants
 - ID D'AMI : `ami-027cf6e71e2e442f4`
 - Système d'exploitation : Windows
 - Fabricant du GPU : NVIDIA
 - Minimum. Taille de stockage (Go) : 30
 - Minimum. RAM (GO) : 4
- Utilisez cette pile logicielle pour lancer des instances Windows-NVIDIA

.....

(2024.04 et 2024.04.01) Échec de la suppression RES dans GovCloud

Le problème

Pendant le processus de suppression RES, le `UnprotectCognitoUserPool` Lambda désactive la protection contre la suppression pour les groupes d'utilisateurs de Cognito qui seront supprimés ultérieurement. L'exécution Lambda est démarrée par le `InstallerStateMachine`

En raison des différences de version de la AWS CLI par défaut entre la version commerciale et les GovCloud régions, l'`update_user_pool` appel dans le Lambda échouera dans les GovCloud régions.

Les clients recevront le message d'erreur suivant lorsqu'ils tenteront de supprimer RES dans une GovCloud région :

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection\n\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,\nSmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,\nVerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,\nDeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,\nAdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Étapes pour reproduire le bogue :

- Déployer RES dans une GovCloud région
- Supprimer la pile RES

Versions concernées

Versions RES 2024.04 et 2024.04.01

Mitigation

Les mesures d'atténuation suivantes ont été testées sur la version 2024.04 de RES :

- Ouvrez le `UnprotectCognitoUserPool` Lambda
 - Convention de dénomination : `<env-name>-InstallTasksUnprotectCognitoUserPool-...`
- Paramètres d'exécution -> Modifier -> Sélectionnez Runtime Python 3.11 -> Enregistrer.
- Ouverte CloudFormation.
- Supprimer la pile RES -> laisser Retain Installer Resource NON COCHÉE -> Supprimer.

.....

(2024.04 - 2024.04.02) Le bureau virtuel Linux peut être bloqué à l'état « REPRISE » au redémarrage

Le problème

Les bureaux virtuels Linux peuvent rester bloqués à l'état « REPRISE » lors du redémarrage après un arrêt manuel ou programmé.

Une fois l'instance redémarrée, le AWS Systems Manager n'exécute aucune commande à distance pour créer une nouvelle session DCV et le message de journal suivant est absent des journaux du contrôleur vdc (sous le groupe de CloudWatch journaux) : `<environment-name>/vdc/controller CloudWatch`

Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT

Versions concernées

2024,04 - 2024,04.02

Mitigation

Pour récupérer les bureaux virtuels bloqués à l'état « REPRISE », procédez comme suit :

1. Connectez-vous en SSH à l'instance problématique depuis la EC2 console.
2. Exécutez les commandes suivantes sur l'instance :

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

3. Attendez que l'instance redémarre.

Pour éviter que les nouveaux bureaux virtuels ne rencontrent le même problème, procédez comme suit :

1. Pour télécharger le script de correctif et le fichier de correctif ([patch.py](#) et [vdi_stuck_in_resuming_status.patch](#)), exécutez la commande suivante en les remplaçant par le répertoire dans lequel vous souhaitez placer les fichiers : `<output-directory>`

Note

- Le correctif ne s'applique qu'à RES 2024.04.02.
- [Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.](#)

- Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

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

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

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

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la <environment-name> remplaçant par le nom de votre environnement RES et <aws-region> par la région dans laquelle RES est déployé :

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

3. Pour redémarrer l'instance de contrôleur VDC pour votre environnement, exécutez les commandes suivantes, en <environment-name> remplaçant par le nom de votre environnement RES :

```
ENVIRONMENT_NAME=<environment-name>
```

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

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

.....

(2024.04.02 et versions antérieures) Impossible de synchroniser les utilisateurs AD dont l'attribut SAMAccount Name inclut des majuscules ou des caractères spéciaux

Le problème

RES ne parvient pas à synchroniser les utilisateurs AD après la configuration du SSO pendant au moins deux heures (deux cycles de synchronisation AD). Les journaux du gestionnaire de clusters (sous le <environment-name>/cluster-manager groupe de CloudWatch journaux) incluent l'erreur suivante lors de la synchronisation AD :

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

L'erreur est due au fait que RES n'accepte qu'un SAMAccount nom d'utilisateur répondant aux exigences suivantes :

- Il ne peut contenir que des lettres ASCII minuscules, des chiffres, un point (.), un trait de soulignement (_).
- Le point ou le trait de soulignement ne sont pas autorisés comme premier ou dernier caractère.
- Il ne peut pas contenir deux points continus ou deux traits de soulignement (par exemple, ..., __, _., _.).

Versions concernées

2024.04.02 et versions antérieures

Mitigation

1. Pour télécharger le script de correctif et le fichier de correctif ([patch.py](#) et [samaccountname_regex.patch](#)), exécutez la commande suivante, en les remplaçant par le répertoire dans lequel vous <output-directory> souhaitez placer les fichiers :

Note

- Le correctif ne s'applique qu'à RES 2024.04.02.
- [Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.](#)

- Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

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

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

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

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la <environment-name> remplaçant par le nom de votre environnement RES :

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

3. Pour redémarrer l'instance de Cluster Manager pour votre environnement, exécutez les commandes suivantes en <environment-name> remplaçant par le nom de votre environnement RES. Vous pouvez également mettre fin à l'instance depuis l'Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>
```

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

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

.....

(2024.04.02 et versions antérieures) La clé privée pour accéder à l'hôte Bastion n'est pas valide

Le problème

Lorsqu'un utilisateur télécharge la clé privée pour accéder à l'hôte Bastion depuis le portail Web RES, la clé n'est pas correctement formatée : plusieurs lignes sont téléchargées en une seule ligne, ce qui rend la clé non valide. L'utilisateur obtiendra le message d'erreur suivant lorsqu'il tentera d'accéder à l'hôte du bastion avec la clé téléchargée :

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

Versions concernées

2024.04.02 et versions antérieures

Mitigation

Nous vous recommandons d'utiliser Chrome pour télécharger les clés, car ce navigateur n'est pas concerné.

Le fichier clé peut également être reformaté en créant une nouvelle ligne après -----BEGIN PRIVATE KEY----- et une autre ligne juste avant. -----END PRIVATE KEY-----

.....

(2024.06 et versions antérieures) Les membres du groupe ne sont pas synchronisés avec RES lors de la synchronisation AD

Description du bogue

Les membres du groupe ne se synchroniseront pas correctement avec RES si le GroupOU est différent de l'UserOU.

RES crée un filtre ldapsearch lorsqu'il tente de synchroniser les utilisateurs d'un groupe AD. Le filtre actuel utilise incorrectement le paramètre UserOu au lieu du paramètre GroupOu. Le résultat est que la recherche ne renvoie aucun utilisateur. Ce comportement ne se produit que dans les cas où UserSOU et GroupOu sont différents.

Versions concernées

Ce problème concerne toutes les versions 2024.06 ou antérieures de RES

Mitigation

Pour résoudre le problème, procédez comme suit :

1. Pour télécharger le script `patch.py` et le fichier `group_member_sync_bug_fix.patch`, exécutez les commandes suivantes, en les remplaçant par `<output-directory>` le répertoire local dans lequel vous souhaitez télécharger les fichiers et par la version de RES que vous souhaitez patcher : `<res_version>`

Note

- [Le script de correctif nécessite la AWS CLI v2, Python 3.9.16 ou supérieur et Boto3.](#)
- Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.
- Le correctif ne prend en charge que les versions RES 2024.04.02 et 2024.06. Si vous utilisez le 2024.04 ou le 2024.04.01, vous pouvez suivre les étapes répertoriées dans la section pour mettre à jour votre environnement [Mises à jour mineures des versions](#) vers le 2024.04.02 avant d'appliquer le correctif.

- Version RES : RES 2024.04.02

Lien de téléchargement du correctif :

[2024.04.02_group_member_sync_bug_fix.patch](#)

- Version RES : RES 2024.06

Lien de téléchargement du correctif : [2024.06_group_member_sync_bug_fix.patch](#)

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

```
RES_VERSION=<res_version>
```

```
mkdir -p ${OUTPUT_DIRECTORY}
```

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

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

2. Accédez au répertoire dans lequel le script de correctif et le fichier de correctif sont téléchargés. Exécutez la commande de correctif suivante, en la `<environment-name>` remplaçant par le nom de votre environnement RES :

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

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

3. Pour redémarrer l'instance de cluster-manager de votre environnement, exécutez les commandes suivantes :

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

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

.....

(2024.06 et versions antérieures) CVE-2024-6387, Regre, vulnérabilité de sécurité dans et Ubuntu SSHion RHEL9 VDI

Description du bogue

[Le CVE-2024-6387](#), baptisé regre, a été identifié sur le SSHion serveur OpenSSH. Cette vulnérabilité permet à des attaquants distants non authentifiés d'exécuter du code arbitraire sur le serveur cible, ce qui représente un risque sérieux pour les systèmes qui utilisent OpenSSH pour sécuriser les communications.

Pour RES, la configuration standard consiste à passer par l'hôte bastion pour accéder en SSH aux bureaux virtuels, et l'hôte bastion n'est pas affecté par cette vulnérabilité. Cependant, l'AMI (Amazon

Machine Image) par défaut que nous fournissons RHEL9 et Ubuntu2024 VDIs (infrastructure de bureau virtuel) dans TOUTES les versions RES utilisent une version OpenSSH vulnérable aux menaces de sécurité.

Cela signifie que les versions existantes RHEL9 et Ubuntu2024 VDIs pourraient être exploitables, mais l'attaquant aurait besoin d'accéder à l'hôte du bastion.

Vous trouverez plus de détails sur le problème [ici](#).

Versions concernées

Ce problème concerne toutes les versions 2024.06 ou antérieures de RES.

Mitigation

Ubuntu RHEL9 et Ubuntu ont publié des correctifs pour OpenSSH qui corrigent la faille de sécurité. Ils peuvent être extraits à l'aide du gestionnaire de packages correspondant à la plateforme.

Si vous avez un système existant RHEL9 ou Ubuntu VDIs, nous vous recommandons de suivre les VDIs instructions relatives au PATCH EXISTING ci-dessous. Pour les futurs patchs VDIs, nous vous recommandons de suivre les VDIs instructions de PATCH FUTURE. Ces instructions décrivent comment exécuter un script pour appliquer la mise à jour de la plateforme sur votre VDIs.

CORRECTIF EXISTANT VDIs

1. Exécutez la commande suivante qui corrigera tous les Ubuntu existants et RHEL9 VDIs :
 - a. Le script de correctif nécessite la [AWS CLI v2](#).
 - b. Configurez la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations de AWS Systems Manager pour envoyer une commande d'exécution de Systems Manager.

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

2. Vous pouvez vérifier que le script a bien été exécuté sur la [page Exécuter la commande](#). Cliquez sur l'onglet Historique des commandes, sélectionnez l'ID de commande le plus récent et vérifiez que toutes les instances IDs ont un message de réussite.

FUTUR DU PATCH VDIs

1. Pour télécharger le script de correctif et le fichier de correctif ([patch.py](#) et [update_openssh.patch](#)), exécutez les commandes suivantes, en les `<output-directory>` remplaçant par le répertoire dans lequel vous souhaitez télécharger les fichiers et `<environment-name>` par le nom de votre environnement RES :

Note

- Le correctif ne s'applique qu'à RES 2024.06.
- [Le script de correctif nécessite AWS CLI \(v2\), Python 3.9.16 ou supérieur et Boto3.](#)
- Configurez votre copie de la AWS CLI pour le compte et la région où RES est déployé, et assurez-vous que vous disposez des autorisations S3 pour écrire dans le compartiment créé par RES.

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

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

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

2. Exécutez la commande de correctif suivante :

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

3. Redémarrez l'instance du contrôleur VDC pour votre environnement à l'aide des commandes suivantes :

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

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

Important

Les futurs correctifs ne VDI sont pris en charge que sur les versions RES 2024.06 et ultérieures. Pour corriger les futurs environnements RES avec des versions antérieures VDI à 2024.06, commencez par mettre à niveau l'environnement RES vers 2024.06 en suivant les instructions disponibles sur : [Mises à jour majeures des versions](#)

.....

Avis

Chaque EC2 instance Amazon 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 EC2 instances Amazon sans RDP et sans avoir besoin de licences RDP. Si des licences Remote Desktop Services supplémentaires sont nécessaires, l'utilisateur de Remote Desktop CALs doit être acheté auprès de Microsoft ou d'un revendeur de licences Microsoft. Les utilisateurs de Remote Desktop bénéficiant d' CALs une assurance logicielle active bénéficient des avantages de la mobilité des licences et peuvent être transférés vers des environnements locaux (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 garantie, représentation ou condition d'aucune sorte, expresse ou implicite. 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
août 2024	- Version de sortie 2024.08 — - Ajout de la prise en charge du montage de compartiments Amazon S3 sur des instances d'infrastructure de bureau virtuel (VDI) Linux. Consultez Compartiments Amazon S3. - Ajout de la prise en charge des autorisations de projet personnalisées, d'un modèle d'autorisation amélioré qui permet de personnaliser les rôles existants et d'ajouter des rôles personnalisés. Consultez Profils d'autorisation. - Guide de l'utilisateur : Résolution des problèmes section élargie.
Juin 2024	- Sortie de la version 2024.06 — Support d'Ubuntu, autorisations du propriétaire du projet. - Guide de l'utilisateur : ajouté Création d'un environnement de démonstration
Avril 2024	Version de publication 2024.04 — Modèles prêts pour le RES AMIs et pour le lancement de projets
Mars 2024	Rubriques de résolution des problèmes supplémentaires, conservation CloudWatch des journaux, désinstallation des versions mineures

Date	Modification
Février 2024	Version de publication 2024.01.01 — modèle de déploiement mis à jour
Janvier 2024	Version de sortie 2024.01
Décembre 2023	GovCloud instructions et modèles ajoutés
Novembre 2023	Première version

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.