사용자 가이드

연구 및 엔지니어링 스튜디오

연구 및 엔지니어링 스튜디오: 사용자 가이드

Table of Contents

개요

Research and Engineering Studio(RES)는 IT 관리자가 과학자와 엔지니어가 에서 기술 컴퓨팅 워크로드를 실행할 수 있는 웹 포털을 제공할 수 있는 AWS 지원되는 오픈 소스 제품입니다 AWS. RES 는 사용자가 보안 가상 데스크톱을 시작하여 과학적 연구, 제품 설계, 엔지니어링 시뮬레이션 또는 데이터 분석 워크로드를 수행할 수 있는 단일 창을 제공합니다. 사용자는 기존 기업 자격 증명을 사용하여 RES 포털에 연결하고 개별 또는 협업 프로젝트를 수행할 수 있습니다.

관리자는 특정 사용자 집합이 공유 리소스에 액세스하고 협업할 수 있도록 프로젝트라는 가상 협업 공간을 생성할 수 있습니다. 관리자는 자체 애플리케이션 소프트웨어 스택(Amazon Machine Images 또는 사용AMIs)을 구축하고 RES 사용자가 Windows 또는 Linux 가상 데스크톱을 시작하고 공유 파일 시스템을 통해 프로젝트 데이터에 액세스할 수 있도록 허용할 수 있습니다. 관리자는 소프트웨어 스택 및 파일 시스템을 할당하고 해당 프로젝트 사용자로만 액세스를 제한할 수 있습니다. 관리자는 기본 제공 원격 측정을 사용하여 환경 사용량을 모니터링하고 사용자 문제를 해결할 수 있습니다. 또한 개별 프로젝트에 대한 예산을 설정하여 리소스의 과다 소비를 방지할 수 있습니다. 제품은 오픈 소스이므로 고객은 RES 포털의 사용자 경험을 자신의 필요에 맞게 사용자 지정할 수도 있습니다.

RES 는 추가 비용 없이 사용할 수 있으며 애플리케이션을 실행하는 데 필요한 AWS 리소스에 대해서만 비용을 지불합니다.

이 안내서는 의 Research and Engineering Studio AWS, 참조 아키텍처 및 구성 요소, 배포 계획 시 고려 사항, Amazon Web Services(AWS) 클라우드에 배포RES하기 위한 구성 단계에 대한 개요를 제공합니다.

기능 및 이점

의 Research and Engineering Studio는 다음과 같은 기능을 AWS 제공합니다.

웹 기반 사용자 인터페이스

RES 는 관리자, 연구원 및 엔지니어가 연구 및 엔지니어링 워크스페이스에 액세스하고 관리하는 데 사용할 수 있는 웹 기반 포털을 제공합니다. 과학자와 엔지니어는 를 사용하기 위해 AWS 계정 또는 클라우드 전문 지식이 필요하지 않습니다RES.

프로젝트 기반 구성

프로젝트를 사용하여 액세스 권한을 정의하고, 리소스를 할당하고, 일련의 작업 또는 활동에 대한 예산을 관리할 수 있습니다. 일관성과 규정 준수를 위해 프로젝트에 특정 소프트웨어 스택(운영 체

제 및 승인된 애플리케이션) 및 스토리지 리소스를 할당합니다. 프로젝트별로 지출을 모니터링하고 관리합니다.

협업 도구

과학자와 엔지니어는 프로젝트의 다른 구성원을 초대하여 협업하도록 하여 해당 동료가 원하는 권한 수준을 설정할 수 있습니다. 이러한 개인은 에 로그인하여 해당 데스크톱RES에 연결할 수 있습니다.

기존 자격 증명 관리 인프라와의 통합

기존 자격 증명 관리 및 디렉터리 서비스 인프라와 통합하여 RES 포털에 사용자의 기존 기업 자격 증명으로 연결하고 기존 사용자 및 그룹 멤버십을 사용하여 프로젝트에 권한을 할당합니다.

지속적인 스토리지 및 공유 데이터에 대한 액세스

사용자에게 가상 데스크톱 세션 전반에서 공유 데이터에 대한 액세스 권한을 제공하려면 기존 파일 시스템에 연결하거나 내에서 새 파일 시스템을 생성합니다RES. 지원되는 스토리지 서비스에는 Amazon Elastic File System for Linux 데스크톱과 Amazon FSx for NetApp ONTAP Windows and Linux 데스크톱이 포함됩니다.

모니터링 및 보고

분석 대시보드를 사용하여 인스턴스 유형, 소프트웨어 스택 및 운영 체제 유형에 대한 리소스 사용량을 모니터링합니다. 또한 대시보드는 보고를 위한 프로젝트별 리소스 사용량에 대한 분석도 제공합니다.

예산 및 비용 관리

프로젝트에 AWS Budgets 연결하여 각 RES 프로젝트의 비용을 모니터링합니다. 예산을 초과하는 경우 VDI 세션 시작을 제한할 수 있습니다.

개념 및 정의

이 섹션에서는 주요 개념을 설명하고 의 Research and Engineering Studio와 관련된 용어를 정의합니다 AWS.

파일 브라우저

파일 브라우저는 현재 로그인한 사용자가 파일 시스템을 볼 수 있는 RES 사용자 인터페이스의 일부입니다.

파일 시스템

파일 시스템은 프로젝트 데이터(종종 데이터 세트라고 함)의 컨테이너 역할을 합니다. 프로젝트의 경계 내에 스토리지 솔루션을 제공하고 협업 및 데이터 액세스 제어를 개선합니다.

글로벌 관리자

RES 환경 전체에서 공유되는 RES 리소스에 액세스할 수 있는 관리 위임자입니다. 범위 및 권한은 여러 프로젝트에 걸쳐 있습니다. 프로젝트를 생성 또는 수정하고 프로젝트 소유자를 할당할 수 있습니다. 프로젝트 소유자와 프로젝트 멤버에게 권한을 위임하거나 할당할 수 있습니다. 조직의 크기에 따라 동일한 사람이 RES 관리자 역할을 하는 경우가 있습니다.

프로젝트

프로젝트는 애플리케이션 내에서 데이터 및 컴퓨팅 리소스의 고유한 경계 역할을 하는 논리적 파티션으로, 데이터 흐름에 대한 거버넌스를 보장하고 프로젝트 간에 데이터와 VDI 호스트를 공유하는 것을 방지합니다.

프로젝트 기반 권한

프로젝트 기반 권한은 여러 프로젝트가 존재할 수 있는 시스템의 데이터와 VDI 호스트의 논리적 파티션을 설명합니다. 프로젝트 내의 데이터 및 VDI 호스트에 대한 사용자의 액세스는 관련 역할(들)에 따라 결정됩니다. 사용자에게 액세스가 필요한 각 프로젝트에 대한 액세스 권한(또는 프로젝트 멤버십)이 할당되어야 합니다. 그렇지 않으면 사용자는 멤버십이 부여되지 않은 VDIs 프로젝트 데이터 및 에 액세스할 수 없습니다.

프로젝트 멤버

RES 리소스(VDI, 스토리지 등)의 최종 사용자입니다. 범위 및 권한은 할당된 프로젝트로 제한됩니다. 권한은 위임하거나 할당할 수 없습니다.

프로젝트 소유자

특정 프로젝트에 대한 액세스 및 소유권이 있는 관리 위임자입니다. 범위 및 권한은 소유한 프로젝트(들)로 제한됩니다. 소유한 프로젝트의 프로젝트 멤버에게 권한을 할당할 수 있습니다.

소프트웨어 스택

소프트웨어 스택은 사용자가 VDI 호스트에 프로비저닝하기 위해 선택한 운영 체제를 기반으로 RES하는 특정 메타데이터가 있는 Amazon Machine Images(AMI)입니다.

VDI 호스트

가상 데스크톱 인스턴스(VDI) 호스트를 사용하면 프로젝트 멤버가 프로젝트별 데이터 및 컴퓨팅 환경에 액세스하여 안전하고 격리된 작업 공간을 보장할 수 있습니다.

AWS 용어에 대한 일반적인 참조는 AWS 일반 참조 의 AWS 용어집을 참조하세요.

아키텍처 개요

이 섹션에서는 이 제품과 함께 배포된 구성 요소에 대한 아키텍처 다이어그램을 제공합니다.

아키텍처 다이어그램

기본 파라미터로 이 제품을 배포하면 에 다음 구성 요소가 배포됩니다 AWS 계정.

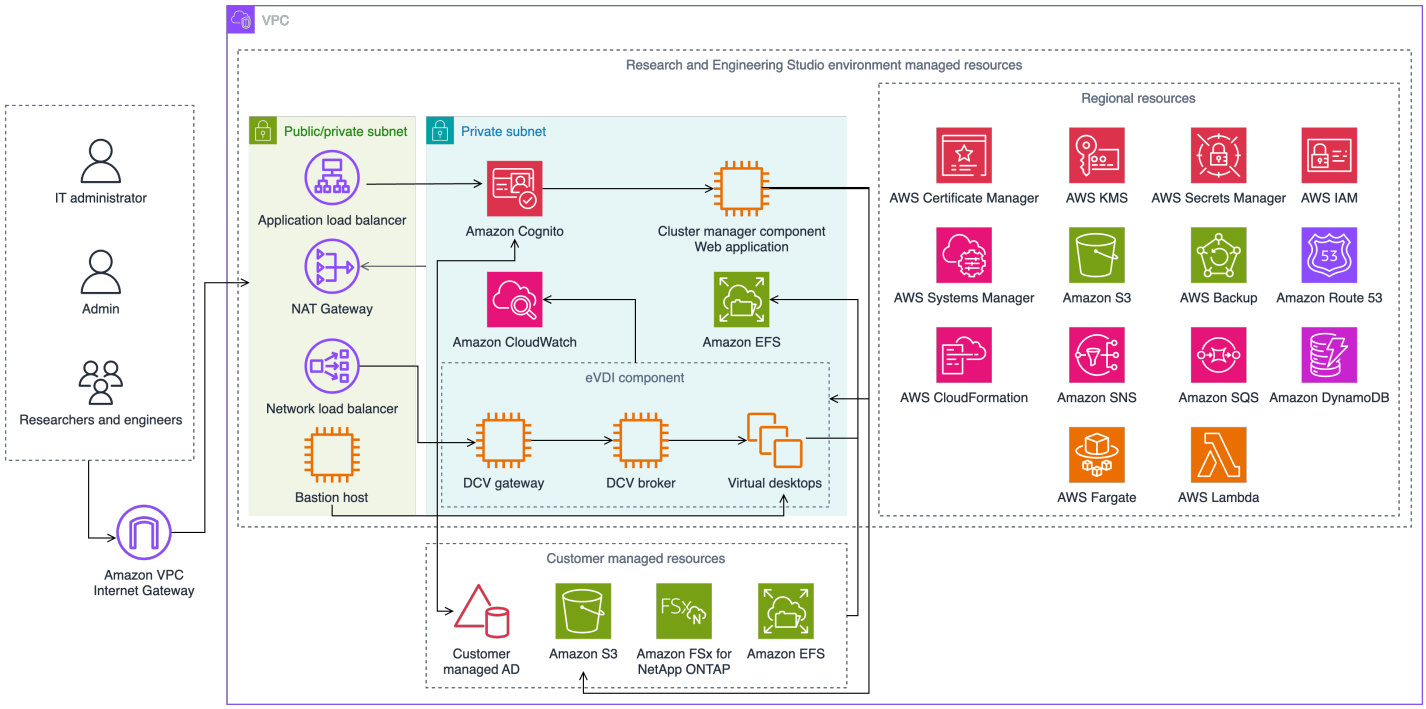


그림 1: AWS 아키텍처에 대한 연구 및 엔지니어링 스튜디오

> **Note**
>
> AWS CloudFormation 리소스는 AWS Cloud Development Kit (AWS CDK) 구성에서 생성됩니다.

템플릿과 함께 AWS CloudFormation 배포된 제품 구성 요소의 상위 수준 프로세스 흐름은 다음과 같습니다.

1. RES 는 웹 포털의 구성 요소와 다음을 설치합니다.
   a. 대화형 워크로드를 위한 엔지니어링 가상 데스크톱(eVDI) 구성 요소

b. 지표 구성 요소

Amazon은 eVDI 구성 요소에서 지표를 CloudWatch 수신합니다.

c. Bastion Host 구성 요소

관리자는 SSH를 사용하여 Bastion 호스트 구성 요소에 연결하여 기본 인프라를 관리할 수 있습니다.

2. RES 는 NAT 게이트웨이 뒤의 프라이빗 서브넷에 구성 요소를 설치합니다. 관리자는 Application Load Balancer(ALB) 또는 Bastion Host 구성 요소를 통해 프라이빗 서브넷에 액세스합니다.
3. Amazon DynamoDB는 환경 구성을 저장합니다.
4. AWS Certificate Manager (ACM)는 Application Load Balancer()에 대한 퍼블릭 인증서를 생성하고 저장합니다ALB.

> **Note**
>
> AWS Certificate Manager 를 사용하여 도메인에 대해 신뢰할 수 있는 인증서를 생성하는 것이 좋습니다.

5. Amazon Elastic File System(EFS)은 해당하는 모든 인프라 호스트 및 eVDI Linux 세션에 탑재된 기본 `/home` 파일 시스템을 호스팅합니다.
6. RES 는 Amazon Cognito를 사용하여 내에서 'clusteradmin'이라는 초기 부트스트랩 사용자를 생성하고 설치 중에 제공된 이메일 주소로 임시 보안 인증을 전송합니다. 'clusteradmin'은 처음 로그인할 때 암호를 변경해야 합니다.
7. Amazon Cognito는 권한 관리를 위해 조직의 Active Directory 및 사용자 자격 증명과 통합됩니다.
8. 보안 영역을 사용하면 관리자가 권한을 기반으로 제품 내의 특정 구성 요소에 대한 액세스를 제한할 수 있습니다.

AWS 이 제품의 서비스

AWS 서비스	유형	설명
Amazon Elastic Compute Cloud	Core	기본 컴퓨팅 서비스를 제공하여 선택한 운영 체제 및 소프트웨어 스택으로 가상 데스크톱을 생성합니다.

AWS 서비스	유형	설명
Elastic Load Balancing	Core	Bastion, 클러스터 관리자 및 VDI 호스트는 로드 밸런서 뒤에 있는 Auto Scaling 그룹에서 생성됩니다. ELB 는 RES 호스트 간에 웹 포털의 트래픽 균형을 맞춥니다.
Amazon Virtual Private Cloud	Core	모든 핵심 제품 구성 요소는 내에서 생성됩니다VPC.
Amazon Cognito	Core	사용자 자격 증명 및 인증을 관리합니다. Active Directory 사용자는 Amazon Cognito 사용자 및 그룹에 매핑되어 액세스 수준을 인증합니다.
Amazon Elastic File System	Core	/home 파일 브라우저 및 VDI 호스트의 파일 시스템과 공유 외부 파일 시스템을 제공합니다.
Amazon DynamoDB	Core	사용자, 그룹, 프로젝트, 파일 시스템 및 구성 요소 설정과 같은 구성 데이터를 저장합니다.
AWS Systems Manager	Core	VDI 세션 관리를 위한 명령을 수행하기 위한 문서를 저장합니다.
AWS Lambda	Core	DynamoDB 테이블 내 설정 업데이트, Active Directory 동기화 워크플로 시작, 접두사 목록 업데이트와 같은 제품 기능을 지원합니다.

AWS 서비스	유형	설명
Amazon CloudWatch	지원	모든 Amazon EC2 호스트 및 Lambda 함수에 대한 지표 및 활동 로그를 제공합니다.
Amazon Simple Storage Service(S3)	지원	호스트 부트스트래핑 및 구성을 위한 애플리케이션 바이너리를 저장합니다.
AWS Key Management Service	지원	Amazon SQS 대기열, DynamoDB 테이블 및 Amazon SNS 주제에서 저장 시 암호화에 사용됩니다.
AWS Secrets Manager	지원	에 대한 Active Directory 및 자체 서명된 인증서에 서비스 계정 자격 증명을 저장합니다 VDIs.
AWS CloudFormation	지원	제품에 대한 배포 메커니즘을 제공합니다.
AWS Identity and Access Management	지원	호스트의 액세스 수준을 제한합니다.
Amazon Route 53	지원	내부 로드 밸런서와 배스션 호스트 도메인 이름을 해결하기 위한 프라이빗 호스팅 영역을 생성합니다.
Amazon Simple Queue Service	지원	비동기 실행을 지원하는 작업 대기열을 생성합니다.
Amazon Simple Notification Service	지원	컨트롤러와 호스트와 같은 VDI 구성 요소 간의 게시 구독자 모델을 지원합니다.

AWS 서비스	유형	설명
AWS Fargate	지원	Fargate 작업을 사용하여 환경을 설치, 업데이트 및 삭제합니다.
Amazon FSx File Gateway	선택 사항	외부 공유 파일 시스템을 제공합니다.
FSx용 Amazon NetApp ONTAP	선택 사항	외부 공유 파일 시스템을 제공합니다.
AWS Certificate Manager	선택 사항	사용자 지정 도메인에 대해 신뢰할 수 있는 인증서를 생성합니다.
AWS Backup	선택 사항	Amazon EC2 호스트, 파일 시스템 및 DynamoDB 에 대한 백업 기능을 제공합니다.

데모 환경 생성

이 섹션의 단계에 따라 에서 Research and Engineering Studio를 사용해 보세요 AWS. 이 데모는 데모 환경 스택 템플릿 에서 Research and Engineering Studio를 사용하여 최소한의 파라미터 집합으로 비프로덕 AWS 션 환경을 배포합니다. 에 Keycloak 서버를 사용합니다SSO.

스택을 배포한 후에는 로그인하기 전에 배포 후 단계 아래 에 따라 환경에서 사용자를 설정해야 합니다.

원클릭 데모 스택 생성

이 AWS CloudFormation 스택은 Research and Engineering Studio에 필요한 모든 구성 요소를 생성합니다.

배포 시간: ~90분

사전 조건

주제

- 관리 사용자 AWS 계정 로 생성
- Amazon EC2 SSH 키 페어 생성
- 서비스 할당량 증가

관리 사용자 AWS 계정 로 생성

관리 사용자가 AWS 계정 있는 이 있어야 합니다.

1. https://portal.aws.amazon.com/billing/가입을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

Amazon EC2 SSH 키 페어 생성

Amazon EC2 SSH 키 페어가 없는 경우 하나를 생성해야 합니다. 자세한 내용은 Amazon 사용 설명서의 Amazon을 사용하여 키 페어 생성을 EC2 참조하세요. EC2

서비스 할당량 증가

다음에 대한 서비스 할당량을 늘리는 것이 좋습니다.

- Amazon VPC
  - NAT 게이트웨이당 탄력적 IP 주소 할당량을 5개에서 8개로 늘립니다.
  - 가용 영역당 NAT 게이트웨이를 5개에서 10개로 늘립니다.
- Amazon EC2
  - EC2-VPC 탄력성을 5IPs에서 10으로 늘립니다.

AWS 계정에는 각 AWS 서비스에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다. 자세한 내용은 the section called “이 제품의 AWS 서비스에 대한 할당량” 단원을 참조하십시오.

리소스 및 입력 파라미터 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudformation 에서 AWS CloudFormation 콘솔을 엽니다.

   > **Note**
   >
   > 관리자 계정에 있는지 확인합니다.

2. 콘솔에서 템플릿을 시작합니다.
3. 파라미터 에서 이 제품 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다.

파라미터	기본값	설명
EnvironmentName	*<res-demo>*	res-, 11자 이하, 대문자 없음으로 시작하는 RES 환경에 지정된 고유한 이름입니다.

파라미터	기본값	설명
AdministratorEmail		제품 설정을 완료하는 사용자의 이메일 주소입니다. 또한 이 사용자는 Active Directory 통합에 대한 단일 로그인 실패가 있는 경우 브레이크 글라스 사용자 역할을 합니다.
KeyPair		인프라 호스트에 연결하는 데 사용되는 키 페어입니다.
ClientIPCidr	<0.0.0.0/0>	시스템에 대한 연결을 제한하는 IP 주소 필터입니다. 배포 ClientIpCidr 후 를 업데이트할 수 있습니다.
InboundPrefixList		(선택 사항) 가 웹 UI에 직접 액세스하고 Bastion 호스트 SSH에 액세스할 수 있도록 IPs 허용하는 관리형 접두사 목록을 제공합니다.

4. 스택 생성을 선택합니다.

배포 후 단계

1. 의 사용자 암호 재설정 `AWS Directory Service`- 데모 스택은 `admin1`, `user1`, 및 와 같이 사용할 수 있는 사용자 이름으로 4명의 사용자를 생성합니다`admin2``user2`.

   a. 디렉터리 서비스 콘솔로 이동합니다.

   b. 환경의 디렉터리 ID를 선택합니다. `<StackName>*DirectoryService*` 스택의 출력에서 디렉터리 ID를 가져올 수 있습니다.

   c. 오른쪽 상단 작업 드롭다운 메뉴에서 사용자 암호 재설정을 선택합니다.

   d. 사용하려는 모든 사용자에 대해 사용자 이름과 유형을 원하는 암호에 입력하고 암호 재설정을 선택합니다.

2. 사용자 암호를 재설정한 후에는 Research and Engineering Studio가 환경에서 사용자를 동기화할 때까지 기다려야 합니다. Research and Engineering Studio는 xx.00에 매시간 사용자를 동기화합니다. 이러한 상황이 발생할 때까지 기다리거나 에 나열된 단계에 따라 사용자를 즉시 동기화Active Directory에 추가되었지만 에서 누락된 사용자 RES할 수 있습니다.

이제 배포가 준비되었습니다. 이메일에서 EnvironmentUrl 받은 를 사용하여 UI에 액세스하거나 배포된 스택의 출력URL에서 동일한 를 가져올 수도 있습니다. 이제 Active Directory에서 암호를 재설정하는 사용자 및 암호를 사용하여 Research and Engineering Studio 환경에 로그인할 수 있습니다.

배포 계획

이 섹션에는 에서 Research and Engineering Studio 배포를 계획하는 데 도움이 되는 비용, 보안, 지원되는 리전 및 할당량에 대한 정보가 포함되어 있습니다 AWS.

비용

의 Research and Engineering Studio AWS 는 추가 비용 없이 사용할 수 있으며 애플리케이션을 실행하는 데 필요한 리소스에 대해서만 AWS 비용을 지불합니다. 자세한 내용은 AWS 이 제품의 서비스 단원을 참조하십시오.

> **Note**
>
> 이 제품을 실행하는 동안 사용되는 AWS 서비스의 비용은 사용자가 부담합니다.
> 비용 관리에 도움이 되도록 를 통해 예산AWS Cost Explorer을 생성하는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은 이 제품에 사용되는 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델 이를 클라우드의 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - 에서 AWS 서비스를 실행하는 인프라를 보호할 AWS 책임이 있습니다 AWS 클라우드. AWS 는 안전하게 사용할 수 있는 서비스도 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 규정 준수 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 의 Research and Engineering Studio에 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 AWS 프로그램 범위 내 서비스 규정 준수 프로그램 범위 내 서비스를 AWS참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

공동 책임 모델을 Research and Engineering Studio에서 사용하는 AWS 서비스에 적용하는 방법을 알아보려면 섹션을 참조하세요이 제품의 서비스에 대한 보안 고려 사항. AWS 보안에 대한 자세한 내용은 AWS 클라우드 보안 섹션을 참조하세요.

IAM 역할

AWS Identity and Access Management (IAM) 역할을 통해 고객은 의 서비스 및 사용자에게 세분화된 액세스 정책 및 권한을 할당할 수 있습니다 AWS 클라우드. 이 제품은 제품의 AWS Lambda 함수와 Amazon EC2 인스턴스에 리전 리소스를 생성할 수 있는 액세스 권한을 부여하는 IAM 역할을 생성합니다.

RES 는 내에서 자격 증명 기반 정책을 지원합니다IAM. 배포되면 는 관리자 권한 및 액세스를 정의하는 정책을 RES 생성합니다. 제품을 구현하는 관리자는 와 통합된 기존 고객 Active Directory 내에서 최종 사용자 및 프로젝트 리더를 생성하고 관리합니다RES. 자세한 내용은 AWS 자격 증명 및 액세스 관리 사용 설명서의 IAM 정책 생성을 참조하세요.

조직의 관리자는 활성 디렉터리를 사용하여 사용자 액세스를 관리할 수 있습니다. 최종 사용자가 RES 사용자 인터페이스에 액세스하면 는 Amazon Cognito로 RES 인증합니다.

보안 그룹

이 제품에서 생성된 보안 그룹은 Lambda 함수, EC2 인스턴스, 파일 시스템 CSR 인스턴스 및 원격 VPN 엔드포인트 간의 네트워크 트래픽을 제어하고 격리하도록 설계되었습니다. 보안 그룹을 검토하고 제품이 배포되면 필요에 따라 액세스를 추가로 제한하는 것이 좋습니다.

데이터 암호화

기본적으로 AWS (RES)의 Research and Engineering Studio는 RES 소유 키를 사용하여 유휴 및 전송 중인 고객 데이터를 암호화합니다. 를 배포할 때 를 지정할 RES수 있습니다 AWS KMS key. RES 는 자격 증명을 사용하여 키 액세스 권한을 부여합니다. 고객이 소유하고 관리하는 를 제공하는 경우 저장 중인 AWS KMS key고객 데이터는 해당 키를 사용하여 암호화됩니다.

RES 는 SSL/를 사용하여 전송 중인 고객 데이터를 암호화합니다TLS. 1.2TLS가 필요하지만 TLS 1.3을 권장합니다.

이 제품의 서비스에 대한 보안 고려 사항

Research and Engineering Studio에서 사용하는 서비스의 보안 고려 사항에 대한 자세한 내용은 다음 표의 링크를 참조하세요.

AWS 서비스 보안 정보	서비스 유형	에서 서비스를 사용하는 방법 RES
Amazon Elastic Compute Cloud	Core	기본 컴퓨팅 서비스를 제공하여 선택한 운영 체제 및 소프트웨어 스택으로 가상 데스크톱을 생성합니다.
Elastic Load Balancing	Core	Bastion, 클러스터 관리자 및 VDI 호스트는 로드 밸런서 뒤에 있는 Auto Scaling 그룹에서 생성됩니다. ELB 는 RES 호스트 간에 웹 포털의 트래픽 균형을 유지합니다.
Amazon Virtual Private Cloud	Core	모든 핵심 제품 구성 요소는 내에 생성됩니다VPC.
Amazon Cognito	Core	사용자 자격 증명 및 인증을 관리합니다. Active Directory 사용자는 Amazon Cognito 사용자 및 그룹에 매핑되어 액세스 수준을 인증합니다.
Amazon Elastic File System	Core	/home 파일 브라우저 및 VDI 호스트의 파일 시스템과 공유 외부 파일 시스템을 제공합니다.
Amazon DynamoDB	Core	사용자, 그룹, 프로젝트, 파일 시스템 및 구성 요소 설정과 같은 구성 데이터를 저장합니다.
AWS Systems Manager	Core	VDI 세션 관리를 위한 명령을 수행하기 위한 문서를 저장합니다.

AWS 서비스 보안 정보	서비스 유형	에서 서비스를 사용하는 방법 RES
AWS Lambda	Core	DynamoDB 테이블 내 설정 업데이트, Active Directory 동기화 워크플로 시작, 접두사 목록 업데이트와 같은 제품 기능을 지원합니다.
Amazon CloudWatch	지원	모든 Amazon EC2 호스트 및 Lambda 함수에 대한 지표 및 활동 로그를 제공합니다.
Amazon Simple Storage Service(S3)	지원	호스트 부트스트래핑 및 구성을 위한 애플리케이션 바이너리를 저장합니다.
AWS Key Management Service	지원	Amazon SQS 대기열, DynamoDB 테이블 및 Amazon SNS 주제에서 저장 시 암호화에 사용됩니다.
AWS Secrets Manager	지원	에 대한 Active Directory 및 자체 서명된 인증서에 서비스 계정 자격 증명을 저장합니다 VDIs.
AWS CloudFormation	지원	제품에 대한 배포 메커니즘을 제공합니다.
AWS Identity and Access Management	지원	호스트의 액세스 수준을 제한합니다.
Amazon Route 53	지원	내부 로드 밸런서와 bastion 호스트 도메인 이름을 해결하기 위한 프라이빗 호스팅 영역을 생성합니다.

AWS 서비스 보안 정보	서비스 유형	에서 서비스를 사용하는 방법 RES
Amazon Simple Queue Service	지원	비동기 실행을 지원하는 작업 대기열을 생성합니다.
Amazon Simple Notification Service	지원	컨트롤러와 호스트와 같은 VDI 구성 요소 간의 게시 구독자 모델을 지원합니다.
AWS Fargate	지원	Fargate 작업을 사용하여 환경을 설치, 업데이트 및 삭제합니다.
Amazon FSx File Gateway	선택 사항	외부 공유 파일 시스템을 제공합니다.
FSx용 Amazon NetApp ONTAP	선택 사항	외부 공유 파일 시스템을 제공합니다.
AWS Certificate Manager	선택 사항	사용자 지정 도메인에 대해 신뢰할 수 있는 인증서를 생성합니다.
AWS Backup	선택 사항	Amazon EC2 호스트, 파일 시스템 및 DynamoDB 에 대한 백업 기능을 제공합니다.

할당량

서비스 할당량은 AWS 계정계정의 최대 서비스 리소스 또는 작업 수입니다.

이 제품의 AWS 서비스에 대한 할당량

이 제품 에 구현된 각 서비스에 대한 할당량이 충분한지 확인합니다. 자세한 내용은 AWS 서비스 할당량을 참조하세요.

이 제품의 경우 다음 서비스에 대한 할당량을 늘리는 것이 좋습니다.

- Amazon Virtual Private Cloud
- Amazon EC2

할당량 증가를 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

AWS CloudFormation 할당량

AWS 계정 에는 이 제품의 스택을 시작할 때 알아야 할 AWS CloudFormation 할당량이 있습니다. 이러한 할당량을 이해하면 이 제품을 성공적으로 배포하지 못하게 하는 제한 오류를 방지할 수 있습니다. 자세한 내용은 사용 설명서의 에서 AWS CloudFormation 할당량을 참조하세요. AWS CloudFormation

복원력 계획

제품은 시스템을 운영하기 위한 Amazon EC2 인스턴스의 최소 수와 크기를 가진 기본 인프라를 배포합니다. 대규모 프로덕션 환경에서 복원력을 개선하려면 인프라의 Auto Scaling 그룹() 내에서 기본 최소 용량 설정을 늘리는 것이 좋습니다ASG. 인스턴스 하나에서 인스턴스 두 개로 값을 늘리면 여러 가용 영역(AZ)의 이점을 얻을 수 있으며 예상치 못한 데이터 손실이 발생할 경우 시스템 기능을 복원하는 시간을 줄일 수 있습니다.

ASG 설정은 의 Amazon EC2 콘솔 내에서 사용자 지정할 수 있습니다https://console.aws.amazon.com/ec2/. 제품은 ASGs 기본적으로 4개를 생성하며 각 이름은 로 끝납니다-asg. 최소 및 원하는 값을 프로덕션 환경에 적합한 양으로 변경할 수 있습니다. 수정하려는 그룹을 선택한 다음 작업을 선택하고 편집을 선택합니다. 에 대한 자세한 내용은 Amazon Auto Scaling 사용 설명서의 Auto Scaling 그룹 크기 조정을 ASGs참조하세요. EC2 Auto Scaling

지원됨 AWS 리전

이 제품은 현재 일부 에서 사용할 수 없는 서비스를 사용합니다 AWS 리전. 모든 서비스를 사용할 수 AWS 리전 있는 에서 이 제품을 시작해야 합니다. 리전별 AWS 서비스의 최신 가용성은 AWS 리전 al Services List를 참조하세요.

의 Research and Engineering Studio AWS 는 다음 에서 지원됩니다 AWS 리전.

지역명	지역	이전 버전	최신 버전(2024년 10월)
미국 동부(버지니아 북부)	us-east-1	예	예
미국 동부(오하이오)	us-east-2	예	예
미국 서부(캘리포니아 북부)	us-west-1	예	예
미국 서부(오레곤)	us-west-2	예	예
아시아 태평양(도쿄)	ap-northeast-1	예	예
아시아 태평양(서울)	ap-northeast-2	예	예
아시아 태평양(뭄바이)	ap-south-1	예	예
아시아 태평양(싱가포르)	ap-southeast-1	예	예
아시아 태평양(시드니)	ap-southeast-2	예	예
캐나다(중부)	ca-central-1	예	예
유럽(프랑크푸르트)	eu-central-1	예	예
유럽(밀라노)	eu-south-1	예	예
유럽(아일랜드)	eu-west-1	예	예
유럽(런던)	eu-west-2	예	예
유럽(파리)	eu-west-3	예	예
유럽(스톡홀름)	eu-north-1	아니요	yes
이스라엘(텔아비브)	il-central-1	예	예

지역명	지역	이전 버전	최신 버전(2024년 10월)
AWS GovCloud (미국 서부)	us-gov-west-1	예	예

제품 배포

> **Note**
>
> 이 제품은 AWS CloudFormation 템플릿과 스택을 사용하여 배포를 자동화합니다. 템플릿은 CloudFormation 이 제품에 포함된 AWS 리소스와 해당 속성을 설명합니다. CloudFormation 스택은 템플릿에 설명된 리소스를 프로비저닝합니다.

제품을 시작하기 전에 이 안내서 앞부분에서 설명한 비용, 아키텍처, 네트워크 보안 및 기타 고려 사항을 검토하세요.

주제

사전 조건

주제

관리 사용자 AWS 계정 로 생성

관리 사용자가 AWS 계정 있는 이 있어야 합니다.

1. https://portal.aws.amazon.com/billing/가입 을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

Amazon EC2 SSH 키 페어 생성

Amazon EC2 SSH 키 페어가 없는 경우 하나를 생성해야 합니다. 자세한 내용은 Amazon 사용 설명서의 Amazon을 사용하여 키 페어 생성을 EC2 참조하세요. EC2

서비스 할당량 증가

다음에 대한 서비스 할당량을 늘리는 것이 좋습니다.

- Amazon VPC
  - NAT 게이트웨이당 탄력적 IP 주소 할당량을 5에서 8로 늘립니다.
  - 가용 영역당 NAT 게이트웨이를 5개에서 10개로 늘립니다.
- Amazon EC2
  - EC2-VPC 탄력성을 5IPs에서 10으로 늘립니다.

AWS 계정에는 각 AWS 서비스에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다. 자세한 내용은 이 제품의 AWS 서비스에 대한 할당량 단원을 참조하십시오.

퍼블릭 도메인 생성(선택 사항)

사용자 친화적인 를 가지려면 제품에 대한 사용자 지정 도메인을 사용하는 것이 좋습니다URL. Amazon Route 53 또는 다른 공급자를 사용하여 도메인을 등록하고 를 사용하여 도메인에 대한 인증서를 가져와야 합니다 AWS Certificate Manager. 이미 퍼블릭 도메인과 인증서가 있는 경우 이 단계를 건너뛸 수 있습니다.

1. 지침에 따라 Route53에 도메인을 등록합니다. 확인 이메일을 받게 됩니다.

2. 도메인의 호스팅 영역을 검색합니다. 이는 Route53에서 자동으로 생성됩니다.

   a. Route53 콘솔을 엽니다.

   b. 왼쪽 탐색에서 호스팅 영역을 선택합니다.

   c. 도메인 이름에 대해 생성된 호스팅 영역을 열고 호스팅 영역 ID를 복사합니다.

3. 를 AWS Certificate Manager 열고 다음 단계에 따라 도메인 인증서를 요청합니다. 솔루션을 배포하려는 리전에 있는지 확인합니다.

4. 탐색에서 인증서 나열을 선택하고 인증서 요청을 찾습니다. 요청은 보류 중이어야 합니다.

5. 인증서 ID를 선택하여 요청을 엽니다.

6. 도메인 섹션에서 Route53에서 레코드 생성을 선택합니다. 요청을 처리하는 데 약 10분이 걸립니다.

7. 인증서가 발급되면 인증서 상태 섹션에서 를 복사ARN합니다.

도메인 생성(GovCloud 만 해당)

AWS GovCloud (미국 서부) 리전에 배포하고 Research and Engineering Studio용 사용자 지정 도메인을 사용하는 경우 이러한 사전 조건 단계를 완료해야 합니다.

1. 퍼블릭 호스팅 도메인이 생성된 상용 파티션 AWS 계정에 인증서 AWS CloudFormation 스택을 배포합니다.

2. 인증서 CloudFormation 출력 에서 `CertificateARN` 및 를 찾아 기록합니다`PrivateKeySecretARN`.

3. GovCloud 파티션 계정에서 `CertificateARN` 출력 값으로 보안 암호를 생성합니다. 새 보안 암호를 기록하고 보안 암호에 두 개의 태그를 ARN 추가하여 가 보안 암호 값에 액세스할 `vdc-gateway` 수 있도록 합니다.

   a. res:ModuleName = virtual-desktop-controller

   b. res:EnvironmentName = [환경 이름](res-demo일 수 있음)

4. GovCloud 파티션 계정에서 `PrivateKeySecretArn` 출력 값으로 보안 암호를 생성합니다. 새 보안 암호를 기록하고 보안 암호에 두 개의 태그를 ARN 추가하여 가 보안 암호 값에 액세스할 `vdc-gateway` 수 있도록 합니다.

   a. res:ModuleName = virtual-desktop-controller

   b. res:EnvironmentName = [환경 이름](res-demo일 수 있음)

외부 리소스 제공

의 Research and Engineering Studio는 배포 시 다음과 같은 외부 리소스가 존재할 것으로 AWS 예상합니다.

- 네트워킹(VPC, 퍼블릭 서브넷 및 프라이빗 서브넷)

  여기에서 RES 환경, Active Directory(AD) 및 공유 스토리지를 호스팅하는 데 사용되는 EC2 인스턴스를 실행합니다.
- 스토리지(AmazonEFS)

  스토리지 볼륨에는 가상 데스크톱 인프라()에 필요한 파일과 데이터가 포함됩니다VDI.
- 디렉터리 서비스(AWS Directory Service for Microsoft Active Directory)

  디렉터리 서비스는 사용자를 RES 환경에 인증합니다.
- 서비스 계정 암호가 포함된 보안 암호

  Research and Engineering Studio는 를 사용하여 서비스 계정 암호를 포함하여 사용자가 제공하는 보안 암호에 액세스합니다AWS Secrets Manager.

> **Tip**
>
> 데모 환경을 배포하고 이러한 외부 리소스를 사용할 수 없는 경우 AWS 고성능 컴퓨팅 레시피를 사용하여 외부 리소스를 생성할 수 있습니다. 계정에 리소스를 배포외부 리소스 생성하려면 다음 섹션인 를 참조하세요.
> AWS GovCloud (미국 서부) 리전의 데모 배포의 경우 의 사전 조건 단계를 완료해야 합니다도메인 생성(GovCloud 만 해당).

LDAPS 환경에서 구성(선택 사항)

환경에서 LDAPS 통신을 사용하려는 경우 다음 단계를 완료하여 AWS Managed Microsoft AD (AD) 도메인 컨트롤러에 인증서를 생성하고 연결하여 AD와 간에 통신을 제공해야 합니다RES.

1. 에 LDAPS 대해 서버 측을 활성화하는 방법에 AWS Managed Microsoft AD 제공된 단계를 따릅니다. 이미 를 활성화한 경우 이 단계를 건너뛸 수 있습니다LDAPS.
2. LDAPS 가 AD에 구성되어 있는지 확인한 후 AD 인증서를 내보냅니다.

a. Active Directory 서버로 이동합니다.

b. 관리자 PowerShell 로 를 엽니다.

c. 를 실행`certmgr.msc`하여 인증서 목록을 엽니다.

d. 먼저 신뢰할 수 있는 루트 인증 기관을 연 다음 인증서를 열어 인증서 목록을 엽니다.

e. AD 서버와 이름이 동일한 인증서를 선택하고 유지(또는 마우스 오른쪽 버튼 클릭)한 다음 모든 작업을 선택한 다음 내보내기를 선택합니다.

f. Base-64 인코딩된 X.509(.CER)를 선택하고 다음 를 선택합니다.

g. 디렉터리를 선택한 다음 다음을 선택합니다.

3. 에서 보안 암호 생성 AWS Secrets Manager:

   Secrets Manager에서 보안 암호를 생성할 때 보안 암호 유형에서 다른 유형의 보안 암호를 선택하고 PEM 인코딩된 인증서를 일반 텍스트 필드에 붙여넣습니다.

4. ARN 생성된 를 기록하고 에 `DomainTLSCertificateSecretARN` 파라미터로 입력합니다1단계: 제품 시작.

프라이빗 구성VPC(선택 사항)

격리된 에 Research and Engineering Studio를 배포하면 조직의 규정 준수 및 거버넌스 요구 사항을 충족하는 향상된 보안이 VPC 제공됩니다. 그러나 표준 RES 배포는 종속성을 설치하기 위해 인터넷 액세스에 의존합니다. 프라이빗 RES에 를 설치하려면 다음 사전 조건을 VPC충족해야 합니다.

주제

- Amazon Machine 이미지 준비(AMIs)
- VPC 엔드포인트 설정
- VPC 엔드포인트 없이 서비스에 연결
- 프라이빗 VPC 배포 파라미터 설정

Amazon Machine 이미지 준비(AMIs)

1. 종속성 을 다운로드합니다. 격리된 에 VPC를 배포하려면 RES 인프라에 퍼블릭 인터넷 액세스 없이 종속성을 사용할 수 있어야 합니다.
2. Amazon S3 읽기 전용 액세스 및 Amazon 로 신뢰할 수 있는 자격 증명이 있는 IAM 역할을 생성합니다EC2.

a. 에서 IAM 콘솔을 엽니다https://console.aws.amazon.com/iam/.

b. 역할 에서 역할 생성을 선택합니다.

c. 신뢰할 수 있는 엔터티 선택 페이지에서:

- 신뢰할 수 있는 엔터티 유형에서 를 선택합니다 AWS 서비스.
- 서비스 또는 사용 사례 의 사용 사례에서 EC2를 선택하고 다음을 선택합니다.

d. 권한 추가에서 다음 권한 정책을 선택한 다음 다음 를 선택합니다.

- AmazonS3ReadOnlyAccess
- AmazonSSMManagedInstanceCore
- EC2InstanceProfileForImageBuilder

e. 역할 이름 및 설명 을 추가한 다음 역할 생성 을 선택합니다.

3. EC2 이미지 빌더 구성 요소 생성:

a. 에서 EC2 Image Builder 콘솔을 엽니다https://console.aws.amazon.com/imagebuilder.

b. 저장된 리소스 에서 구성 요소를 선택하고 구성 요소 생성 을 선택합니다.

c. 구성 요소 생성 페이지에서 다음 세부 정보를 입력합니다.

- 구성 요소 유형 에서 빌드를 선택합니다.
- 구성 요소 세부 정보에서 다음을 선택합니다.

파라미터	사용자 항목
이미지 운영 체제(OS)	Linux
호환되는 OS 버전	Amazon Linux 2
구성 요소 이름	다음과 같은 이름을 입력합니다.*<research-and-engineering-studio-infrastructure>*
구성 요소 버전입니다.	1.0.0으로 시작하는 것이 좋습니다.
설명	선택적 사용자 항목입니다.

d. 구성 요소 생성 페이지에서 문서 콘텐츠 정의를 선택합니다.

i. 정의 문서 콘텐츠를 입력하기 전에 tar.gz 파일에 URI 대한 파일이 필요합니다. 에서 제공하는 tar.gz 파일을 Amazon S3 버킷RES에 업로드하고 버킷 속성URI에서 파일을 복사합니다.

ii. 다음을 입력합니다.

> **Note**
>
> `AddEnvironmentVariables` 는 선택 사항이며 인프라 호스트에 사용자 지정 환경 변수가 필요하지 않은 경우 제거할 수 있습니다.
> `http_proxy` 및 `https_proxy` 환경 변수를 설정하는 경우 인스턴스가 프록시를 사용하여 localhost, 인스턴스 메타데이터 IP 주소 및 VPC 엔드포인트를 지원하는 서비스를 쿼리하는 것을 방지하기 위해 `no_proxy` 파라미터가 필요합니다.

```
#  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. 구성 요소 생성을 선택합니다.

4. Image Builder 이미지 레시피를 생성합니다.

a. 레시피 생성 페이지에서 다음을 입력합니다.

섹션	파라미터	사용자 항목
레시피 세부 정보	이름	res-recipe-linux-x86과 같은 적절한 이름을 입력합니다.
	버전	일반적으로 1.0.0으로 시작하는 버전을 입력합니다.
	설명	선택적 설명을 추가합니다.
기본 이미지	이미지 선택	관리형 이미지를 선택합니다.
	OS	Amazon Linux
	이미지 오리진	빠른 시작(Amazon 관리형)
	이미지 이름	Amazon Linux 2 x86
	자동 버전 지정 옵션	사용 가능한 최신 OS 버전을 사용합니다.

섹션	파라미터	사용자 항목
인스턴스 구성	–	모든 항목을 기본 설정으로 유지하고 파이프라인 실행 후 SSM 에이전트 제거가 선택되지 않았는지 확인합니다.
작업 디렉터리	작업 디렉터리 경로	/root/bootstrap/res_종속성
구성 요소	구성 요소 빌드	다음을 검색하고 선택합니다. • Amazon 관리형: aws-cli-version-2-linux • Amazon 관리형: amazon-cloudwatch-agent-linux • 소유자: 이전에 생성된 Amazon EC2 구성 요소입니다. AWS 리전 필드에 AWS 계정 ID와 현재를 입력합니다.
	구성 요소 테스트	를 검색하고 선택합니다. • Amazon 관리형: simple-boot-test-linux

b. 레시피 생성을 선택합니다.

5. Image Builder 인프라 구성을 생성합니다.

a. 저장된 리소스 에서 인프라 구성 을 선택합니다.

b. 인프라 구성 생성을 선택합니다.

c. 인프라 구성 생성 페이지에서 다음을 입력합니다.

섹션	파라미터	사용자 항목
일반	이름	res-infra-linux-x86과 같은 적절한 이름을 입력합니다.
	설명	선택적 설명을 추가합니다.
	IAM 역할	이전에 생성한 IAM 역할을 선택합니다.
AWS 인프라	인스턴스 유형	t3.medium을 선택합니다.

	VPC, 서브넷 및 보안 그룹	Amazon S3 버킷에 대한 인터넷 액세스 및 액세스를 허용하는 옵션을 선택합니다. 보안 그룹을 생성해야 하는 경우 다음 입력으로 Amazon EC2 콘솔에서 그룹을 생성할 수 있습니다.
		• VPC: 인프라 구성에 VPC 사용되는 것과 동일한 항목을 선택합니다. 인터넷에 액세스할 수 있어야 VPC 합니다.
		• 인바운드 규칙:
		  • 유형: SSH
		  • 소스: 사용자 지정
		  • CIDR 블록: 0.0.0.0/0

d. 인프라 구성 생성을 선택합니다.

6. 새 EC2 Image Builder 파이프라인 생성:

a. 이미지 파이프라인 으로 이동하여 이미지 파이프라인 생성 을 선택합니다.

b. 파이프라인 세부 정보 지정 페이지에서 다음을 입력하고 다음을 선택합니다.

- 파이프라인 이름 및 선택적 설명

- 빌드 일정 에서 일정을 설정하거나 베이킹 프로세스를 수동으로 시작하려면 수동AMI을 선택합니다.

c. 레시피 선택 페이지에서 기존 레시피 사용을 선택하고 이전에 생성한 레시피 이름을 입력합니다. Next(다음)를 선택합니다.

d. 이미지 프로세스 정의 페이지에서 기본 워크플로를 선택하고 다음을 선택합니다.

e. 인프라 구성 정의 페이지에서 기존 인프라 구성 사용을 선택하고 이전에 생성한 인프라 구성의 이름을 입력합니다. Next(다음)를 선택합니다.

f. 배포 설정 정의 페이지에서 선택 사항에 대해 다음을 고려합니다.

- 가 인프라 호스트 인스턴스를 제대로 시작할 RES 수 있도록 출력 이미지는 배포된 RES 환경과 동일한 리전에 있어야 합니다. 서비스 기본값을 사용하면 EC2 Image Builder 서비스가 사용되는 리전에서 출력 이미지가 생성됩니다.
- 여러 리전RES에 배포하려는 경우 새 배포 설정 생성을 선택하고 그곳에 리전을 더 추가할 수 있습니다.

g. 선택을 검토하고 파이프라인 생성 을 선택합니다.

7. EC2 Image Builder 파이프라인을 실행합니다.

a. 이미지 파이프라인 에서 생성한 파이프라인을 찾아 선택합니다.

b. 작업 을 선택하고 파이프라인 실행 을 선택합니다.

파이프라인에서 AMI 이미지를 생성하는 데 약 45분에서 1시간이 걸릴 수 있습니다.

8. 생성된 의 AMI ID를 기록하고 의 InfrastructureHostAMI 파라미터 입력으로 AMI 사용합니다the section called “1단계: 제품 시작”.

VPC 엔드포인트 설정

가상 데스크톱을 배포RES하고 시작하려면 프라이빗 서브넷에 대한 액세스 권한이 AWS 서비스 필요합니다. 필요한 액세스를 제공하도록 VPC 엔드포인트를 설정해야 하며 각 엔드포인트에 대해 이러한 단계를 반복해야 합니다.

1. 엔드포인트가 이전에 구성되지 않은 경우 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여에 액세스 에 제공된 지침을 따릅니다.
2. 두 가용 영역 각각에서 프라이빗 서브넷 하나를 선택합니다.

AWS 서비스	서비스 이름
애플리케이션 Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*cloudformation.
Amazon CloudWatch	com.amazonaws.*region*.모니터링
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
Amazon DynamoDB	com.amazonaws.*region*.dynamodb(게이트웨이 엔드포인트 필요)
Amazon EC2	com.amazonaws.*region*.ec2
Amazon ECR	com.amazonaws.*region*.ecr.api
	com.amazonaws.*region*.ecr.dkr
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon EventBridge	com.amazonaws.*region*.events
Amazon FSx	com.amazonaws.*region*.fsx
AWS Key Management Service	com.amazonaws.*region*kms.
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
AWS Lambda	com.amazonaws.*region*.lambda
Amazon S3	com.amazonaws.*region*.s3(에서 기본적으로 생성되는 게이트웨이 엔드포인트가 필요합니다RES.) 격리된 환경에서 버킷을 교차 탑재하려면 추가 Amazon S3 인터페이스 엔드포인트가 필요합니다. Amazon Simple Storage Service 인터페이스 엔드포인트 액세스를 참조하세요.

AWS 서비스	서비스 이름
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
Amazon SES	com.amazonaws.*region*.email-smtp(ex-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 및 cac1-az4 가용 영역에서는 지원되지 않음)
AWS Security Token Service	com.amazonaws.*region*.sts
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssmmessages

VPC 엔드포인트 없이 서비스에 연결

VPC 엔드포인트를 지원하지 않는 서비스와 통합하려면 의 퍼블릭 서브넷에 프록시 서버를 설정할 수 있습니다VPC. AWS Identity Center를 자격 증명 공급자로 사용하여 Research and Engineering Studio 배포에 필요한 최소 액세스 권한이 있는 프록시 서버를 생성하려면 다음 단계를 따르세요.

1. RES 배포에 VPC 사용할 의 퍼블릭 서브넷에서 Linux 인스턴스를 시작합니다.
   - Linux 패밀리 - Amazon Linux 2 또는 Amazon Linux 3
   - 아키텍처 – x86
   - 인스턴스 유형 - t2.micro 이상
   - 보안 그룹 - 포트 3128TCP의 0.0.0.0/0부터
2. 인스턴스에 연결하여 프록시 서버를 설정합니다.
   a. http 연결을 엽니다.
   b. 모든 관련 서브넷에서 다음 도메인에 대한 연결을 허용합니다.
      - .amazonaws.com(일반 AWS 서비스의 경우)

- .amazoncognito.com(Amazon Cognito)
- .awsapps.com(ID 센터용)
- .signin.aws(ID 센터용)
- .amazonaws-us-gov.com(Gov Cloud용)

c. 다른 모든 연결을 거부합니다.

d. 프록시 서버를 활성화하고 시작합니다.

e. 프록시 서버가 수신 대기하는 PORT 에 유의하세요.

3. 프록시 서버에 대한 액세스를 허용하도록 라우팅 테이블을 구성합니다.

   a. VPC 콘솔로 이동하여 인프라 호스트 및 VDI 호스트에 사용할 서브넷의 라우팅 테이블을 식별합니다.

   b. 모든 수신 연결이 이전 단계에서 생성된 프록시 서버 인스턴스로 이동할 수 있도록 라우팅 테이블을 편집합니다.

   c. Infrastructure/에 사용할 모든 서브넷(인터넷 액세스 없음)의 라우팅 테이블에 대해 이 작업을 수행합니다VDIs.

4. 프록시 서버 EC2 인스턴스의 보안 그룹을 수정하고 프록시 서버가 수신 대기 중인 PORT 에서 인바운드 TCP 연결을 허용하는지 확인합니다.

프라이빗 VPC 배포 파라미터 설정

에서는 AWS CloudFormation 템플릿에 특정 파라미터를 the section called “1단계: 제품 시작”입력해야 합니다. VPC 방금 구성한 프라이빗에 성공적으로 배포하려면 다음 파라미터를 명시된 대로 설정해야 합니다.

파라미터	Input
InfrastructureHostAMI	에서 생성된 인프라 AMI ID를 사용합니다the section called “Amazon Machine 이미지 준비(AMIs)”.
IsLoadBalancerInternetFacing	false로 설정합니다.
LoadBalancerSubnets	인터넷 액세스가 없는 프라이빗 서브넷을 선택합니다.

파라미터	Input
InfrastructureHostSubnets	인터넷 액세스가 없는 프라이빗 서브넷을 선택합니다.
VdiSubnets	인터넷 액세스가 없는 프라이빗 서브넷을 선택합니다.
[ClientIP]	모든 VPC IP 주소에 대한 액세스를 허용 VPCCIDR하도록 를 선택할 수 있습니다.

외부 리소스 생성

이 CloudFormation 스택은 네트워킹, 스토리지, 액티브 디렉터리 및 도메인 인증서 (PortalDomainName 가 제공된 경우)를 생성합니다. 제품을 배포하려면 이러한 외부 리소스를 사용할 수 있어야 합니다.

배포 전에 레시피 템플릿을 다운로드할 수 있습니다.

배포 시간: 약 40~90분

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudformation 에서 AWS CloudFormation 콘솔을 엽니다.

   > **Note**
   > 관리자 계정에 있는지 확인합니다.

2. 콘솔에서 템플릿을 시작합니다.

   AWS GovCloud (미국 서부) 리전에 배포하는 경우 GovCloud 파티션 계정에서 템플릿을 시작합니다.

3. 템플릿 파라미터를 입력합니다.

파라미터	기본값	설명
DomainName	`corp.res.com`	Active Directory에 사용되는 도메인입니다. 기본값은 부

파라미터	기본값	설명
		트스트랩 사용자를 설정하는 LDIF 파일에 제공됩니다. 기본 사용자를 사용하려면 값을 기본값으로 둡니다. 값을 변경하려면 업데이트하고 별도의 LDIF 파일을 제공합니다. Active Directory에 사용되는 도메인과 일치할 필요는 없습니다.
SubDomain (GovCloud 만 해당)		이 파라미터는 상용 리전의 경우 선택 사항이지만 GovCloud 리전의 경우 필수입니다. 를 제공하는 경우 파라미터 SubDomain는 DomainName 제공된 에 접두사로 지정됩니다. 제공된 Active Directory 도메인 이름은 하위 도메인이 됩니다.

파라미터	기본값	설명
AdminPassword		Active Directory 관리자(사용자 이름 `Admin`)의 암호입니다. 이 사용자는 초기 부트스트래핑 단계의 활성 디렉터리에 생성되며 이후에 사용되지 않습니다. 중요: 이 필드의 형식은 (1) 일반 텍스트 암호 또는 (2) 키/값 페어 형식ARN의 AWS 보안 암호 형식일 수 있습니다`{"password":"somepassword"}` . 참고: 이 사용자의 암호는 액티브 디렉터리 의 암호 복잡성 요구 사항을 충족해야 합니다.
ServiceAccountPassword		서비스 계정()을 생성하는 데 사용되는 암호입니다`ReadOnlyUser` . 이 계정은 동기화에 사용됩니다. 중요: 이 필드의 형식은 (1) 일반 텍스트 암호 또는 (2) 키/값 페어 형식ARN의 AWS 보안 암호의 형식일 수 있습니다`{"password":"somepassword"}` . 참고: 이 사용자의 암호는 액티브 디렉터리 의 암호 복잡성 요구 사항을 충족해야 합니다.

파라미터	기본값	설명
키페어		SSH 클라이언트를 사용하여 관리 인스턴스를 연결합니다. 참고: AWS Systems Manager Session Manager를 사용하여 인스턴스에 연결할 수도 있습니다.
LDIFS3Path	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	Active Directory 설정의 부트스트래핑 단계에서 가져온 LDIF 파일의 Amazon S3 경로입니다. 자세한 내용은 LDIF 지원 섹션을 참조하세요. 파라미터는 액티브 디렉터리에 여러 사용자를 생성하는 파일로 미리 채워집니다. 파일을 보려면 에서 사용할 수 있는 res.ldif 파일을 참조하세요 GitHub.
ClientIpCidr		사이트에 액세스할 IP 주소입니다. 예를 들어 IP 주소를 선택하고 `[IPADDRESS]/32` 를 사용하여 호스트에서만 액세스를 허용할 수 있습니다. 이 배포 후를 업데이트할 수 있습니다.
ClientPrefixList		활성 디렉터리 관리 노드에 대한 액세스를 제공하려면 접두사 목록을 입력합니다. 관리형 접두사 목록 생성에 대한 자세한 내용은 고객 관리형 접두사 목록 작업을 참조하세요.

파라미터	기본값	설명
EnvironmentName	`res-[environment name]`	`PortalDomainName` 이 제공되는 경우 이 파라미터는 생성된 보안 암호에 태그를 추가하여 환경 내에서 사용할 수 있도록 하는 데 사용됩니다. 이는 RES 스택을 생성할 때 사용되는 `EnvironmentName` 파라미터와 일치해야 합니다. 계정에 여러 환경을 배포하는 경우 고유해야 합니다.
PortalDomainName		GovCloud 배포의 경우 이 파라미터를 입력하지 마세요. 인증서와 보안 암호는 사전 요구 사항 중에 수동으로 생성되었습니다. 계정의 Amazon Route 53의 도메인 이름입니다. 이렇게 하면 퍼블릭 인증서와 키 파일이 생성되어 에 업로드됩니다 AWS Secrets Manager. 자체 도메인 및 인증서가 있는 경우 이 파라미터 및 를 비워 둘 `EnvironmentName` 수 있습니다.

4. 기능 의 모든 확인란을 확인하고 스택 생성 을 선택합니다.

1단계: 제품 시작

이 섹션의 step-by-step 지침에 따라 제품을 구성하고 계정에 배포합니다.

배포 시간: 약 60분

배포하기 전에 이 제품의 CloudFormation 템플릿을 다운로드할 수 있습니다.

AWS GovCloud (미국 서부)에 배포하는 경우 이 템플릿 을 사용합니다.

재스택 - 이 템플릿을 사용하여 제품 및 모든 관련 구성 요소를 시작합니다. 기본 구성은 RES 기본 스택 및 인증, 프런트엔드 및 백엔드 리소스를 배포합니다.

> **Note**
>
> AWS CloudFormation 리소스는 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 구성에서 생성됩니다.

AWS CloudFormation 템플릿은 의 AWS 에 Research and Engineering Studio를 배포합니다 AWS 클라우드. 스택을 시작하기 전에 사전 조건을 충족해야 합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudformation 에서 AWS CloudFormation 콘솔을 엽니다.
2. 템플릿 을 시작합니다.

   AWS GovCloud (미국 서부)에 배포하려면 이 템플릿 을 시작합니다.
3. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 에서 솔루션을 시작하려면 콘솔 탐색 모음의 리전 선택기를 AWS 리전사용합니다.

   > **Note**
   >
   > 이 제품은 현재 일부 에서 사용할 수 없는 Amazon Cognito 서비스를 사용합니다 AWS 리전. Amazon Cognito를 사용할 수 AWS 리전 있는 에서 이 제품을 시작해야 합니다. 리전별 최신 가용성은 AWS 리전 al Services List를 참조하세요.
4. 파라미터 에서 이 제품 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 자동화된 외부 리소스를 배포한 경우 외부 리소스 스택의 출력 탭에서 이러한 파라미터를 찾을 수 있습니다.

파라미터	기본값	설명
EnvironmentName	*<res-demo>*	res-, 11자 이하, 대문자 없음으로 시작하는 RES 환경에 지정된 고유한 이름입니다.

파라미터	기본값	설명
AdministratorEmail		제품 설정을 완료하는 사용자의 이메일 주소입니다. 또한 이 사용자는 통합 실패 시 활성 디렉터리 단일 서명이 있는 경우 브레이크 글라스 사용자 역할을 합니다.
InfrastructureHostAMI	ami-*[numbers or letters only]*	(선택 사항) 모든 인프라 호스트에 사용할 사용자 지정 AMI ID를 제공할 수 있습니다. 현재 지원되는 기본 OS는 Amazon Linux 2입니다. 자세한 내용은 구성 RES준비 완료 AMIs 단원을 참조하십시오.
SSHKeyPair		인프라 호스트에 연결하는 데 사용되는 키 페어입니다.
[ClientIP]	*x.x.x*.0/24 또는 *x.x.x*.0/32	시스템에 대한 연결을 제한하는 IP 주소 필터입니다. 배포 ClientIpCidr 후 를 업데이트할 수 있습니다.
ClientPrefixList		(선택 사항) 가 웹 UI에 직접 액세스하고 Bastion 호스트 SSH에 액세스할 수 있도록 IPs 허용하는 관리형 접두사 목록을 제공합니다.
IAMPermissionBoundary		(선택 사항) 에서 생성된 모든 역할에 권한 경계로 ARN 연결되는 관리형 정책을 제공할 수 있습니다RES. 자세한 내용은 사용자 지정 권한 경계 설정 단원을 참조하십시오.

파라미터	기본값	설명
VpcId		인스턴스가 시작될 VPC 의 ID입니다.
IsLoadBalancerInternetFacing		인터넷 연결 로드 밸런서를 배포하려면 true를 선택합니다(로드 밸런서에 대한 퍼블릭 서브넷 필요). 제한된 인터넷 액세스가 필요한 배포의 경우 false를 선택합니다.
LoadBalancerSubnets		로드 밸런서가 시작될 서로 다른 가용 영역에서 최소 두 개의 서브넷을 선택합니다. 제한된 인터넷 액세스가 필요한 배포의 경우 프라이빗 서브넷을 선택합니다. 인터넷 액세스가 필요한 배포의 경우 퍼블릭 서브넷을 선택합니다. 외부 네트워킹 스택에서 2개 이상 생성된 경우 생성된 모든 항목을 선택합니다.
InfrastructureHostSubnets		인프라 호스트가 시작될 서로 다른 가용 영역에서 최소 2개의 프라이빗 서브넷을 선택합니다. 외부 네트워킹 스택에서 2개 이상 생성된 경우 생성된 모든 항목을 선택합니다.
VdiSubnets		VDI 인스턴스가 시작될 서로 다른 가용 영역에서 최소 2개의 프라이빗 서브넷을 선택합니다. 외부 네트워킹 스택에서 2개 이상 생성된 경우 생성된 모든 항목을 선택합니다.

파라미터	기본값	설명
ActiveDirectoryName	*corp.res.com*	Active Directory의 도메인입니다. 포털 도메인 이름과 일치할 필요는 없습니다.
ADShortName	*corp*	활성 디렉터리의 짧은 이름입니다. 이를 NetBIOS 이름이라고도 합니다.
LDAP 기본	***DC=corp,DC=res,DC=com***	LDAP 계층 구조 내의 기본 LDAP 경로입니다.
LDAPConnectionURI		Active Directory의 호스트 서버에서 연결할 수 있는 단일 ldap:// 경로입니다. 기본 AD 도메인과 함께 자동화된 외부 리소스를 배포한 경우 ldap://corp.res.com 사용할 수 있습니다.
ServiceAccountCredentialsSecretArn		사용자 이름:암호 키/값 페어 형식의 Active Directory ServiceAccount 사용자의 사용자 이름 및 암호가 ARN 포함된 보안 암호를 제공합니다.
UsersOU		동기화할 사용자의 AD 내 조직 단위입니다.
GroupsOU		동기화할 그룹의 AD 내 조직 단위입니다.

파라미터	기본값	설명
SudoersGroupName	RESAdministrators	설치 시 인스턴스에 대한 sudoer 액세스 권한이 있는 모든 사용자와 의 관리자 액세스 권한이 포함된 그룹 이름입니다RES.
ComputersOU		인스턴스가 조인할 AD 내 조직 단위입니다.
D omainTLSCertificate보안 암호ARN		(선택 사항) 도메인 TLS 인증서 암호를 제공하여 AD에 대한 TLS 통신을 ARN 활성화합니다.
EnableLdapIDMapping		UID 및 GID 번호가 에서 생성되는지 SSSD 또는 AD에서 제공하는 번호가 사용되는지 여부를 결정합니다. SSSD 생성 UID 및 를 사용하려면 True로 설정하고 AD에서 UID 사용하고 GID 제공하는 경우 GIDFalse로 설정합니다. 대부분의 경우 이 파라미터를 True로 설정해야 합니다.
DisableADJoin	False	Linux 호스트가 디렉터리 도메인에 가입하지 못하도록 하려면 True로 변경합니다. 그렇지 않으면 기본 설정인 False를 그대로 둡니다.
ServiceAccountUserDN		디렉터리에 서비스 계정 사용자의 고유 이름(DN)을 입력합니다.

파라미터	기본값	설명
SharedHomeFilesystemID		Linux VDI 호스트용 공유 홈 파일 시스템에 사용할 EFS ID입니다.
CustomDomainNamefo rWebApp		(선택 사항) 웹 포털에서 시스템의 웹 부분에 대한 링크를 제공하는 데 사용되는 하위 도메인입니다.
CustomDomainNameforVDI		(선택 사항) 웹 포털에서 시스템 VDI 부분에 대한 링크를 제공하는 데 사용되는 하위 도메인입니다.
ACMCertificateARNf orWebApp		(선택 사항) 기본 구성을 사용하는 경우 제품은 amazonaws.com 도메인에서 웹 애플리케이션을 호스팅합니다. 도메인에서 제품 서비스를 호스팅할 수 있습니다. 자동화된 외부 리소스를 배포한 경우 이 리소스가 자동으로 생성되었으며 res-bi 스택의 출력에서 정보를 찾을 수 있습니다. 웹 애플리케이션에 대한 인증서를 생성해야 하는 경우 섹션을 참조하세요구성 가이드.

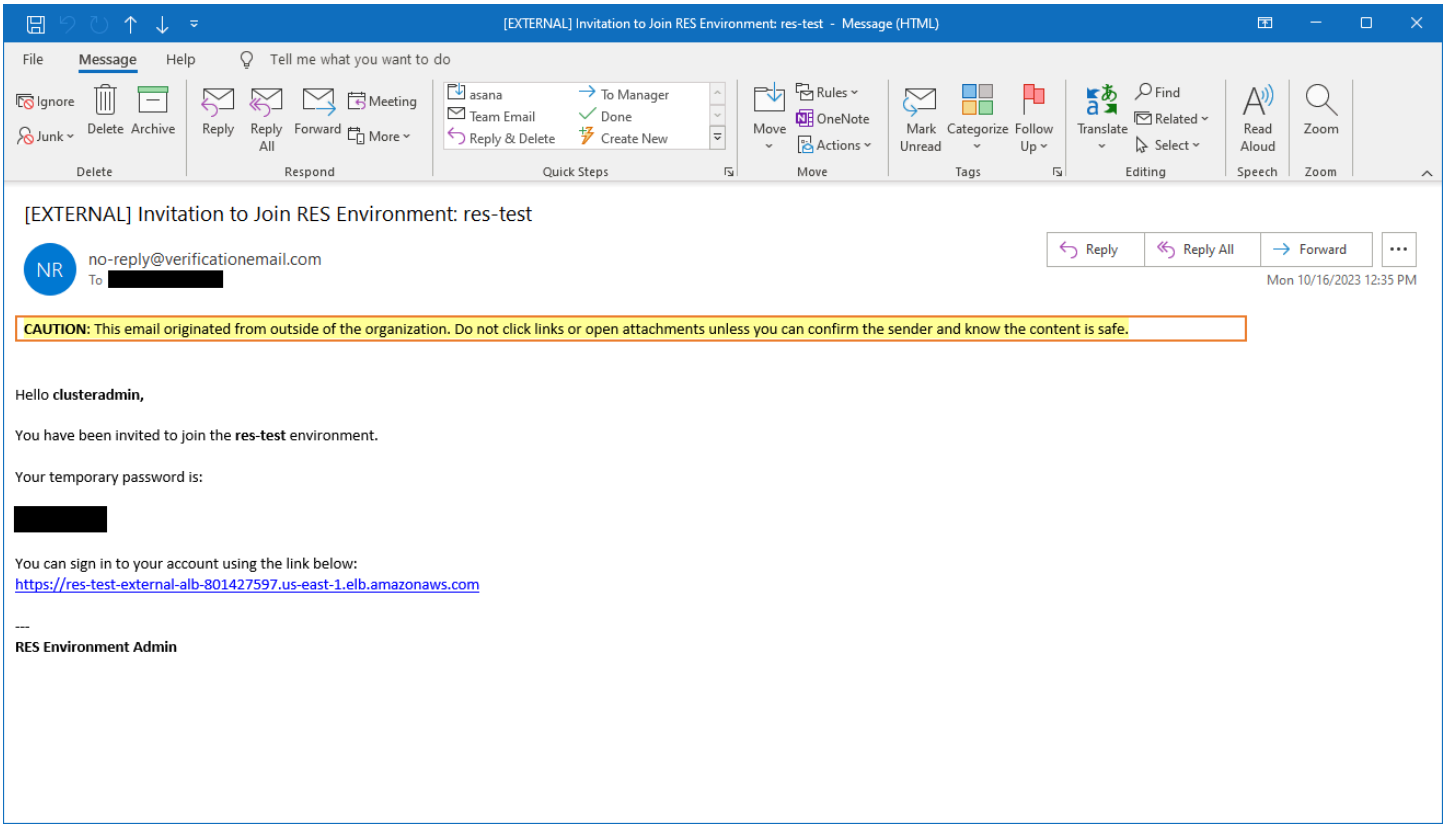
파라미터	기본값	설명
CertificateSecretARNforVDI		(선택 사항) 이 ARN 보안 암호는 웹 포털의 퍼블릭 인증서에 대한 퍼블릭 인증서를 저장합니다. 자동화된 외부 리소스에 포털 도메인 이름을 설정한 경우 res-bi 스택의 출력 탭에서 이 값을 찾을 수 있습니다.
PrivateKeySecretARNforVDI		(선택 사항) 이 ARN 보안 암호는 웹 포털 인증서의 프라이빗 키를 저장합니다. 자동화된 외부 리소스에 포털 도메인 이름을 설정한 경우 res-bi 스택의 출력 탭에서 이 값을 찾을 수 있습니다.

5. [스택 생성(Create stack)]을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 60분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

2단계: 처음 로그인

제품 스택이 계정에 배포되면 보안 인증 정보가 포함된 이메일을 받게 됩니다. URL 를 사용하여 계정에 로그인하고 다른 사용자를 위해 워크스페이스를 구성합니다.



처음 로그인한 후에는 웹 포털에서 SSO 공급자에 연결하도록 설정을 구성할 수 있습니다. 배포 후 구성 정보는 섹션을 참조하세요구성 가이드. `clusteradmin` 는 브레이크 글라스 계정입니다. 이 계정을 사용하여 프로젝트를 생성하고 해당 프로젝트에 사용자 또는 그룹 멤버십을 할당할 수 있으며, 소프트웨어 스택을 할당하거나 데스크톱을 배포할 수 없습니다.

제품 업데이트

Research and Engineering Studio(RES)에는 버전 업데이트가 메이저인지 마이너인지에 따라 제품을 업데이트하는 두 가지 방법이 있습니다.

RES 는 날짜 기반 버전 관리 체계를 사용합니다. 메이저 릴리스는 연도와 월을 사용하며, 마이너 릴리스는 필요한 경우 시퀀스 번호를 추가합니다. 예를 들어 버전 2024.01은 2024년 1월에 메이저 릴리스로 릴리스되었으며 버전 2024.01.01은 해당 버전의 마이너 릴리스 업데이트였습니다.

주제

메이저 버전 업데이트

Research and Engineering Studio는 스냅샷을 사용하여 환경 설정을 잃지 않고 이전 RES 환경에서 최신 환경으로의 마이그레이션을 지원합니다. 또한 이 프로세스를 사용하여 사용자를 온보딩하기 전에 환경에 대한 업데이트를 테스트하고 확인할 수 있습니다.

최신 버전의 로 환경을 업데이트하려면RES:

1. 현재 환경의 스냅샷을 생성합니다. the section called “스냅샷 생성”을 참조하세요.
2. 새 버전으로 재배포RES합니다. the section called “1단계: 제품 시작”을 참조하세요.
3. 업데이트된 환경에 스냅샷을 적용합니다. the section called “스냅샷 적용”을 참조하세요.
4. 모든 데이터가 새 환경으로 성공적으로 마이그레이션되었는지 확인합니다.

마이너 버전 업데이트

에 대한 마이너 버전 업데이트RES의 경우 새 설치가 필요하지 않습니다. AWS CloudFormation 템플릿을 업데이트하여 기존 RES 스택을 업데이트할 수 있습니다. 업데이트를 배포 AWS CloudFormation 하기 전에 에서 현재 RES 환경의 버전을 확인합니다. 템플릿 시작 부분에서 버전 번호를 찾을 수 있습니다.

예: `"Description": "RES_2024.1"`

마이너 버전을 업데이트하려면:

1. 에서 최신 AWS CloudFormation 템플릿을 다운로드합니다the section called “1단계: 제품 시작”.
2. https://console.aws.amazon.com/cloudformation에서 AWS CloudFormation 콘솔을 엽니다.
3. 스택 에서 기본 스택을 찾아 선택합니다. 로 표시되어야 합니다*<stack-name>*.
4. 업데이트를 선택합니다.
5. 현재 템플릿 바꾸기 를 선택합니다.
6. 템플릿 소스로 템플릿 파일 업로드를 선택합니다.
7. 파일 선택을 선택하고 다운로드한 템플릿을 업로드합니다.
8. 스택 세부 정보 지정에서 다음 를 선택합니다. 파라미터를 업데이트할 필요가 없습니다.
9. 스택 옵션 구성에서 다음 를 선택합니다.
10. <stack-name> 검토에서 제출을 선택합니다.

제품 제거

AWS Management Console 또는 를 사용하여 AWS 제품에서 Research and Engineering Studio를 제거할 수 있습니다 AWS Command Line Interface. 이 제품에서 생성한 Amazon Simple Storage Service(Amazon S3) 버킷을 수동으로 삭제해야 합니다. 보존할 데이터를 저장한 경우 이 제품은 <EnvironmentName>-shared-storage-security-group 를 자동으로 삭제하지 않습니다.

사용 AWS Management Console

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 스택 페이지에서 이 제품의 설치 스택을 선택합니다.
3. Delete(삭제)를 선택합니다.

사용 AWS Command Line Interface

환경에서 AWS Command Line Interface (AWS CLI)를 사용할 수 있는지 확인합니다. 설치 지침은 AWS CLI 사용 설명서의 정의 AWS Command Line Interface 섹션을 참조하세요. AWS CLI 가 사용 가능하고 제품이 배포된 리전의 관리자 계정에 구성되어 있는지 확인한 후 다음 명령을 실행합니다.

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

삭제 shared-storage-security-group

> **Warning**
>
> 제품은 의도하지 않은 데이터 손실로부터 보호하기 위해 기본적으로 이 파일 시스템을 유지합니다. 보안 그룹 및 관련 파일 시스템을 삭제하기로 선택하면 해당 시스템 내에 보관된 모든 데이터가 영구적으로 삭제됩니다. 데이터를 백업하거나 새 보안 그룹에 데이터를 재할당하는 것이 좋습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/efs/에서 Amazon EFS 콘솔을 엽니다.
2. 와 연결된 모든 파일 시스템을 삭제합니다*<RES-stack-name>*-shared-storage-security-group. 또는 이러한 파일 시스템을 다른 보안 그룹에 재할당하여 데이터를 유지할 수 있습니다.

3. 에 로그인 AWS Management Console 하고 에서 Amazon EC2 콘솔을 엽니다https://console.aws.amazon.com/ec2/.
4. *<RES-stack-name>*-shared-storage-security-group를 삭제합니다.

Amazon S3 버킷 삭제

이 제품은 우발적 데이터 손실을 방지하기 위해 AWS CloudFormation 스택을 삭제하기로 결정하는 경우 제품 생성 Amazon S3 버킷(옵트인 리전에 배포용)을 유지하도록 구성됩니다. 제품을 제거한 후 데이터를 보존할 필요가 없는 경우 이 S3 버킷을 수동으로 삭제할 수 있습니다. Amazon S3 버킷을 삭제하는 방법은 다음과 같습니다.

1. 에 로그인 AWS Management Console 하고 에서 Amazon S3 콘솔을 엽니다https://console.aws.amazon.com/s3/.
2. 탐색 창에서 버킷을 선택합니다.
3. S3 버킷을stack-name 찾습니다.
4. 각 Amazon S3 버킷을 선택한 다음 비어 있음 을 선택합니다. 각 버킷을 비워야 합니다.
5. S3 버킷을 선택하고 삭제를 선택합니다.

를 사용하여 S3 버킷을 삭제하려면 다음 명령을 AWS CLI실행합니다.

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

> **Note**
>
> --force 명령은 버킷의 내용을 비웁니다.

구성 가이드

이 구성 가이드는 AWS 제품에서 Research and Engineering Studio를 추가로 사용자 지정하고 통합하는 방법에 대한 배포 후 지침을 기술 대상에게 제공합니다.

주제

사용자 및 그룹 관리

Research and Engineering Studio는 모든 SAML 2.0 준수 자격 증명 공급자를 사용할 수 있습니다. 외부 리소스를 RES 사용하여 배포했거나 IAM Identity Center를 사용할 계획인 경우 섹션을 참조하세요IAM Identity Center를 사용하여 Single Sign-On 설정(SSO). 자체 SAML 2.0 호환 자격 증명 공급자가 있는 경우 섹션을 참조하세요Single Sign-On을 위한 자격 증명 공급자 구성(SSO).

주제

IAM Identity Center를 사용하여 Single Sign-On 설정(SSO)

관리형 Active Directory에 연결된 자격 증명 센터가 아직 없는 경우 로 시작합니다1단계: 자격 증명 센터 설정. 관리형 Active Directory와 연결된 자격 증명 센터가 이미 있는 경우 로 시작합니다2단계: 자격 증명 센터에 연결.

> **Note**
>
> AWS GovCloud (미국 서부) 리전에 배포하는 경우 Research and Engineering Studio를 AWS GovCloud (US) 배포한 파티션 계정에 SSO를 설정합니다.

1단계: 자격 증명 센터 설정

IAM Identity Center 활성화

1. AWS Identity and Access Management 콘솔에 로그인합니다.
2. Identity Center 를 엽니다.
3. 활성화를 선택합니다.
4. 에서 활성화를 AWS Organizations 선택합니다.
5. 계속을 선택합니다.

> **Note**
>
> 관리형 Active Directory가 있는 리전과 동일한 리전에 있어야 합니다.

관리형 Active Directory에 IAM Identity Center 연결

IAM Identity Center를 활성화한 후 다음 권장 설정 단계를 완료합니다.

1. 탐색 창에서 설정을 선택합니다.
2. 자격 증명 소스 에서 작업을 선택하고 자격 증명 소스 변경을 선택합니다.
3. 기존 디렉터리 에서 디렉터리를 선택합니다.
4. Next(다음)를 선택합니다.
5. 변경 사항을 검토하고 확인 상자에 **ACCEPT** 를 입력합니다.
6. ID 소스 변경을 선택합니다.

사용자 및 그룹을 자격 증명 센터에 동기화

의 변경 사항이 관리형 Active Directory에 IAM Identity Center 연결 완료되면 녹색 확인 배너가 나타납니다.

1. 확인 배너에서 가이드 설정 시작 을 선택합니다.
2. 속성 매핑 구성 에서 다음을 선택합니다.
3. 사용자 섹션에서 동기화할 사용자를 입력합니다.
4. 추가를 선택합니다.
5. Next(다음)를 선택합니다.
6. 변경 사항을 검토한 다음 구성 저장을 선택합니다.
7. 동기화 프로세스에 몇 분 정도 걸릴 수 있습니다. 동기화되지 않는 사용자에 대한 경고 메시지가 표시되면 동기화 재개 를 선택합니다.

사용자 활성화

1. 메뉴에서 사용자 를 선택합니다.
2. 액세스를 활성화하려는 사용자(들)를 선택합니다.
3. 사용자 액세스 활성화를 선택합니다.

2단계: 자격 증명 센터에 연결

IAM Identity Center에서 애플리케이션 설정

1. IAM Identity Center 콘솔 을 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 추가를 선택합니다.
4. 설정 기본 설정에서 설정하려는 애플리케이션이 있음을 선택합니다.
5. 애플리케이션 유형에서 SAML 2.0을 선택합니다.
6. Next(다음)를 선택합니다.
7. 사용하려는 표시 이름과 설명을 입력합니다.
8. IAM Identity Center 메타데이터 에서 IAM Identity Center SAML 메타데이터 파일의 링크를 복사합니다. RES 포털로 IAM Identity Center를 구성할 때 이 정보가 필요합니다.
9. 애플리케이션 속성 에서 애플리케이션 시작 URL을 입력합니다. 예: `<your-portal-domain>/sso`.
10. 애플리케이션 ACS URLURL에서 RES 포털의 리디렉션을 입력합니다. 이를 찾으려면:

    a. 환경 관리에서 일반 설정 을 선택합니다.

b. 자격 증명 공급자 탭을 선택합니다.

c. Single Sign-On 에서 SAML 리디렉션 URL을 찾을 수 있습니다.

11. 애플리케이션 SAML 대상 에서 Amazon Cognito 를 입력합니다URN.

    urn을 생성하려면:

    a. RES 포털에서 일반 설정 을 엽니다.

    b. 자격 증명 공급자 탭에서 사용자 풀 ID를 찾습니다.

    c. 이 문자열에 사용자 풀 ID를 추가합니다.

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

12. Amazon Cognito 를 입력한 후 제출을 URN선택합니다.

애플리케이션에 대한 속성 매핑 구성

1. Identity Center 에서 생성된 애플리케이션의 세부 정보를 엽니다.
2. 작업 을 선택한 다음 속성 매핑 편집 을 선택합니다.
3. 제목에 **`${user:email}`**을 입력합니다.
4. 형식에서 를 선택합니다emailAddress.
5. 새 속성 매핑 추가를 선택합니다.
6. 애플리케이션의 사용자 속성 에 '이메일'을 입력합니다.
7. IAM Identity Center의 이 문자열 값 또는 사용자 속성에 매핑에서 를 입력합니다**`${user:email}`**.
8. 형식 에서 '지정되지 않음'을 입력합니다.
9. Save changes(변경 사항 저장)를 선택합니다.

IAM Identity Center의 애플리케이션에 사용자 추가

1. Identity Center에서 생성된 애플리케이션에 할당된 사용자를 열고 사용자 할당을 선택합니다.
2. 애플리케이션 액세스를 할당할 사용자를 선택합니다.
3. 사용자 배정를 선택합니다.

RES 환경 내에서 IAM Identity Center 설정

1. 연구 및 엔지니어링 스튜디오 환경의 환경 관리에서 일반 설정 을 엽니다.
2. 자격 증명 공급자 탭을 엽니다.
3. Single Sign-On에서 편집(상태 옆)을 선택합니다.
4. 다음 정보로 양식을 작성합니다.
   a. 를 선택합니다SAML.
   b. 공급자 이름 에 사용자 친화적 이름을 입력합니다.
   c. 메타데이터 문서 엔드포인트 입력을 URL선택합니다.
   d. 에서 복사URL한 를 입력합니다IAM Identity Center에서 애플리케이션 설정.
   e. 공급자 이메일 속성 에서 '이메일'을 입력합니다.
   f. 제출을 선택합니다.
5. 페이지를 새로 고치고 상태가 활성화된 것으로 표시되는지 확인합니다.

Single Sign-On을 위한 자격 증명 공급자 구성(SSO)

Research and Engineering Studio는 SAML 2.0 자격 증명 공급자와 통합되어 RES 포털에 대한 사용자 액세스를 인증합니다. 이 단계에서는 선택한 SAML 2.0 자격 증명 공급자와 통합하는 방법을 제공합니다. IAM Identity Center를 사용하려면 섹션을 참조하세요IAM Identity Center를 사용하여 Single Sign-On 설정(SSO).

> **Note**
>
> 사용자의 이메일은 어IDPSAML설션 및 Active Directory에서 일치해야 합니다. 자격 증명 공급자를 Active Directory에 연결하고 주기적으로 사용자를 동기화해야 합니다.

주제

- 자격 증명 공급자 구성
- 자격 증명 공급자RES를 사용하도록 구성
- 비프로덕션 환경에서 자격 증명 공급자 구성
- SAML IdP 문제 디버깅

자격 증명 공급자 구성

이 섹션에서는 RES Amazon Cognito 사용자 풀의 정보로 자격 증명 공급자를 구성하는 단계를 제공합니다.

1. RES 는 RES 포털 및 프로젝트에 액세스할 수 있는 사용자 ID가 있는 AD(AWS 관리형 AD 또는 자체 프로비저닝 AD)가 있다고 가정합니다. AD를 자격 증명 서비스 공급자에 연결하고 사용자 자격 증명을 동기화합니다. 자격 증명 공급자의 설명서를 확인하여 AD를 연결하고 사용자 자격 증명을 동기화하는 방법을 알아봅니다. 예를 들어 AWS IAM Identity Center 사용 설명서의 Active Directory를 자격 증명 소스로 사용을 참조하세요.
2. 자격 증명 공급자(IdP)RES에서 SAML 용 2.0 애플리케이션을 구성합니다. 이 구성에는 다음 파라미터가 필요합니다.
   - SAML 리디렉션 URL - IdPURL가 서비스 제공업체에 SAML 2.0 응답을 보내는 데 사용하는 입니다.

     > **Note**
     >
     > IdP 에 따라 SAML리디렉션의 이름이 다를 URL 수 있습니다.
     >
     > - 애플리케이션 URL
     > - 어설션 소비자 서비스(ACS) URL
     > - ACS POST 바인딩 URL

     를 가져오려면 URL

     1. 관리자 또는 clusteradminRES으로 에 로그인합니다.
     2. 환경 관리 ⇒ 일반 설정 ⇒ 자격 증명 공급자 로 이동합니다.
     3. SAML 리디렉션을 URL선택합니다.

   - SAML 대상 URI - 서비스 공급자 측 SAML 대상 엔터티의 고유 ID입니다.

     > **Note**
     >
     > IdP 에 따라 SAML 대상의 이름이 다를 URI 수 있습니다.
     >
     > - ClientID

- 애플리케이션 SAML 대상
- SP 엔터티 ID

다음 형식으로 입력을 제공합니다.

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

SAML 대상을 찾으려면 URI

1. 관리자 또는 clusteradminRES으로 에 로그인합니다.
2. 환경 관리 ⇒ 일반 설정 ⇒ 자격 증명 공급자 로 이동합니다.
3. 사용자 풀 ID를 선택합니다.

3. 에 게시된 어SAML설션에는 다음 필드/클레임이 사용자의 이메일 주소로 설정되어 있어야 RES 합니다.
   - SAML 제목 또는 NameID
   - SAML 이메일
4. IdP는 구성에 따라 SAML어설션에 필드/클레임을 추가합니다. RES 에는 이러한 필드가 필요합니다. 대부분의 공급자는 기본적으로 이러한 필드를 자동으로 채웁니다. 구성해야 하는 경우 다음 필드 입력 및 값을 참조하세요.

   - AudienceRestriction - 를 로 설정합니다`urn:amazon:cognito:sp:user-pool-id`. Replace *`user-pool-id`* Amazon Cognito 사용자 풀의 ID를 사용합니다.

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

   - 응답 - 를 `InResponseTo`로 설정합니다`https://user-pool-domain/saml2/idpresponse`. Replace *`user-pool-domain`* Amazon Cognito 사용자 풀의 도메인 이름을 사용합니다.

     ```
     <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 - 사용자 풀 `saml2/idpresponse` 엔드포인트와 원래 SAML 요청 IDInResponseTo로 `Recipient` 설정합니다.

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

- AuthnStatement - 를 다음과 같이 구성합니다.

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

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

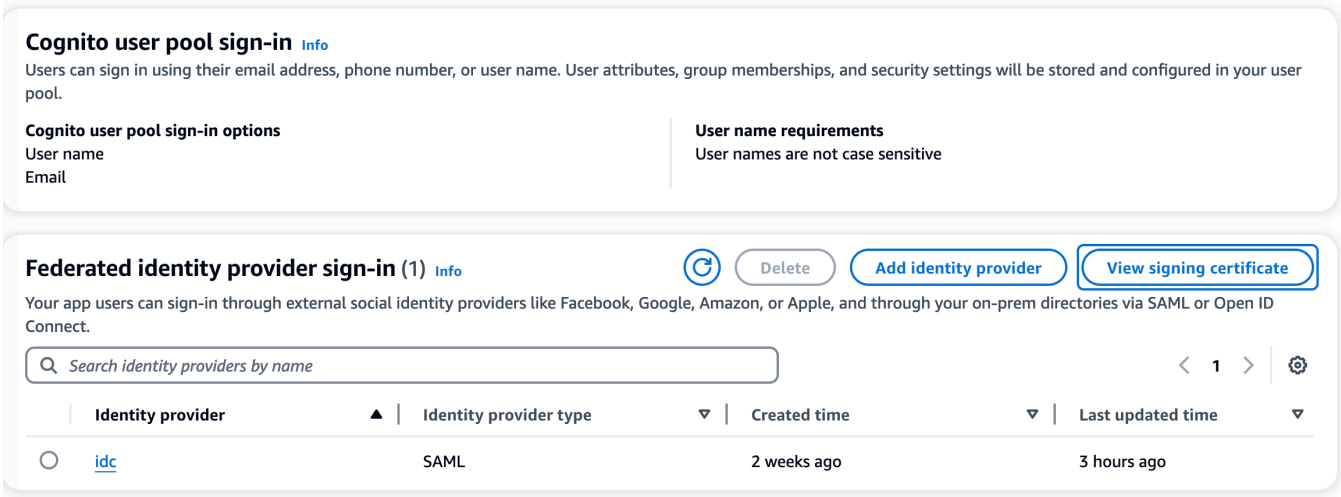
5. SAML 애플리케이션에 로그아웃 URL 필드가 있는 경우 로 설정합니다*<domain-url>*`/saml2/logout`.

   도메인을 가져오려면 URL

   1. 관리자 또는 clusteradminRES으로 에 로그인합니다.
   2. 환경 관리 ⇒ 일반 설정 ⇒ 자격 증명 공급자 로 이동합니다.
   3. 도메인 URL을 선택합니다.
6. IdP가 서명 인증서를 수락하여 Amazon Cognito 와 신뢰를 쌓는 경우 Amazon Cognito 서명 인증서를 다운로드하여 IdP 에 업로드합니다.

서명 인증서를 가져오려면

1. 시작하기에서 Amazon Cognito 콘솔을 엽니다. AWS Management Console
2. 사용자 풀을 선택합니다. 사용자 풀은 여야 합니다`res-<environment name>-user-pool`.
3. 로그인 환경 탭을 선택합니다.
4. 페더레이션 자격 증명 공급자 로그인 섹션에서 서명 인증서 보기를 선택합니다.



이 인증서를 사용하여 Active Directory를 설정하고IDP, 를 추가하고`relying party trust`, 이 의존 당사자에 대한 SAML 지원을 활성화할 수 있습니다.

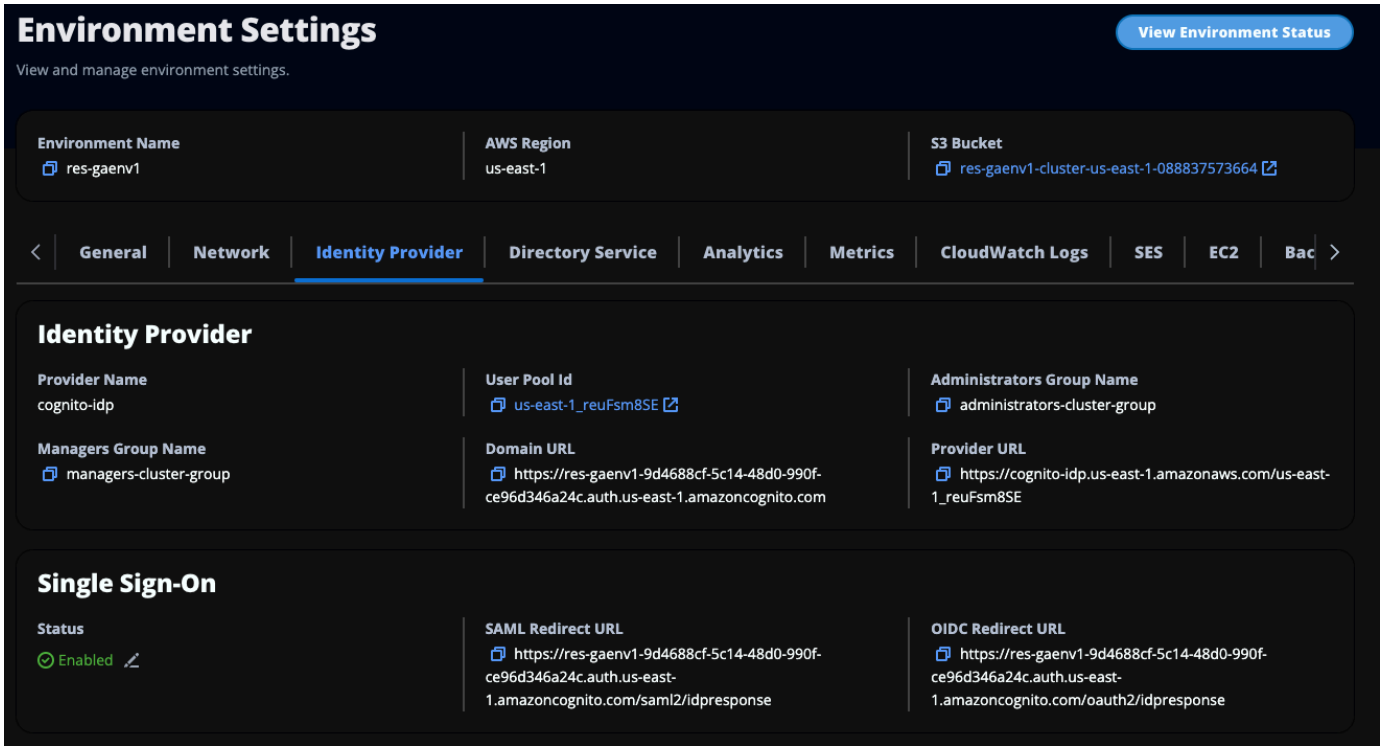
> **Note**
>
> 이는 Keycloak 및 에는 적용되지 않습니다IDC.

5. 애플리케이션 설정이 완료되면 SAML 2.0 애플리케이션 메타데이터 XML 또는 를 다운로드합니다URL. 다음 섹션에서 사용합니다.

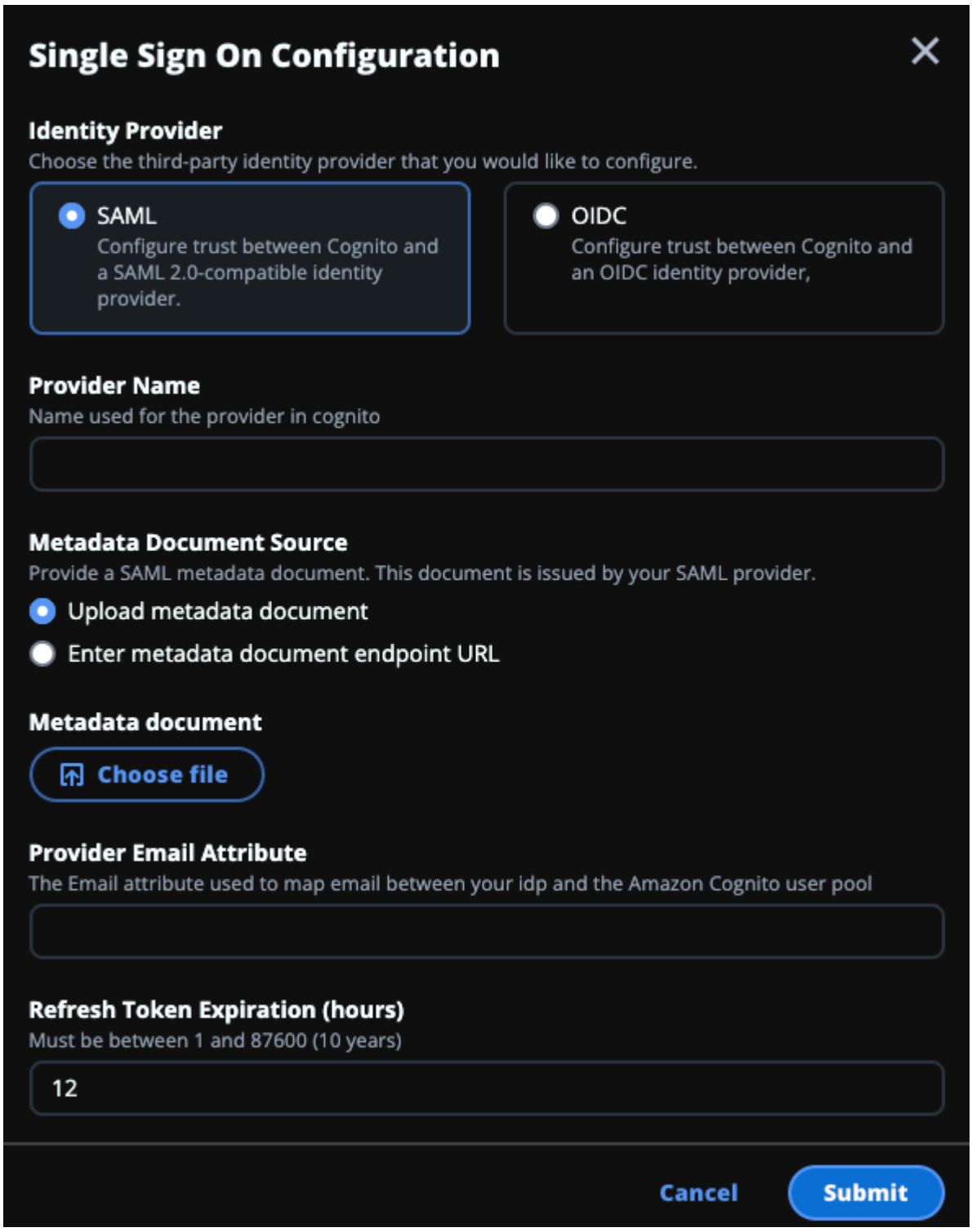
자격 증명 공급자RES를 사용하도록 구성

에 대한 Single Sign-On 설정을 완료하려면 RES

1. 관리자 또는 clusteradminRES으로 에 로그인합니다.
2. 환경 관리 ⇒ 일반 설정 ⇒ 자격 증명 공급자 로 이동합니다.



3. Single Sign-On 에서 상태 표시기 옆의 편집 아이콘을 선택하여 Single Sign-On 구성 페이지를 엽니다.



a. 자격 증명 공급자 에서 를 선택합니다SAML.

b. 공급자 이름 에 자격 증명 공급자의 고유한 이름을 입력합니다.

> **Note**
>
> 다음 이름은 허용되지 않습니다.
>
> - Cognito
> - IdentityCenter

c. 메타데이터 문서 소스 에서 적절한 옵션을 선택하고 메타데이터 XML 문서를 업로드하거나 자격 증명 공급자URL의 를 제공합니다.

d. 공급자 이메일 속성 에 텍스트 값 를 입력합니다`email`.

e. 제출을 선택합니다.

4. 환경 설정 페이지를 다시 로드합니다. 구성이 올바른 경우 Single Sign-On이 활성화됩니다.

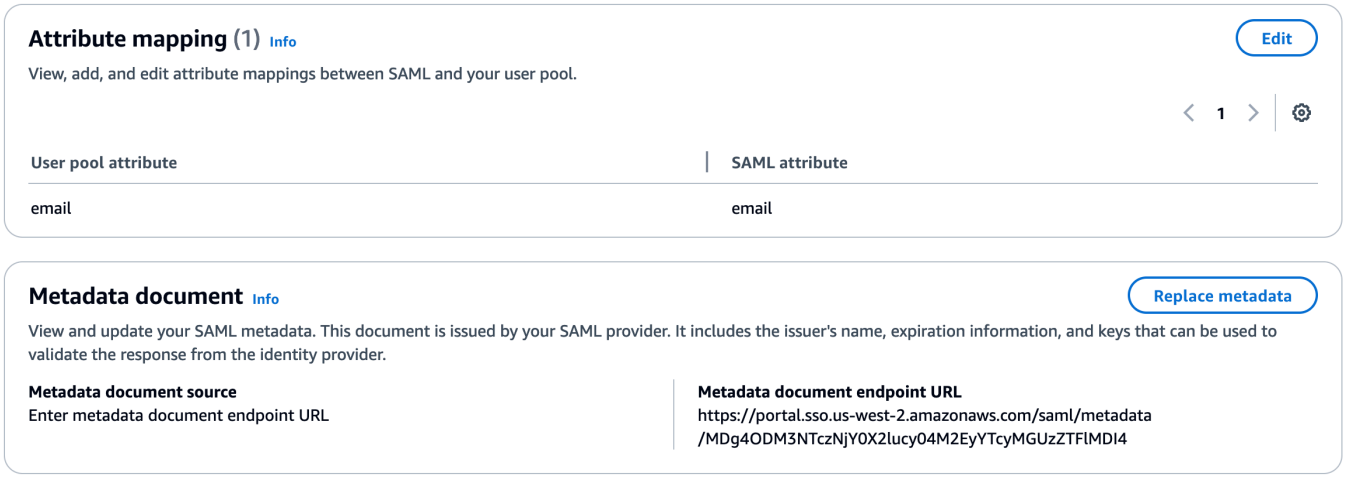
비프로덕션 환경에서 자격 증명 공급자 구성

제공된 외부 리소스를 사용하여 비프로덕션 RES 환경을 생성하고 IAM Identity Center를 자격 증명 공급자로 구성한 경우 Okta와 같은 다른 자격 증명 공급자를 구성해야 할 수 있습니다. RES SSO 활성화 양식에는 세 가지 구성 파라미터가 필요합니다.

1. 공급자 이름 - 수정할 수 없음
2. 메타데이터 문서 또는 URL - 수정할 수 있습니다.
3. 공급자 이메일 속성 - 수정할 수 있습니다.

메타데이터 문서 및 공급자 이메일 속성을 수정하려면 다음을 수행합니다.

1. Amazon Cognito 콘솔로 이동합니다.
2. 탐색에서 사용자 풀 을 선택합니다.
3. 사용자 풀 개요 를 보려면 사용자 풀을 선택합니다.
4. 로그인 환경 탭에서 페더레이션 자격 증명 공급자 로그인으로 이동하여 구성된 자격 증명 공급자를 엽니다.
5. 일반적으로 메타데이터를 변경하고 속성 매핑을 변경하지 않고 그대로 두면 됩니다. 속성 매핑을 업데이트하려면 편집을 선택합니다. 메타데이터 문서 를 업데이트하려면 메타데이터 바꾸기 를 선택합니다.



6. 속성 매핑을 편집한 경우 DynamoDB 에서 `<environment name>.cluster-settings` 테이블을 업데이트해야 합니다.

   a. DynamoDB 콘솔을 열고 탐색에서 테이블을 선택합니다.

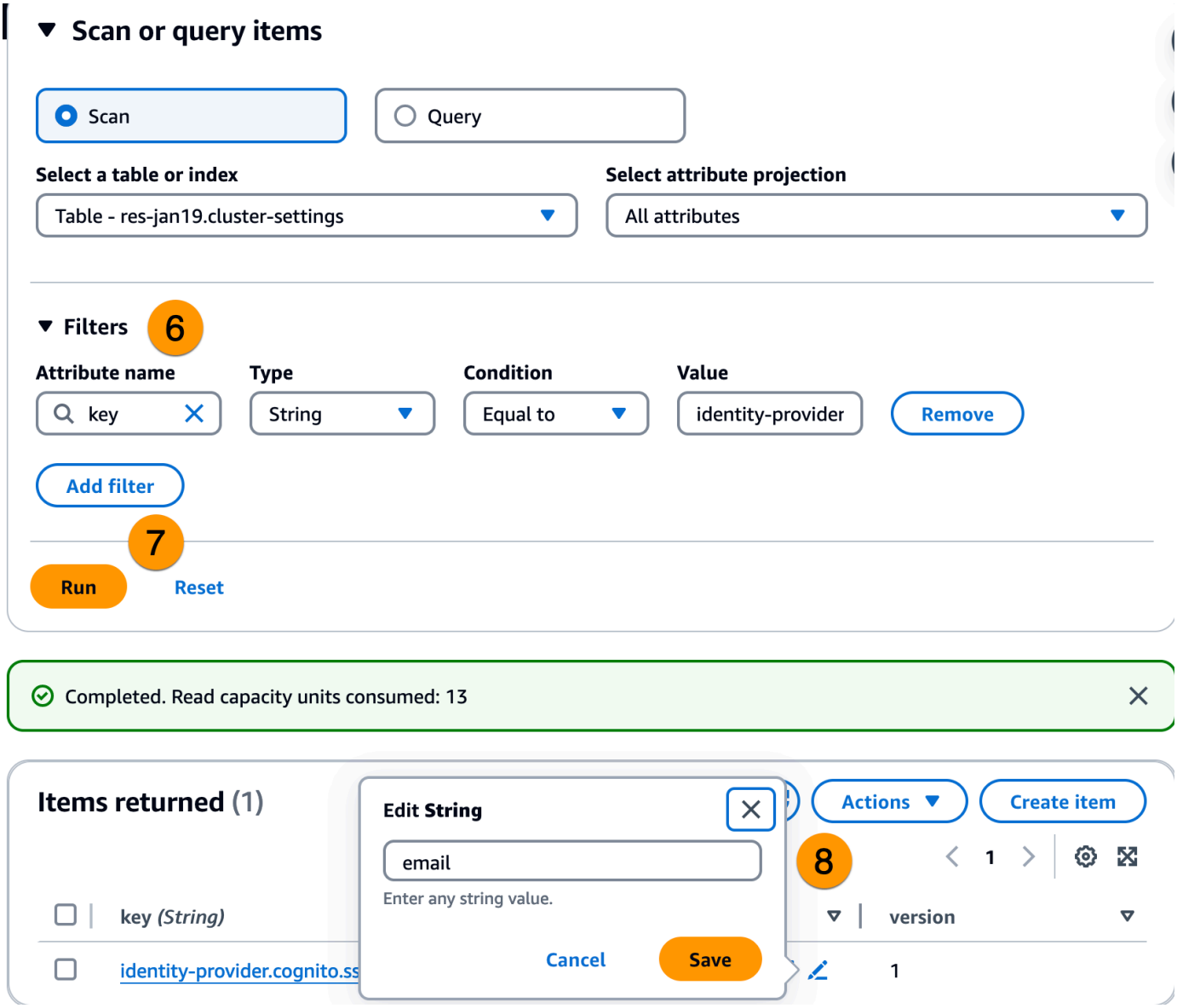
   b. `<environment name>.cluster-settings` 테이블을 찾아 선택하고 작업 메뉴에서 항목 탐색을 선택합니다.

   c. 스캔 또는 쿼리 항목에서 필터로 이동하여 다음 파라미터를 입력합니다.

      - 속성 이름 - `key`
      - 값 - `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Run(실행)을 선택합니다.

7. 반환된 항목에서 `identity-provider.cognito.sso_idp_provider_email_attribute` 문자열을 찾고 편집을 선택하여 Amazon Cognito의 변경 사항과 일치하도록 문자열을 수정합니다.



SAML IdP 문제 디버깅

SAML-tracer — Chrome 브라우저에 이 확장을 사용하여 SAML 요청을 추적하고 어SAML설션 값을 확인할 수 있습니다. 자세한 내용은 Chrome 웹 스토어의 SAML-tracer를 참조하세요.

SAML 개발자 도구 - SAML 인코딩된 값을 디코딩하고 SAML어설션의 필수 필드를 확인하는 데 사용할 수 있는 도구를 OneLogin 제공합니다. 자세한 내용은 OneLogin 웹 사이트의 Base 64 Decode + Inflate를 참조하세요.

Amazon CloudWatch Logs - RES 로그에서 오류 또는 경고가 있는지 CloudWatch 로그를 확인할 수 있습니다. 로그는 이름 형식이 인 로그 그룹에 있습니다*res-environment-name*/cluster-manager.

Amazon Cognito 설명서 - Amazon Cognito와의 SAML 통합에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 사용자 풀에 SAML 자격 증명 공급자 추가를 참조하세요.

사용자의 암호 설정

1. AWS Directory Service 콘솔에서 생성된 스택의 디렉터리를 선택합니다.
2. 작업 메뉴에서 사용자 암호 재설정을 선택합니다.
3. 사용자를 선택하고 새 암호를 입력합니다.
4. 암호 재설정을 선택합니다.

하위 도메인 생성

사용자 지정 도메인을 사용하는 경우 포털의 웹 및 VDI 부분을 지원하도록 하위 도메인을 설정해야 합니다.

> **Note**
>
> AWS GovCloud (미국 서부) 리전에 배포하는 경우 도메인 퍼블릭 호스팅 영역을 호스팅하는 상용 파티션 계정에서 웹 애플리케이션과 VDI 하위 도메인을 설정합니다.

1. Route 53 콘솔 을 엽니다.
2. 생성한 도메인을 찾아 레코드 생성을 선택합니다.
3. '웹'을 레코드 이름 로 입력합니다.
4. 를 레코드 유형 CNAME으로 선택합니다.
5. 값 에 초기 이메일에서 받은 링크를 입력합니다.
6. 레코드 생성을 선택합니다.
7. 에 대한 레코드를 생성하려면 NLB 주소를 VDC검색합니다.
    a. AWS CloudFormation 콘솔을 엽니다.
    b. <environment-name>-vdc를 선택합니다.

c. 리소스를 선택하고 를 엽니다<environmentname>-vdc-external-nlb.

d. 에서 DNS 이름을 복사합니다NLB.

8. Route 53 콘솔 을 엽니다.
9. 도메인을 찾아 레코드 생성 을 선택합니다.
10. 레코드 이름 아래에 를 입력합니다vdc.
11. 레코드 유형에서 를 선택합니다CNAME.
12. 에 를 NLB입력합니다DNS.
13. Create Record Set(레코드 세트 생성)를 선택합니다.

ACM 인증서 생성

기본적으로 는 도메인 amazonaws.com 사용하여 애플리케이션 로드 밸런서에서 웹 포털을 RES 호스팅합니다. 자체 도메인을 사용하려면 사용자가 제공하거나 AWS Certificate Manager ()에서 요청한 퍼블릭SSL/TLS인증서를 구성해야 합니다ACM. 를 사용하는 경우 클라이언트와 웹 서비스 호스트 간의 SSL/TLS 채널을 암호화하는 파라미터로 제공해야 하는 AWS 리소스 이름을 ACM받게 됩니다.

> **Tip**
>
> 외부 리소스 데모 패키지를 배포하는 경우 에서 외부 리소스 스택을 배포할 PortalDomainName 때 에 선택한 도메인을 입력해야 합니다외부 리소스 생성.

사용자 지정 도메인에 대한 인증서를 생성하려면:

1. 콘솔에서 AWS Certificate Manager 를 열어 퍼블릭 인증서를 요청합니다. AWS GovCloud (미국 서부)에 배포하는 경우 GovCloud 파티션 계정에서 인증서를 생성합니다.
2. 퍼블릭 인증서 요청을 선택하고 다음 를 선택합니다.
3. 도메인 이름 에서 *.PortalDomainName 및 모두에 대한 인증서를 요청합니다PortalDomainName.
4. 검증 방법에서 DNS 검증을 선택합니다.
5. 요청을 선택합니다.
6. 인증서 목록에서 요청된 인증서를 엽니다. 각 인증서에는 보류 중인 유효성 검사가 상태로 표시됩니다.

> **Note**
>
> 인증서가 표시되지 않으면 목록을 새로 고칩니다.

7. 다음 중 하나를 수행합니다.
   - 상용 배포:

     요청된 각 인증서의 인증서 세부 정보에서 Route 53에서 레코드 생성을 선택합니다. 인증서 상태가 발급됨 으로 변경되어야 합니다.
   - GovCloud 배포:

     AWS GovCloud (미국 서부)에 배포하는 경우 CNAME 키와 값을 복사합니다. 상용 파티션 계정에서 값을 사용하여 퍼블릭 호스팅 영역에 새 레코드를 생성합니다. 인증서 상태가 발급됨으로 변경되어야 합니다.
8. 새 인증서를 의 파라미터로 입력ARN에 복사합니다`ACMCertificateARNforWebApp`.

Amazon CloudWatch Logs

Research and Engineering Studio는 설치 CloudWatch 중에 에 다음 로그 그룹을 생성합니다. 기본 보존은 다음 표를 참조하세요.

CloudWatch 로그 그룹	Retention
`/aws/lambda/ <installation-stack-name>-cluster-endpoints`	만료되지 않음
`/aws/lambda/ <installation-stack-name>-cluster-manager-scheduled-ad-sync`	만료되지 않음
`/aws/lambda/ <installation-stack-name>-cluster-settings`	만료되지 않음
`/aws/lambda/ <installation-stack-name>-oauth-credentials`	만료되지 않음

CloudWatch 로그 그룹	Retention
/aws/lambda/ *<installation-stack-name>*-self-signed-certificate	만료되지 않음
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	만료되지 않음
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	만료되지 않음
/aws/lambda/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope	만료되지 않음
/*<installation-stack-name>* / cluster-manager	3개월
/*<installation-stack-name>* /vdc/ controller	3개월
/*<installation-stack-name>* /vdc/ dcv-broker	3개월
/*<installation-stack-name>* /vdc/ dcv-connection-gateway	3개월

로그 그룹의 기본 보존을 변경하려면 CloudWatch 콘솔로 이동하여 CloudWatch 로그에서 로그 데이터 보존 변경 의 지침을 따르세요.

사용자 지정 권한 경계 설정

2024년 4월부터 사용자 지정 권한 경계를 연결하여 RES에서 생성한 역할을 선택적으로 수정할 수 있습니다. 사용자 지정 권한 경계는 권한 경계를 IAMPermissionBoundary 파라미터의 일부로 제공하여 RES AWS CloudFormation 설치의 ARN 일부로 정의할 수 있습니다. 이 파라미터를 비워 두면 RES 역할에 권한 경계가 설정되지 않습니다. 다음은 RES 역할이 운영해야 하는 작업 목록입니다. 사용하려는 권한 경계가 다음 작업을 명시적으로 허용하는지 확인합니다.

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

구성 RES준비 완료 AMIs

RES준비된 Amazon Machine Images(AMIs)를 사용하면 사용자 지정 에 가상 데스크톱 인스턴스(VDIs)에 대한 RES 종속성을 사전 설치할 수 있습니다AMIs. RES-ready를 사용하면 미리 베이킹된 이

미지를 사용하는 VDI 인스턴스의 부팅 시간을 AMIs 개선할 수 있습니다. EC2 Image Builder를 사용하여 를 빌드하고 새 소프트웨어 스택AMIs으로 등록할 수 있습니다. Image Builder에 대한 자세한 내용은 Image Builder 사용 설명서 섹션을 참조하세요.

시작하기 전에 최신 버전의 를 배포RES해야 합니다.

주제

- RES 환경에 액세스할 IAM 역할 준비
- EC2 Image Builder 구성 요소 생성
- EC2 Image Builder 레시피 준비
- EC2 Image Builder 인프라 구성
- Image Builder 이미지 파이프라인 구성
- Image Builder 이미지 파이프라인 실행
- 에 새 소프트웨어 스택 등록 RES

RES 환경에 액세스할 IAM 역할 준비

EC2 Image Builder에서 RES 환경 서비스에 액세스하려면 RES-라는 IAM 역할을 생성하거나 수정해야 합니다EC2InstanceProfileForImageBuilder. Image Builder에서 사용할 IAM 역할을 구성하는 방법에 대한 자세한 내용은 Image Builder 사용 설명서의 AWS Identity and Access Management (IAM)를 참조하세요.

역할에는 다음이 필요합니다.

- 신뢰할 수 있는 관계에는 Amazon EC2 서비스가 포함됩니다.
- mazonSSMManagedInstanceCore 및 EC2InstanceProfileForImageBuilder 정책.
- 배포된 RES 환경에 대한 DynamoDB 및 Amazon S3 액세스가 제한된 사용자 지정 RES 정책입니다.

  (이 정책은 고객 관리형 또는 고객 인라인 정책 문서일 수 있습니다.)

신뢰할 수 있는 관계 엔터티:

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

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

RES 정책:

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

EC2 Image Builder 구성 요소 생성

Image Builder 사용 설명서의 Image Builder 콘솔을 사용하여 구성 요소 생성 지침을 따릅니다.

구성 요소 세부 정보를 입력합니다.

1. 유형 에서 빌드를 선택합니다.
2. 이미지 운영 체제(OS)에서 Linux 또는 Windows를 선택합니다.
3. 구성 요소 이름 에 와 같은 의미 있는 이름을 입력합니다**research-and-engineering-studio-vdi-<operating-system>**.
4. 구성 요소의 버전 번호를 입력하고 선택적으로 설명을 추가합니다.
5. 정의 문서 에 다음 정의 파일을 입력합니다. 오류가 발생하는 경우 YAML 파일은 공간에 민감하며 가장 가능성이 높은 원인입니다.

   Linux

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

```
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

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

```
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

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

```
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

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

```
            delaySeconds: 0
```

6. 선택적 태그를 생성하고 구성 요소 생성 을 선택합니다.

EC2 Image Builder 레시피 준비

EC2 Image Builder 레시피는 이미지를 사용자 지정하고 모든 것이 예상대로 작동하는지 확인하기 위해 추가하는 구성 요소 세트와 함께 새 이미지를 생성하는 시작점으로 사용할 기본 이미지를 정의합니다. 필요한 RES 소프트웨어 종속성을 AMI 사용하여 대상을 구성하려면 레시피를 생성하거나 수정해야 합니다. 레시피에 대한 자세한 내용은 레시피 관리를 참조하세요.

RES 는 다음 이미지 운영 체제를 지원합니다.

- Amazon Linux 2(x86 및 ARM64)
- Ubuntu 22.04.3(x86)
- RHEL 8(x86) 및 9(x86)
- Windows 2019, 2022(x86)

Create a new recipe

1. 에서 EC2 Image Builder 콘솔을 엽니다https://console.aws.amazon.com/imagebuilder.
2. 저장된 리소스 에서 이미지 레시피 를 선택합니다.
3. 이미지 레시피 생성을 선택합니다.
4. 고유한 이름과 버전 번호를 입력합니다.
5. 에서 지원하는 기본 이미지를 선택합니다RES.
6. 인스턴스 구성 에서 SSM 에이전트가 사전 설치되지 않은 경우 에이전트를 설치합니다. 사용자 데이터 및 기타 필요한 사용자 데이터에 정보를 입력합니다.

   > **Note**
   >
   > SSM 에이전트를 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요.
   >
   > - Linux용 EC2 인스턴스에 SSM 에이전트를 수동으로 설치합니다.
   > - Windows Server용 EC2 인스턴스에 SSM 에이전트를 수동으로 설치 및 제거합니다.

7. Linux 기반 레시피의 경우 Amazon 관리형 `aws-cli-version-2-linux` 빌드 구성 요소를 레시피에 추가합니다. RES 설치 스크립트는 를 AWS CLI 사용하여 DynamoDB 클러스터 설정

의 구성 값에 대한 VDI 액세스를 제공합니다. Windows에는 이 구성 요소가 필요하지 않습니다.

8. Linux 또는 Windows 환경을 위해 생성된 EC2 Image Builder 구성 요소를 추가하고 필요한 파라미터 값을 입력합니다. 필수 입력은 AWSAccountID, RESEnvRegion, RESEnvName및 입니다RESEnvReleaseVersion.

> **Important**
>
> Linux 환경의 경우 먼저 `aws-cli-version-2-linux` 빌드 구성 요소가 추가된 순서대로 이러한 구성 요소를 추가해야 합니다.

9. (권장) Amazon 관리형 `simple-boot-test-<linux-or-windows>` 테스트 구성 요소를 추가하여 를 시작할 AMI 수 있는지 확인합니다. 이는 최소 권장 사항입니다. 요구 사항에 맞는 다른 테스트 구성 요소를 선택할 수 있습니다.
10. 필요한 경우 선택적 섹션을 완료하고 원하는 다른 구성 요소를 추가한 다음 레시피 생성을 선택합니다.

Modify a recipe

기존 EC2 Image Builder 레시피가 있는 경우 다음 구성 요소를 추가하여 사용할 수 있습니다.

1. Linux 기반 레시피의 경우 Amazon 관리형 `aws-cli-version-2-linux` 빌드 구성 요소를 레시피에 추가합니다. RES 설치 스크립트는 AWS CLI 를 사용하여 DynamoDB 클러스터 설정의 구성 값에 대한 VDI 액세스를 제공합니다. Windows에는 이 구성 요소가 필요하지 않습니다.
2. Linux 또는 Windows 환경을 위해 생성된 EC2 Image Builder 구성 요소를 추가하고 필요한 파라미터 값을 입력합니다. 필수 입력은 AWSAccountID, RESEnvRegion, RESEnvName및 입니다RESEnvReleaseVersion.

> **Important**
>
> Linux 환경의 경우 먼저 `aws-cli-version-2-linux` 빌드 구성 요소가 추가된 순서대로 이러한 구성 요소를 추가해야 합니다.

3. 필요한 경우 선택적 섹션을 완료하고 원하는 다른 구성 요소를 추가한 다음 레시피 생성을 선택합니다.

EC2 Image Builder 인프라 구성

인프라 구성을 사용하여 Image Builder가 Image Builder 이미지를 빌드하고 테스트하는 데 사용하는 Amazon EC2 인프라를 지정할 수 있습니다. 와 함께 사용하려면 새 인프라 구성을 생성하거나 기존 인프라 구성을 사용하도록 선택할 RES수 있습니다.

- 새 인프라 구성을 생성하려면 인프라 구성 생성을 참조하세요.
- 기존 인프라 구성을 사용하려면 인프라 구성을 업데이트합니다.

Image Builder 인프라를 구성하려면:

1. IAM 역할 에 이전에 에서 구성한 역할을 입력합니다RES 환경에 액세스할 IAM 역할 준비.
2. 인스턴스 유형 에서 메모리가 4GB 이상인 유형을 선택하고 선택한 기본 AMI 아키텍처를 지원합니다. Amazon EC2 인스턴스 유형 을 참조하세요.
3. VPC, 서브넷 및 보안 그룹 의 경우 소프트웨어 패키지를 다운로드하려면 인터넷 액세스를 허용해야 합니다. RES 환경의 `cluster-settings` DynamoDB 테이블 및 Amazon S3 클러스터 버킷에 대한 액세스도 허용되어야 합니다.

Image Builder 이미지 파이프라인 구성

Image Builder 이미지 파이프라인은 기본 이미지, 빌드 및 테스트용 구성 요소, 인프라 구성 및 배포 설정을 조립합니다. RES에 대해 이미지 파이프라인을 구성하려면 새 파이프라인을 생성하거나 기존 파이프라인을 사용하도록 선택할 AMIs수 있습니다. 자세한 내용은 Image Builder 사용 설명서의 AMI 이미지 파이프라인 생성 및 업데이트를 참조하세요.

Create a new Image Builder pipeline

1. 에서 Image Builder 콘솔을 엽니다https://console.aws.amazon.com/imagebuilder.
2. 탐색 창에서 이미지 파이프라인 을 선택합니다.
3. 이미지 파이프라인 생성을 선택합니다.
4. 고유한 이름, 선택적 설명, 일정 및 빈도를 입력하여 파이프라인 세부 정보를 지정합니다.
5. 레시피 선택 에서 기존 레시피 사용을 선택하고 에서 생성된 레시피를 선택합니다EC2 Image Builder 레시피 준비. 레시피 세부 정보가 올바른지 확인합니다.
6. 이미지 생성 프로세스 정의 에서 사용 사례에 따라 기본 워크플로 또는 사용자 지정 워크플로를 선택합니다. 대부분의 경우 기본 워크플로로 충분합니다. 자세한 내용은 Image Builder 파이프라인의 EC2 이미지 워크플로 구성을 참조하세요.

7. 인프라 구성 정의 에서 기존 인프라 구성 선택을 선택하고 에서 생성된 인프라 구성을 선택합니다EC2 Image Builder 인프라 구성. 인프라 세부 정보가 올바른지 확인합니다.
8. 배포 설정 정의 에서 서비스 기본값 을 사용하여 배포 설정 생성을 선택합니다. 출력 이미지는 RES 환경 AWS 리전 과 동일한 에 있어야 합니다. 서비스 기본값을 사용하면 Image Builder가 사용되는 리전에 이미지가 생성됩니다.
9. 파이프라인 세부 정보를 검토하고 파이프라인 생성 을 선택합니다.

Modify an existing Image Builder pipeline

1. 기존 파이프라인을 사용하려면 세부 정보를 수정하여 에서 생성된 레시피를 사용합니다EC2 Image Builder 레시피 준비.
2. Save changes(변경 사항 저장)를 선택합니다.

Image Builder 이미지 파이프라인 실행

구성된 출력 이미지를 생성하려면 이미지 파이프라인을 시작해야 합니다. 이미지 레시피의 구성 요소 수에 따라 빌드 프로세스에 최대 1시간이 걸릴 수 있습니다.

이미지 파이프라인을 실행하려면:

1. 이미지 파이프라인 에서 에서 생성된 파이프라인을 선택합니다Image Builder 이미지 파이프라인 구성.
2. 작업 에서 파이프라인 실행 을 선택합니다.

에 새 소프트웨어 스택 등록 RES

1. 의 지침에 따라 소프트웨어 스택을 등록the section called “소프트웨어 스택(AMIs)”합니다.
2. AMI ID 에 에 내장된 출력 이미지의 AMI ID를 입력합니다Image Builder 이미지 파이프라인 실행.

관리자 안내서

이 관리자 안내서는 기술 대상을 위한 추가 지침을 제공하며 AWS , 제품에서 Research and Engineering Studio를 추가로 사용자 지정하고 통합하는 방법을 설명합니다.

주제

보안 암호 관리

Research and Engineering Studio는 를 사용하여 다음 보안 암호를 유지합니다 AWS Secrets Manager. RES 는 환경 생성 중에 보안 암호를 자동으로 생성합니다. 환경 생성 중에 관리자가 입력한 보안 암호는 파라미터로 입력됩니다.

비밀 이름	설명	RES 생성됨	관리자가 입력됨
`<envname> -sso-client-secret`	환경을 위한 Single Sign-On OAuth2 Client Secret	✓	
`<envname> -vdc-client-secret`	vdc ClientSecret	✓	
`<envname> -vdc-client-id`	vdc ClientId	✓	
`<envname> -vdc-gateway-certificate-private-key`	도메인의 자체 서명된 인증서 프라이빗 키	✓	
`<envname> -vdc-gateway-`	도메인에 대한 자체 서명 인증서	✓	

비밀 이름	설명	RES 생성됨	관리자가 입력됨
certificate-certificate			
<envname> -cluster-manager-client-secret	클러스터 관리자 ClientSecret	✓	
<envname> -cluster-manager-client-id	클러스터 관리자 ClientId	✓	
<envname> -external-private-key	도메인의 자체 서명된 인증서 프라이빗 키	✓	
<envname> -external-certificate	도메인에 대한 자체 서명 인증서	✓	
<envname> -internal-private-key	도메인의 자체 서명된 인증서 프라이빗 키	✓	
<envname> -internal-certificate	도메인에 대한 자체 서명 인증서	✓	
<envname> -directoryservice-ServiceAccountUserDN	ServiceAccount 사용자의 고유 이름(DN) 속성입니다.	✓	

다음 보안 암호 ARN 값은 DynamoDB의 *<envname>*-cluster-settings 테이블에 포함됩니다.

키	소스
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	스택
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	스택
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	스택
directoryservice.root_username_secret_arn	
vdc.client_secret	스택
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	스택
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	스택
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	스택
cluster-manager.client_secret	

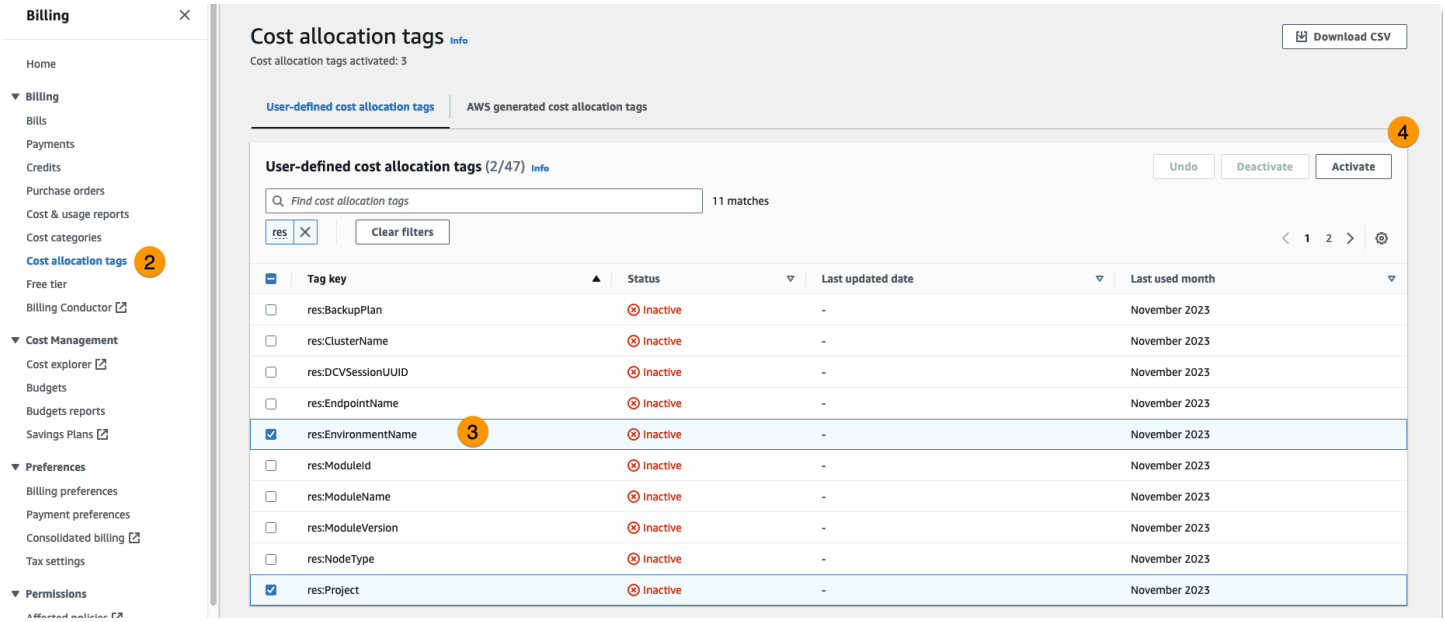
비용 모니터링 및 제어

> **Note**
>
> 연구 및 엔지니어링 스튜디오 프로젝트를 에 연결하는 AWS Budgets 것은 에서 지원되지 않습니다 AWS GovCloud (US).

비용 관리에 도움이 되도록 AWS Cost Explorer를 통해 예산을 생성하는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은 각 의 요금 웹 페이지를 참조하세요the section called “AWS 이 제품의 서비스”.

비용 추적을 지원하기 위해 RES 프로젝트를 내에서 생성된 예산에 연결할 수 있습니다 AWS Budgets. 먼저 청구 비용 할당 태그 내에서 환경 태그를 활성화해야 합니다.

1. 에 로그인 AWS Management Console 하고 에서 AWS Billing 콘솔을 엽니다https://console.aws.amazon.com/billing/.
2. 비용 할당 태그 를 선택합니다.
3. `res:Project` 및 `res:EnvironmentName` 태그를 검색하고 선택합니다.
4. 활성화를 선택합니다.

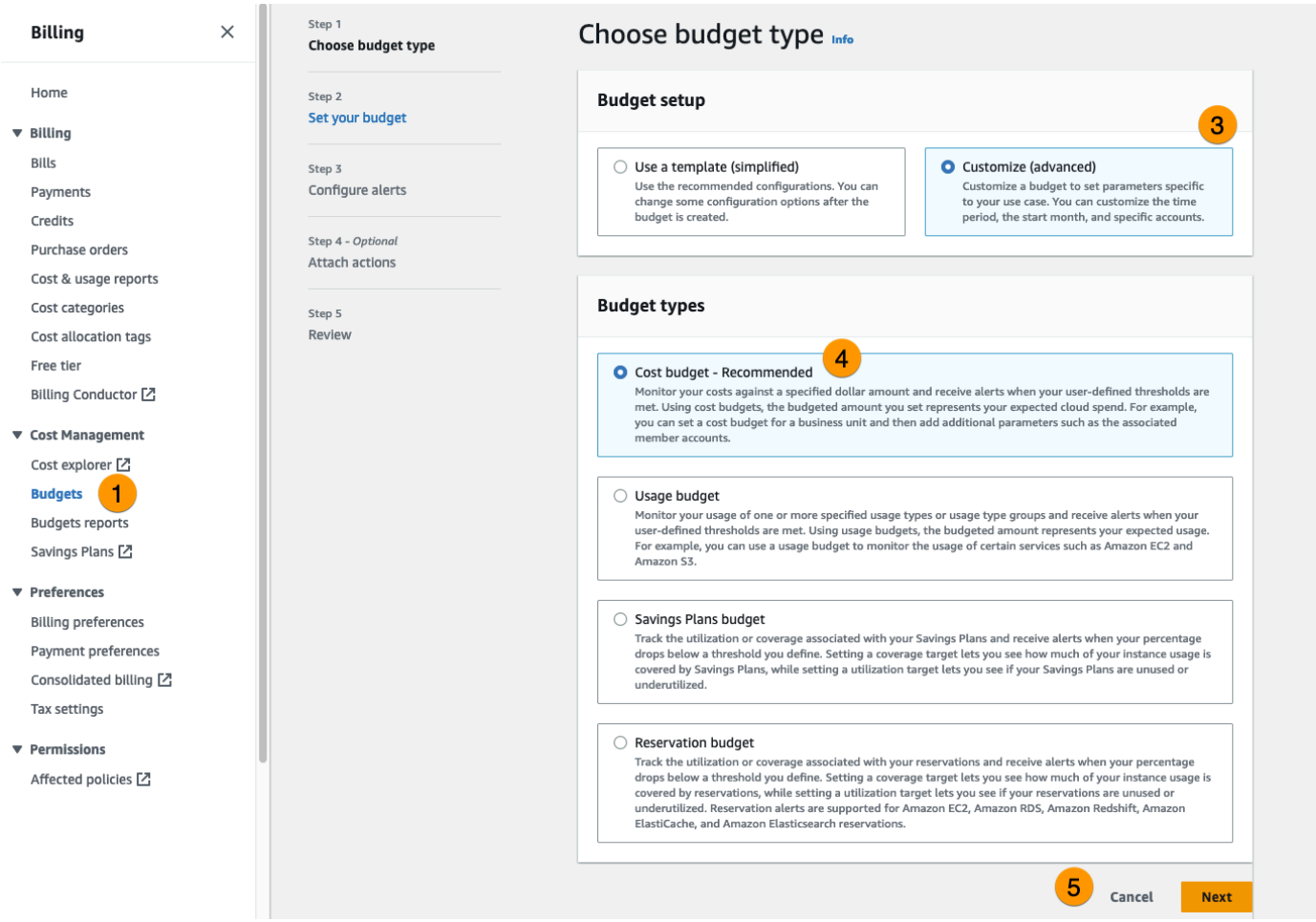


> **Note**
>
> 배포 후 RES 태그가 나타나는 데 최대 하루가 걸릴 수 있습니다.

RES 리소스에 대한 예산을 생성하려면:

1. 결제 콘솔에서 예산을 선택합니다.
2. 예산 생성을 선택합니다.
3. 예산 설정에서 사용자 지정(고급)을 선택합니다.

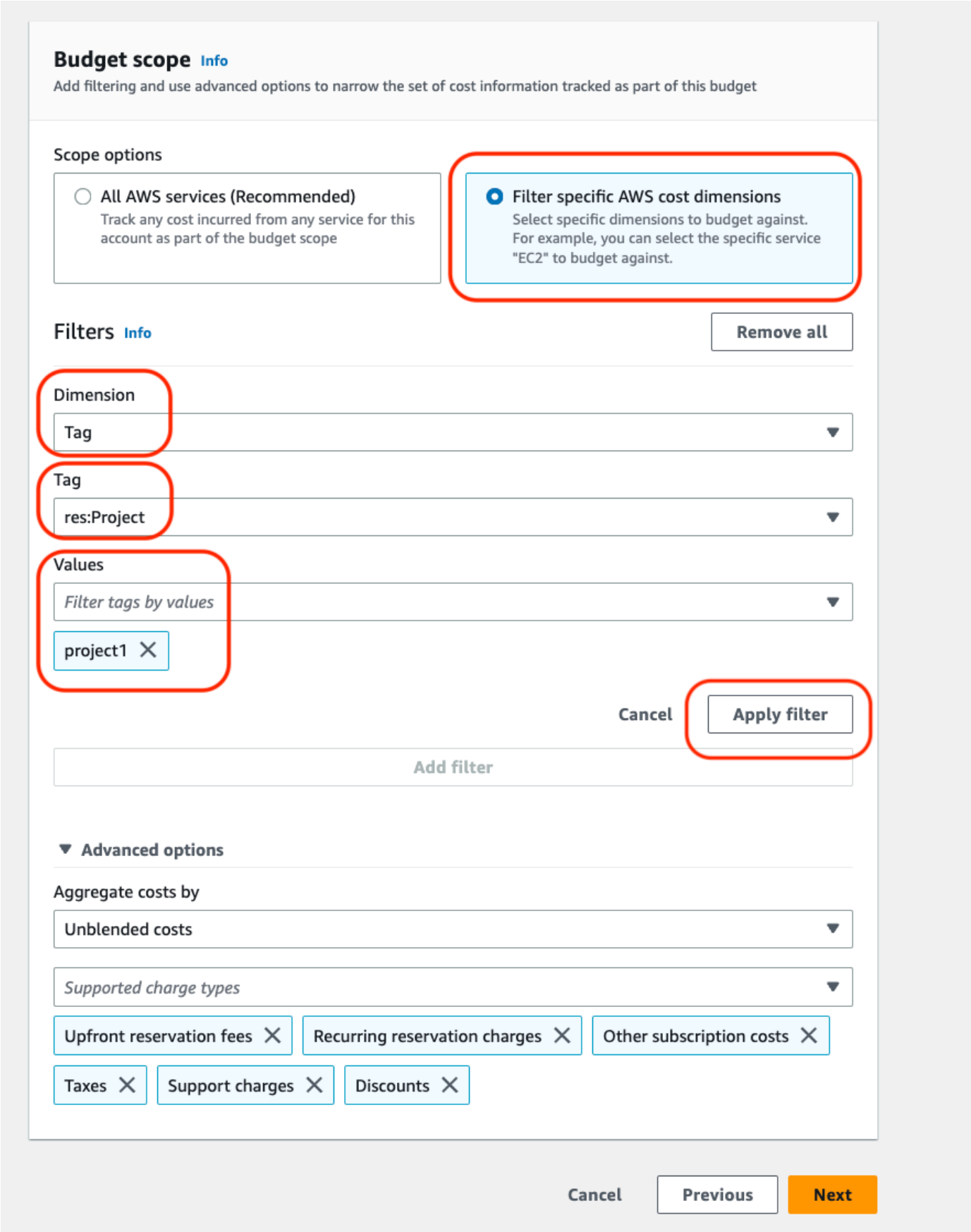
4. 예산 유형에서 비용 예산 - 권장 을 선택합니다.
5. Next(다음)를 선택합니다.



6. 세부 정보 에서 예산의 의미 있는 예산 이름을 입력하여 계정의 다른 예산과 구분합니다. 예: *<EnvironmentName>-<ProjectName>-<BudgetName>*.
7. 예산 금액 설정에서 프로젝트에 예산을 책정한 금액을 입력합니다.
8. 예산 범위 에서 특정 AWS 비용 차원 필터링 을 선택합니다.
9. [Add filter]를 선택합니다.
10. 차원에서 태그 를 선택합니다.
11. 태그 에서 res:Project 를 선택합니다.

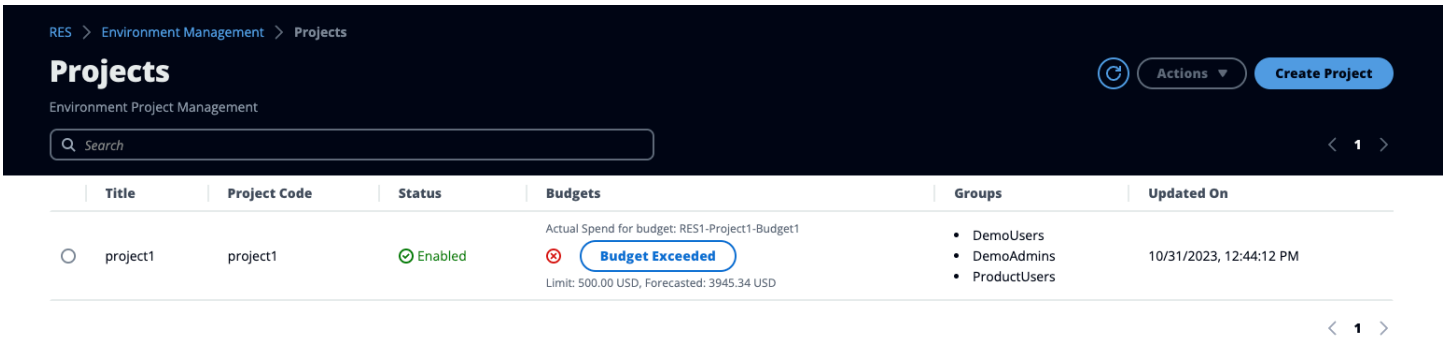
> **Note**
>
> 태그와 값을 사용할 수 있게 되려면 최대 2일이 걸릴 수 있습니다. 프로젝트 이름을 사용할 수 있게 되면 예산을 생성할 수 있습니다.

12. 값 아래에서 프로젝트 이름을 선택합니다.
13. 필터 적용을 선택하여 프로젝트 필터를 예산에 연결합니다.
14. Next(다음)를 선택합니다.


Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Filters Info
Remove all
Dimension
Tag
Tag
res:Project
Values
Filter tags by values
project1
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. (선택 사항) 알림 임계값을 추가합니다.
16. Next(다음)를 선택합니다.
17. (선택 사항) 알림이 구성된 경우 작업 연결을 사용하여 알림으로 원하는 작업을 구성합니다.
18. Next(다음)를 선택합니다.
19. 예산 구성을 검토하고 추가 예산 파라미터 아래에 올바른 태그가 설정되었는지 확인합니다.
20. 예산 생성을 선택합니다.

이제 예산이 생성되었으므로 프로젝트의 예산을 활성화할 수 있습니다. 프로젝트의 예산을 설정하려면 섹션을 참조하세요the section called “프로젝트 편집”. 예산이 초과되면 가상 데스크톱이 시작되지 않습니다. 데스크톱이 시작되는 동안 예산이 초과되면 데스크톱은 계속 작동합니다.



예산을 변경해야 하는 경우 콘솔로 돌아가 예산 금액을 편집합니다. 변경 사항이 내에서 적용되려면 최대 15분이 걸릴 수 있습니다RES. 또는 프로젝트를 편집하여 예산을 비활성화할 수 있습니다.

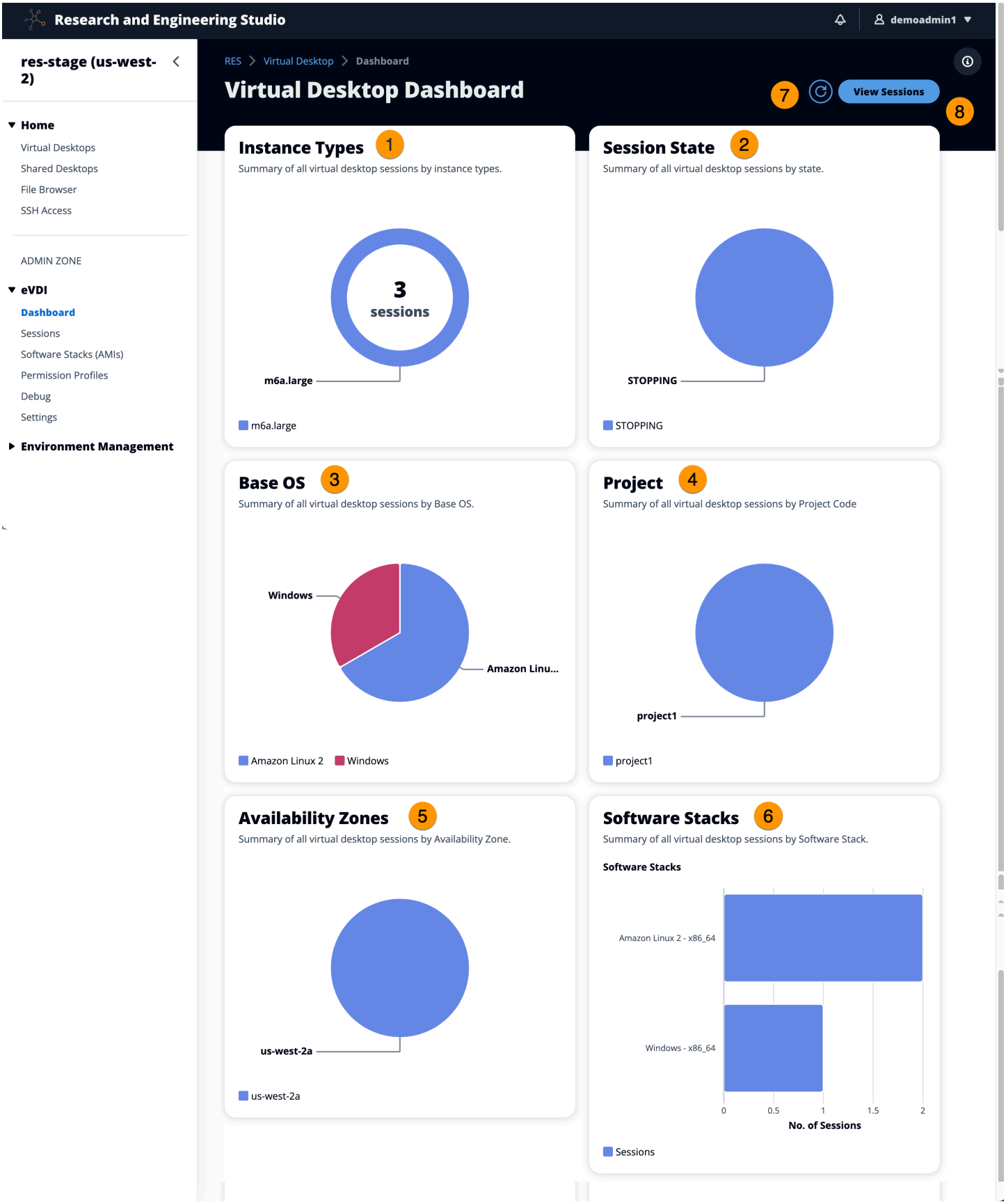
세션 관리

세션 관리는 세션을 개발하고 테스트하기 위한 유연하고 대화형 환경을 제공합니다. 관리 사용자는 사용자가 프로젝트 환경 내에서 대화형 세션을 생성하고 관리하도록 허용할 수 있습니다.

주제

- 대시보드
- 세션
- 소프트웨어 스택(AMIs)
- 디버깅
- 데스크톱 설정

대시보드


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

세션 관리 대시보드는 관리자에게 다음에 대한 빠른 보기를 제공합니다.

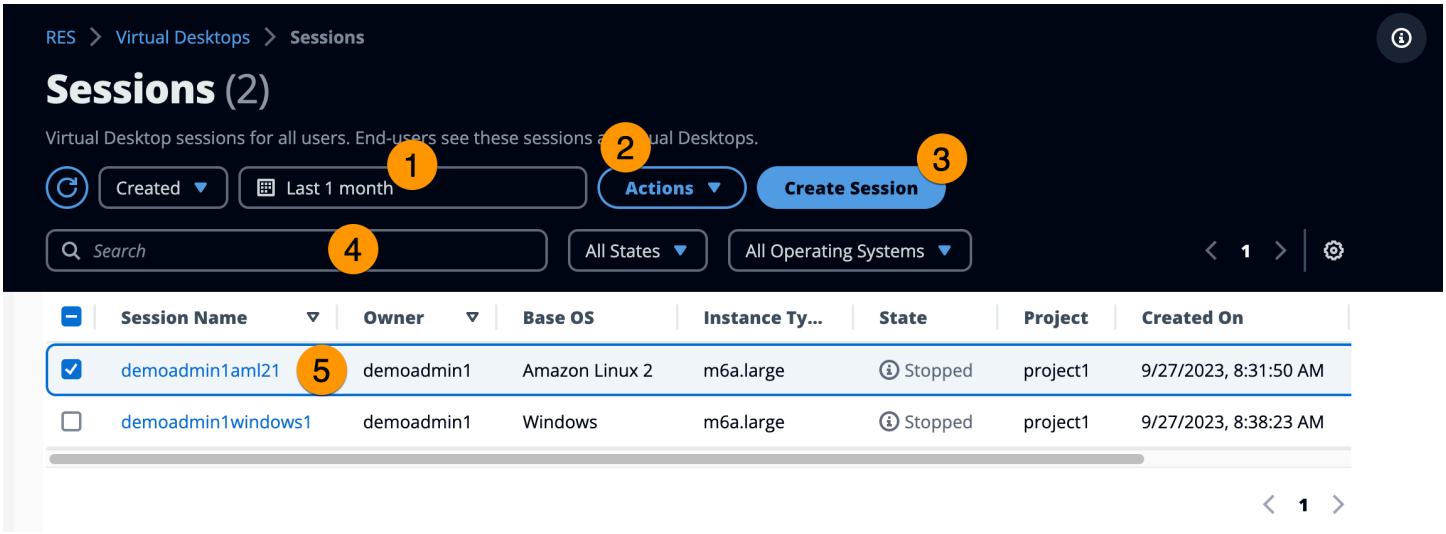
1. 인스턴스 타입
2. 세션 상태
3. 기본 OS
4. 프로젝트
5. 가용 영역
6. 소프트웨어 스택

또한 관리자는 다음을 수행할 수 있습니다.

7. 대시보드를 새로 고쳐 정보를 업데이트합니다.
8. 세션 보기를 선택하여 세션으로 이동합니다.

세션

세션에는 Research and Engineering Studio 내에서 생성된 모든 가상 데스크톱이 표시됩니다. 세션 페이지에서 세션 정보를 필터링 및 보거나 새 세션을 생성할 수 있습니다.



1. 메뉴를 사용하여 지정된 기간 내에 생성되거나 업데이트된 세션별로 결과를 필터링합니다.
2. 세션을 선택하고 작업 메뉴를 사용하여 다음을 수행합니다.
   a. 세션 재개(들)
   b. 세션 중지/최대 절전 모드(들)

c. 강제 중지/최대 절전 모드 세션(들)

d. 세션 종료(들)

e. 강제 종료 세션(들)

f. 세션(들) 상태

g. 소프트웨어 스택 생성

3. 세션 생성을 선택하여 새 세션을 생성합니다.
4. 이름으로 세션을 검색하고 상태 및 운영 체제로 필터링합니다.
5. 세션 이름을 선택하여 자세한 내용을 확인합니다.

세션 생성

1. 세션 생성을 선택합니다. 새 Virtual Desktop 모달 시작이 열립니다.
2. 새 세션의 세부 정보를 입력합니다.
3. (선택 사항) 고급 옵션 표시를 켜면 서브넷 ID 및 DCV 세션 유형과 같은 추가 세부 정보를 제공합니다.
4. 제출을 선택합니다.

Launch New Virtual Desktop

Session Name
Enter a name for the virtual desktop

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

User
Select the user to create the session for

Project
Select the project under which the session will get created

Operating System
Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack
Select the software stack for your virtual desktop

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

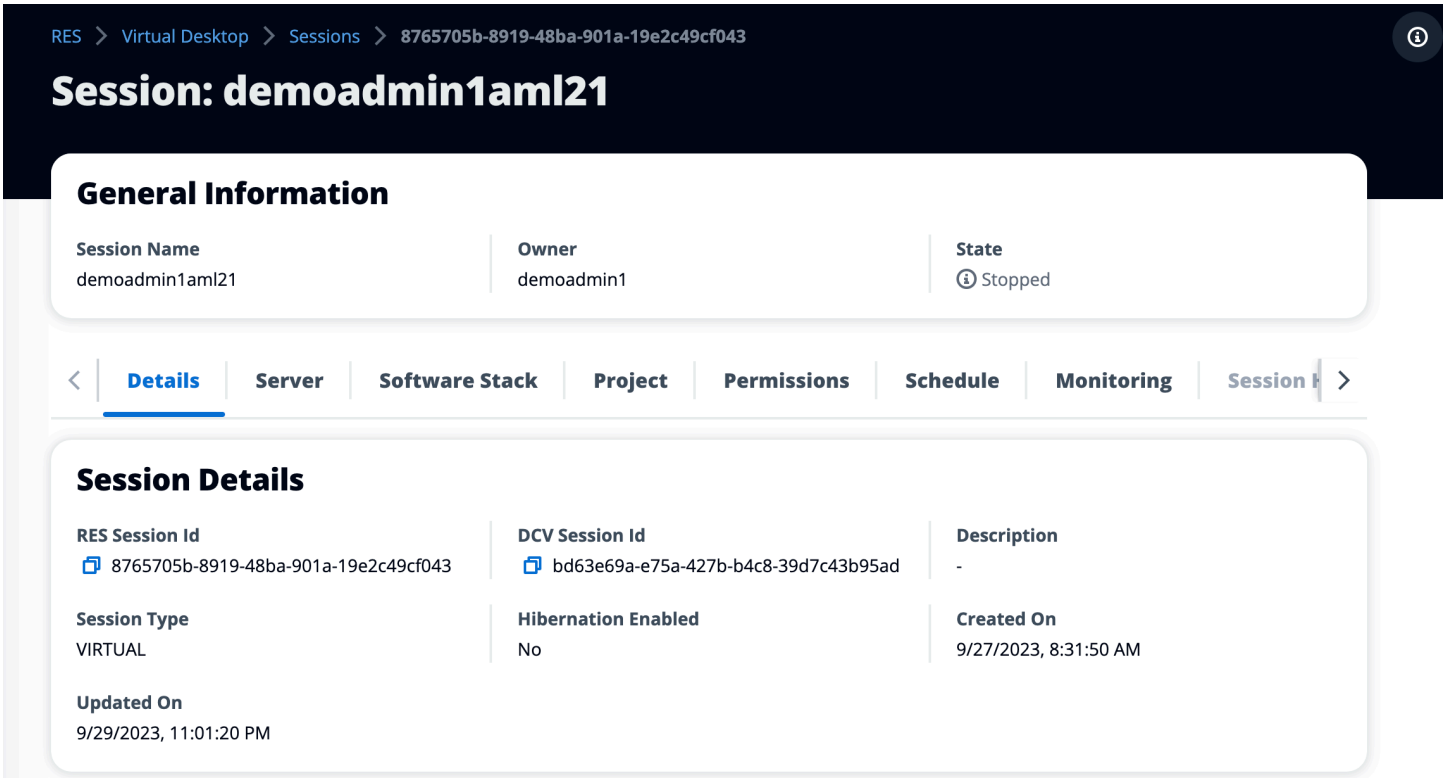
Virtual Desktop Size
Select a virtual desktop instance type

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

10

세션 세부 정보

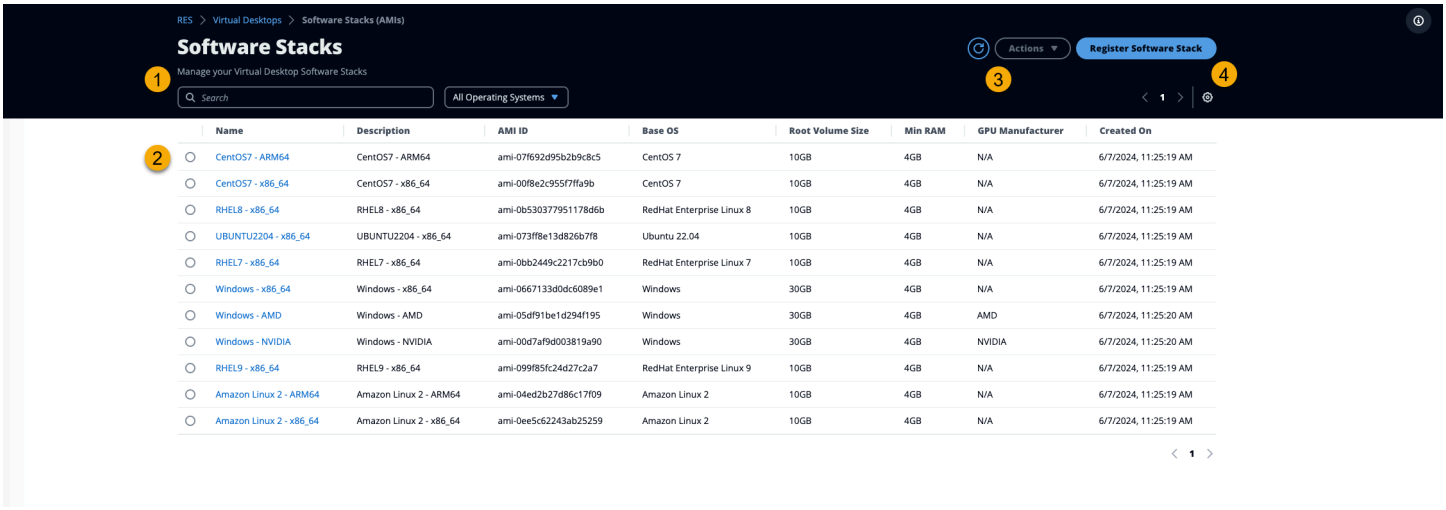
세션 목록에서 세션 이름을 선택하여 세션 세부 정보를 봅니다.



소프트웨어 스택(AMIs)

> **Note**
>
> 에서 제공된 CentSO7 소프트웨어 스택을 실행하려면 연결된 표준 계정 을 AWS Marketplace 사용하여 AMI 내에서 를 구독 AWS GovCloud (US)해야 합니다.

소프트웨어 스택 페이지에서 Amazon Machine Images(AMIs)를 구성하거나 기존 이미지를 관리할 수 있습니다.



1. 기존 소프트웨어 스택을 검색하려면 운영 체제 드롭다운을 사용하여 OS별로 필터링합니다.
2. 소프트웨어 스택의 이름을 선택하여 스택에 대한 세부 정보를 확인합니다.
3. 소프트웨어 스택을 선택한 후 작업 메뉴를 사용하여 스택을 편집하고 스택을 프로젝트에 할당합니다.
4. 소프트웨어 스택 등록 버튼을 사용하면 새 스택을 생성할 수 있습니다.

    1. 소프트웨어 스택 등록을 선택합니다.
    2. 새 소프트웨어 스택의 세부 정보를 입력합니다.
    3. 제출을 선택합니다.

Register new Software Stack

Name
Enter a name for the software stack

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

Description
Enter a user friendly description for the software stack

AMI Id
Enter the AMI Id

AMI Id must start with ami-xxx

Operating System
Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer
Select the GPU Manufacturer for the software stack

N/A

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

10

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

10

Projects
Select applicable projects for the software stack

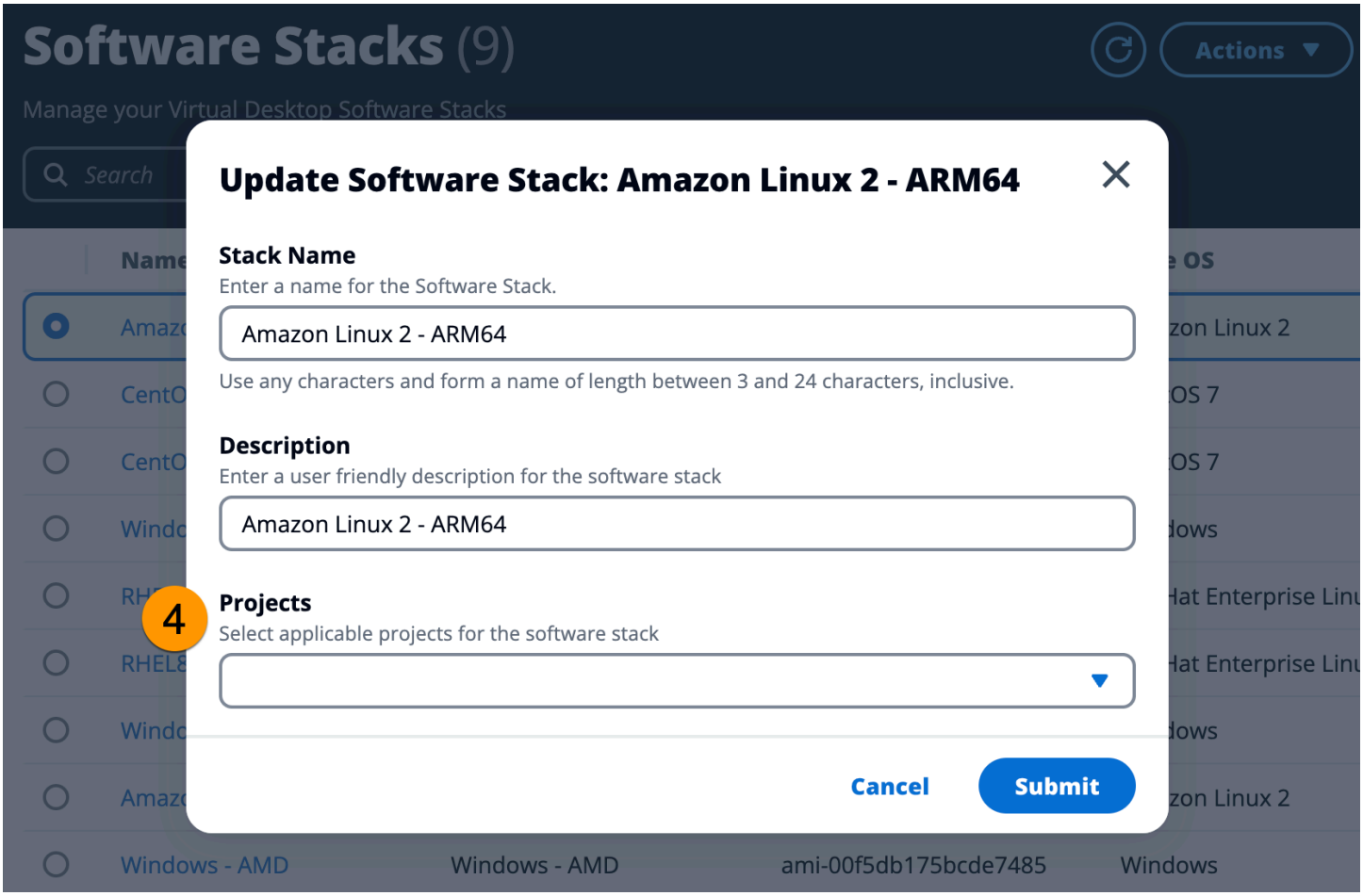
프로젝트에 소프트웨어 스택 할당

새 소프트웨어 스택을 생성할 때 프로젝트에 스택을 할당할 수 있습니다. 초기 생성 후 프로젝트에 스택을 추가해야 하는 경우 다음을 수행합니다.

> **Note**
>
> 멤버인 프로젝트에만 소프트웨어 스택을 할당할 수 있습니다.

1. 소프트웨어 스택 페이지에서 프로젝트에 추가해야 하는 소프트웨어 스택을 선택합니다.
2. 작업을 선택합니다.
3. 편집을 선택합니다.
4. 프로젝트 드롭다운을 사용하여 프로젝트를 선택합니다.
5. 제출을 선택합니다.

스택 세부 정보 페이지에서 소프트웨어 스택을 편집할 수도 있습니다.

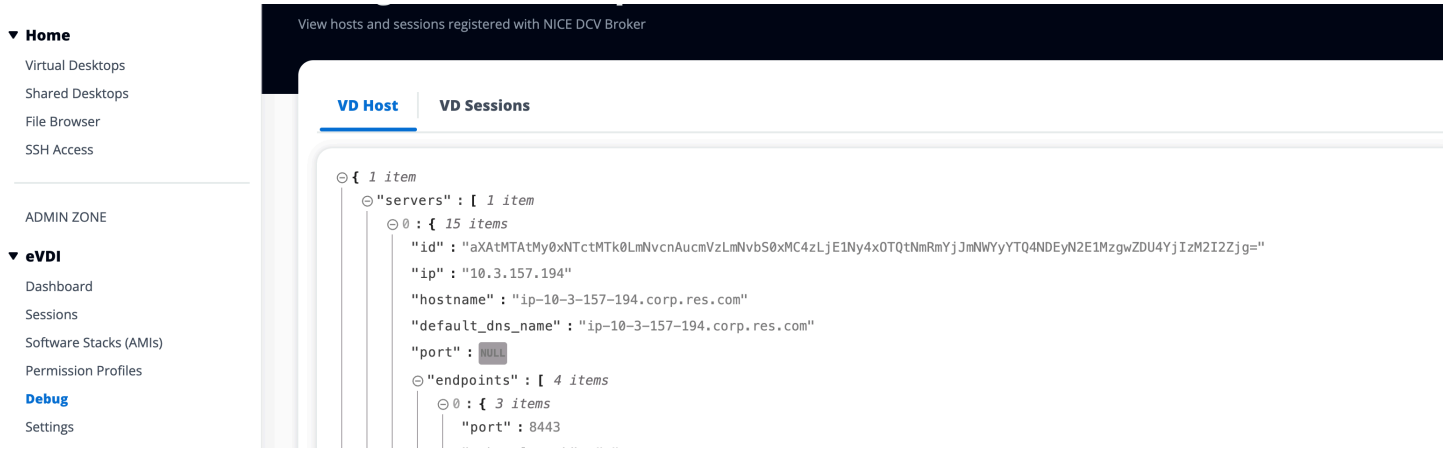


소프트웨어 스택 세부 정보 보기

소프트웨어 스택 목록에서 소프트웨어 스택 이름을 선택하여 세부 정보를 확인합니다. 세부 정보 페이지에서 편집을 선택하여 소프트웨어 스택을 편집할 수도 있습니다.

디버깅

디버깅 패널에는 가상 데스크톱과 연결된 메시지 트래픽이 표시됩니다. 이 패널을 사용하여 호스트 간의 활동을 관찰할 수 있습니다. VD 호스트 탭에는 인스턴스별 활동이 표시되고 VD 세션 탭에는 진행 중인 세션 활동이 표시됩니다.



데스크톱 설정

데스크톱 설정 페이지를 사용하여 가상 데스크톱과 연결된 리소스를 구성할 수 있습니다. 서버 탭에서는 다음과 같은 설정에 액세스할 수 있습니다.

DCV 세션 유휴 제한 시간

DCV 세션이 자동으로 연결 해제되는 시간입니다. 이렇게 하면 데스크톱 세션의 상태가 변경되지 않고 DCV 클라이언트 또는 웹 브라우저에서만 세션이 종료됩니다.

유휴 제한 시간 경고

클라이언트에 유휴 경고가 제공되는 시간입니다.

CPU 사용률 임계값

유휴로 간주될 CPU 사용률입니다.

사용자당 허용된 세션 수

개별 사용자가 지정된 시간에 가질 수 있는 VDI 세션 수입니다. 사용자가 이 값을 충족하거나 초과하면 My Virtual Desktops 페이지에서 새 세션을 시작할 수 없습니다. 세션 페이지를 통해 세션을 시작하는 기능은 이 값의 영향을 받지 않습니다.

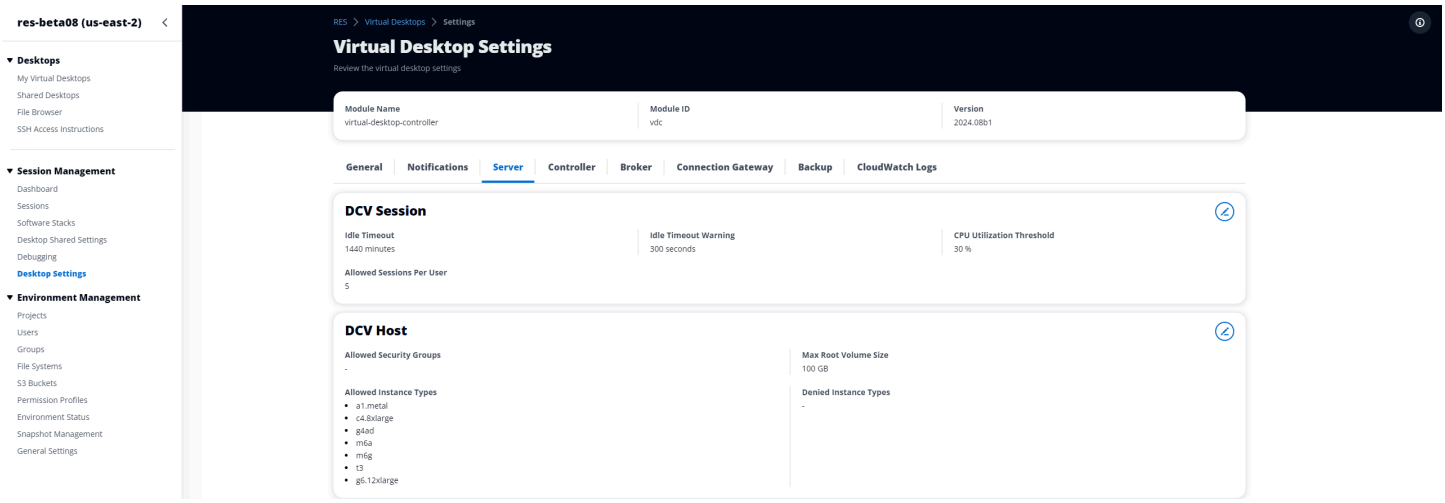
최대 루트 볼륨 크기

가상 데스크톱 세션에서 루트 볼륨의 기본 크기입니다.

허용되는 인스턴스 유형

이 RES 환경에서 시작할 수 있는 인스턴스 패밀리 및 크기 목록입니다. 인스턴스 패밀리와 인스턴스 크기 조합은 모두 허용됩니다. 예를 들어 'm7a'를 지정하면 모든 크기의 m7a 패밀리를 VDI 세션

으로 시작할 수 있습니다. 'm7a.24xlarge'를 지정하면 m7a.24xlarge만 VDI 세션으로 시작할 수 있습니다. 이 목록은 환경의 모든 프로젝트에 영향을 미칩니다.



환경 관리

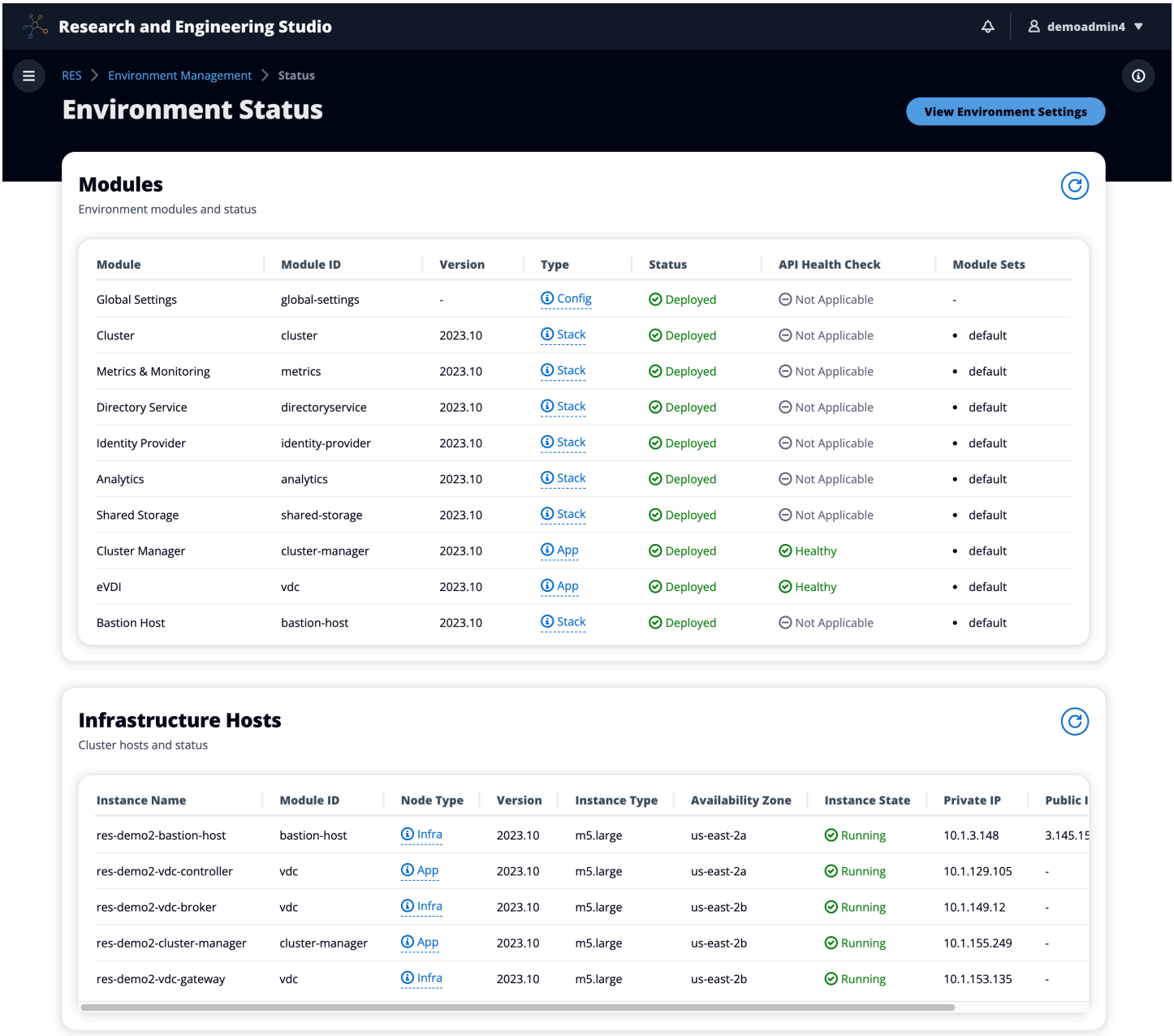
의 환경 관리 섹션에서 RES관리 사용자는 연구 및 엔지니어링 프로젝트를 위한 격리된 환경을 생성하고 관리할 수 있습니다. 이러한 환경에는 안전한 환경 내에서 컴퓨팅 리소스, 스토리지 및 기타 필요한 구성 요소가 포함될 수 있습니다. 사용자는 프로젝트의 특정 요구 사항을 충족하도록 이러한 환경을 구성하고 사용자 지정하여 다른 프로젝트 또는 환경에 영향을 주지 않고 솔루션을 더 쉽게 실험, 테스트 및 반복할 수 있습니다.

주제

- 환경 상태
- 환경 설정
- 사용자
- 그룹
- 프로젝트
- 권한 정책
- 파일 시스템
- 스냅샷 관리
- Amazon S3 버킷

환경 상태

환경 상태 페이지에는 배포된 소프트웨어와 제품 내 호스트가 표시됩니다. 여기에는 소프트웨어 버전, 모듈 이름 및 기타 시스템 정보와 같은 정보가 포함됩니다.



환경 설정

환경 설정 페이지에는 다음과 같은 제품 구성 세부 정보가 표시됩니다.

- 일반

제품을 프로비저닝한 사용자의 관리자 사용자 이름 및 이메일과 같은 정보를 표시합니다. 웹 포털 제목과 저작권 텍스트를 편집할 수 있습니다.

- ID 제공업체

  Single Sign-On 상태와 같은 정보를 표시합니다.

- 네트워크

  액세스IDs에 대한 VPC ID, 접두사 목록을 표시합니다.

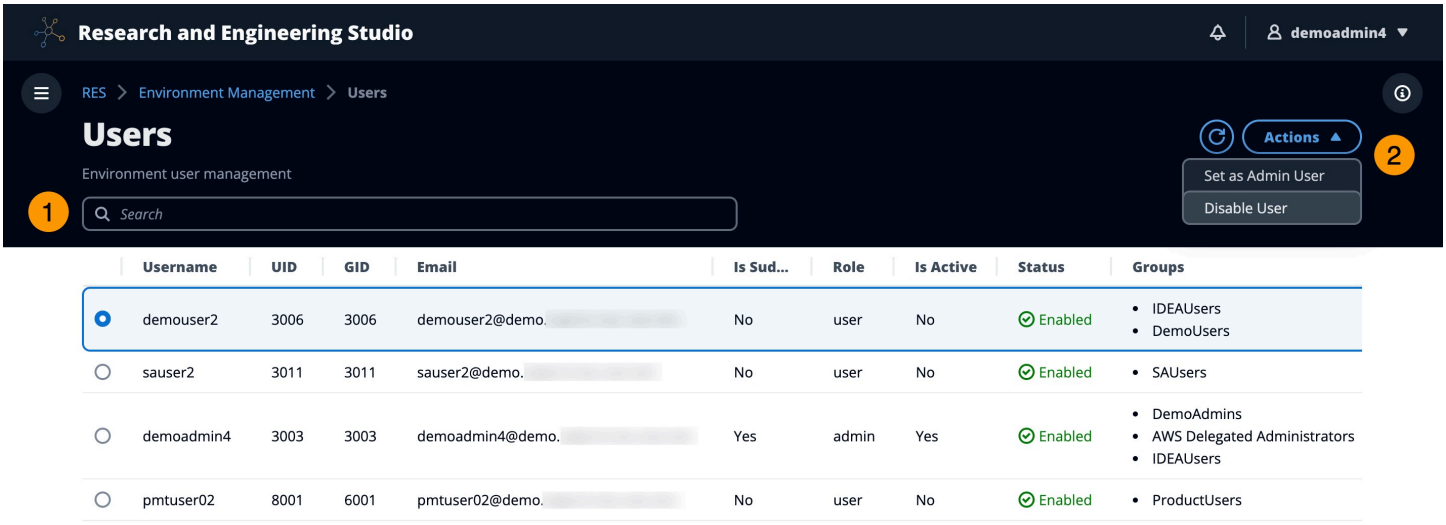
- Directory Service

  사용자 이름 및 암호에 ARN 대한 활성 디렉터리 설정 및 서비스 계정 보안 암호 관리자를 표시합니다.

사용자

Active Directory에서 동기화된 모든 사용자가 사용자 페이지에 표시됩니다. 사용자는 제품 구성 중에 클러스터 관리자 사용자에 의해 동기화됩니다. 초기 사용자 구성에 대한 자세한 내용은 섹션을 참조하세요구성 가이드.

> **Note**
>
> 관리자는 활성 사용자에 대한 세션만 생성할 수 있습니다. 기본적으로 모든 사용자는 제품 환경에 로그인할 때까지 비활성 상태가 됩니다. 사용자가 비활성 상태인 경우 세션을 생성하기 전에 로그인하도록 요청합니다.

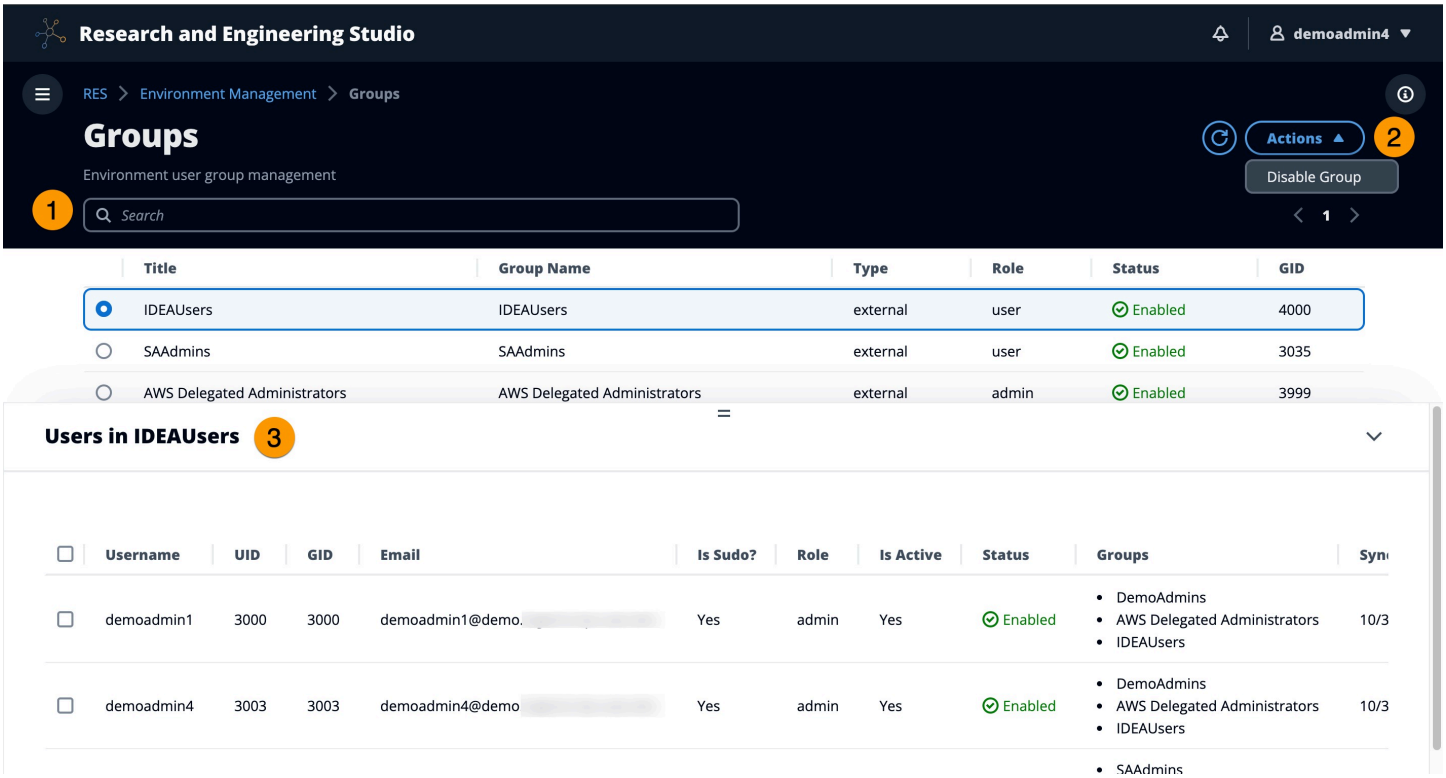


사용자 페이지에서 다음을 수행할 수 있습니다.

1. 사용자를 검색합니다.
2. 사용자 이름을 선택하면 작업 메뉴를 사용하여 다음을 수행합니다.
    a. 관리자 사용자로 설정
    b. 사용자 비활성화

그룹

활성 디렉터리에서 동기화된 모든 그룹은 그룹 페이지에 표시됩니다. 그룹 구성 및 관리에 대한 자세한 내용은 섹션을 참조하세요구성 가이드.



그룹 페이지에서 다음을 수행할 수 있습니다.

1. 사용자 그룹을 검색합니다.
2. 사용자 그룹을 선택한 경우 작업 메뉴를 사용하여 그룹을 비활성화하거나 활성화합니다.
3. 사용자 그룹을 선택하면 화면 하단의 사용자 창을 확장하여 그룹의 사용자를 볼 수 있습니다.

프로젝트

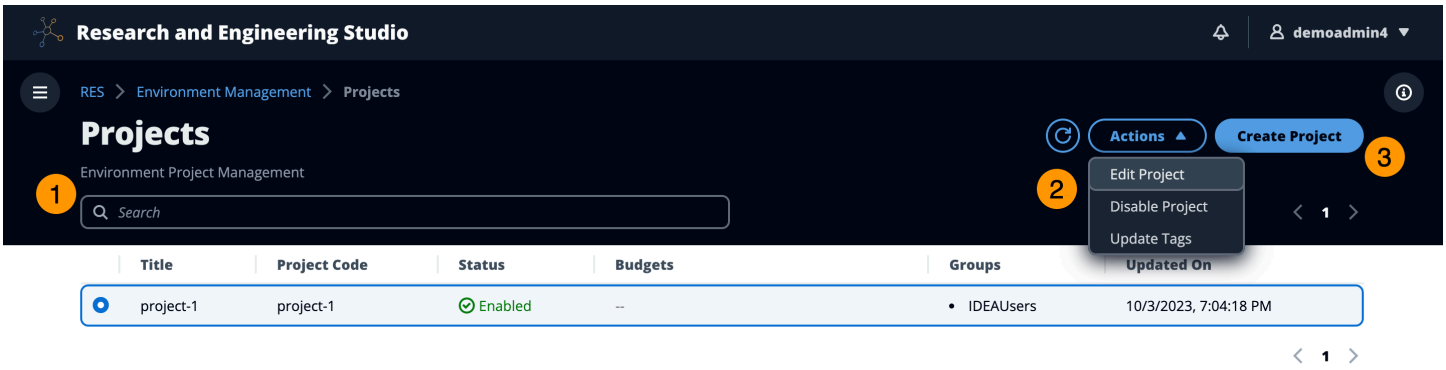
프로젝트는 가상 데스크톱, 팀 및 예산의 경계를 형성합니다. 프로젝트를 생성할 때 이름, 설명 및 환경 구성과 같은 설정을 정의합니다. 프로젝트에는 일반적으로 컴퓨팅 리소스의 유형 및 크기, 소프트웨어 스택, 네트워킹 구성과 같은 프로젝트의 특정 요구 사항을 충족하도록 사용자 지정할 수 있는 하나 이상의 환경이 포함됩니다.

주제

- 프로젝트 보기
- 프로젝트 생성
- 프로젝트 편집
- 프로젝트에서 태그 추가 또는 제거

- 프로젝트와 연결된 파일 시스템 보기
- 시작 템플릿 추가

프로젝트 보기



프로젝트 대시보드는 사용 가능한 프로젝트 목록을 제공합니다. 프로젝트 대시보드에서 다음을 수행할 수 있습니다.

1. 검색 필드를 사용하여 프로젝트를 찾을 수 있습니다.
2. 프로젝트를 선택하면 작업 메뉴를 사용하여 다음을 수행할 수 있습니다.
   a. 프로젝트 편집
   b. 프로젝트 비활성화 또는 활성화
   c. 프로젝트 태그 업데이트
3. 프로젝트 생성을 선택하여 새 프로젝트를 생성할 수 있습니다.

프로젝트 생성

1. 프로젝트 생성을 선택합니다.
2. 프로젝트 세부 정보를 입력합니다.

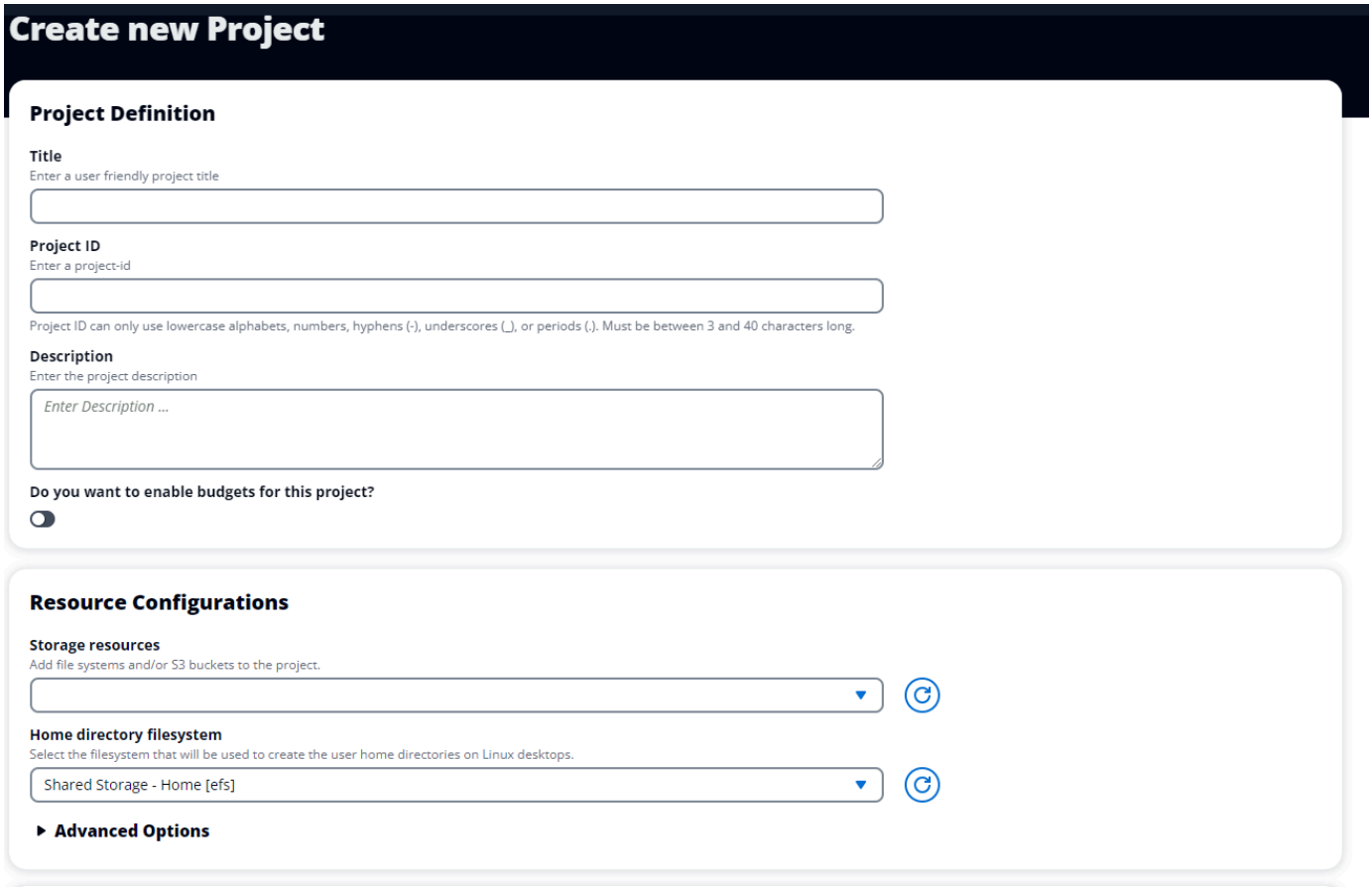
   프로젝트 ID는 에서 비용 할당을 추적하는 데 사용할 수 있는 리소스 태그입니다 AWS Cost Explorer Service. 자세한 내용은 사용자 정의 비용 할당 태그 활성화를 참조하세요.

> **Important**
>
> 프로젝트 ID는 생성 후 변경할 수 없습니다.

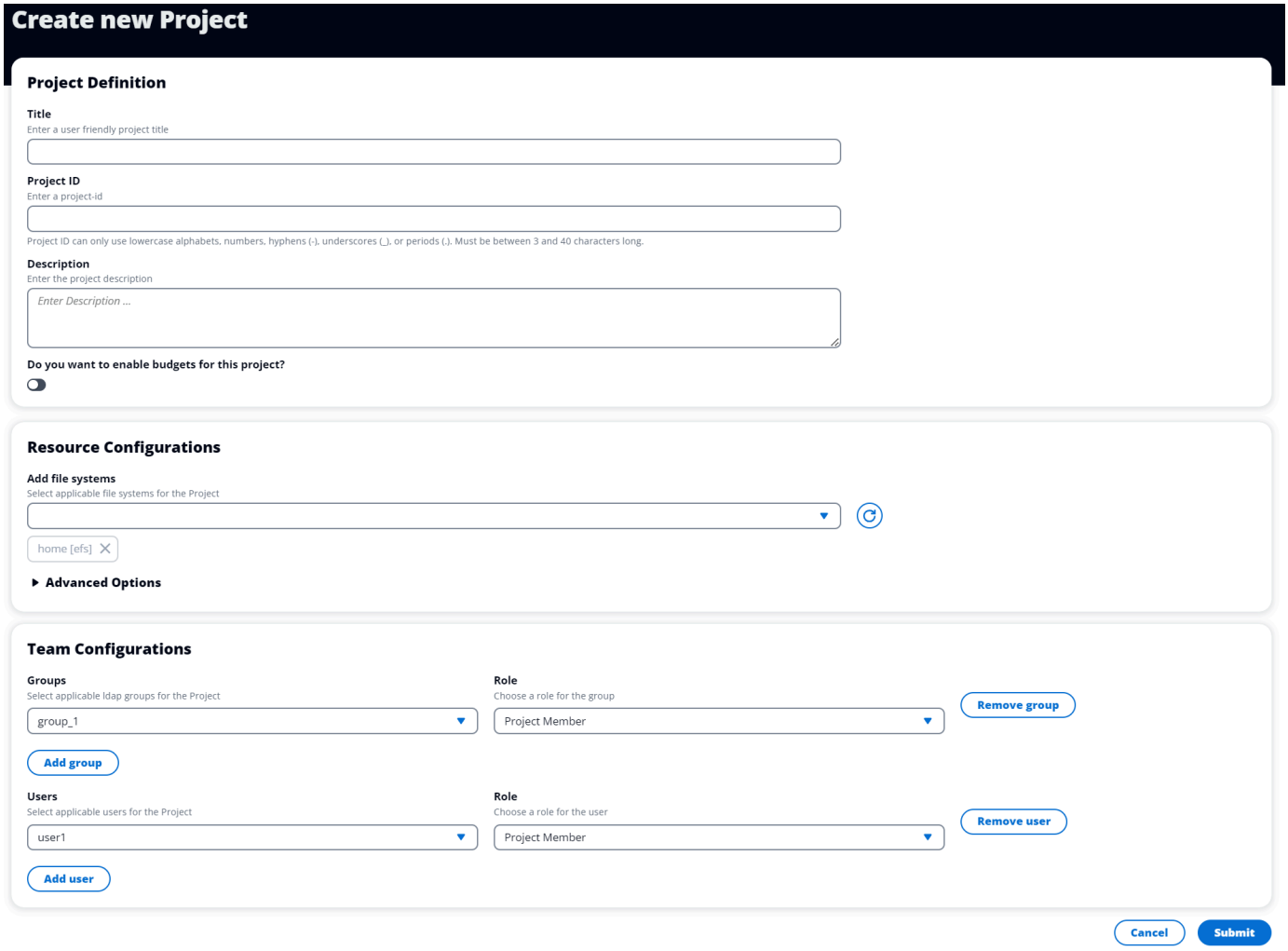
고급 옵션에 대한 자세한 내용은 섹션을 참조하세요시작 템플릿 추가.

3. (선택 사항) 프로젝트의 예산을 켭니다. 예산에 대한 자세한 내용은 섹션을 참조하세요비용 모니터링 및 제어.
4. 홈 디렉터리 파일 시스템은 공유 홈 파일 시스템(기본값), EFS, for Lustre, FSx NetApp ONTAP또는 EBS 볼륨 스토리지FSx를 사용할 수 있습니다.

   EFSFSx Lustre용 공유 홈 파일 시스템인 및 는 여러 프로젝트 및 간에 공유할 FSx NetApp ONTAP 수 있다는 점에 유의해야 합니다VDIs. 그러나 EBS 볼륨 스토리지 옵션을 사용하려면 해당 프로젝트의 모든 VDI에 다른 VDIs 또는 프로젝트 간에 공유되지 않는 자체 홈 디렉터리가 있어야 합니다.

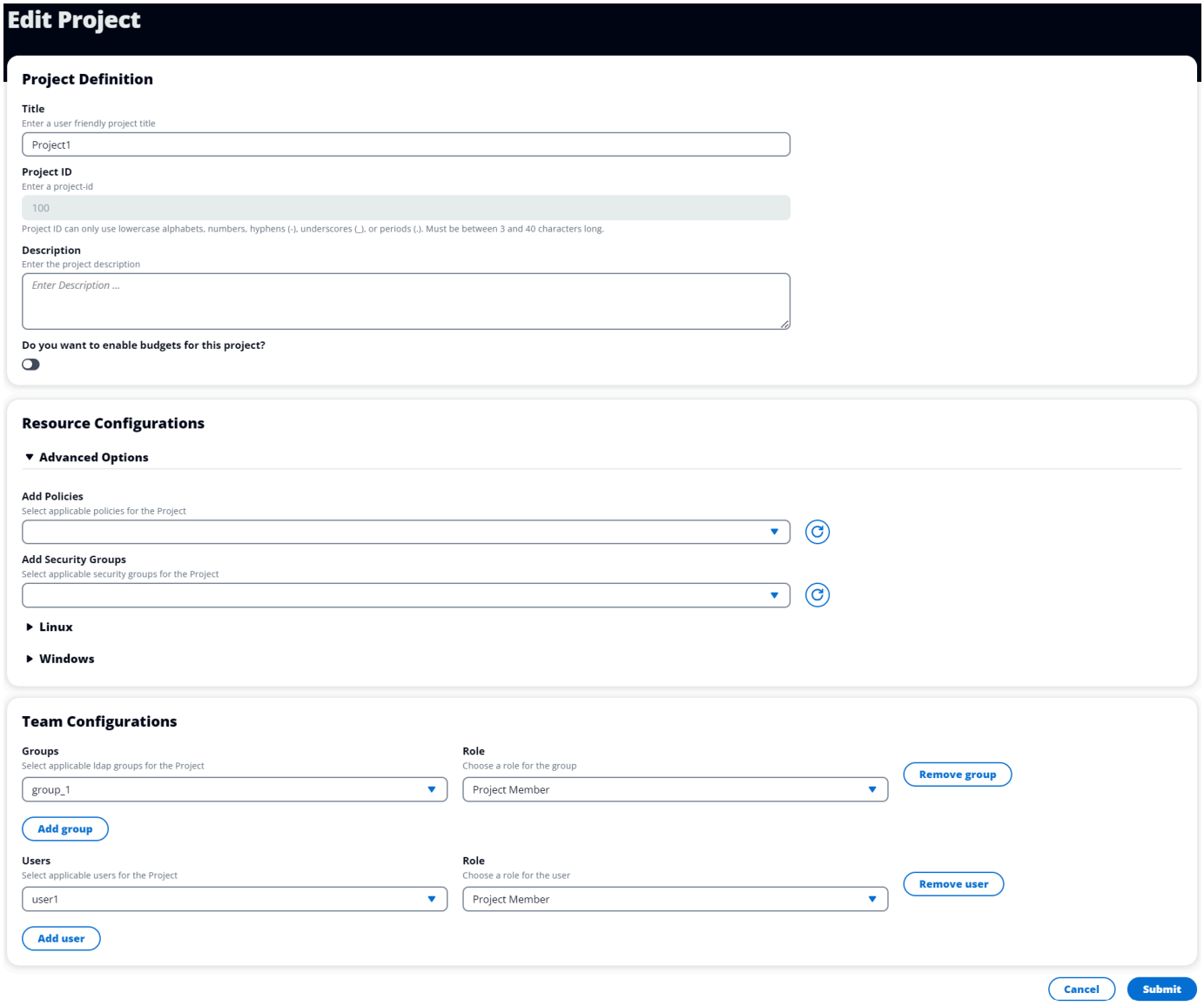


5. 사용자 및/또는 그룹에 적절한 역할('프로젝트 멤버' 또는 '프로젝트 소유자')을 할당합니다. 각 역할이 수행할 수 있는 작업은 기본 권한 프로파일 섹션을 참조하세요.
6. 제출을 선택합니다.



프로젝트 편집

1. 프로젝트 목록에서 프로젝트를 선택합니다.
2. 작업 메뉴에서 프로젝트 편집을 선택합니다.
3. 업데이트를 입력합니다. 예산을 활성화하려는 경우 자세한 내용은 비용 모니터링 및 제어 섹션을 참조하세요. 고급 옵션에 대한 자세한 내용은 섹션을 참조하세요시작 템플릿 추가.
4. 제출을 선택합니다.



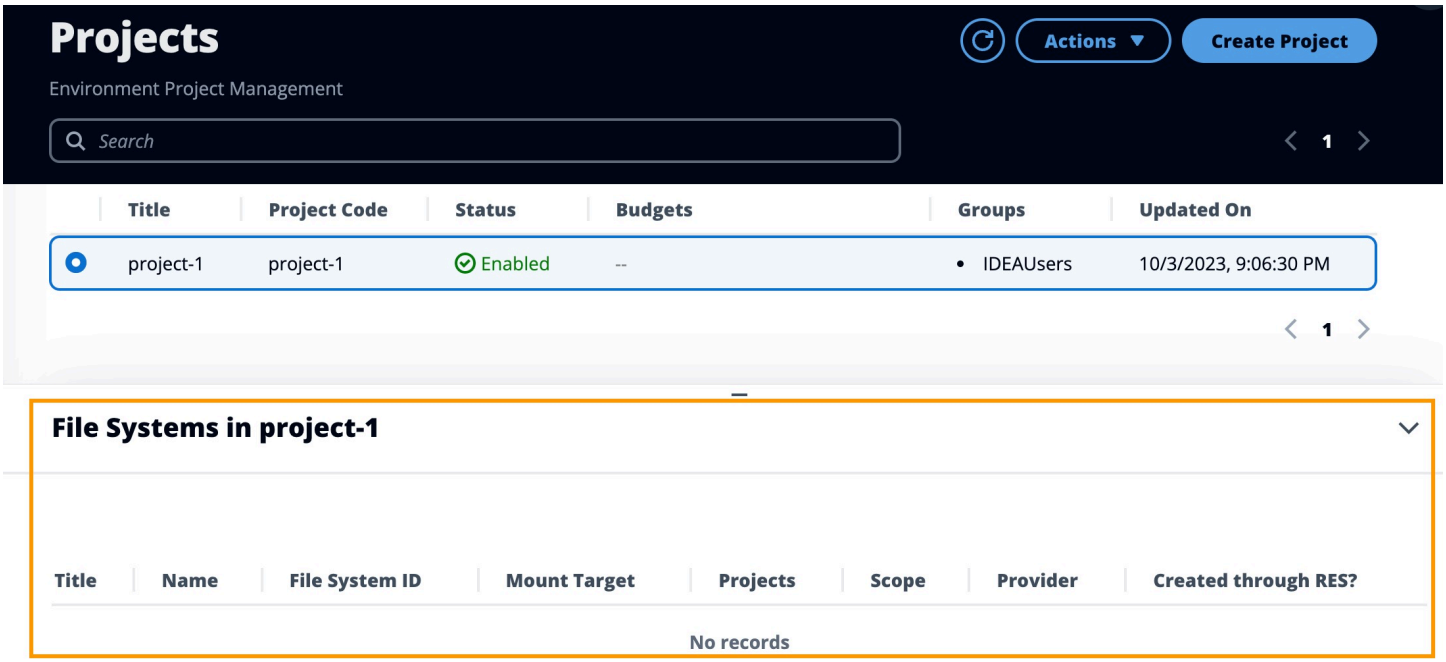
프로젝트에서 태그 추가 또는 제거

프로젝트 태그는 해당 프로젝트에서 생성된 모든 인스턴스에 태그를 할당합니다.

1. 프로젝트 목록에서 프로젝트를 선택합니다.
2. 작업 메뉴에서 태그 업데이트를 선택합니다.
3. 태그 추가를 선택하고 키 값을 입력합니다.
4. 태그를 제거하려면 제거하려는 태그 옆에 있는 제거를 선택합니다.

프로젝트와 연결된 파일 시스템 보기

프로젝트를 선택하면 화면 하단의 파일 시스템 창을 확장하여 프로젝트와 연결된 파일 시스템을 볼 수 있습니다.



시작 템플릿 추가

프로젝트를 생성하거나 편집할 때 프로젝트 구성 내의 고급 옵션을 사용하여 시작 템플릿을 추가할 수 있습니다. 시작 템플릿은 보안 그룹, IAM 정책 및 시작 스크립트와 같은 추가 구성을 프로젝트 내 모든 VDI 인스턴스에 제공합니다.

정책 추가

프로젝트를 통해 배포된 모든 인스턴스에 대한 VDI 액세스를 제어하는 IAM 정책을 추가할 수 있습니다. 정책을 온보딩하려면 다음 키-값 페어로 정책에 태그를 지정합니다.

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

IAM 역할에 대한 자세한 내용은 의 정책 및 권한을 IAM참조하세요.

보안 그룹 추가

보안 그룹을 추가하여 프로젝트의 모든 VDI 인스턴스에 대한 송신 및 수신 데이터를 제어할 수 있습니다. 보안 그룹을 온보딩하려면 다음 키-값 페어로 보안 그룹에 태그를 지정합니다.

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

보안 그룹에 대한 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹을 사용하여 리소스에 대한 트래픽 제어를 참조하세요 AWS.

시작 스크립트 추가

프로젝트 내 모든 VDI 세션에서 시작되는 시작 스크립트를 추가할 수 있습니다. RES 는 Linux 및 Windows에 대한 스크립트 시작을 지원합니다. 스크립트 시작의 경우 다음 중 하나를 선택할 수 있습니다.

VDI 시작 시 스크립트 실행

이 옵션은 RES 구성 또는 설치가 실행되기 전에 VDI 인스턴스 시작 시 스크립트를 시작합니다.

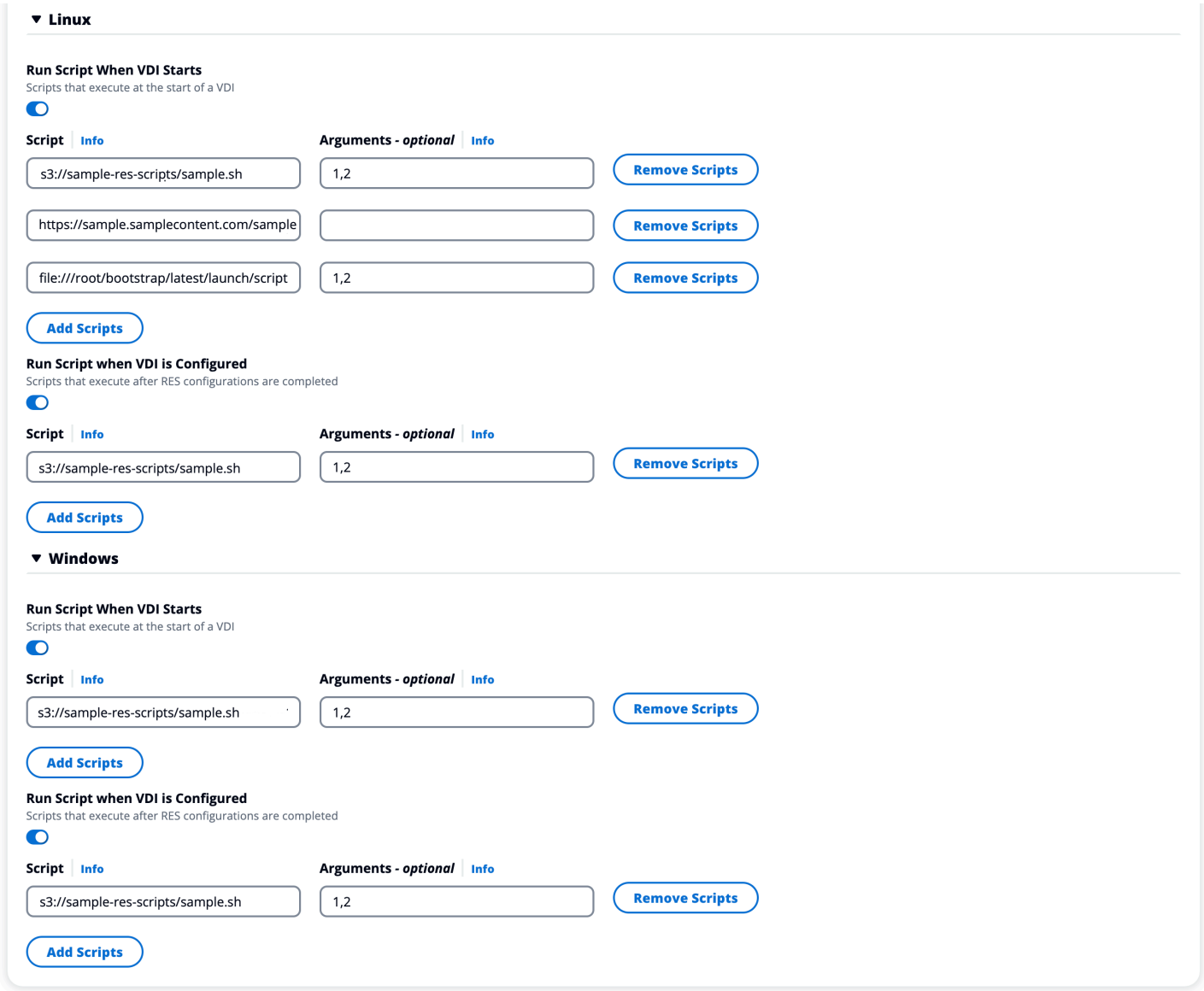
VDI 가 구성된 경우 스크립트 실행

이 옵션은 RES 구성이 완료된 후 스크립트를 시작합니다.

스크립트는 다음 옵션을 지원합니다.

스크립트 구성	예
S3 URI	s3://bucketname/script.sh
HTTPS URL	https://sample.samplecontent.com/샘플
로컬 파일	file:///user/scripts/example.sh

인수 의 경우 쉼표로 구분된 모든 인수를 제공합니다.



프로젝트 구성의 예

권한 정책

Research and Engineering Studio(RES)를 사용하면 관리 사용자가 선택한 사용자에게 자신이 속한 프로젝트를 관리할 수 있는 추가 권한을 부여하는 사용자 지정 권한 프로파일을 생성할 수 있습니다. 각 프로젝트에는 배포 후 사용자 지정할 수 있는 '프로젝트 멤버'와 '프로젝트 소유자'라는 두 가지 기본 권한 프로파일이 제공됩니다.

현재 관리자는 권한 프로파일을 사용하여 두 가지 권한 모음을 부여할 수 있습니다.

1. 지정된 사용자가 다른 사용자와 그룹을 프로젝트에 추가하거나 프로젝트에서 제거할 수 있는 '프로젝트 멤버십 업데이트'와 지정된 사용자가 프로젝트를 활성화 또는 비활성화할 수 있는 '프로젝트 상태 업데이트'로 구성된 프로젝트 관리 권한입니다.
2. VDI 지정된 사용자가 프로젝트 내에서 VDI 세션을 생성할 수 있는 '세션 생성'과 지정된 사용자가 프로젝트 내에서 다른 사용자의 세션을 생성하거나 종료할 수 있는 '다른 사용자의 세션 생성/종료'로 구성된 세션 관리 권한입니다.

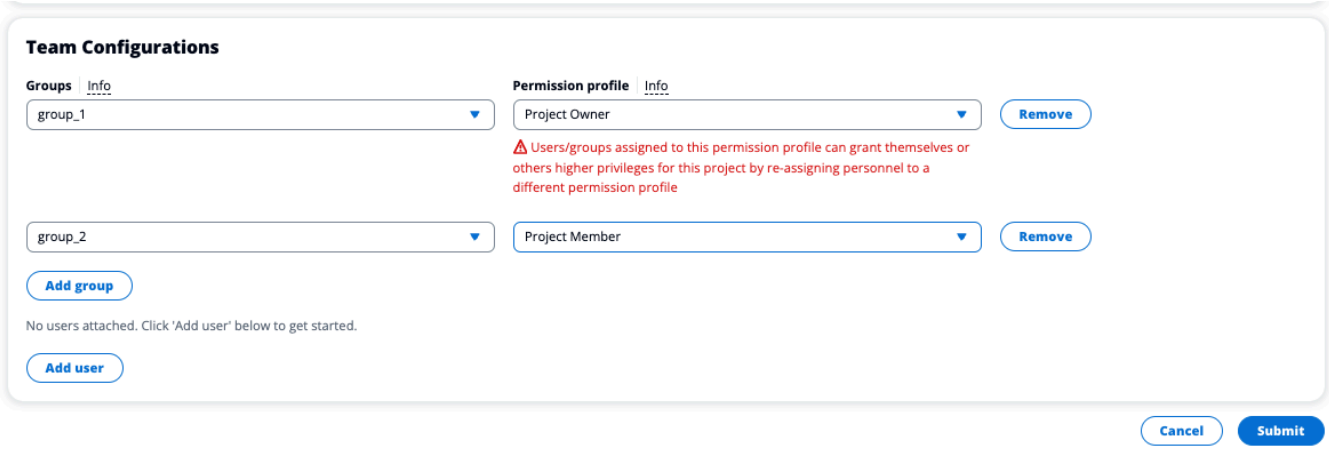
이렇게 하면 관리자는 환경의 관리자가 아닌 사람에게 프로젝트 기반 권한을 위임할 수 있습니다.

주제

프로젝트 관리 권한

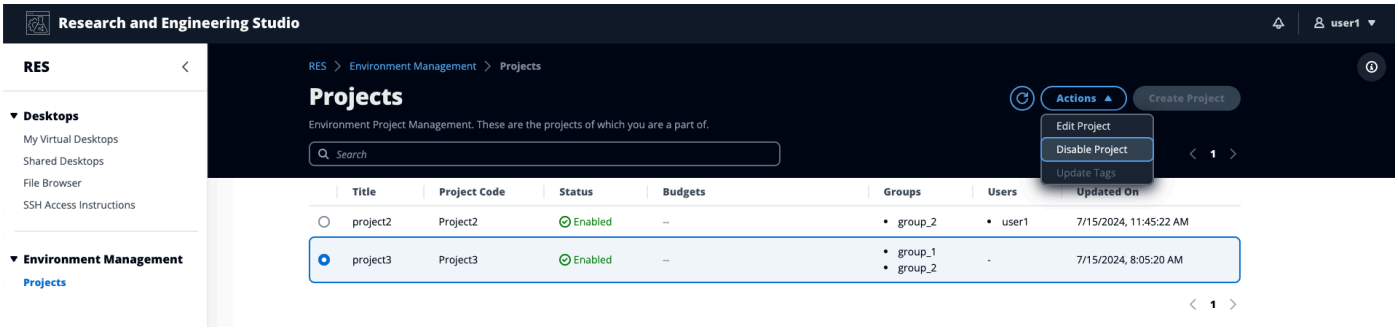
프로젝트 멤버십 업데이트

이 권한을 부여받은 관리자가 아닌 사용자는 프로젝트에서 사용자 또는 그룹을 추가하고 제거할 수 있습니다. 또한 권한 프로파일을 설정하고 해당 프로젝트의 다른 모든 사용자 및 그룹에 대한 액세스 수준을 결정할 수 있습니다.



프로젝트 상태 업데이트

이 권한을 부여받은 관리자가 아닌 사용자는 프로젝트 페이지의 작업 버튼을 사용하여 프로젝트를 활성화하거나 비활성화할 수 있습니다.

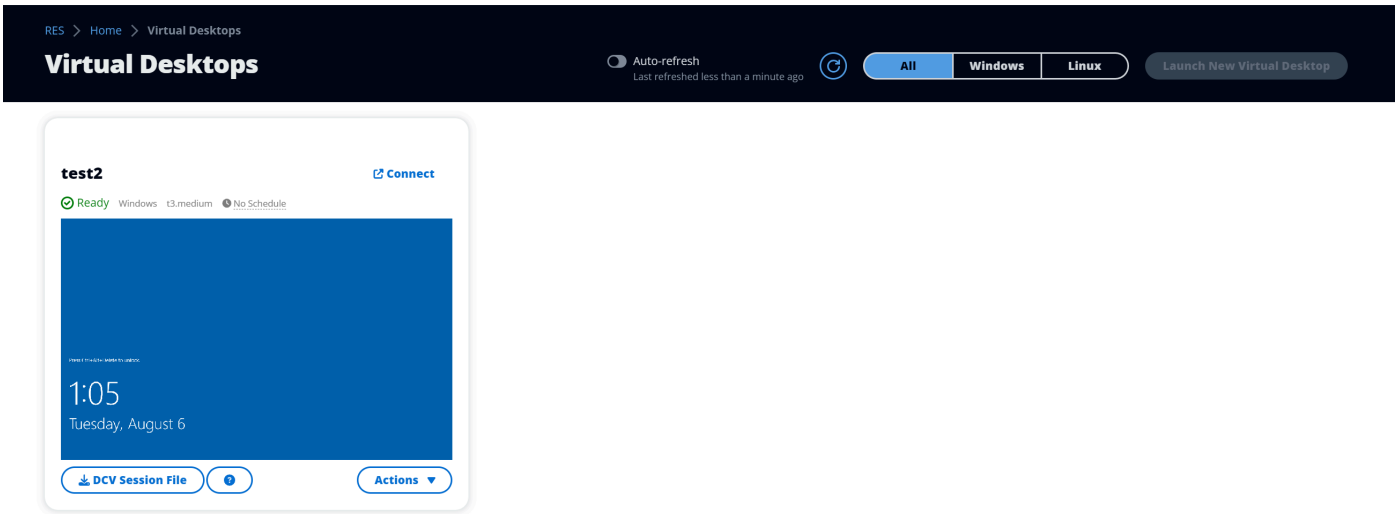


VDI 세션 관리 권한

세션 생성

사용자가 My Virtual Desktops 페이지에서 자체 VDI 세션을 시작할 수 있는지 여부를 제어합니다. 관리자가 아닌 사용자에게 자체 VDI 세션을 시작할 수 있는 기능을 거부하려면 이 옵션을 비활성화합니다. 사용자는 언제든지 자신의 VDI 세션을 중지하고 종료할 수 있습니다.

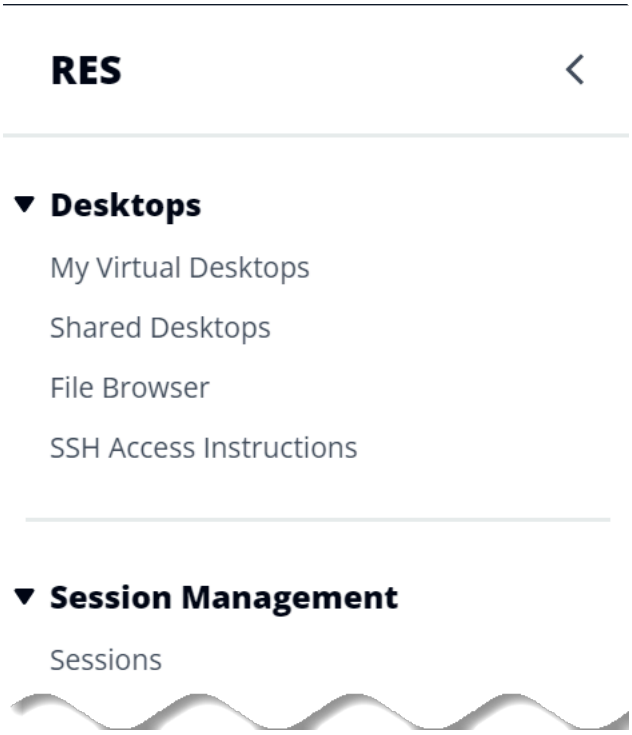
관리자가 아닌 사용자에게 세션을 생성할 권한이 없는 경우 새 Virtual Desktop 시작 버튼이 다음과 같이 비활성화됩니다.



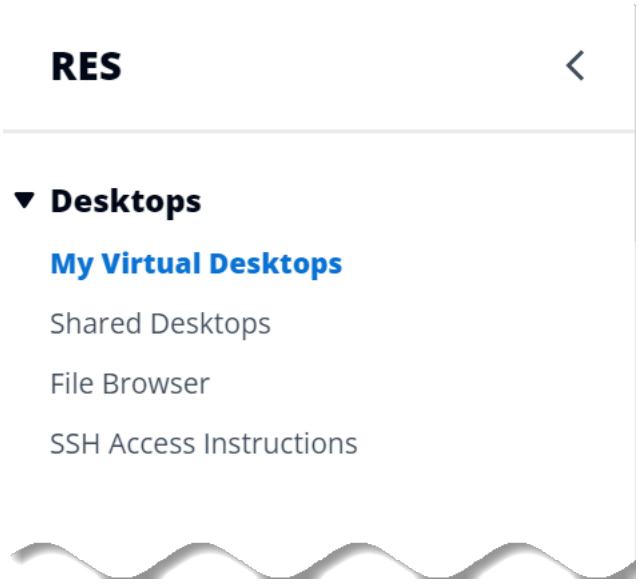
다른 사람의 세션 생성 또는 종료

관리자가 아닌 사용자가 왼쪽 탐색 창에서 세션 페이지에 액세스할 수 있도록 허용합니다. 이러한 사용자는 이 권한이 부여된 프로젝트의 다른 사용자를 위한 VDI 세션을 시작할 수 있습니다.

관리자가 아닌 사용자에게 다른 사용자에 대한 세션을 시작할 수 있는 권한이 있는 경우 왼쪽 탐색 창에는 다음과 같이 세션 관리 아래에 세션 링크가 표시됩니다.



관리자가 아닌 사용자에게 다른 사용자를 위한 세션을 생성할 권한이 없는 경우 왼쪽 탐색 창에는 다음과 같이 세션 관리가 표시되지 않습니다.

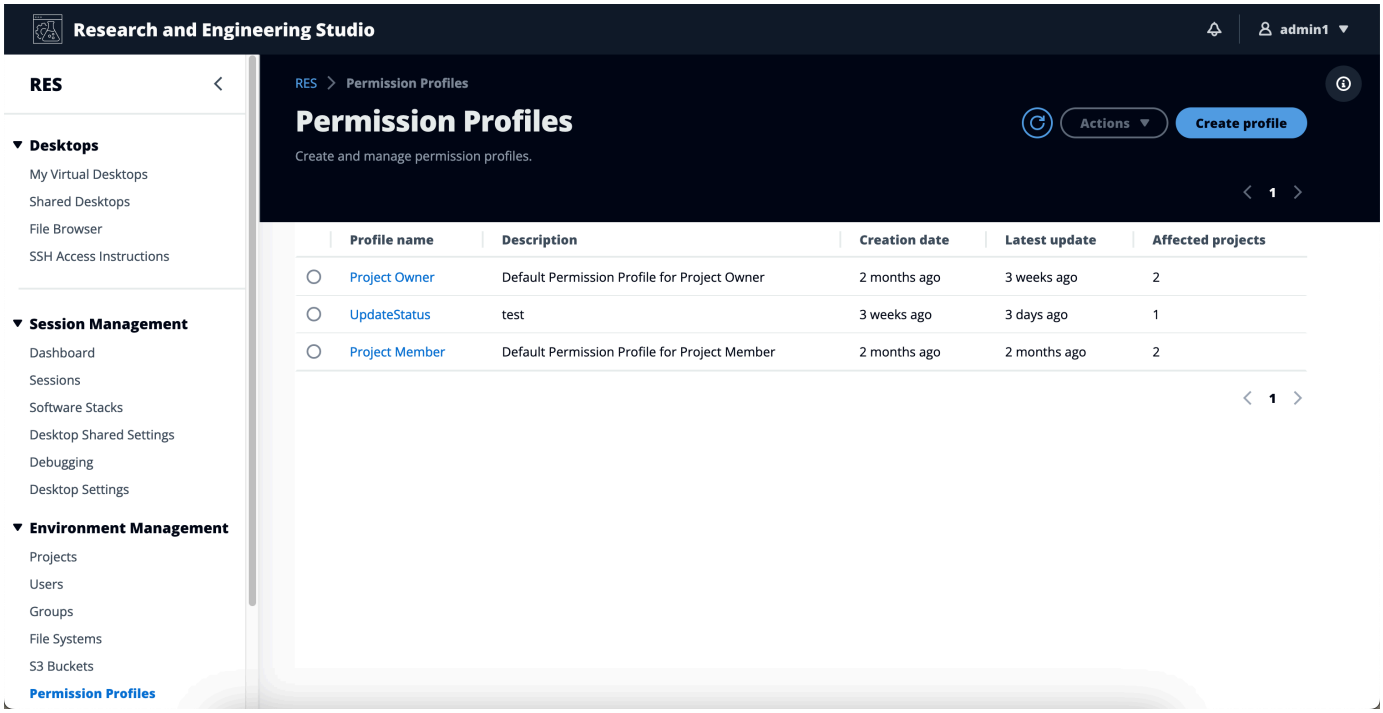


권한 프로필 관리

RES 관리자는 다음 작업을 수행하여 권한 프로파일을 관리할 수 있습니다.

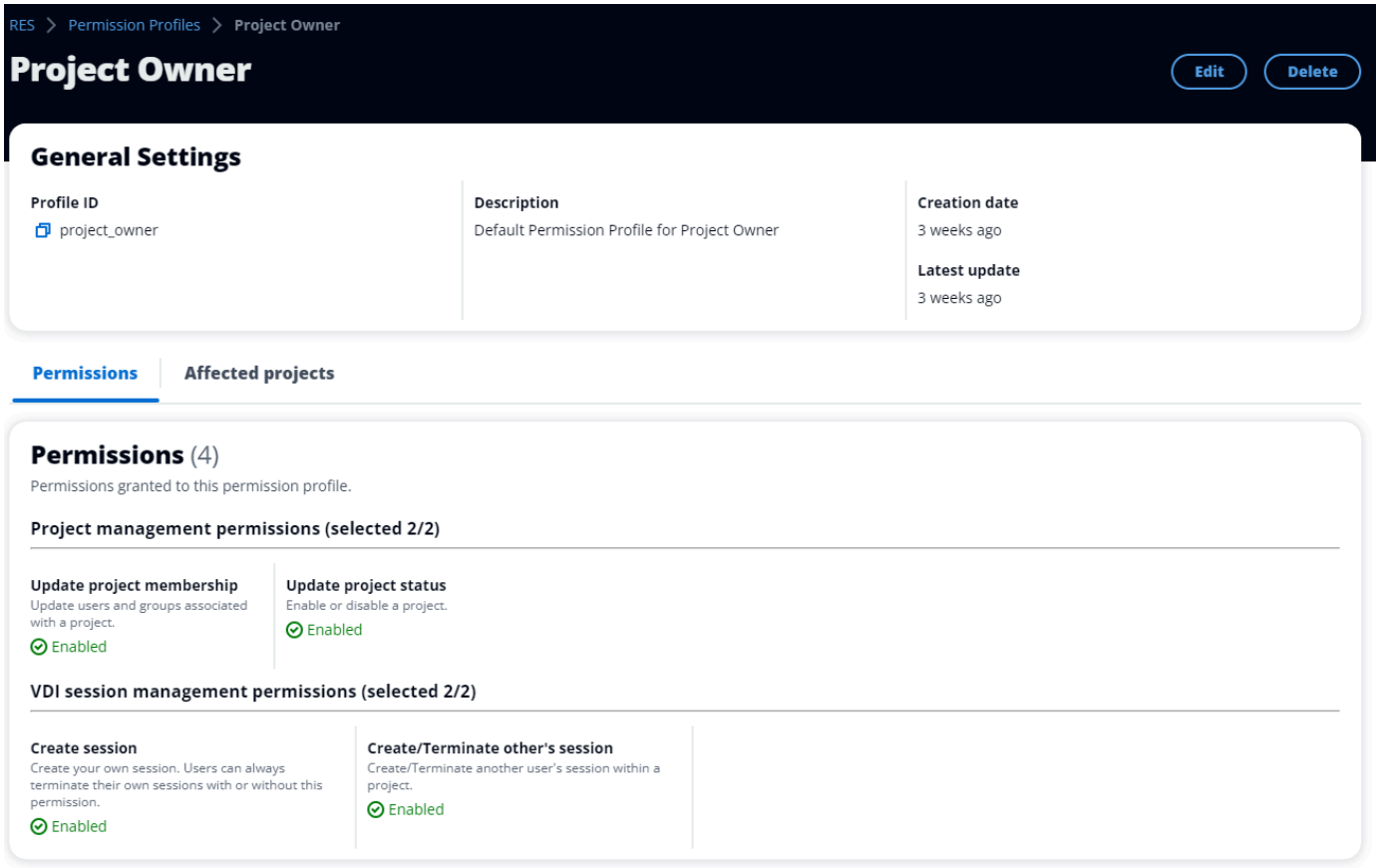
권한 프로필 나열

- 연구 및 엔지니어링 스튜디오 콘솔 페이지에서 왼쪽 탐색 창에서 권한 프로파일을 선택합니다. 이 페이지에서 권한 프로파일을 생성, 업데이트, 나열, 보기 및 삭제할 수 있습니다.

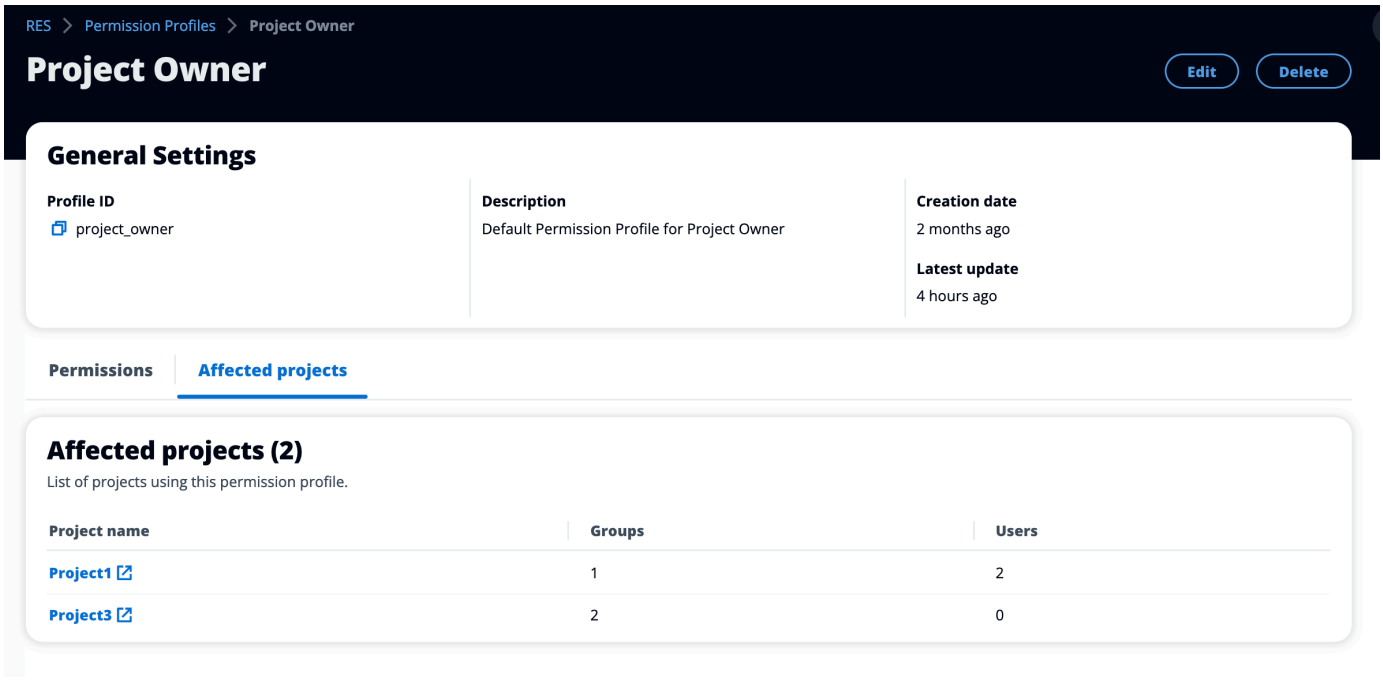


권한 프로필 보기

1. 기본 권한 프로필 페이지에서 보려는 권한 프로필의 이름을 선택합니다. 이 페이지에서 선택한 권한 프로파일을 편집하거나 삭제할 수 있습니다.

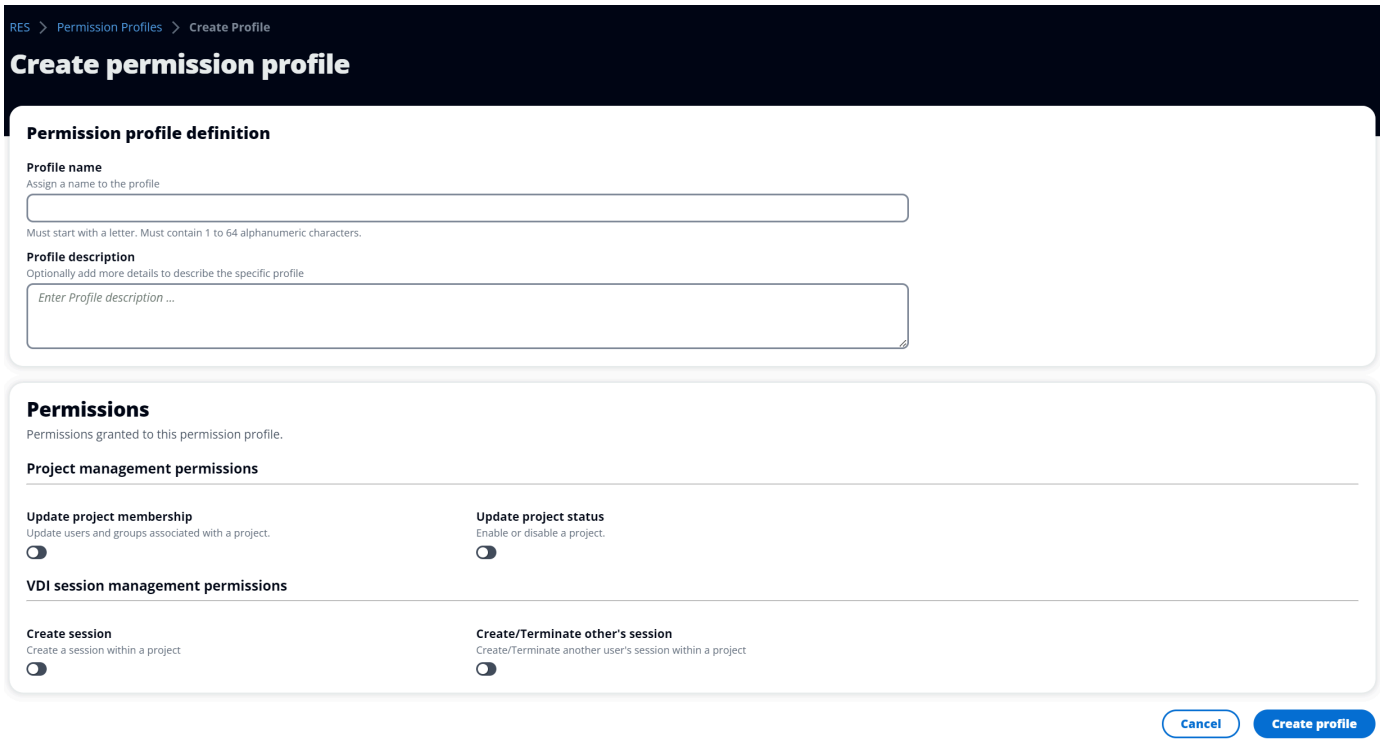


2. 영향을 받는 프로젝트 탭을 선택하여 현재 권한 프로파일을 사용하는 프로젝트를 봅니다.



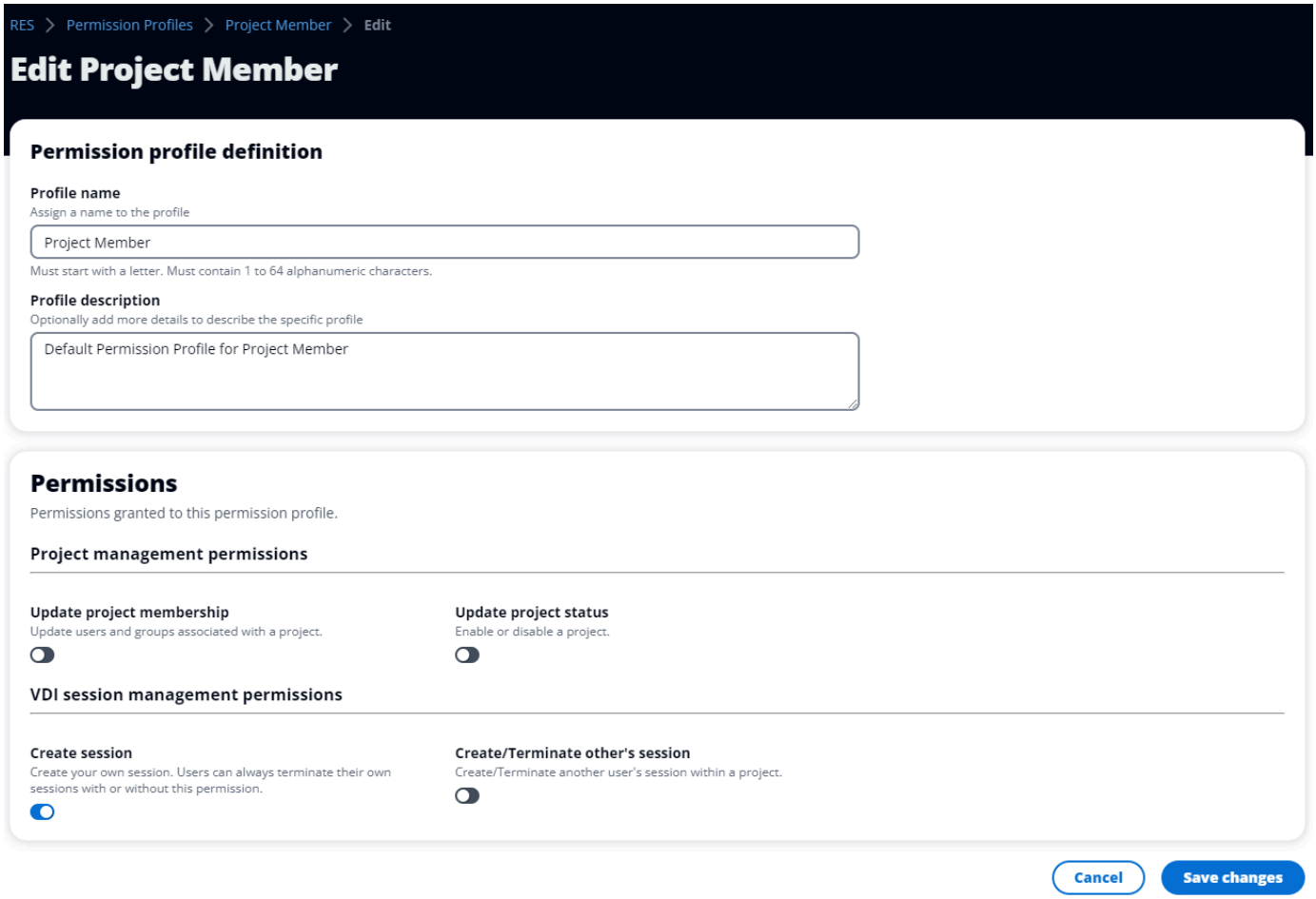
권한 프로필 생성

1. 기본 권한 프로필 페이지에서 프로필 생성을 선택하여 권한 프로필을 생성합니다.
2. 권한 프로필 이름과 설명을 입력한 다음 이 프로필에 할당한 사용자 또는 그룹에 부여할 권한을 선택합니다.



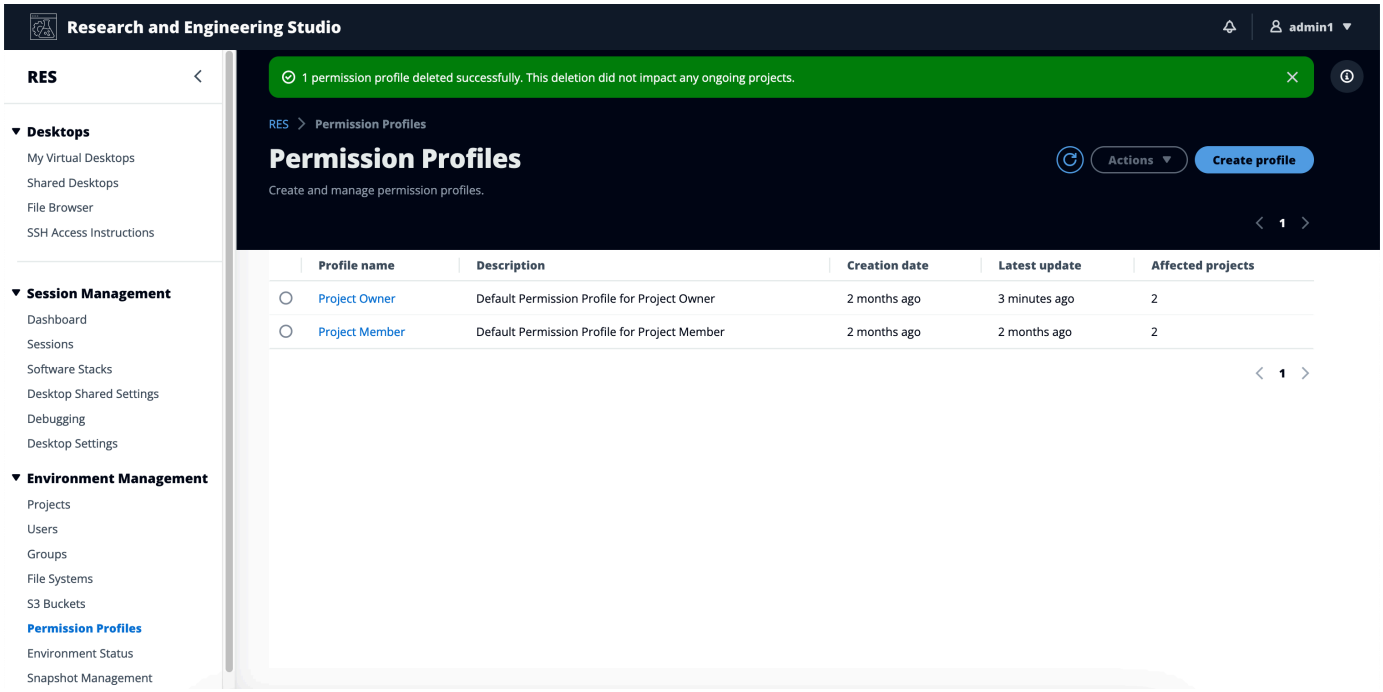
권한 프로필 편집

- 기본 권한 프로필 페이지에서 옆에 있는 원을 클릭하여 프로필을 선택하고 작업 을 선택한 다음 프로필 편집을 선택하여 권한 프로필을 업데이트합니다.



권한 프로필 삭제

- 기본 권한 프로필 페이지에서 옆에 있는 원을 클릭하여 프로필을 선택하고 작업 을 선택한 다음 프로필 삭제 를 선택합니다. 기존 프로젝트에서 사용하는 권한 프로필은 삭제할 수 없습니다.



기본 권한 프로파일

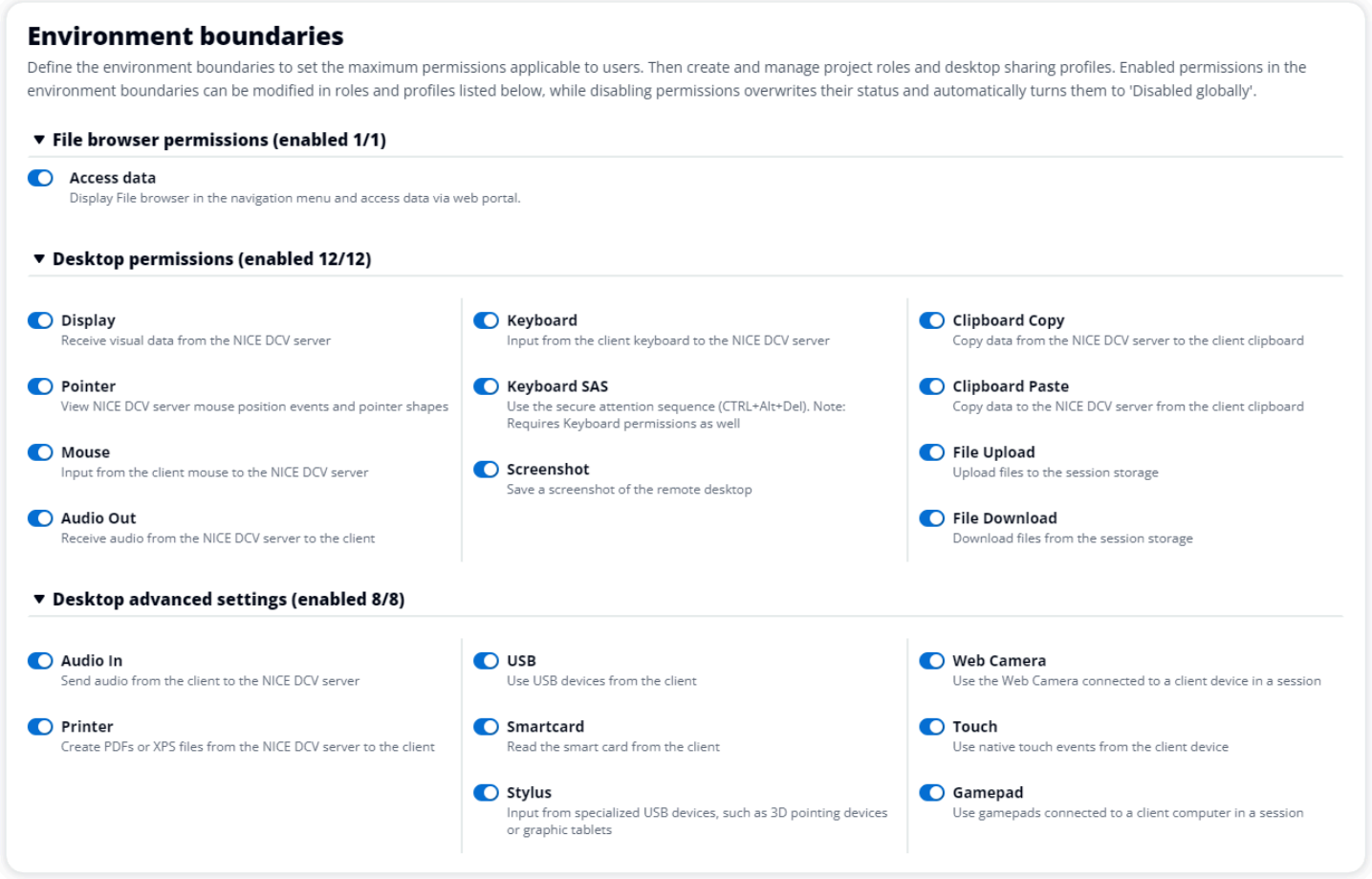
모든 RES 프로젝트에는 글로벌 관리자가 구성할 수 있는 두 가지 기본 권한 프로파일이 제공됩니다. (또한 글로벌 관리자는 프로젝트에 대한 새 권한 프로파일을 생성하고 수정할 수 있습니다.) 다음 표에는 기본 권한 프로파일 '프로젝트 멤버' 및 '프로젝트 소유자'에 허용되는 권한이 나와 있습니다. 권한 프로필과 프로젝트 사용자를 선택할 수 있는 권한은 자신이 속한 프로젝트에만 적용됩니다. 글로벌 관리자는 모든 프로젝트에서 아래 권한을 모두 가진 슈퍼 사용자입니다.

권한	설명	프로젝트 멤버	프로젝트 소유자	
세션 생성	자체 세션을 생성합니다. 사용자는 언제든지 이 권한 유무에 관계없이 자신의 세션을 중지하고 종료할 수 있습니다.	X	X	
다른 사람의 세션 생성/종료	프로젝트 내에서 다른 사용자의 세		X	

권한	설명	프로젝트 멤버	프로젝트 소유자	
	션을 생성하거나 종료합니다.			
프로젝트 멤버십 업데이트	프로젝트와 연결된 사용자 및 그룹을 업데이트합니다.		X	
프로젝트 상태 업데이트	프로젝트를 활성화 또는 비활성화합니다.		X	

환경 경계

환경 경계를 통해 관리자는 모든 사용자에게 전역적으로 적용되는 권한을 구성할 수 있습니다. 여기에는 파일 브라우저 액세스 및 데스크톱 권한과 같은 권한이 포함됩니다.



파일 브라우저 액세스 구성

관리자는 파일 브라우저 권한 에서 데이터 액세스를 켜거나 끌 수 있습니다. 액세스 데이터가 꺼지면 웹 포털에서 파일 브라우저 탐색이 표시되지 않으며 글로벌 파일 시스템에 연결된 데이터를 업로드하거나 다운로드할 수 없습니다. 액세스 데이터가 활성화되면 사용자는 웹 포털에서 파일 브라우저 탐색에 액세스하여 글로벌 파일 시스템에 연결된 데이터를 업로드하거나 다운로드할 수 있습니다.

데이터 액세스 기능을 켠 다음 나중에 끄면 웹 포털에 이미 로그인한 사용자는 해당 페이지에 있더라도 파일을 업로드하거나 다운로드할 수 없습니다. 또한 페이지를 새로 고치면 탐색 메뉴가 사라집니다.

데스크톱 권한 구성

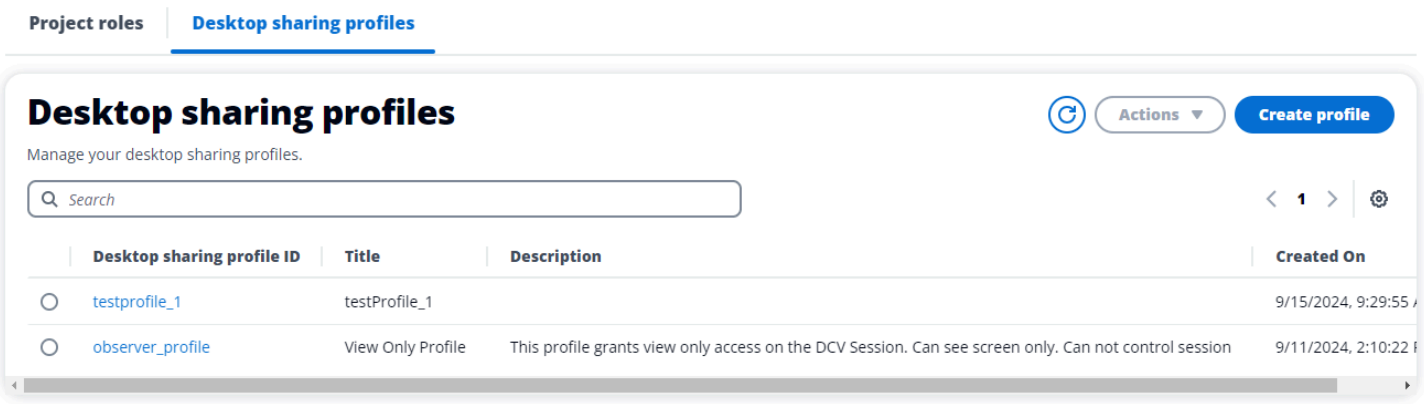
관리자는 데스크톱 권한을 켜거나 꺼서 모든 소유자의 VDI 기능을 전체적으로 관리할 수 있습니다. 이러한 모든 권한 또는 하위 집합을 사용하여 데스크톱을 공유하는 사용자가 수행할 수 있는 작업을 결정하는 데스크톱 공유 프로필을 생성할 수 있습니다. 데스크톱 권한이 비활성화된 경우 데스크톱 공유 프로필 에서 해당 권한이 자동으로 비활성화됩니다. 이러한 권한에는 “전 세계적으로 비활성화됨” 레이블이 지정됩니다. 관리자가 이 데스크톱 권한을 다시 활성화하더라도 관리자가 수동으로 활성화할 때까지 데스크톱 공유 프로필의 권한은 비활성화된 상태로 유지됩니다.

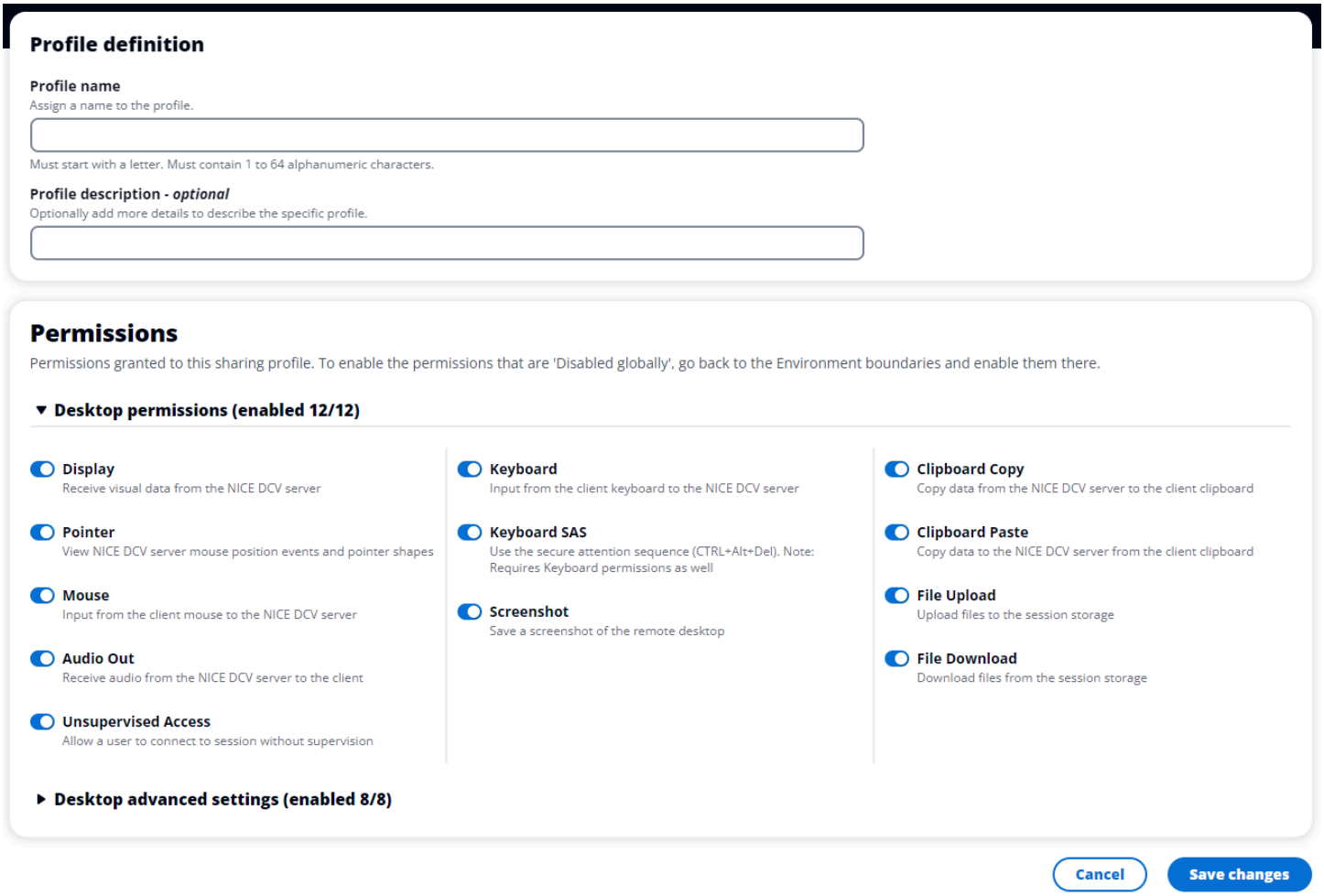
데스크톱 공유 프로필

관리자는 새 프로필을 생성하고 사용자 지정할 수 있습니다. 이러한 프로필은 모든 사용자가 액세스할 수 있으며 다른 사용자와 세션을 공유할 때 사용됩니다. 이러한 프로필 내에서 부여된 최대 권한은 전역적으로 허용되는 데스크톱 권한을 초과할 수 없습니다.

프로필 생성

관리자는 프로필 생성을 선택하여 새 프로필을 생성할 수 있습니다. 그런 다음 프로필 이름 , 프로필 설명 을 입력하고, 원하는 권한을 설정하고, 변경 사항을 저장할 수 있습니다.



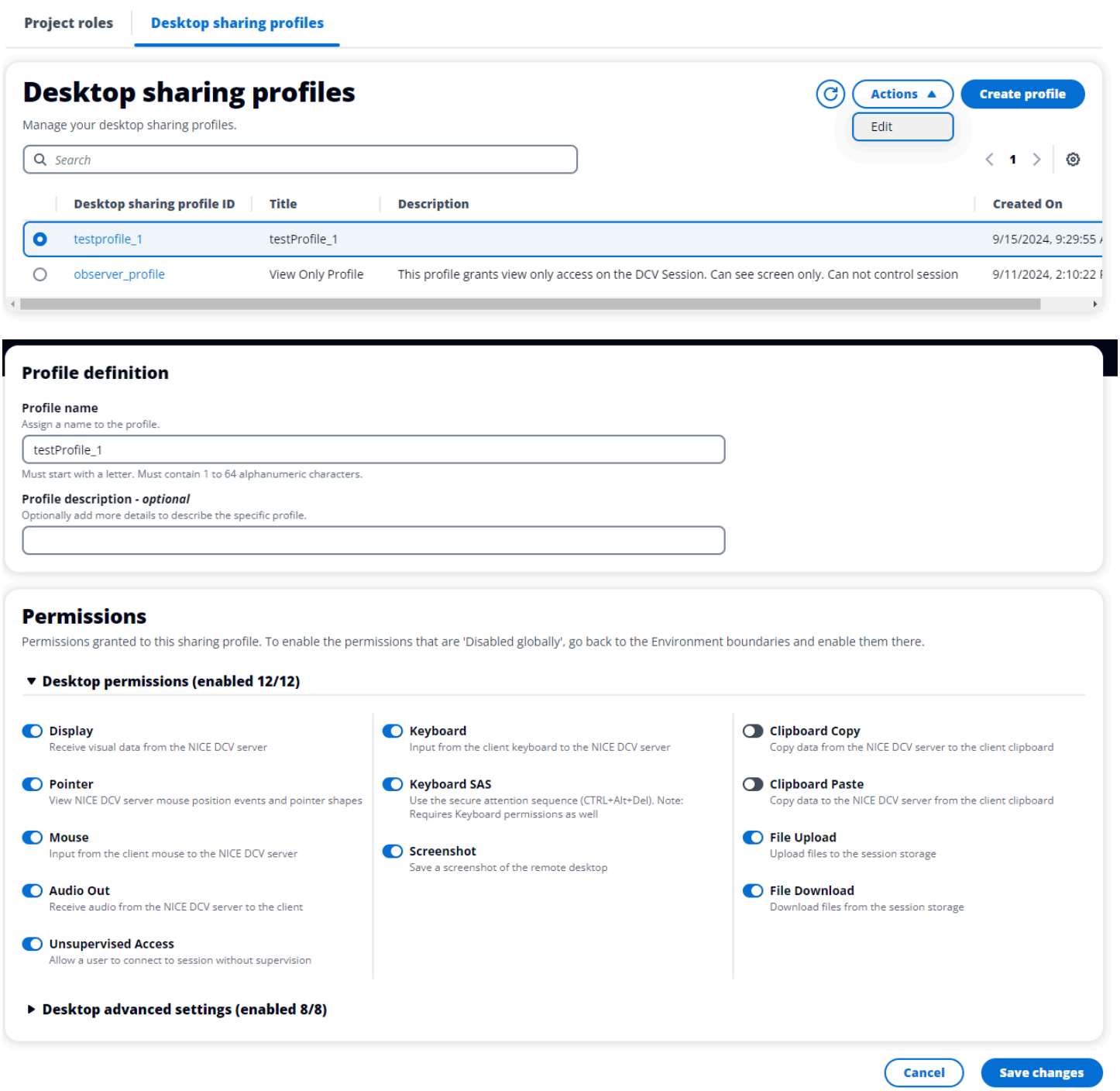


프로필 편집

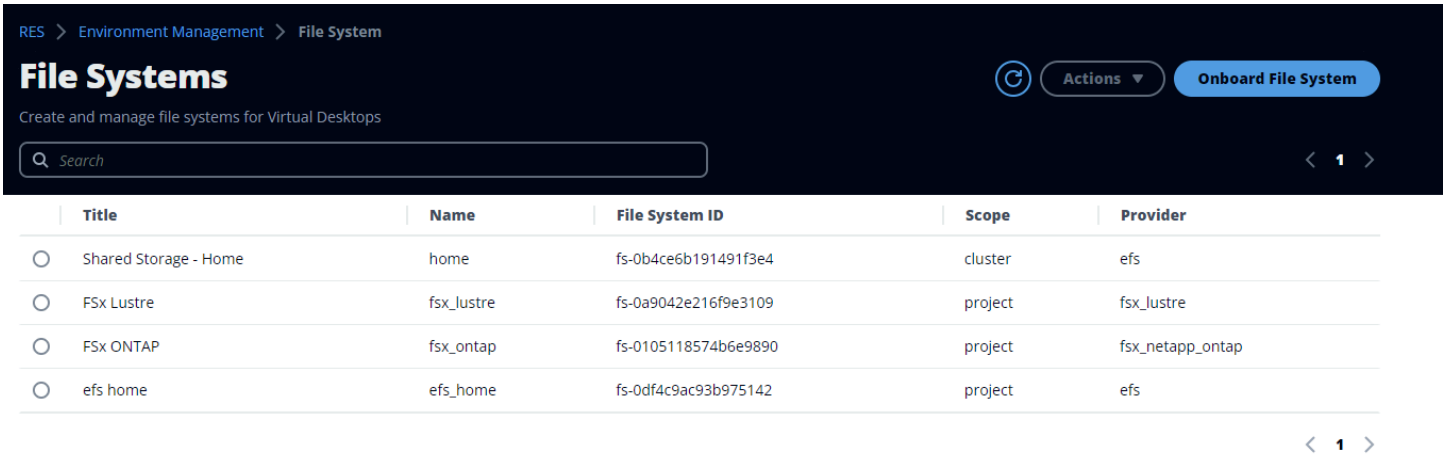
프로필을 편집하려면:

1. 원하는 프로파일을 선택합니다.
2. 작업 을 선택한 다음 편집을 선택하여 프로필을 수정합니다.
3. 필요에 따라 권한을 조정합니다.
4. Save changes(변경 사항 저장)를 선택합니다.

프로필에 대한 모든 변경 사항은 현재 열려 있는 세션에 즉시 적용됩니다.


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

파일 시스템



파일 시스템 페이지에서 다음을 수행할 수 있습니다.

1. 파일 시스템을 검색합니다.
2. 파일 시스템을 선택한 경우 작업 메뉴를 사용하여 다음을 수행합니다.
    a. 프로젝트에 파일 시스템을 추가합니다.
    b. 프로젝트에서 파일 시스템 제거
3. 새 파일 시스템을 온보딩합니다.
4. 파일 시스템을 생성합니다.
5. 파일 시스템을 선택하면 화면 하단의 창을 확장하여 파일 시스템 세부 정보를 볼 수 있습니다.

주제

- 파일 시스템 생성
- 파일 시스템 온보딩

파일 시스템 생성

1. 파일 시스템 생성을 선택합니다.
2. 새 파일 시스템의 세부 정보를 입력합니다.
3. IDs 에서 서브넷을 제공합니다VPC. 환경 관리 > 설정 > 네트워크 IDs 탭에서 를 찾을 수 있습니다.
4. 제출을 선택합니다.

Create new File System

Title

Enter a user friendly file system title

Eg. EFS 01

Name

Enter a file system name

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

File System Provider

Select applicable file system type

EFS

Projects

Select applicable project

Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

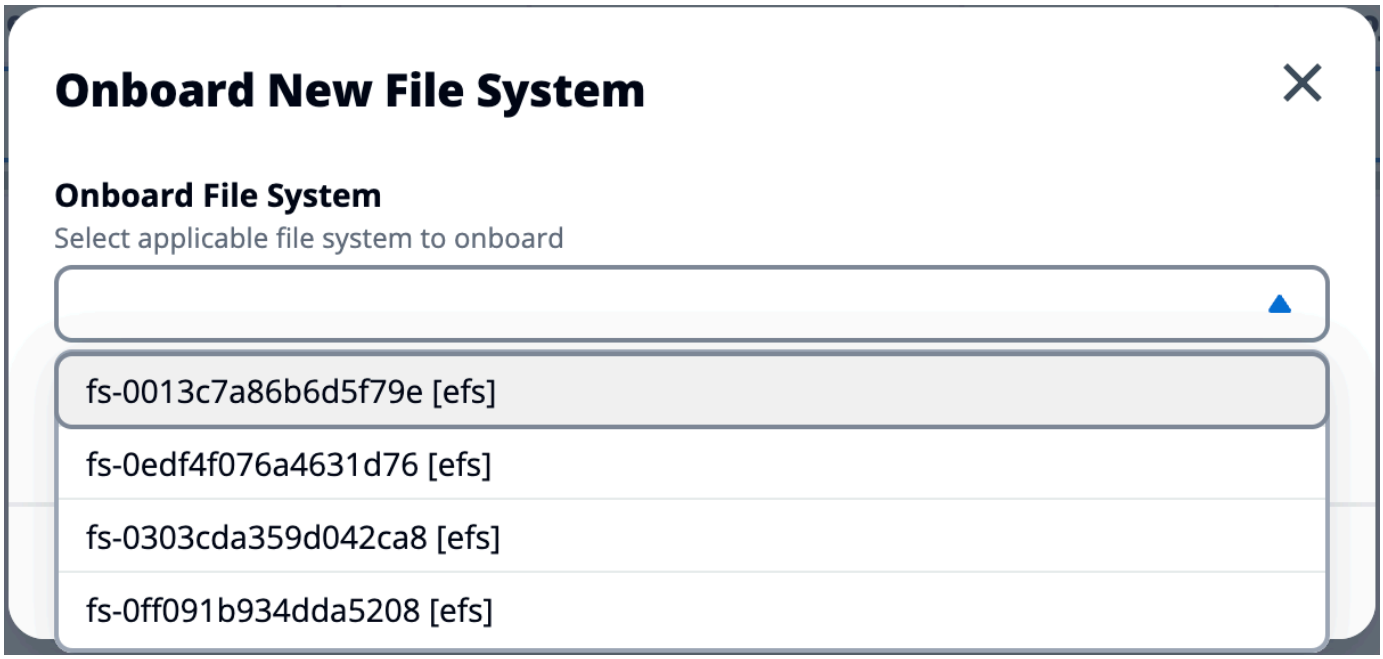
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

Enter directory to mount the file system

파일 시스템 온보딩

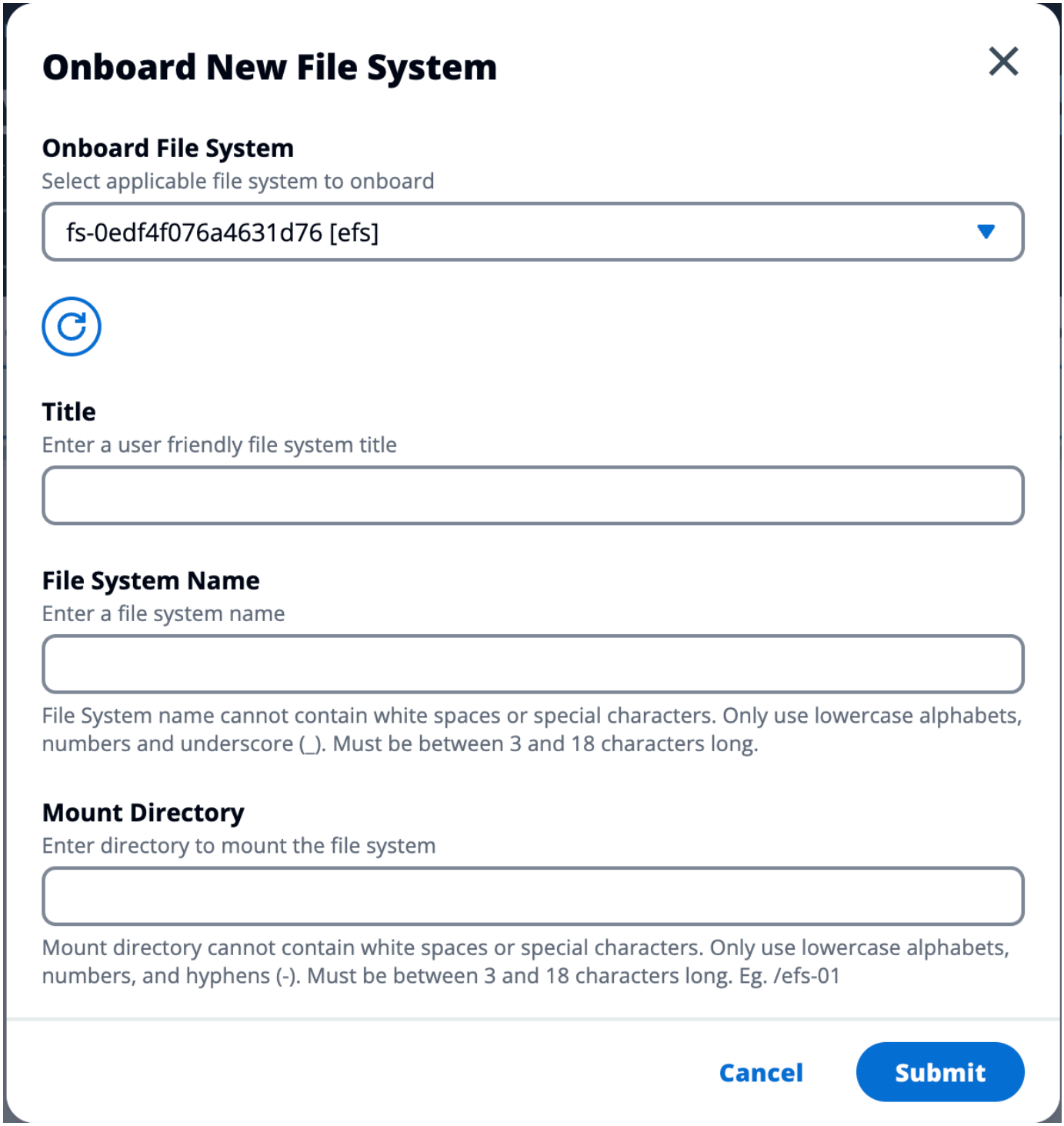
1. 온보드 파일 시스템 을 선택합니다.
2. 드롭다운에서 파일 시스템을 선택합니다. 모달은 추가 세부 항목과 함께 확장됩니다.



3. 파일 시스템 세부 정보를 입력합니다.

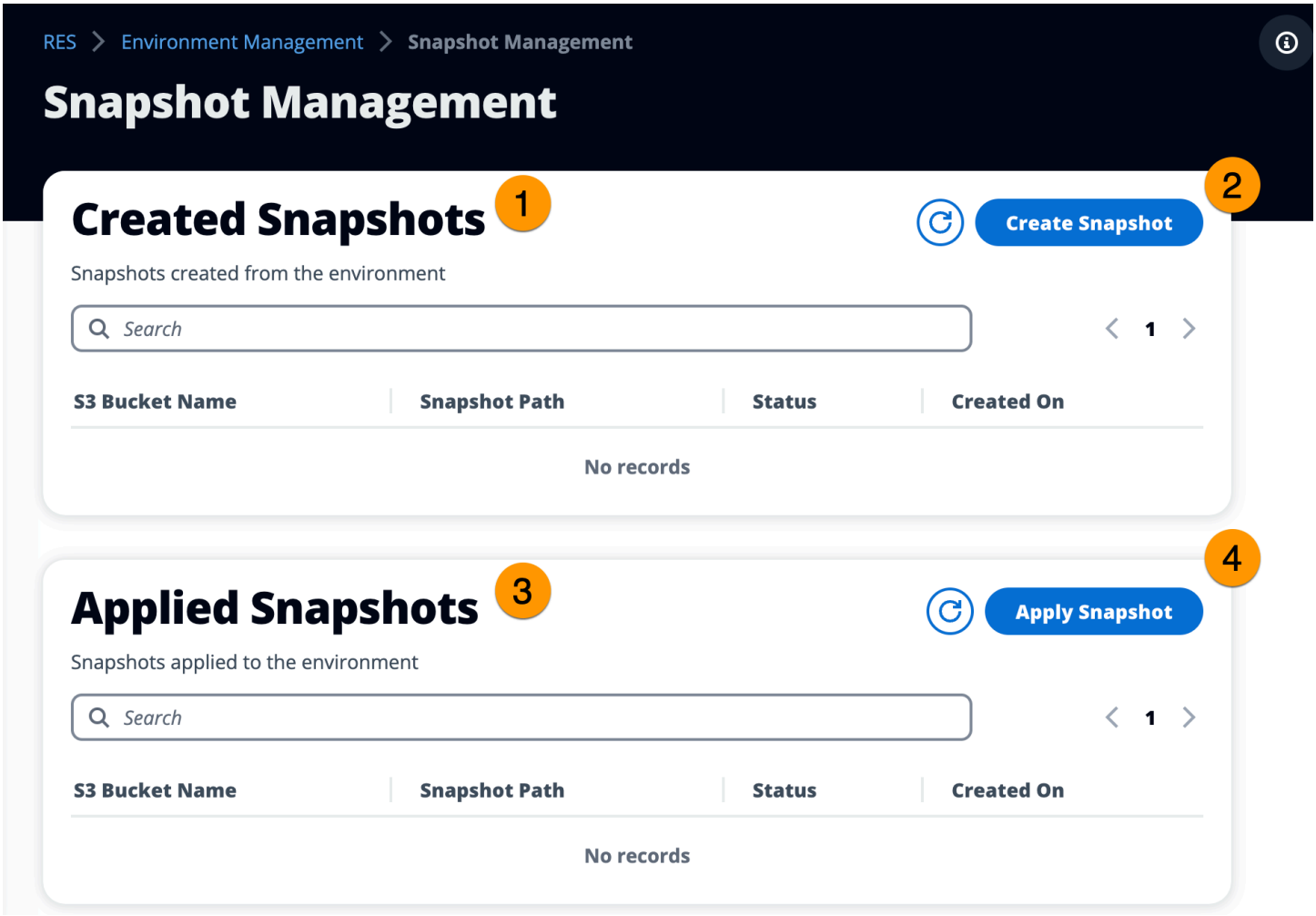
> **Note**
>
> 기본적으로 관리자와 프로젝트 소유자는 새 프로젝트를 생성할 때 홈 파일 시스템을 선택할 수 있으며, 나중에 편집할 수 없습니다.
> 프로젝트의 홈 디렉터리로 사용할 파일 시스템은 Mount Directory 경로를 로 설정하여 온보딩해야 합니다/home. 이렇게 하면 홈 디렉터리 파일 시스템 드롭다운 옵션에 온보딩된 파일 시스템이 채워집니다. 이 기능은 프로젝트와 연결된 사용자만 를 통해 파일 시스템에 액세스할 수 있으므로 프로젝트 간에 데이터를 격리하는 데 도움이 됩니다VDIs. VDIs 는 파일 시스템을 온보딩하는 동안 선택한 마운트 지점에 파일 시스템을 마운트합니다.

4. 제출을 선택합니다.


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

스냅샷 관리

스냅샷 관리는 환경 간에 데이터를 저장하고 마이그레이션하는 프로세스를 간소화하여 일관성과 정확성을 보장합니다. 스냅샷을 사용하면 환경 상태를 저장하고 동일한 상태의 새 환경으로 데이터를 마이그레이션할 수 있습니다.



스냅샷 관리 페이지에서 다음을 수행할 수 있습니다.

1. 생성된 모든 스냅샷과 해당 상태를 봅니다.
2. 스냅샷을 생성합니다. 스냅샷을 생성하려면 먼저 적절한 권한이 있는 버킷을 생성해야 합니다.
3. 적용된 모든 스냅샷과 해당 상태를 봅니다.
4. 스냅샷을 적용합니다.

주제

- 스냅샷 생성

- 스냅샷 적용

스냅샷 생성

스냅샷을 생성하기 전에 Amazon S3 버킷에 필요한 권한을 제공해야 합니다. 버킷 생성에 대한 자세한 내용은 버킷 생성을 참조하세요. 버킷 버전 관리 및 서버 액세스 로깅을 활성화하는 것이 좋습니다. 이러한 설정은 프로비저닝 후 버킷의 속성 탭에서 활성화할 수 있습니다.

> **Note**
>
> 이 Amazon S3 버킷의 수명 주기는 제품 내에서 관리되지 않습니다. 콘솔에서 버킷 수명 주기를 관리해야 합니다.

버킷에 권한을 추가하려면:

1. 버킷 목록에서 생성한 버킷을 선택합니다.
2. 권한 탭을 선택합니다.
3. 버킷 정책에서 편집을 선택합니다.
4. 버킷 정책에 다음 문을 추가합니다. 이 값들을 사용자의 값으로 대체합니다.

    - AWS_ACCOUNT_ID
    - RES_ENVIRONMENT_NAME
    - AWS_REGION
    - S3_BUCKET_NAME

> **Important**
>
> 에서 지원하는 버전 문자열은 제한적입니다 AWS. 자세한 내용은 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html 단원을 참조하십시오.

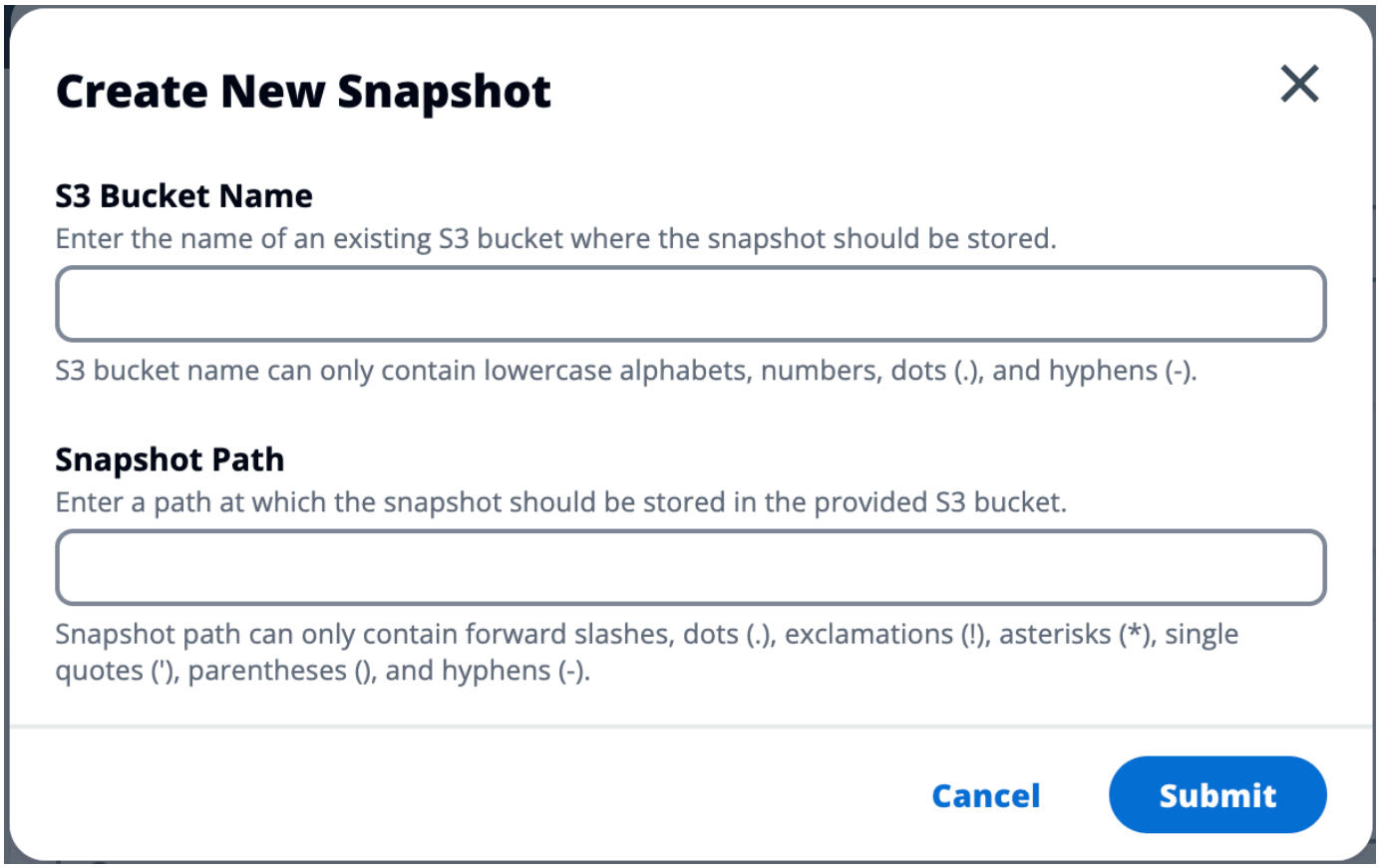
```
{
    "Version": "2012-10-17",
    "Statement": [
```

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

스냅샷을 생성하려면:

1. [스냅샷 생성(Create Snapshot)]을 클릭합니다.
2. 생성한 Amazon S3 버킷의 이름을 입력합니다.
3. 버킷 내에 스냅샷을 저장할 경로를 입력합니다. 예: **october2023/23**.

4. 제출을 선택합니다.



5. 5~10분 후 스냅샷 페이지에서 새로 고침을 선택하여 상태를 확인합니다. 스냅샷은 상태가 IN_PROGRESS에서 로 변경될 때까지 유효하지 않습니다COMPLETED.

스냅샷 적용

환경의 스냅샷을 생성한 후에는 해당 스냅샷을 새 환경에 적용하여 데이터를 마이그레이션할 수 있습니다. 환경이 스냅샷을 읽을 수 있도록 버킷에 새 정책을 추가해야 합니다.

스냅샷을 적용하면 사용자 권한, 프로젝트, 소프트웨어 스택, 권한 프로파일 및 새 환경에 대한 연결이 있는 파일 시스템과 같은 데이터가 복사됩니다. 사용자 세션은 복제되지 않습니다. 스냅샷이 적용되면 각 리소스 레코드의 기본 정보를 확인하여 이미 존재하는지 확인합니다. 중복 레코드의 경우 스냅샷은 새 환경에서 리소스 생성을 건너뜁니다. 이름 또는 키 공유와 같이 유사하지만 다른 기본 리소스 정보는 다양한 레코드의 경우 다음 규칙을 사용하여 수정된 이름 및 키로 새 레코드를 생성합니다`RecordName_SnapshotRESVersion_ApplySnapshotID`. 는 타임스탬프처럼 `ApplySnapshotID` 보이고 스냅샷을 적용하려는 각 시도를 식별합니다.

스냅샷 애플리케이션 중에 스냅샷은 리소스의 가용성을 확인합니다. 새 환경에서 사용할 수 없는 리소스는 생성되지 않습니다. 종속 리소스가 있는 리소스의 경우 스냅샷은 종속 리소스의 가용성을 확인합니다. 종속 리소스를 사용할 수 없는 경우 종속 리소스 없이 기본 리소스를 생성합니다.

새 환경이 예상과 다르거나 실패하는 경우 CloudWatch 로그 그룹에 있는 로그에서 세부 정보를 확인할 수 `/res-<env-name>/cluster-manager` 있습니다. 각 로그에는 [스냅샷 적용] 태그가 있습니다. 스냅샷을 적용한 후에는 the section called “스냅샷 관리” 페이지에서 스냅샷 상태를 확인할 수 있습니다.

버킷에 권한을 추가하려면:

1. 버킷 목록에서 생성한 버킷을 선택합니다.
2. 권한 탭을 선택합니다.
3. 버킷 정책에서 편집을 선택합니다.
4. 버킷 정책에 다음 문을 추가합니다. 이 값들을 사용자의 값으로 대체합니다.

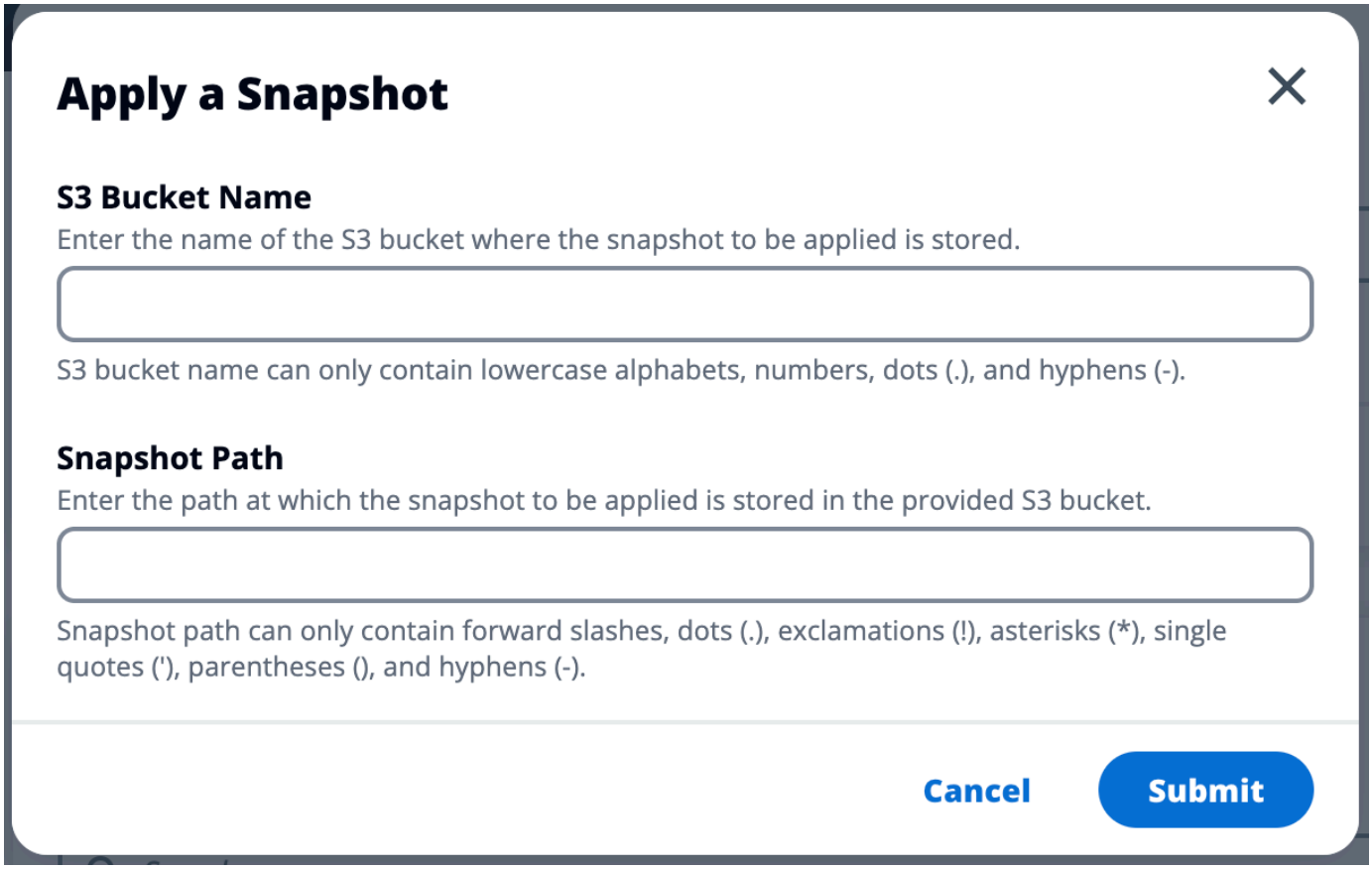
    - AWS_ACCOUNT_ID
    - RES_ENVIRONMENT_NAME
    - AWS_REGION
    - S3_BUCKET_NAME

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

```
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

스냅샷을 적용하려면:

1. 스냅샷 적용을 선택합니다.
2. 스냅샷이 포함된 Amazon S3 버킷의 이름을 입력합니다.
3. 버킷 내의 스냅샷에 대한 파일 경로를 입력합니다.
4. 제출을 선택합니다.



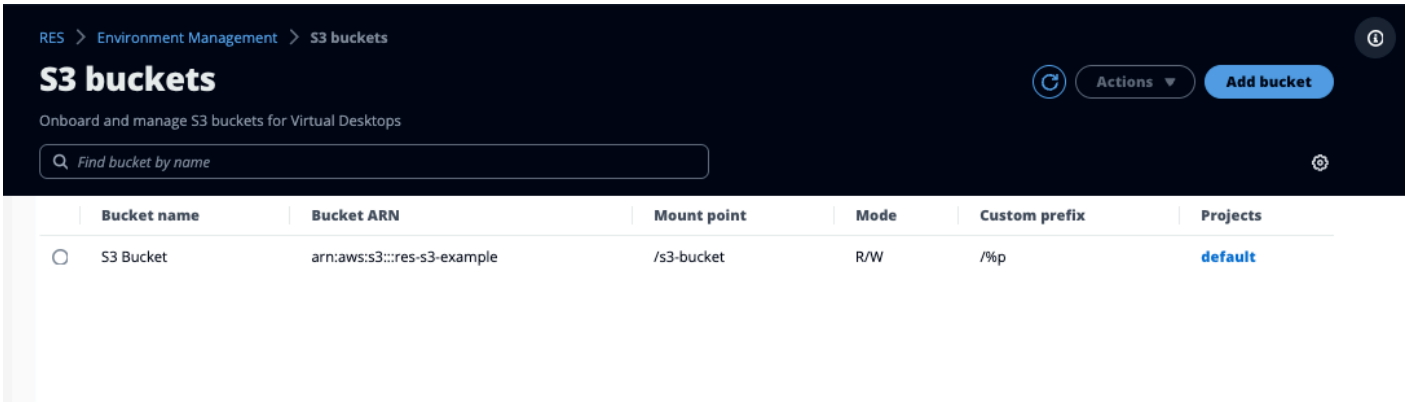
5. 5~10분 후 스냅샷 관리 페이지에서 새로 고침을 선택하여 상태를 확인합니다.

Amazon S3 버킷

Research and Engineering Studio(RES)는 Amazon S3 버킷을 Linux Virtual Desktop Infrastructure(VDI) 인스턴스에 탑재하는 것을 지원합니다. RES 관리자는 환경 관리 의 S3 버킷 탭에서 S3 버킷을 에 온보딩하고RES, 프로젝트에 연결하고, 구성을 편집하고, 버킷을 제거할 수 있습니다.

S3 버킷 대시보드는 사용자가 사용할 수 있는 온보딩된 S3 버킷 목록을 제공합니다. S3 버킷 대시보드에서 다음을 수행할 수 있습니다.

1. 버킷 추가를 사용하여 S3 버킷을 에 온보딩합니다RES.
2. S3 버킷을 선택하고 작업 메뉴를 사용하여 다음을 수행합니다.
   - 버킷 편집
   - 버킷 제거
3. 검색 필드를 사용하여 버킷 이름으로 검색하고 온보딩된 S3 버킷을 찾습니다.



다음 섹션에서는 RES 프로젝트에서 Amazon S3 버킷을 관리하는 방법을 설명합니다.

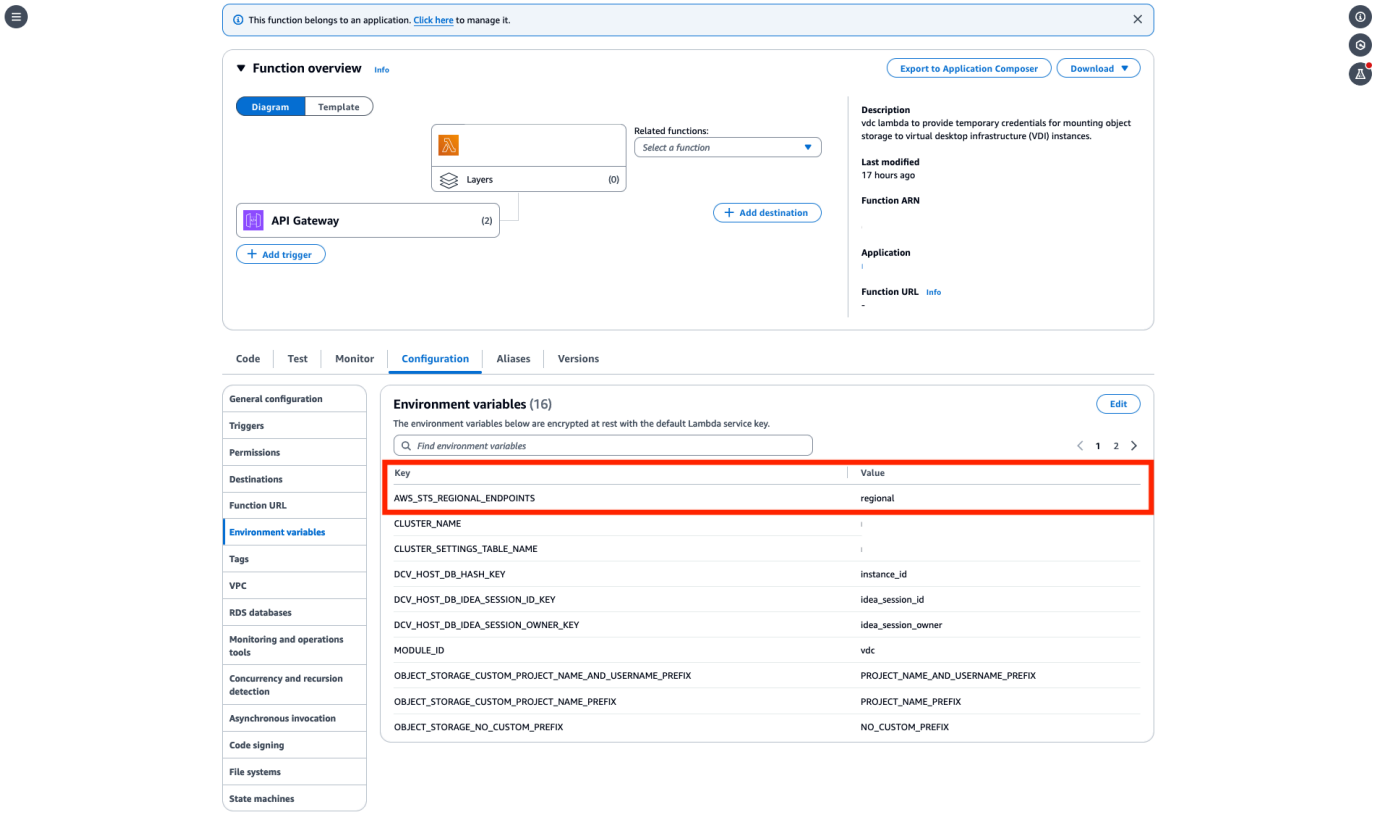
주제

- 격리된 VPC 배포를 위한 Amazon S3 버킷 사전 조건
- Amazon S3 버킷 추가
- Amazon S3 버킷 편집
- Amazon S3 버킷 제거
- 데이터 격리
- 교차 계정 버킷 액세스
- 프라이빗에서 데이터 유출 방지 VPC
- 문제 해결
- 활성화 CloudTrail

격리된 VPC 배포를 위한 Amazon S3 버킷 사전 조건

격리된 에 Research and Engineering Studio를 배포하는 경우 VPC다음 단계에 따라 AWS 계정에 배포한 후 lambda 구성 파라미터를 업데이트RES합니다.

1. Research and Engineering Studio가 배포된 AWS 계정의 Lambda 콘솔에 로그인합니다.
2. 라는 Lambda 함수를 찾아 탐색합니다`<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`.
3. 함수의 구성 탭을 선택합니다.



4. 왼쪽에서 환경 변수를 선택하여 해당 섹션을 봅니다.
5. 편집을 선택하고 함수에 다음과 같은 새 환경 변수를 추가합니다.
   - 키: `AWS_STS_REGIONAL_ENDPOINTS`
   - 값: `regional`
6. 저장(Save)을 선택합니다.

Amazon S3 버킷 추가

RES 환경에 S3 버킷을 추가하려면:

1. Add bucket(버킷 추가)을 선택합니다.
2. 버킷 이름, 및 마운트 포인트ARN와 같은 버킷 세부 정보를 입력합니다.

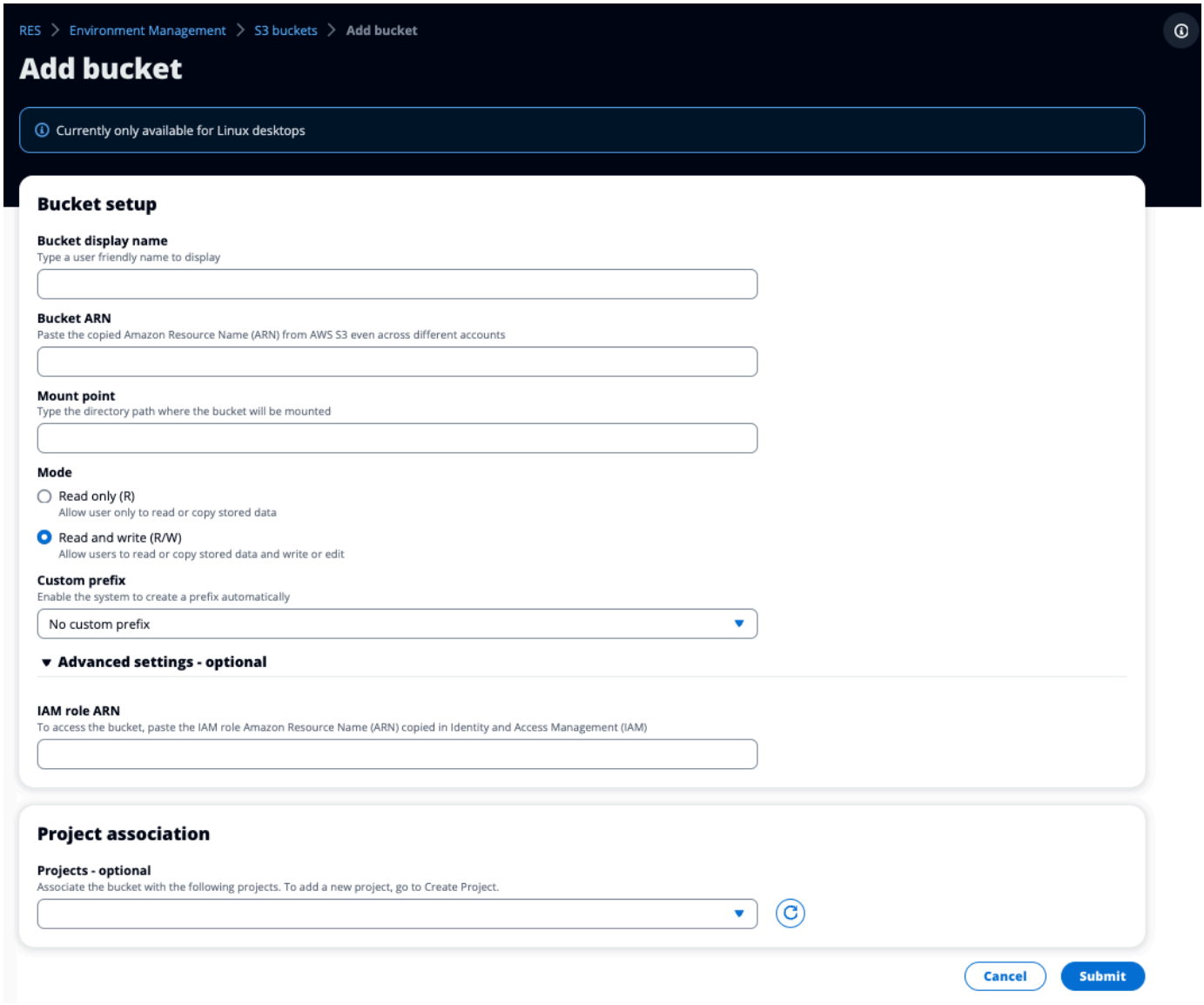
> **Important**
>
> - 제공된 버킷 ARN, 마운트 포인트 및 모드는 생성 후 변경할 수 없습니다.

- 버킷에는 온보딩된 S3 버킷을 해당 접두사로 격리하는 접두사가 포함될 ARN 수 있습니다.

3. 버킷을 온보딩할 모드를 선택합니다.

> **Important**
>
> - 특정 모드를 사용한 데이터 격리와 관련된 데이터 격리 자세한 내용은 섹션을 참조하세요.

4. 고급 옵션 에서 교차 계정 액세스를 위해 버킷을 탑재ARN하는 IAM 역할을 제공할 수 있습니다. 의 단계에 따라 크로스 계정 액세스에 필요한 IAM 역할을 교차 계정 버킷 액세스 생성합니다.
5. (선택 사항) 나중에 변경할 수 있는 프로젝트와 버킷을 연결합니다. 하지만 S3 버킷은 프로젝트의 기존 VDI 세션에 탑재할 수 없습니다. 프로젝트가 버킷과 연결된 후 시작된 세션만 버킷을 마운트합니다.
6. 제출을 선택합니다.

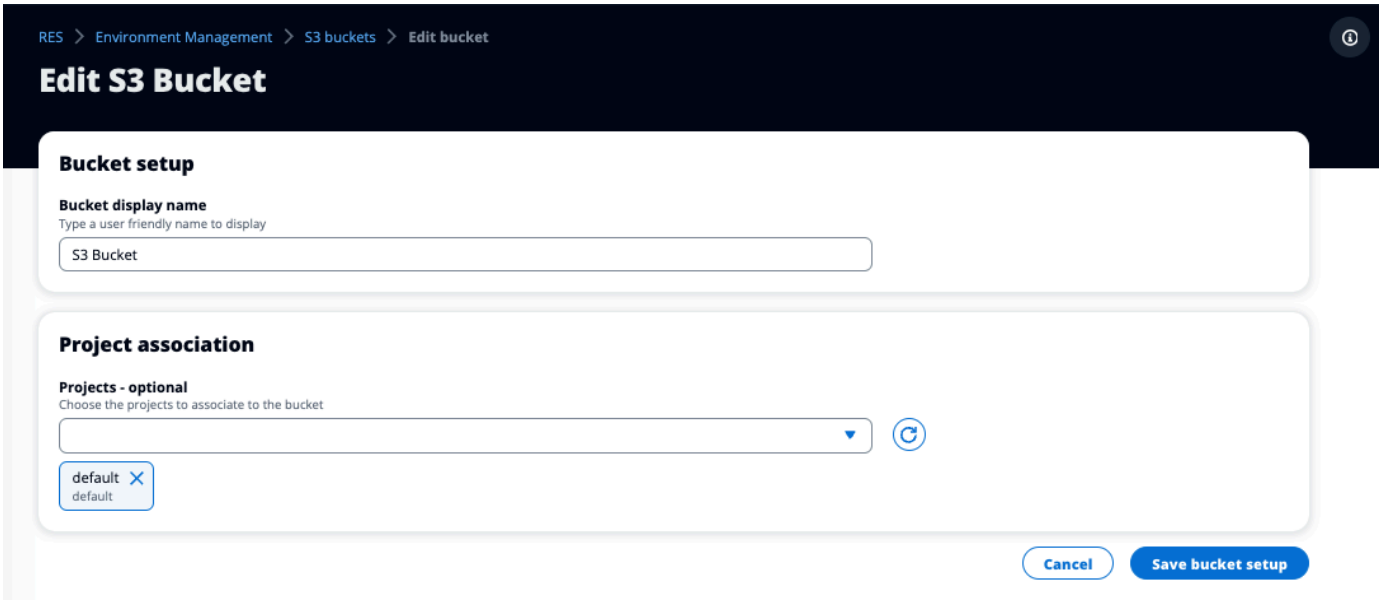


Amazon S3 버킷 편집

1. S3 버킷 목록에서 S3 버킷을 선택합니다.
2. 작업 메뉴에서 편집을 선택합니다.
3. 업데이트를 입력합니다.

> **Important**
>
> - 프로젝트를 S3 버킷과 연결하면 버킷이 해당 프로젝트의 기존 가상 데스크톱 인프라(VDI) 인스턴스에 탑재되지 않습니다. 버킷은 버킷이 해당 프로젝트와 연결된 후에만 프로젝트에서 시작된 VDI 세션에 탑재됩니다.
> - S3 버킷에서 프로젝트를 연결 해제해도 S3 버킷의 데이터는 영향을 받지 않지만 데스크톱 사용자는 해당 데이터에 액세스할 수 없게 됩니다.

4. 버킷 설정 저장을 선택합니다.



Amazon S3 버킷 제거

1. S3 버킷 목록에서 S3 버킷을 선택합니다.
2. 작업 메뉴에서 제거를 선택합니다.

> **Important**
>
> - 먼저 버킷에서 모든 프로젝트 연결을 제거해야 합니다.
> - 제거 작업은 S3 버킷의 데이터에 영향을 주지 않습니다. S3 버킷과 의 연결만 제거합니다RES.

- 버킷을 제거하면 해당 VDI 세션의 자격 증명이 만료될 때(~1시간) 기존 세션이 해당 버킷의 콘텐츠에 액세스할 수 없게 됩니다.

데이터 격리

에 S3 버킷을 추가하면 버킷 내의 데이터를 특정 프로젝트 및 사용자와 격리할 RES수 있는 옵션이 있습니다. 버킷 추가 페이지에서 읽기 전용(R) 또는 읽기 및 쓰기(R/W) 모드를 선택할 수 있습니다.

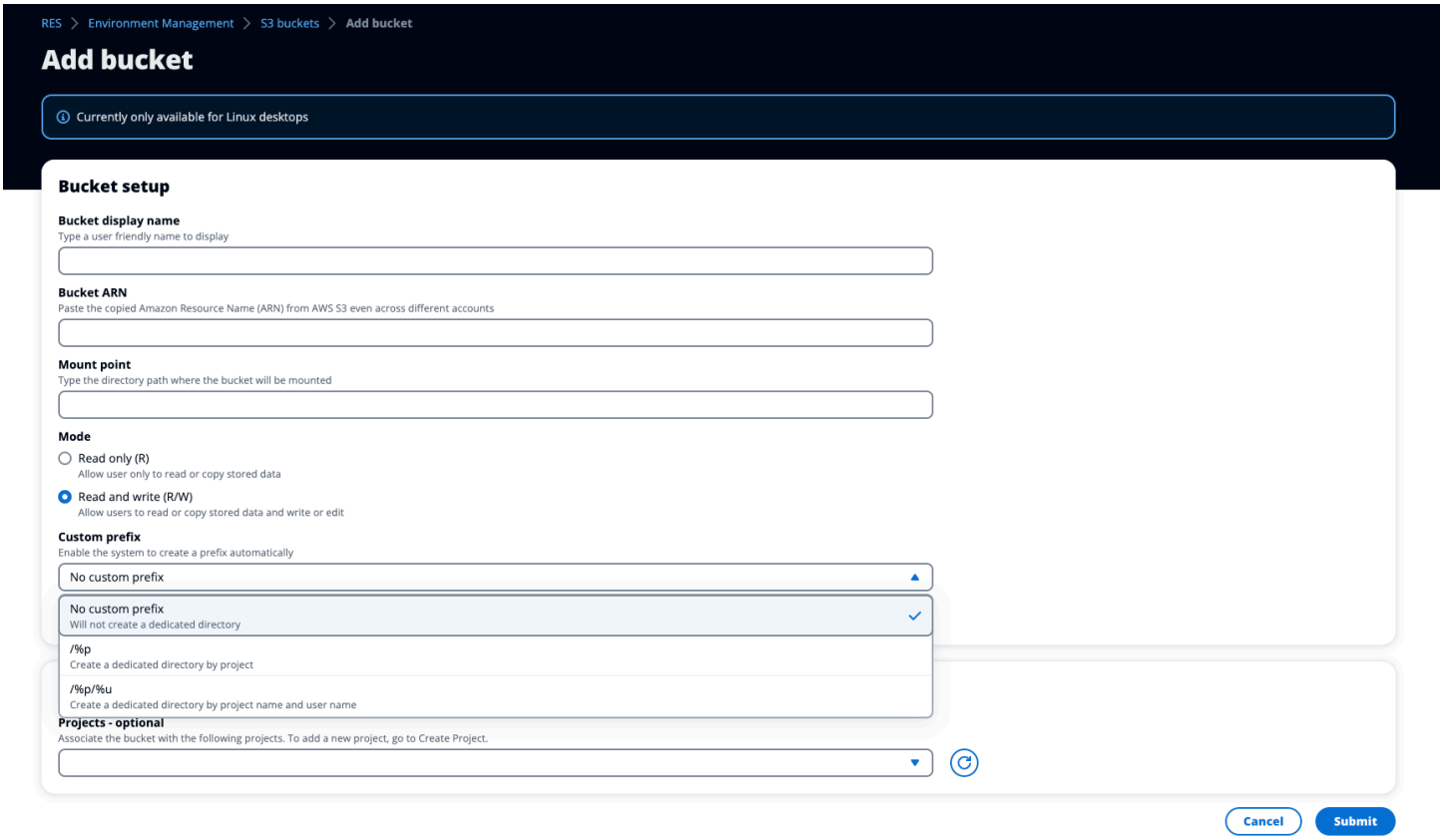
읽기 전용

`Read Only (R)` 이 선택되면 버킷의 접두사ARN(Amazon 리소스 이름)를 기반으로 데이터 격리가 적용됩니다. 예를 들어 관리자가 를 RES 사용하여 버킷을 에 추가ARN`arn:aws:s3:::`*`bucket-name/example-data`*`/`하고 이 버킷을 프로젝트 A 및 프로젝트 B와 연결하면 프로젝트 A 및 프로젝트 B VDIs 내에서 시작하는 사용자는 경로 *`bucket-name`* 아래에 있는 에 있는 데이터만 읽을 수 있습니다*`/example-data`*. 해당 경로 외부의 데이터에 액세스할 수 없습니다. 버킷 에 접두사가 추가되지 않은 경우 ARN전체 버킷은 연결된 모든 프로젝트에 사용할 수 있습니다.

읽기 및 쓰기

`Read and Write (R/W)` 이 선택되어도 위에서 설명한 ARN대로 버킷의 접두사 를 기반으로 데이터 격리가 계속 적용됩니다. 이 모드에는 관리자가 S3 버킷에 대해 변수 기반 접두사를 제공할 수 있도록 허용하는 추가 옵션이 있습니다. `Read and Write (R/W)` 를 선택하면 다음 옵션이 포함된 드롭다운 메뉴를 제공하는 사용자 지정 접두사 섹션을 사용할 수 있습니다.

- 사용자 지정 접두사 없음
- /%p
- /%p/%u



사용자 지정 데이터 격리 없음

사용자 지정 접두사 에 대해 `No custom prefix`를 선택하면 사용자 지정 데이터 격리 없이 버킷이 추가됩니다. 이렇게 하면 버킷과 연결된 모든 프로젝트에 읽기 및 쓰기 액세스 권한이 부여됩니다. 예를 들어 관리자가 `No custom prefix` ARN`arn:aws:s3:::`*`bucket-name`*를 RES 사용하여 에 버킷을 추가하고 이 버킷을 프로젝트 A 및 프로젝트 B와 연결하면 프로젝트 A 및 프로젝트 B VDIs 내에서 시작하는 사용자는 버킷에 대한 무제한 읽기 및 쓰기 액세스 권한을 갖습니다.

프로젝트별 수준의 데이터 격리

`/%p` 가 사용자 지정 접두사 에 대해 선택되면 버킷의 데이터가 연결된 각 특정 프로젝트로 격리됩니다. `%p` 변수는 프로젝트 코드를 나타냅니다. 예를 들어 관리자가 를 `/%p` 선택한 ARN `arn:aws:s3:::`*`bucket-name`* 와 함께 사용하고 의 마운트 포인트를 RES 사용하여 에 버킷을 추가하는 경우 */bucket*이 버킷을 프로젝트 A 및 프로젝트 B와 연결하면 프로젝트 A의 사용자 A가 에 파일을 쓸 수 있습니다./*bucket*. 프로젝트 A의 사용자 B는 사용자 A가 작성한 파일을 볼 수도 있습니다./*bucket*. 그러나 사용자 B가 프로젝트 BVDI에서 를 시작하고 를 보는 경우 */bucket*, 데이터가 프로젝트별로 격리되므로 사용자 A가 작성한 파일은 표시되지 않습니다. 사용자 A가 작

성한 파일은 접두사 아래의 S3 버킷에서 찾을 수 /ProjectA 있지만 사용자 B는 프로젝트 BVDIs에서 를 사용할 /ProjectB 때만 액세스할 수 있습니다.

프로젝트별, 사용자별 데이터 격리

/%p/%u 가 사용자 지정 접두사 에 대해 선택되면 버킷의 데이터가 해당 프로젝트와 연결된 각 특정 프로젝트 및 사용자에게 격리됩니다. %p 변수는 프로젝트 코드를 나타내고 사용자 이름을 %u 나타냅니다. 예를 들어, 관리자는 를 /%p/%u 선택한 ARN arn:aws:s3:::*bucket-name* 와 의 마운트 포인트를 RES 사용하여 에 버킷을 추가합니다./*bucket*. 이 버킷은 프로젝트 A 및 프로젝트 B와 연결되어 있습니다. 프로젝트 A의 사용자 A는 에 파일을 쓸 수 있습니다./*bucket*. %p 격리만 있는 이전 시나리오와 달리 이 경우 사용자 B는 의 프로젝트 A에서 사용자 A가 작성한 파일을 볼 수 없습니다./*bucket*프로젝트와 사용자 모두가 데이터를 격리합니다. 사용자 A가 작성한 파일은 접두사 아래의 S3 버킷에서 찾을 수 /ProjectA/UserA 있지만 사용자 B는 프로젝트 AVDIs에서 를 사용할 /ProjectA/UserB 때만 액세스할 수 있습니다.

교차 계정 버킷 액세스

RES 는 버킷에 적절한 권한이 있는 경우 다른 AWS 계정에서 버킷을 탑재할 수 있습니다. 다음 시나리오에서는 계정 A의 RES 환경이 계정 B에 S3 버킷을 탑재하려고 합니다.

1단계: 에 배포RES된 계정에서 IAM 역할 생성(이를 계정 A라고 함):

1. S3 버킷(계정 A)에 액세스해야 하는 RES 계정의 AWS 관리 콘솔에 로그인합니다.
2. IAM 콘솔을 엽니다.
   a. IAM 대시보드로 이동합니다.
   b. 탐색 창에서 Policies를 선택합니다.
3. 정책 생성:
   a. 정책 생성을 선택합니다.
   b. JSON 탭을 선택합니다.
   c. 다음 JSON 정책을 붙여넣습니다(계정 B에 있는 S3 버킷의 *<BUCKET-NAME>* 이름으로 바꿉니다).

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

```
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

d. Next(다음)를 선택합니다.

4. 정책을 검토하고 생성합니다.

   a. 정책의 이름을 입력합니다(예: “S3AccessPolicy”).

   b. 선택적 설명을 추가하여 정책의 목적을 설명합니다.

   c. 정책을 검토하고 정책 생성 을 선택합니다.

5. IAM 콘솔을 엽니다.

   a. IAM 대시보드로 이동합니다.

   b. 탐색 창에서 Roles를 선택합니다.

6. 역할 생성:

   a. 역할 생성을 선택합니다.

   b. 신뢰할 수 있는 엔터티 유형으로 사용자 지정 신뢰 정책을 선택합니다.

   c. 다음 JSON 정책을 붙여 넣습니다(A 계정의 실제 계정 ID*<ACCOUNT_ID>*, RES 배포의 *<ENVIRONMENT_NAME>* 환경 이름, AWS 리전RES이 배포된 *<REGION>* 상태로 대체).

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

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. Next(다음)를 선택합니다.

7. 권한 정책 연결:

a. 이전에 생성한 정책을 검색하고 선택합니다.

b. Next(다음)를 선택합니다.

8. 역할에 태그 지정, 검토 및 생성:

a. 역할 이름(예: “S3AccessRole”)을 입력합니다.

b. 3단계에서 태그 추가를 선택한 다음 다음 키와 값을 입력합니다.

- 키: `res:Resource`
- 값: `s3-bucket-iam-role`

c. 역할을 검토하고 역할 생성 을 선택합니다.

9. 에서 IAM 역할 사용RES:

a. 생성한 IAM 역할을 복사ARN합니다.

b. RES 콘솔에 로그인합니다.

c. 왼쪽 탐색 창에서 S3 버킷 을 선택합니다.

d. 버킷 추가를 선택하고 교차 계정 S3 버킷 로 양식을 작성합니다ARN.

e. 고급 설정 - 선택적 드롭다운을 선택합니다.

f. 역할 ARN 필드에 IAM 역할을 입력합니다ARN.

g. 버킷 추가를 선택합니다.

2단계: 계정 B에서 버킷 정책 수정

1. 계정 B의 AWS 관리 콘솔에 로그인합니다.

2. S3 콘솔을 엽니다.

a. S3 대시보드로 이동합니다.

b. 액세스 권한을 부여할 버킷을 선택합니다.

3. 버킷 정책 편집:

   a. 권한 탭을 선택하고 버킷 정책 을 선택합니다.

   b. 다음 정책을 추가하여 계정 A의 IAM 역할에 버킷에 대한 액세스 권한을 부여합니다(교체 *<AccountA_ID>* 계정 A의 실제 계정 ID와 *<BUCKET-NAME>* S3 버킷 이름 포함):

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

   c. 저장(Save)을 선택합니다.

프라이빗에서 데이터 유출 방지 VPC

사용자가 보안 S3 버킷의 데이터를 계정의 자체 S3 버킷으로 유출하지 못하도록 VPC 엔드포인트를 연결하여 프라이빗 를 보호할 수 있습니다VPC. 다음 단계에서는 계정 내의 S3 버킷에 대한 액세스와 교차 계정 버킷이 있는 추가 계정에 대한 액세스를 지원하는 S3 서비스에 대한 VPC 엔드포인트를 생성하는 방법을 보여줍니다.

1. Amazon VPC 콘솔을 엽니다.

   a. AWS 관리 콘솔에 로그인합니다.

b. 에서 Amazon VPC 콘솔을 엽니다 https://console.aws.amazon.com/vpc/.

2. S3용 VPC 엔드포인트 생성:

a. 왼쪽 탐색 창에서 엔드포인트를 선택합니다.

b. 엔드포인트 생성을 선택합니다.

c. 서비스 범주에서 AWS 서비스를 선택해야 합니다.

d. 서비스 이름 필드에 `com.amazonaws.<region>.s3` (해당 AWS 리전*<region>*으로 바꾸기)를 입력하거나 “S3”를 검색합니다.

e. 목록에서 S3 서비스를 선택합니다.

3. 엔드포인트 설정 구성:

a. 에서 엔드포인트를 생성할 VPC 를 VPC선택합니다.

b. 서브넷 에서 배포 중에 서브넷에 사용되는 프라이빗 VDI 서브넷을 모두 선택합니다.

c. DNS 이름 활성화 에서 옵션이 선택되어 있는지 확인합니다. 이렇게 하면 프라이빗 DNS 호스트 이름을 엔드포인트 네트워크 인터페이스로 확인할 수 있습니다.

4. 액세스를 제한하도록 정책을 구성합니다.

a. 정책 에서 사용자 지정 을 선택합니다.

b. 정책 편집기에서 계정 또는 특정 계정 내의 리소스에 대한 액세스를 제한하는 정책을 입력합니다. 다음은 예제 정책입니다(교체 *mybucket* S3 버킷 이름과 *111122223333* 그리고 *444455556666* 액세스 IDs 권한을 부여하려는 적절한 AWS 계정을 사용하여):

```
{
    "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. 엔드포인트 생성:

    a. 설정을 검토합니다.

    b. Create endpoint(엔드포인트 생성)을 선택합니다.

6. 엔드포인트 확인:

    a. 엔드포인트가 생성되면 VPC 콘솔의 엔드포인트 섹션으로 이동합니다.

    b. 새로 생성된 엔드포인트를 선택합니다.

    c. 상태가 사용 가능한지 확인합니다.

다음 단계에 따라 계정 또는 지정된 계정 ID 내의 리소스로 제한된 S3 액세스를 허용하는 VPC 엔드포인트를 생성합니다.

문제 해결

버킷이 에 탑재되지 않는지 확인하는 방법 VDI

버킷이 에 탑재되지 않는 경우 오류를 확인할 수 있는 몇 VDI가지 위치가 있습니다. 아래 단계를 따릅니다.

1. VDI 로그 확인:

    a. AWS 관리 콘솔에 로그인합니다.

    b. EC2 콘솔을 열고 인스턴스 로 이동합니다.

    c. 시작한 VDI 인스턴스를 선택합니다.

    d. 세션 관리자를 VDI 통해 에 연결합니다.

    e. 다음 명령을 실행합니다.

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

여기에서 부트스트랩 로그를 확인할 수 있습니다. 실패에 대한 세부 정보는 `configure.log.{time}` 파일에 있습니다.

또한 `/etc/message` 로그에서 자세한 내용을 확인하세요.

2. 사용자 지정 자격 증명 브로커 Lambda CloudWatch 로그 확인:

   a. AWS 관리 콘솔에 로그인합니다.

   b. CloudWatch 콘솔을 열고 로그 그룹 으로 이동합니다.

   c. 로그 그룹 를 검색합니다`/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.

   d. 첫 번째 사용 가능한 로그 그룹을 검사하고 로그 내에서 오류를 찾습니다. 이러한 로그에는 S3 버킷을 탑재하기 위한 임시 사용자 지정 자격 증명을 제공하는 잠재적 문제에 대한 세부 정보가 포함됩니다.

3. 사용자 지정 자격 증명 브로커 API 게이트웨이 CloudWatch 로그 확인:

   a. AWS 관리 콘솔에 로그인합니다.

   b. CloudWatch 콘솔을 열고 로그 그룹 으로 이동합니다.

   c. 로그 그룹 를 검색합니다`<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`.

   d. 첫 번째 사용 가능한 로그 그룹을 검사하고 로그 내에서 오류를 찾습니다. 이러한 로그에는 S3 버킷을 탑재하는 데 필요한 사용자 지정 자격 증명에 대한 API Gateway에 대한 요청 및 응답에 대한 세부 정보가 포함됩니다.

온보딩 후 버킷의 IAM 역할 구성을 편집하는 방법

1. AWS DynamoDB 콘솔 에 로그인합니다.
2. 테이블을 선택합니다.

   a. 왼쪽 탐색 창에서 테이블을 선택합니다.

   b. 를 찾아 선택합니다`<stack-name>.cluster-settings`.

3. 테이블을 스캔합니다.

   a. 테이블 항목 탐색을 선택합니다.

   b. 스캔이 선택되어 있는지 확인합니다.

4. 필터 추가:

a. 필터를 선택하여 필터 항목 섹션을 엽니다.
b. 키를 일치하도록 필터를 설정합니다.

- 속성 : 키를 입력합니다.
- 조건 : 로 시작을 선택합니다.
- 값: `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` 교체 입력 `<filesystem_id>` 수정해야 하는 파일 시스템의 값을 포함합니다.

5. 스캔 실행:

   실행을 선택하여 필터로 스캔을 실행합니다.

6. 값을 확인합니다.

   항목이 있는 경우 값이 올바른 IAM 역할 로 올바르게 설정되었는지 확인합니다ARN.

   항목이 없는 경우:

   a. 항목 생성을 선택합니다.
   b. 항목 세부 정보를 입력합니다.

   - 키 속성에 를 입력합니다`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
   - 올바른 IAM 역할 을 추가합니다ARN.

   c. 저장을 선택하여 항목을 추가합니다.

7. VDI 인스턴스를 다시 시작합니다.

   인스턴스를 재부팅하여 잘못된 IAM 역할의 영향을 VDIs 받는 이 다시 탑재ARN되도록 합니다.

활성화 CloudTrail

CloudTrail 콘솔을 사용하여 계정 CloudTrail 에서 를 활성화하려면 사용 설명서의 CloudTrail 콘솔로 추적 생성에 제공된 지침을 따릅니다. CloudTrail 는 액세스한 IAM 역할을 기록하여 S3 버킷에 대한 액세스를 기록합니다. AWS CloudTrail 이는 프로젝트 또는 사용자에 연결된 인스턴스 ID에 다시 연결할 수 있습니다.

제품 사용

이 섹션에서는 가상 데스크톱을 사용하여 다른 사용자와 협업하는 방법에 대한 지침을 사용자에게 제공합니다.

주제

SSH 액세스

SSH 를 사용하여 Bastion 호스트에 액세스하려면:

1. 메뉴에서 SSH 액세스를 RES 선택합니다.
2. 화면에 표시되는 지침에 따라 SSH 또는 PuTTY를 사용하여 액세스합니다.

가상 데스크톱

가상 데스크톱 인터페이스(VDI) 모듈을 사용하면 사용자가 에서 Windows 또는 Linux 가상 데스크톱을 생성하고 관리할 수 있습니다 AWS. 사용자는 선호하는 도구와 애플리케이션이 사전 설치 및 구성된 상태에서 Amazon EC2 인스턴스를 시작할 수 있습니다.

지원되는 운영 체제

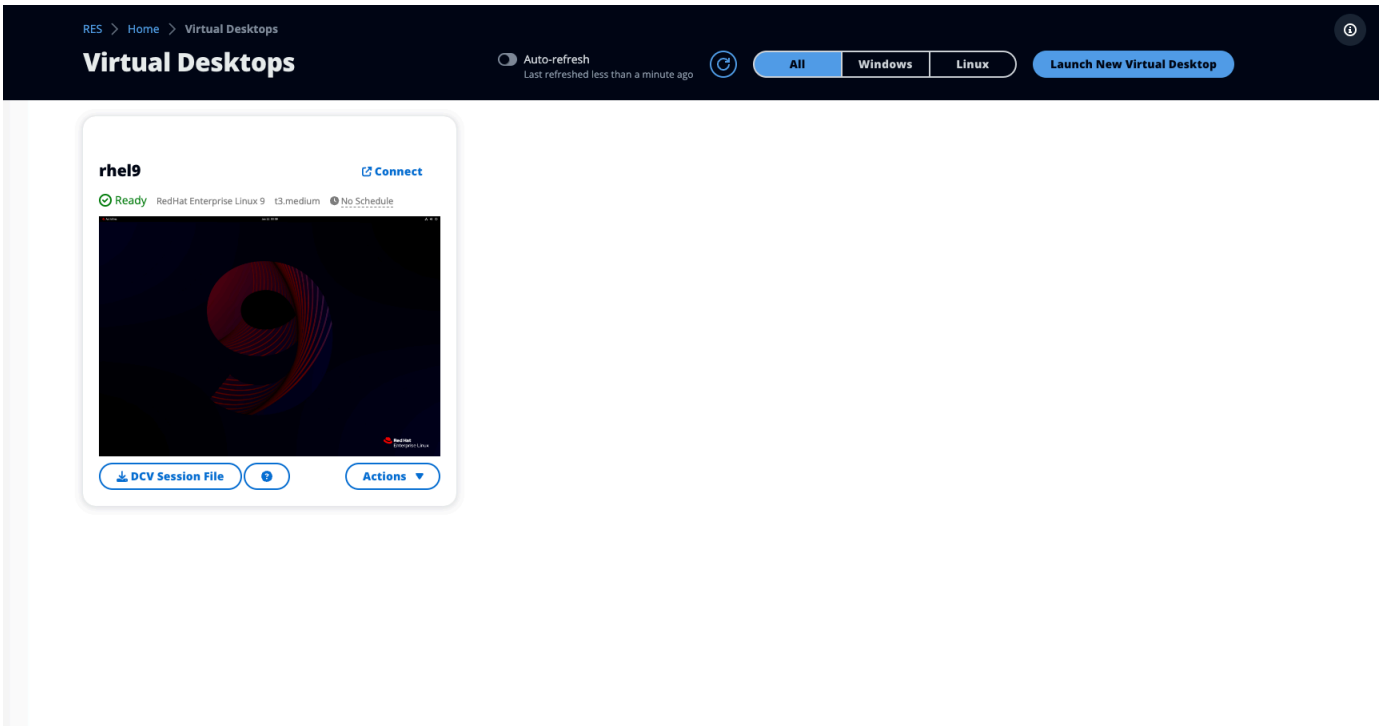
RES 는 현재 다음 운영 체제를 사용하여 가상 데스크톱 시작을 지원합니다.

- Amazon Linux 2(x86 및 ARM64)
- Ubuntu 22.04.03(x86)
- RHEL 8(x86) 및 9(x86)
- Windows 2019, 2022(x86)

주제

새 데스크톱 시작

1. 메뉴에서 내 Virtual Desktops를 선택합니다.
2. 새 Virtual Desktop 시작을 선택합니다.



3. 새 데스크톱의 세부 정보를 입력합니다.
4. 제출을 선택합니다.

데스크톱 정보가 포함된 새 카드가 즉시 표시되며 10~15분 이내에 데스크톱을 사용할 수 있습니다. 시작 시간은 선택한 이미지에 따라 달라집니다. RES 는 GPU 인스턴스를 감지하고 관련 드라이버를 설치합니다.

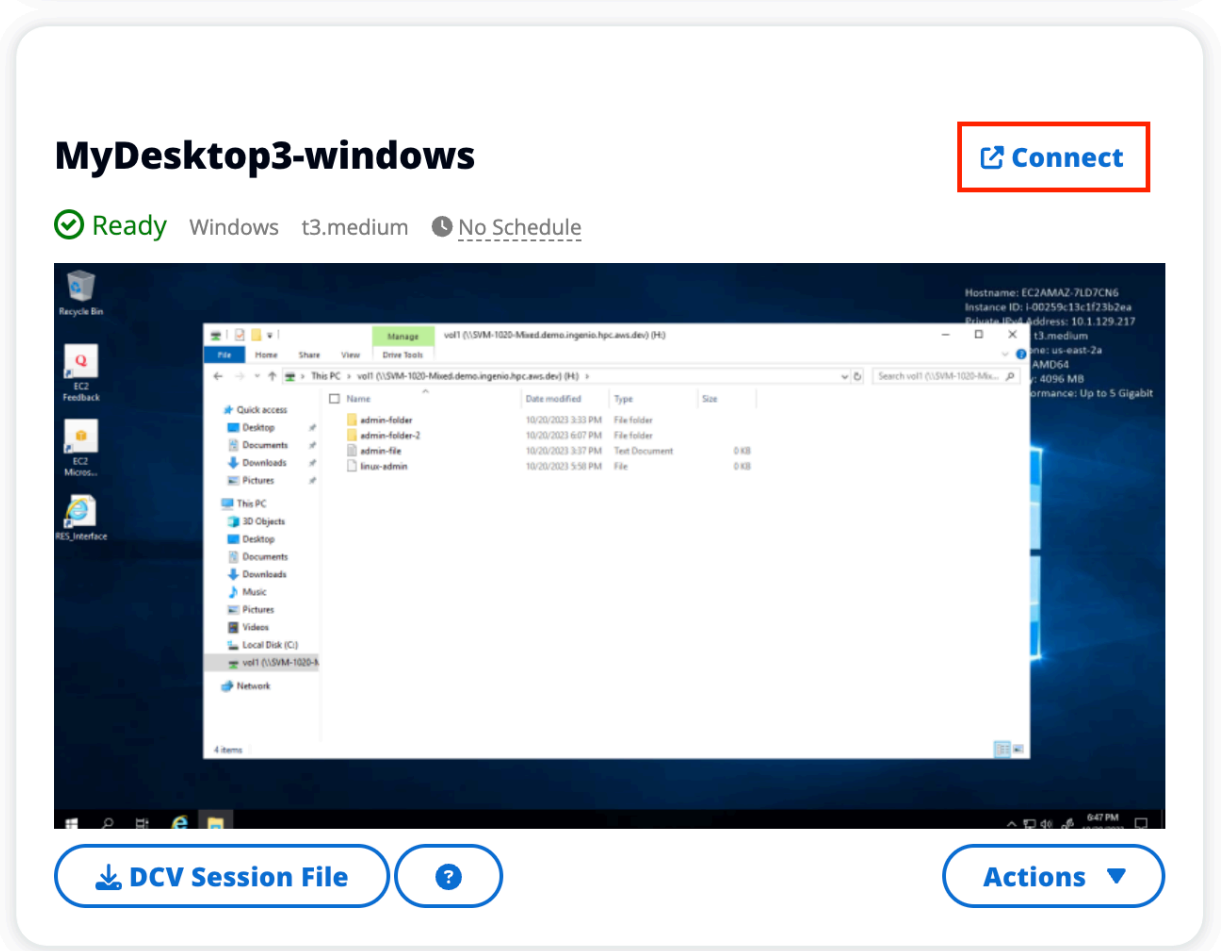
데스크톱 액세스

가상 데스크톱에 액세스하려면 데스크톱의 카드를 선택하고 웹 또는 DCV 클라이언트를 사용하여 연결합니다.

Web connection

웹 브라우저를 통해 데스크톱에 액세스하는 것이 가장 쉬운 연결 방법입니다.

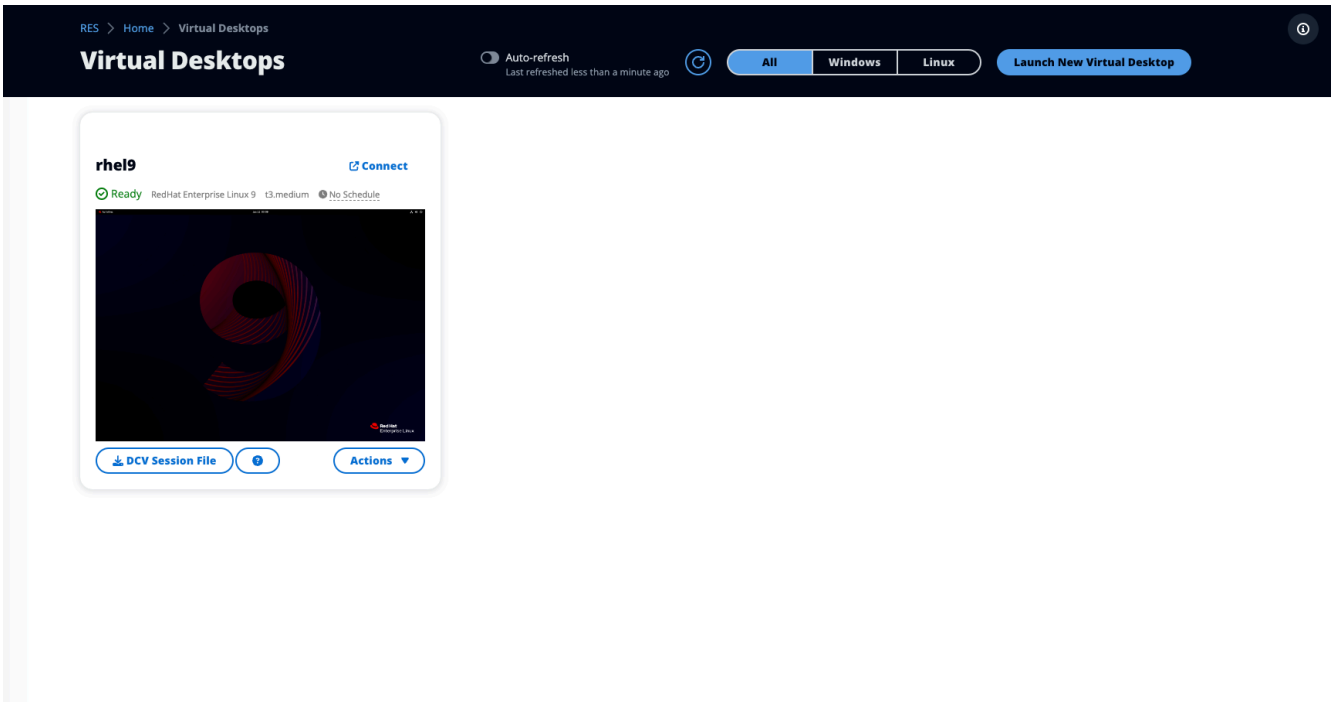
- 연결을 선택하거나 썸네일을 선택하여 브라우저를 통해 데스크톱에 직접 액세스합니다.



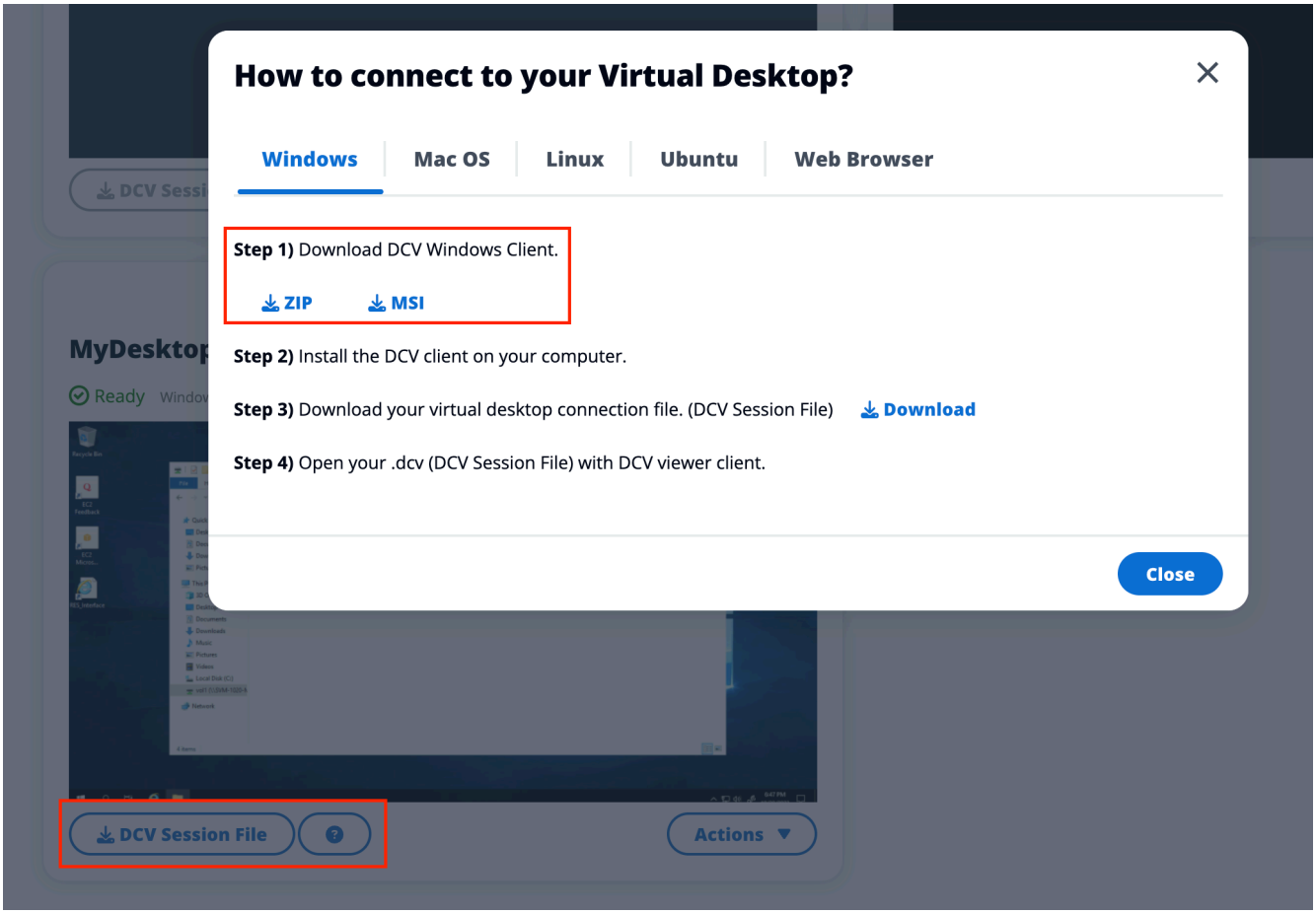
DCV connection

DCV 클라이언트를 통해 데스크톱에 액세스하면 최상의 성능을 얻을 수 있습니다. 를 통해 에 액세스하려면DCV:

1. DCV 세션 파일을 선택하여 `.dcv` 파일을 다운로드합니다. 시스템에 DCV 클라이언트를 설치해야 합니다.



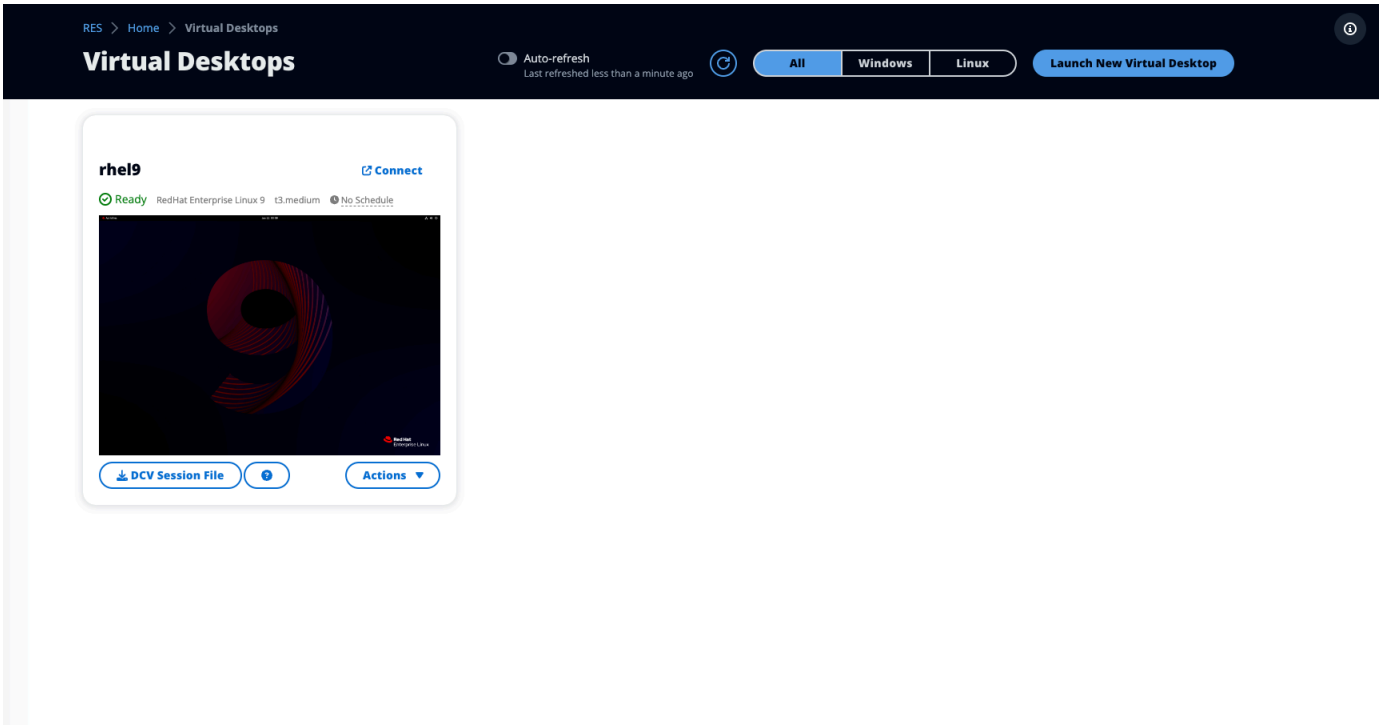
2. 설치 지침에서 ? 아이콘을 선택합니다.



데스크톱 상태 제어

데스크톱 상태를 제어하려면:

1. 작업을 선택합니다.



2. Virtual Desktop 상태 를 선택합니다. 다음 네 가지 상태에서 선택할 수 있습니다.

   - 중지

     중지된 세션은 데이터 손실이 발생하지 않으며 언제든지 중지된 세션을 다시 시작할 수 있습니다.

   - 재부팅

     현재 세션을 재부팅합니다.

   - 종료

     세션을 영구적으로 종료합니다. 임시 스토리지를 사용하는 경우 세션을 종료하면 데이터가 손실될 수 있습니다. 종료하기 전에 RES 파일 시스템에 데이터를 백업해야 합니다.

   - 최대 절전 모드

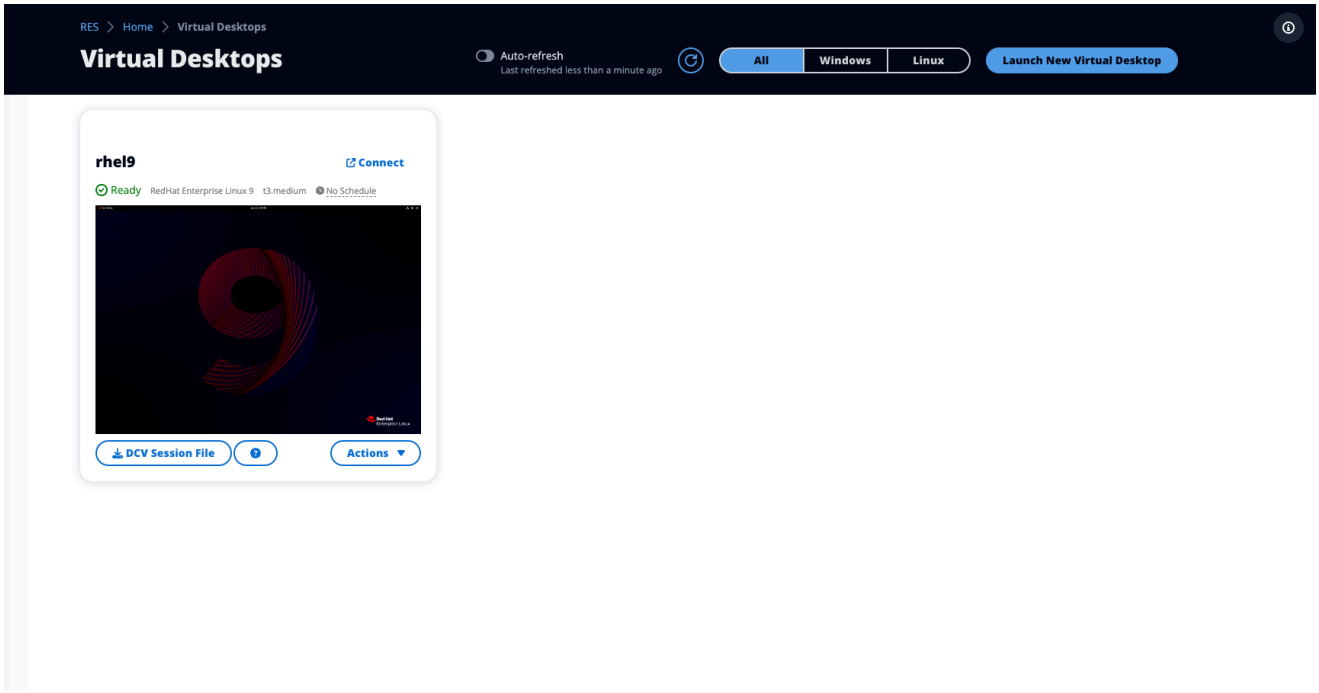
     데스크톱 상태가 메모리에 저장됩니다. 데스크톱을 다시 시작하면 애플리케이션이 다시 시작되지만 원격 연결이 끊어질 수 있습니다. 모든 인스턴스가 최대 절전 모드를 지원하는 것은 아니며, 옵션은 인스턴스 생성 중에 활성화된 경우에만 사용할 수 있습니다. 인스턴스가 이 상태를 지원하는지 확인하려면 최대 절전 모드 사전 조건 을 참조하세요.

가상 데스크톱 수정

가상 데스크톱의 하드웨어를 업데이트하거나 세션 이름을 변경할 수 있습니다.

1. 인스턴스 크기를 변경하려면 먼저 세션을 중지해야 합니다.

   a. 작업을 선택합니다.



   b. Virtual Desktop 상태 를 선택합니다.

   c. 중지를 선택합니다.

> **Note**
>
> 최대 절전 모드 세션의 데스크톱 크기는 업데이트할 수 없습니다.

2. 데스크톱이 중지되었음을 확인한 후 작업을 선택한 다음 세션 업데이트를 선택합니다.
3. 세션 이름을 변경하거나 원하는 데스크톱 크기를 선택합니다.
4. 제출을 선택합니다.
5. 인스턴스가 업데이트되면 데스크톱을 다시 시작합니다.

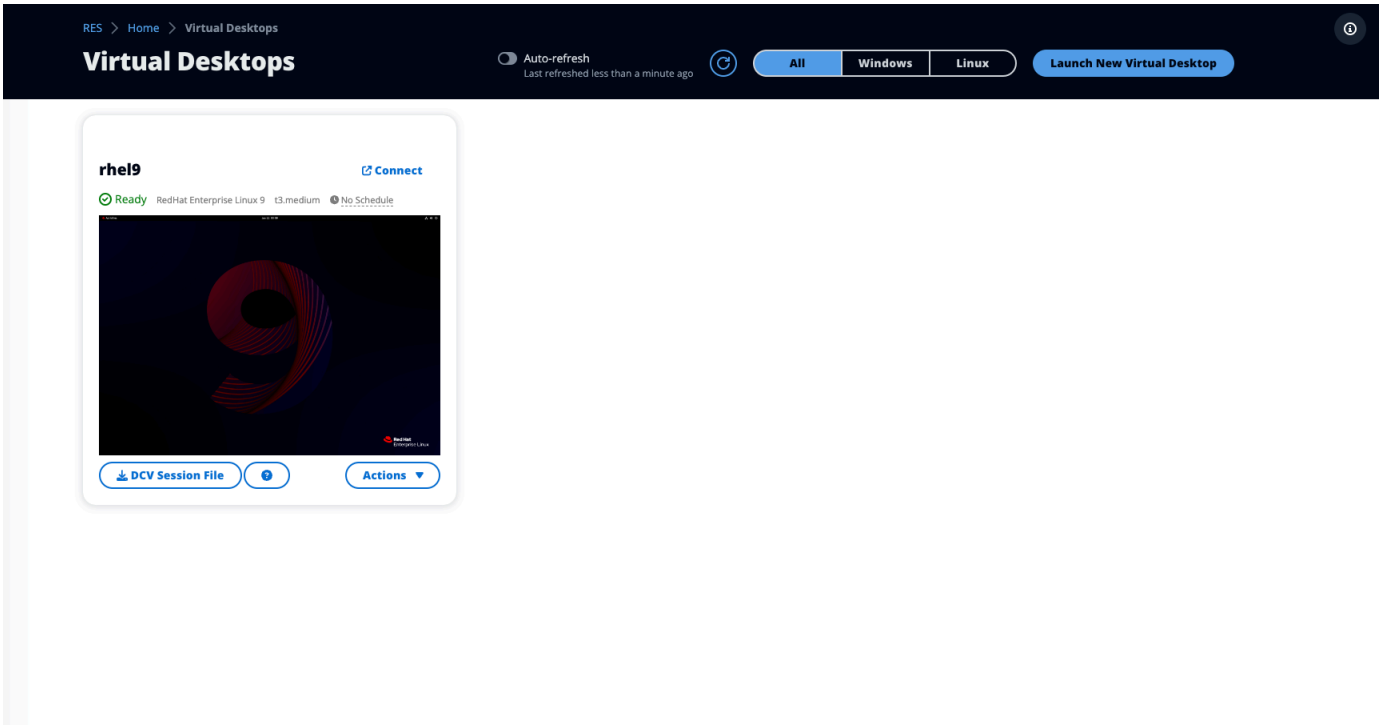
   a. 작업을 선택합니다.

   b. Virtual Desktop 상태 를 선택합니다.

c. 시작을 선택합니다.

세션 정보 검색

1. 작업을 선택합니다.

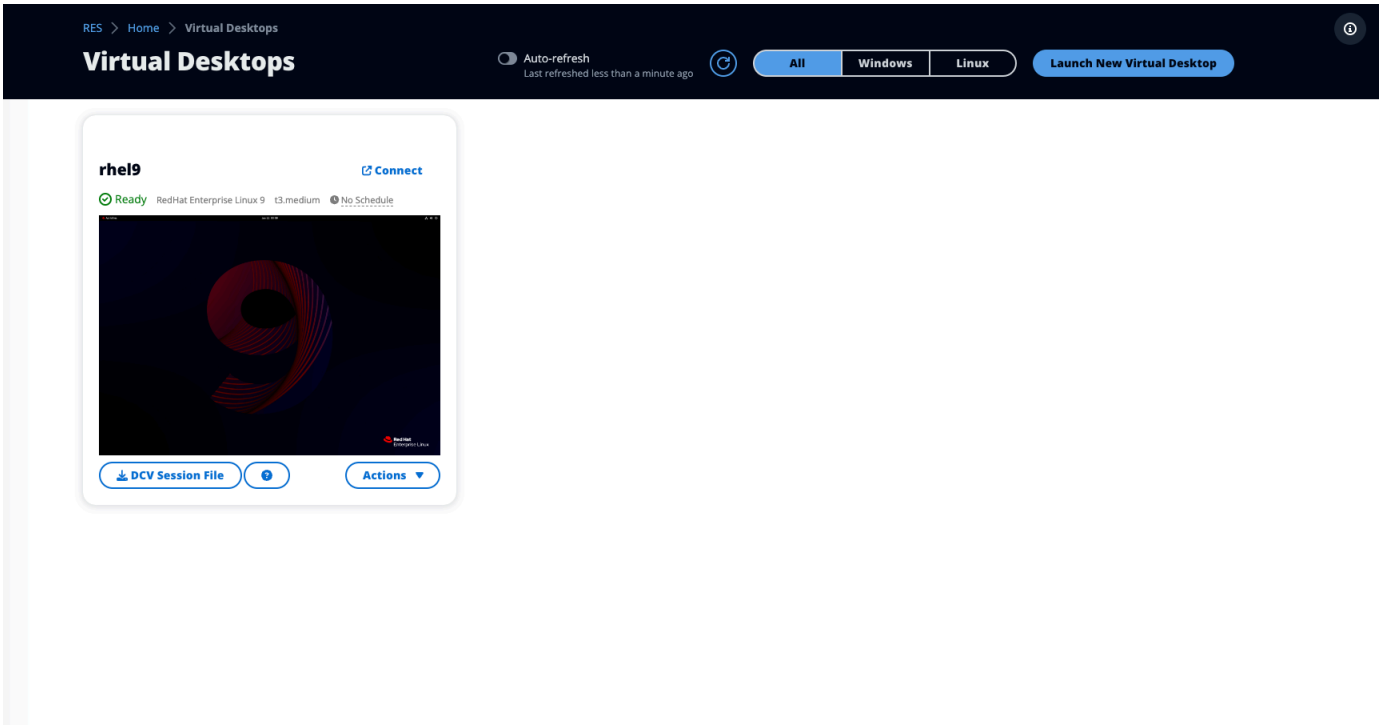


2. 정보 표시를 선택합니다.

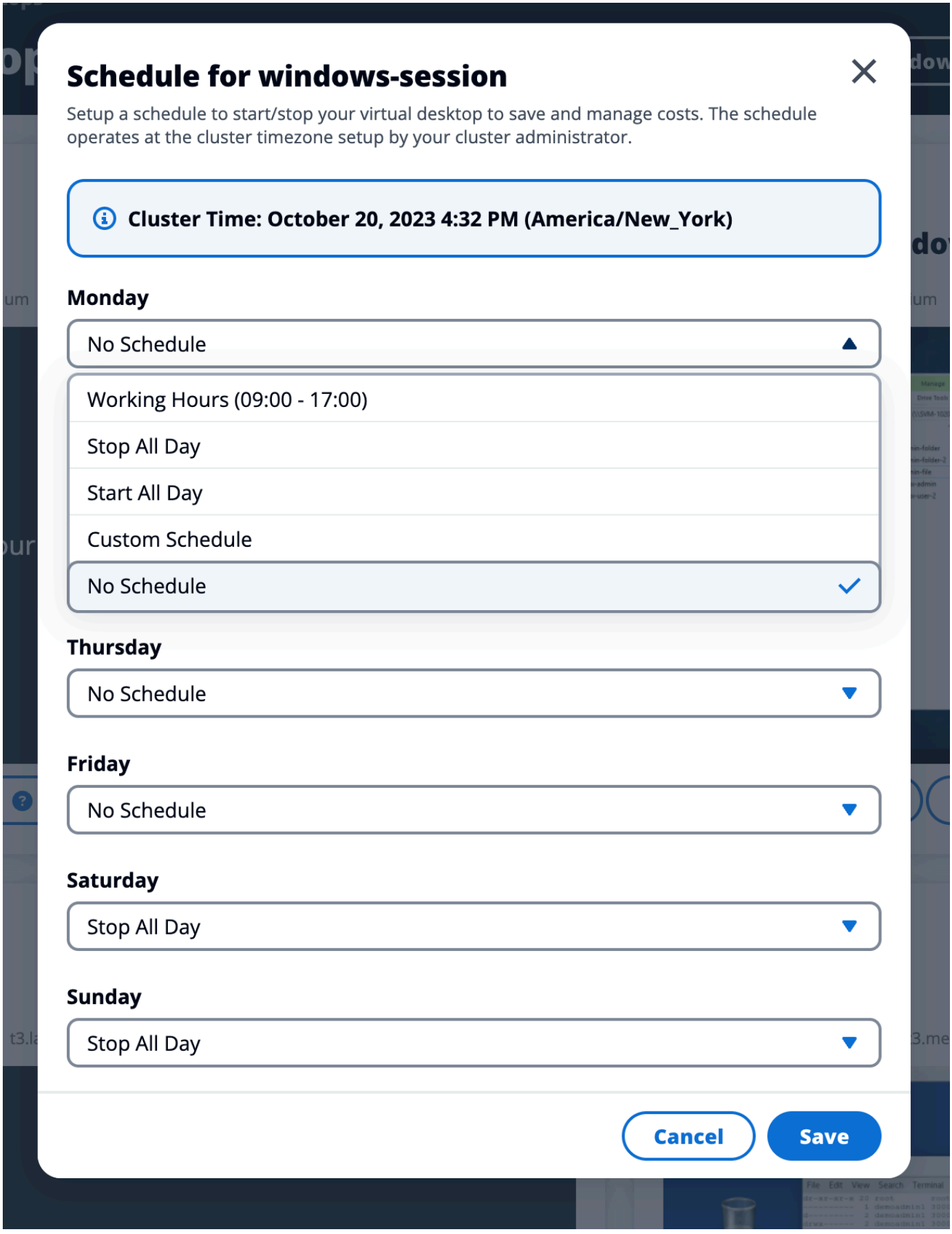
가상 데스크톱 예약

기본적으로 가상 데스크톱에는 일정이 없으며 세션을 중지하거나 종료할 때까지 활성 상태로 유지됩니다. 또한 실수로 중지되지 않도록 유휴 상태인 경우에도 데스크톱이 중지됩니다. 유휴 상태는 최소 15분 동안 활성 연결 및 CPU 사용량이 15% 미만인 경우 결정됩니다. 데스크톱을 자동으로 시작하고 중지하도록 일정을 구성할 수 있습니다.

1. 작업을 선택합니다.



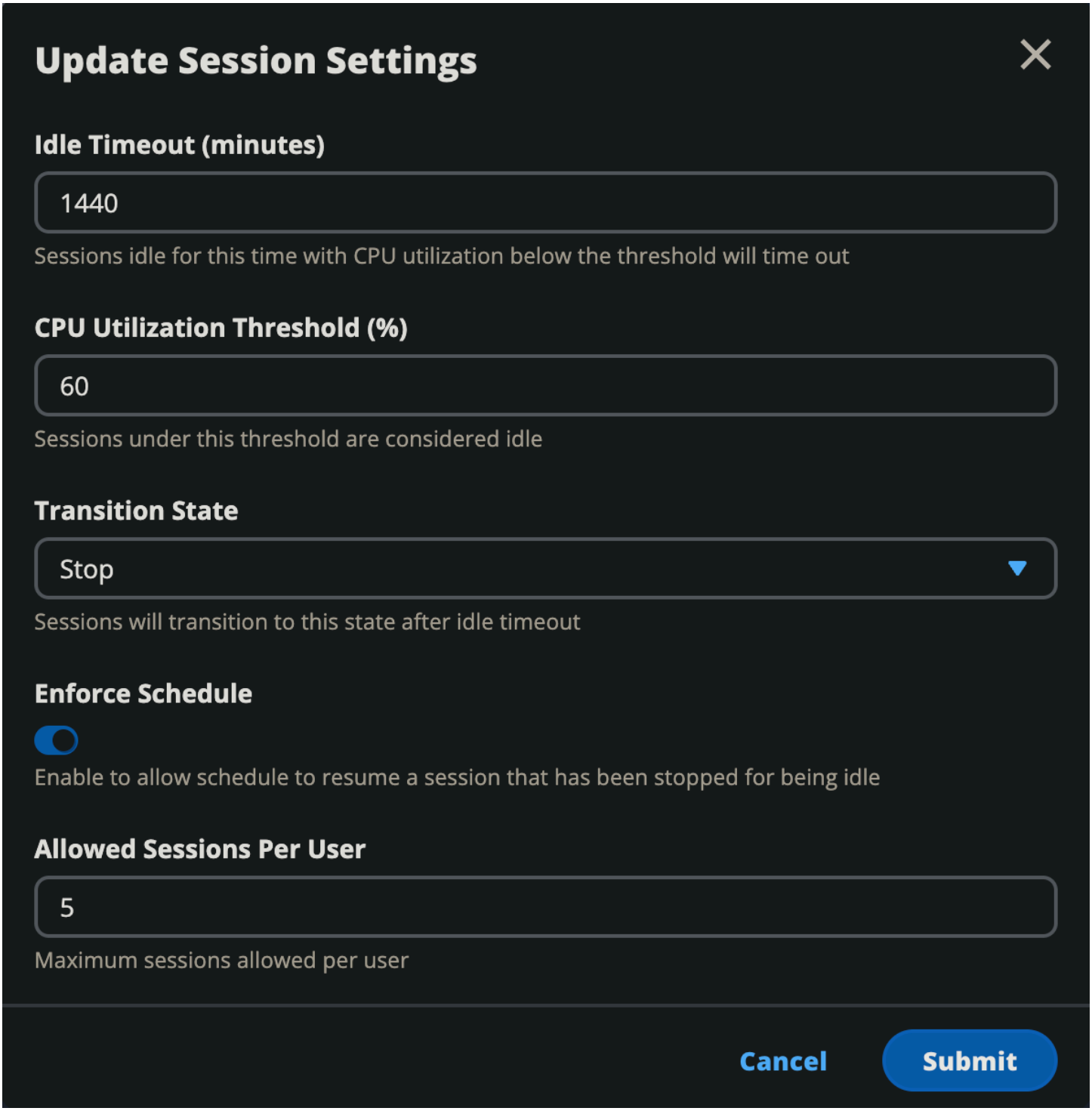
2. 일정을 선택합니다.
3. 매일 일정을 설정합니다.
4. 저장(Save)을 선택합니다.


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

가상 데스크톱 인터페이스 자동 중지

관리자는 유휴가 중지되거나 종료되도록 설정을 구성할 VDIs 수 있습니다. 구성 가능한 설정은 4가지 입니다.

1. 유휴 제한 시간: 이 시간 동안 유휴 상태이고 CPU 사용률이 임계값 미만인 세션은 제한 시간이 초과 됩니다.
2. CPU 사용률 임계값: 상호 작용이 없고 이 임계값 미만인 세션은 유휴 상태로 간주됩니다. 이 값을 0 으로 설정하면 세션이 유휴 상태로 간주되지 않습니다.
3. 전환 상태: 유휴 시간 초과 후 세션이 이 상태로 전환됩니다(중지 또는 종료됨).
4. 일정 적용: 이 옵션을 선택하면 유휴 상태로 인해 중지된 세션을 일일 일정에 따라 재개할 수 있습니다.

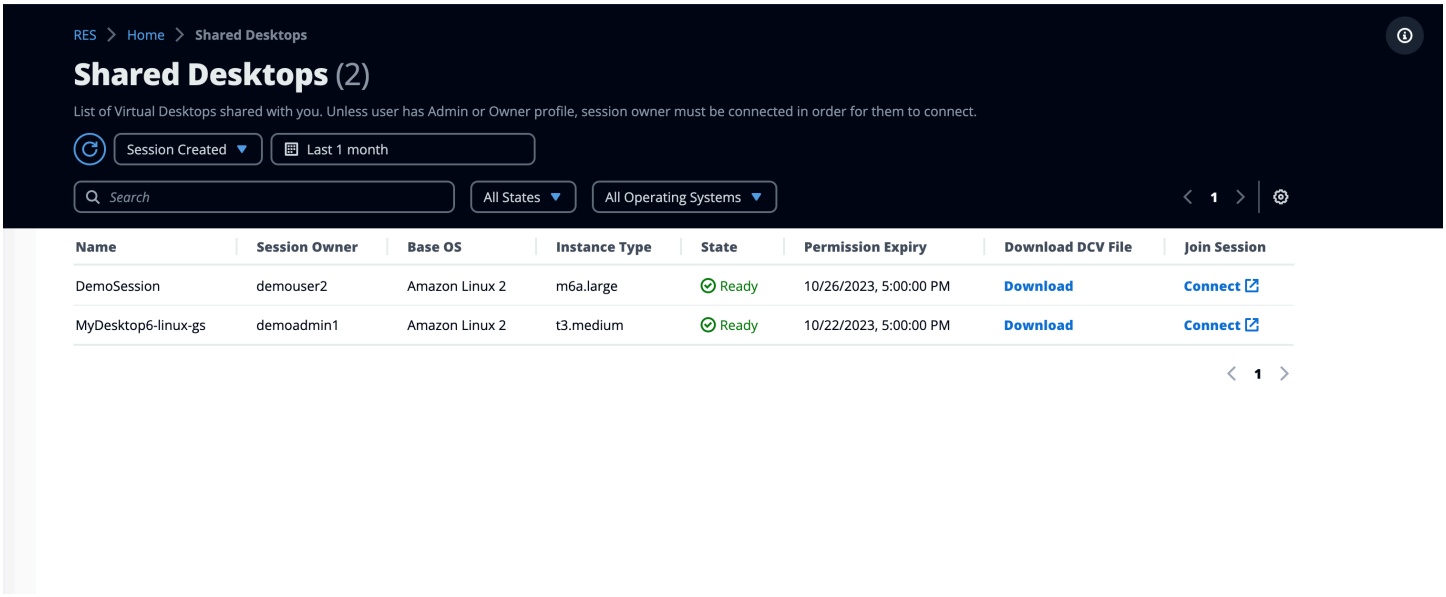


이러한 설정은 서버 탭 아래의 데스크톱 설정 페이지에 있습니다. 요구 사항에 따라 설정을 업데이트한 후 제출을 클릭하여 설정을 저장합니다. 새 세션은 업데이트된 설정을 사용하지만 기존 세션은 시작 시 있던 설정을 계속 사용합니다.

시간이 초과되면 세션이 종료되거나 구성에 따라 STOPPED_IDLE 상태로 전환됩니다. 사용자는 UI에서 STOPPED_IDLE 세션을 시작할 수 있습니다.

공유 데스크톱

공유 데스크톱에서는 공유된 데스크톱을 볼 수 있습니다. 데스크톱에 연결하려면 관리자 또는 소유자가 아닌 한 세션 소유자도 연결해야 합니다.



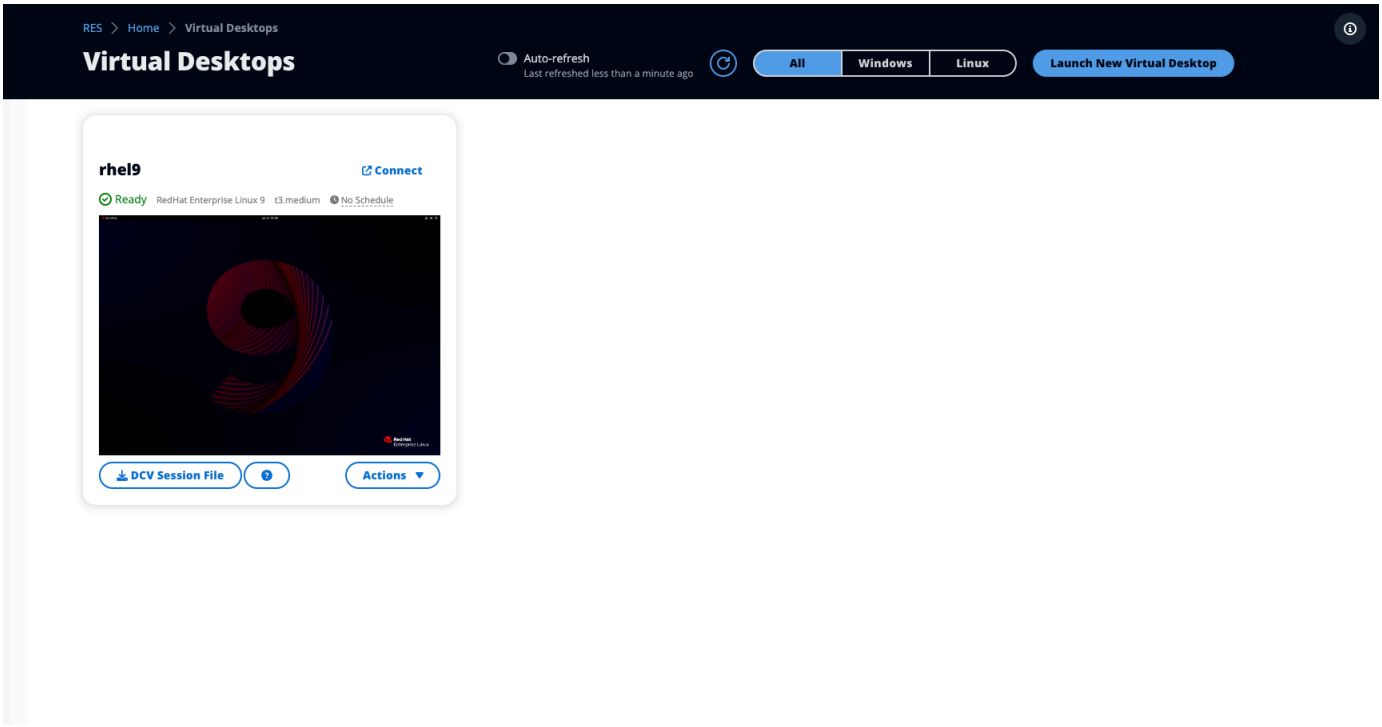
세션을 공유하는 동안 공동 작업자에 대한 권한을 구성할 수 있습니다. 예를 들어 협업 중인 팀원에게 읽기 전용 액세스 권한을 부여할 수 있습니다.

주제

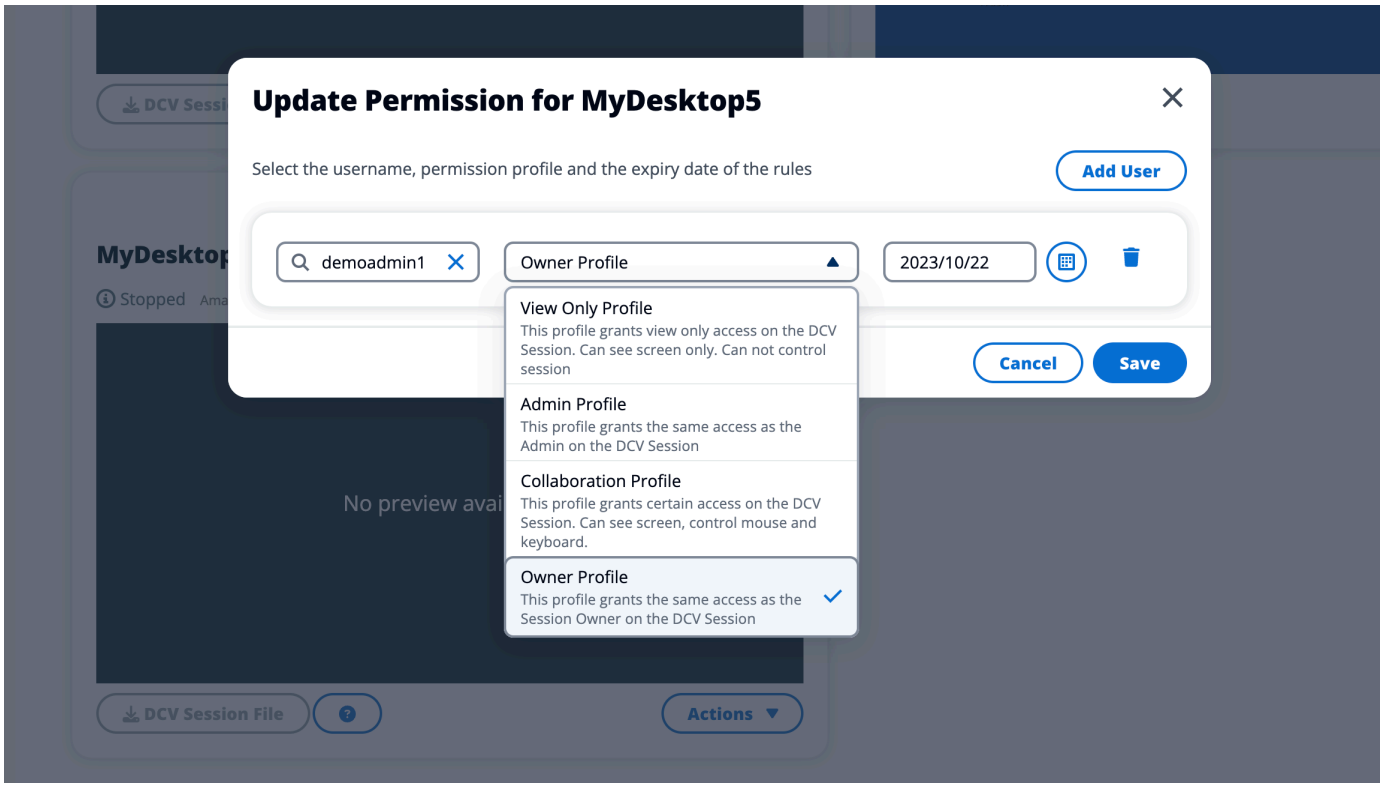
- 데스크톱 공유
- 공유 데스크톱 액세스

데스크톱 공유

1. 데스크톱 세션에서 작업 을 선택합니다.



2. 세션 권한 을 선택합니다.
3. 사용자 및 권한 수준을 선택합니다. 만료 시간을 설정할 수도 있습니다.
4. 저장(Save)을 선택합니다.



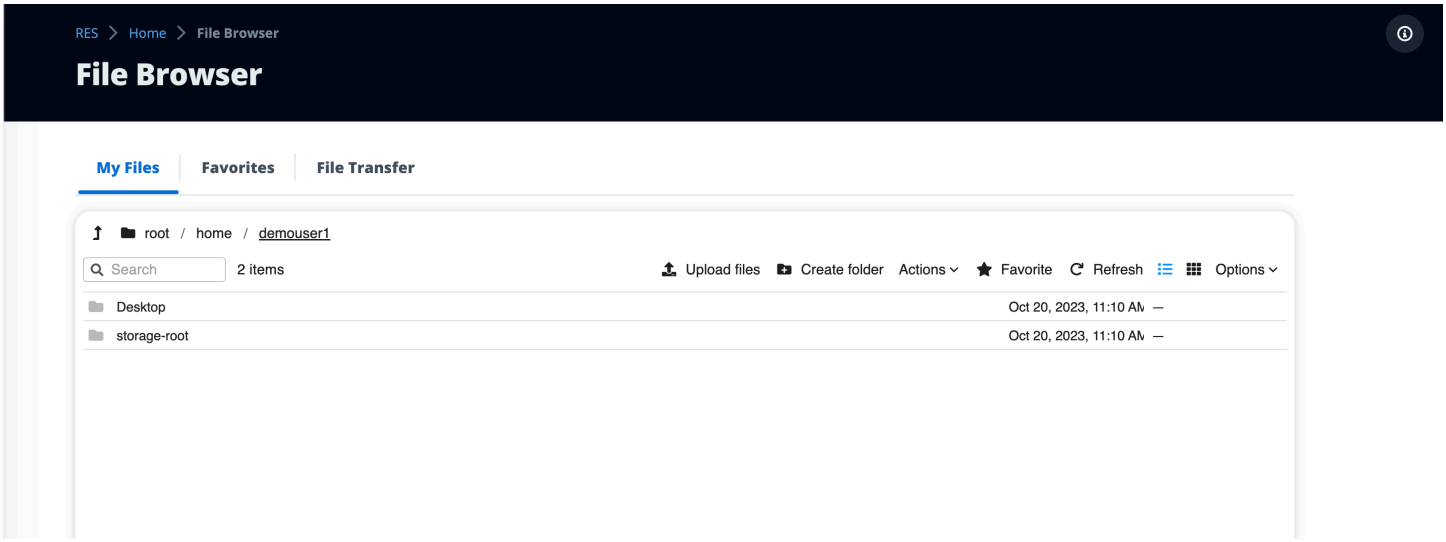
권한에 대한 자세한 내용은 섹션을 참조하세요the section called “권한 정책”.

공유 데스크톱 액세스

공유 데스크톱에서 공유된 데스크톱을 보고 인스턴스에 연결할 수 있습니다. 웹 브라우저 또는 를 사용하여 가입할 수 있습니다DCV. 연결하려면 의 지침을 따르세요데스크톱 액세스.

파일 브라우저

파일 브라우저를 사용하면 웹 포털을 통해 파일 시스템에 액세스할 수 있습니다. 기본 파일 시스템에서 액세스할 수 있는 권한이 있는 사용 가능한 모든 파일을 관리할 수 있습니다. 백엔드 스토리지(Amazon EFS)는 모든 Linux 노드에서 사용할 수 있습니다. Linux 및 Windows 노드의 경우 FSx 용 ONTAP 를 사용할 수 있습니다. 가상 데스크톱에서 파일을 업데이트하는 것은 터미널 또는 웹 기반 파일 브라우저를 통해 파일을 업데이트하는 것과 동일합니다.

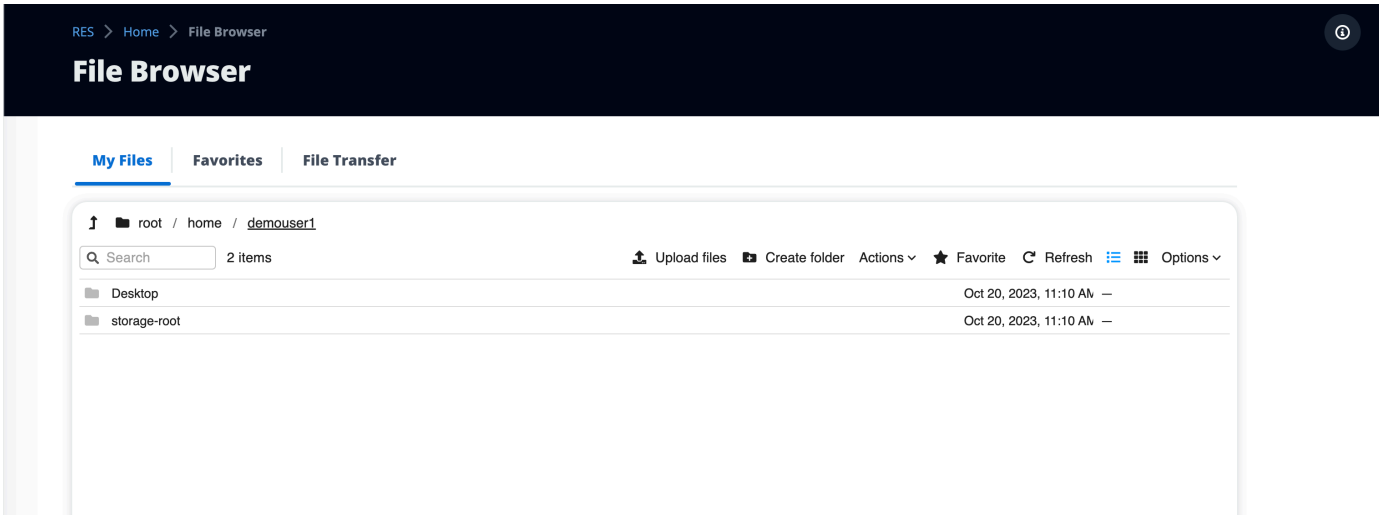


주제

- 업로드 파일(들)
- 파일(들) 삭제
- 즐겨찾기 관리
- 파일 편집
- 파일 전송

업로드 파일(들)

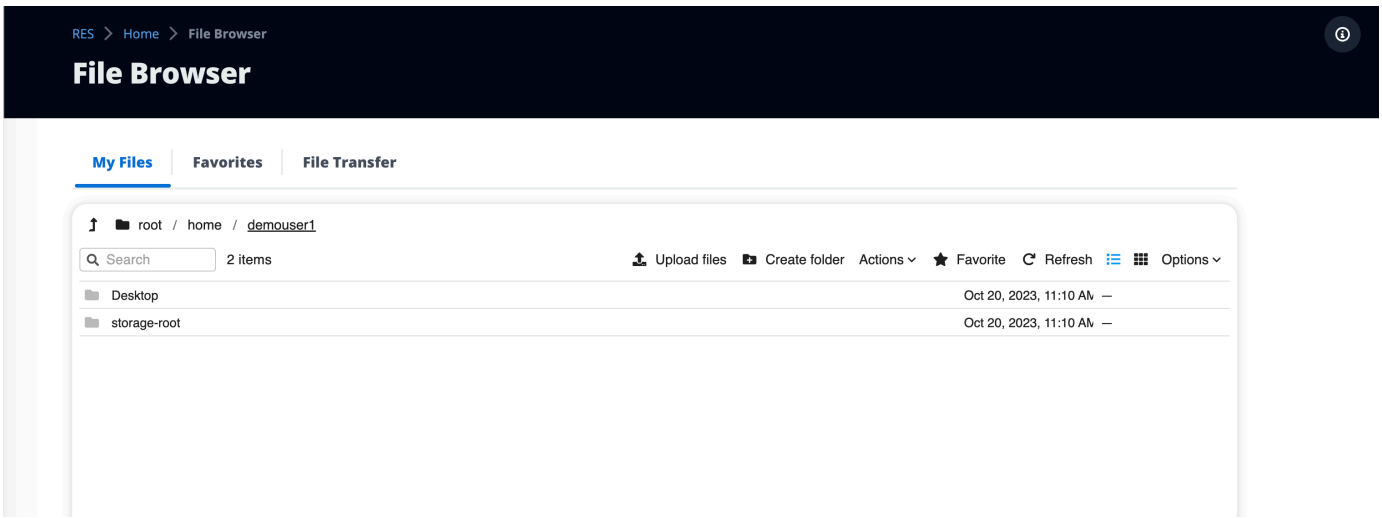
1. 파일 업로드를 선택합니다.



2. 파일을 삭제하거나 업로드할 파일을 찾습니다.
3. 파일 업로드(n)를 선택합니다.

파일(들) 삭제

1. 삭제할 파일(들)을 선택합니다.



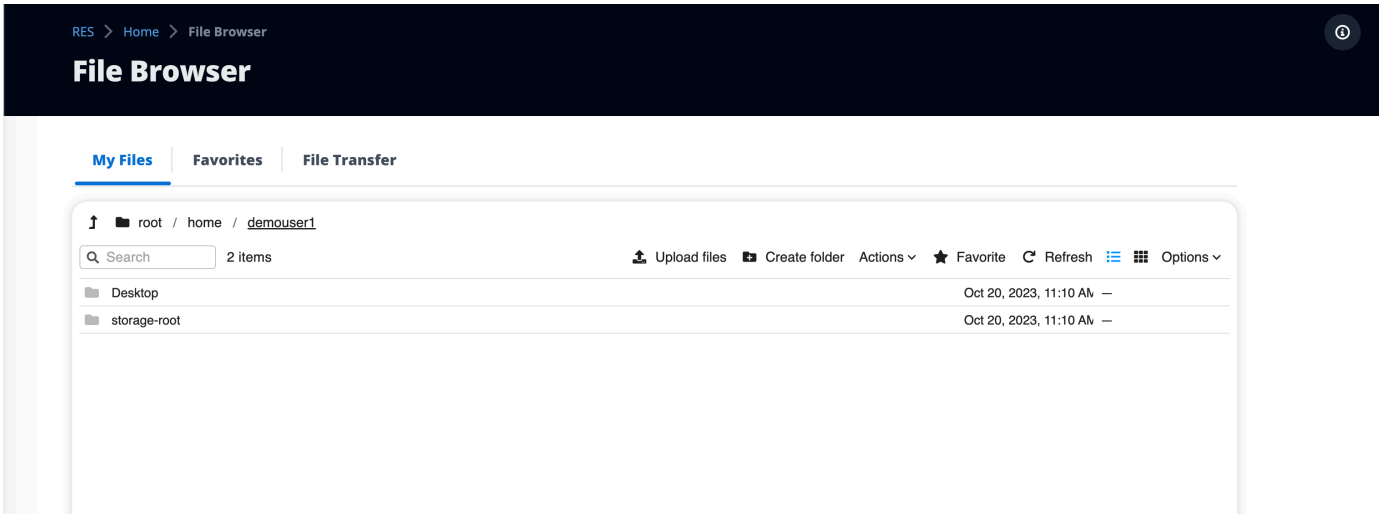
2. 작업을 선택합니다.
3. 파일 삭제 를 선택합니다.

또는 파일 또는 폴더를 마우스 오른쪽 버튼으로 클릭하고 파일 삭제를 선택할 수도 있습니다.

즐겨찾기 관리

중요한 파일과 폴더를 고정하려면 즐겨찾기에 추가할 수 있습니다.

1. 파일 또는 폴더를 선택합니다.



2. 즐겨찾기 를 선택합니다.

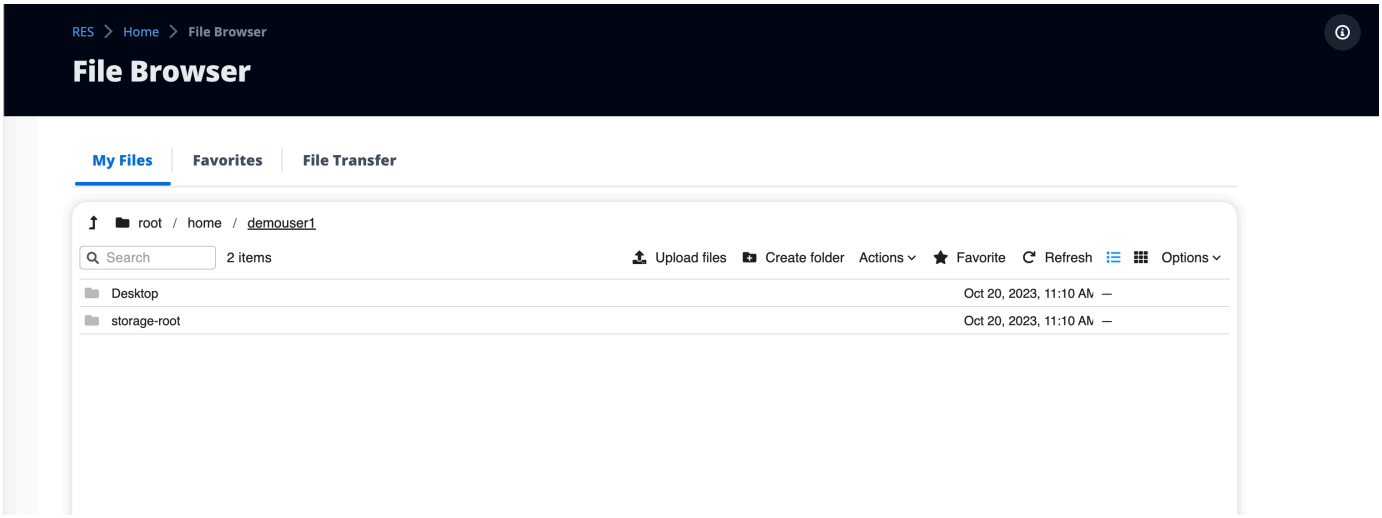
또는 파일 또는 폴더를 마우스 오른쪽 버튼으로 클릭하고 즐겨찾기 를 선택할 수 있습니다.

> **Note**
>
> 즐겨찾기는 로컬 브라우저에 저장됩니다. 브라우저를 변경하거나 캐시를 지우는 경우 즐겨찾기를 다시 고정해야 합니다.

파일 편집

웹 포털 내에서 텍스트 기반 파일의 콘텐츠를 편집할 수 있습니다.

1. 업데이트할 파일을 선택합니다. 파일 콘텐츠와 함께 모달이 열립니다.

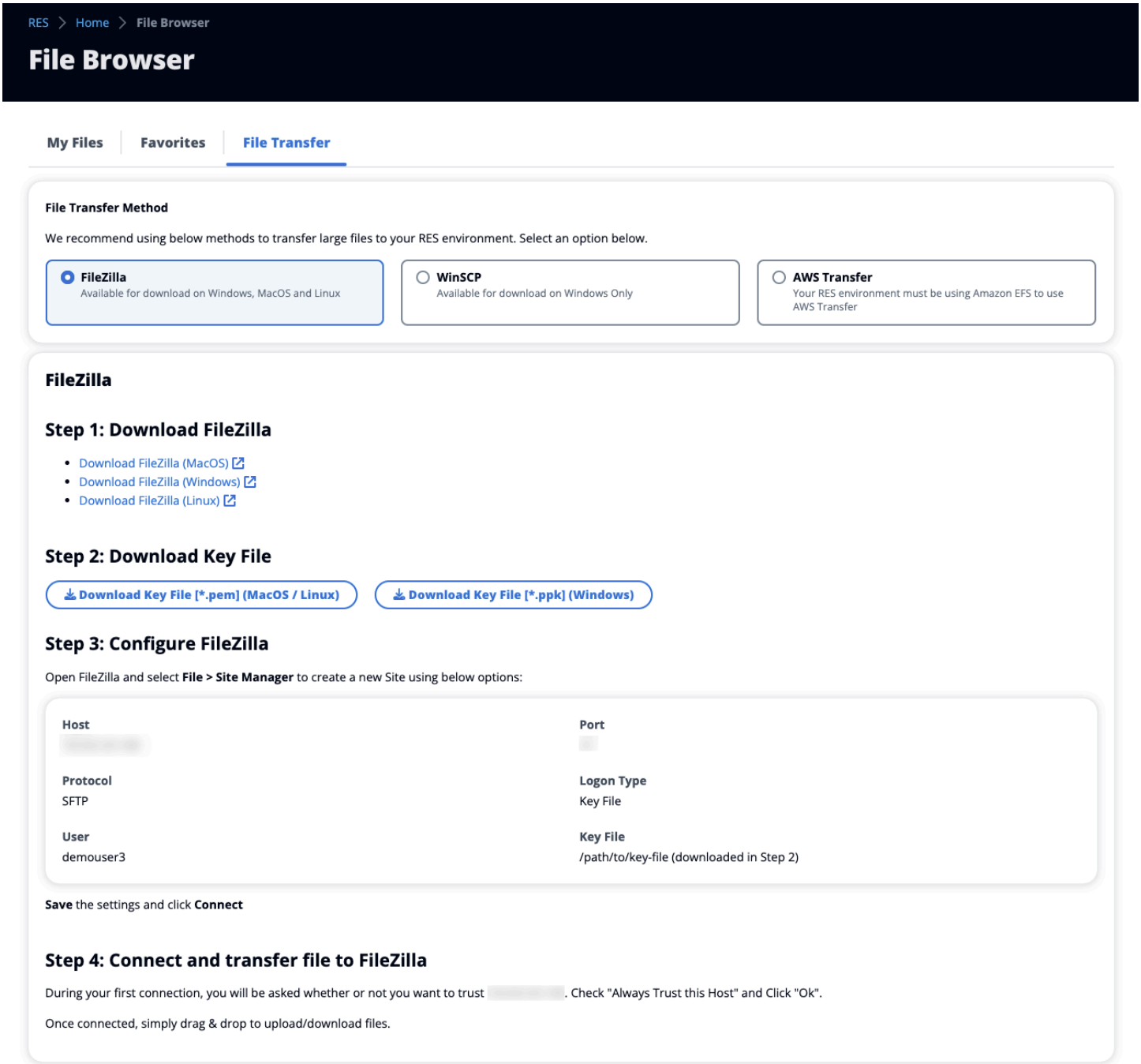


2. 업데이트하고 저장을 선택합니다.

파일 전송

파일 전송을 사용하여 외부 파일 전송 애플리케이션을 사용하여 파일을 전송합니다. 다음 애플리케이션 중에서 선택하고 화면 지침에 따라 파일을 전송할 수 있습니다.

- 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
Port
Protocol
SFTP
Logon Type
Key File
User
demouser3
Key File
/path/to/key-file (downloaded in Step 2)
Save the settings and click Connect
Step 4: Connect and transfer file to FileZilla
During your first connection, you will be asked whether or not you want to trust . Check "Always Trust this Host" and Click "Ok".
Once connected, simply drag & drop to upload/download files.

문제 해결

이 섹션에는 시스템을 모니터링하는 방법과 발생할 수 있는 특정 문제를 해결하는 방법에 대한 정보가 포함되어 있습니다.

주제

세부 내용:

- (2024.04.02 이하) SAMAccountName 속성에 대문자 또는 특수 문자가 포함된 AD 사용자를 동기화하지 못함
- (2024.04.02 이하) Bastion 호스트에 액세스하기 위한 프라이빗 키가 유효하지 않습니다.
- (2024.06 이하) AD 동기화 RES 중에 그룹 멤버가 에 동기화되지 않음
- (2024.06 이하) CVE-2024-6387, R egreSSHion, RHEL9 및 Ubuntu의 보안 취약성 VDIs

일반 디버깅 및 모니터링

이 섹션에는 내에서 정보를 찾을 수 있는 위치에 대한 정보가 포함되어 있습니다RES.

- 유용한 로그 및 이벤트 정보 소스
  - Amazon EC2 인스턴스 환경의 로그 파일
  - CloudFormation 스택
  - 문제로 인한 시스템 실패로 Amazon EC2 Auto Scaling Group Activity에 반영됨
- 일반적인 Amazon EC2 콘솔 모양
  - 인프라 호스트
  - 인프라 호스트 및 가상 데스크톱
  - 종료된 상태의 호스트
  - 참조를 위한 유용한 Active Directory(AD) 관련 명령
- Windows DCV 디버깅
- Amazon DCV 버전 정보 찾기

유용한 로그 및 이벤트 정보 소스

문제 해결 및 모니터링 사용을 위해 참조할 수 있는 다양한 정보 소스가 보존되어 있습니다.

Amazon EC2 인스턴스 환경의 로그 파일

로그 파일은 에서 사용 중인 Amazon EC2 인스턴스에 있습니다RES. SSM Session Manager를 사용하여 이러한 파일을 검사하기 위해 인스턴스에 대한 세션을 열 수 있습니다.

클러스터 관리자 및 vdc 컨트롤러와 같은 인프라 인스턴스의 경우 애플리케이션 및 기타 로그는 다음 위치에서 찾을 수 있습니다.

- /opt/idea/app/logs/application.log

- /root/bootstrap/logs/
- /var/log/
- /var/log/ssd/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

Linux 가상 데스크톱에서 유용한 로그 파일은 다음과 같습니다.

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

Windows 가상 데스크톱 인스턴스의 로그는 에서 찾을 수 있습니다.

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

Windows에서 일부 애플리케이션 로깅은 다음에서 찾을 수 있습니다.

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

Windows의 NICE DCV 인증서 파일은 다음에서 찾을 수 있습니다.

- C:\Windows\System32\config\systemprofileAppData\\Local\NICE\dcv\

Amazon CloudWatch 로그 그룹

Amazon EC2 및 AWS Lambda 컴퓨팅 리소스는 Amazon CloudWatch Log Groups에 정보를 기록합니다. 로그 항목은 잠재적 문제를 해결할 때 유용한 정보를 제공하거나 일반 정보를 제공할 수 있습니다.

이러한 그룹의 이름은 다음과 같습니다.

- `/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

로그 그룹을 검사할 때 다음과 같은 대문자 및 소문자 문자열을 사용하여 필터링하는 것이 도움이 될 수 있습니다. 이렇게 하면 언급된 문자열이 포함된 메시지만 출력됩니다.

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

문제를 모니터링하는 또 다른 방법은 관심 데이터를 표시하는 위젯이 포함된 Amazon CloudWatch 대시보드를 생성하는 것입니다.

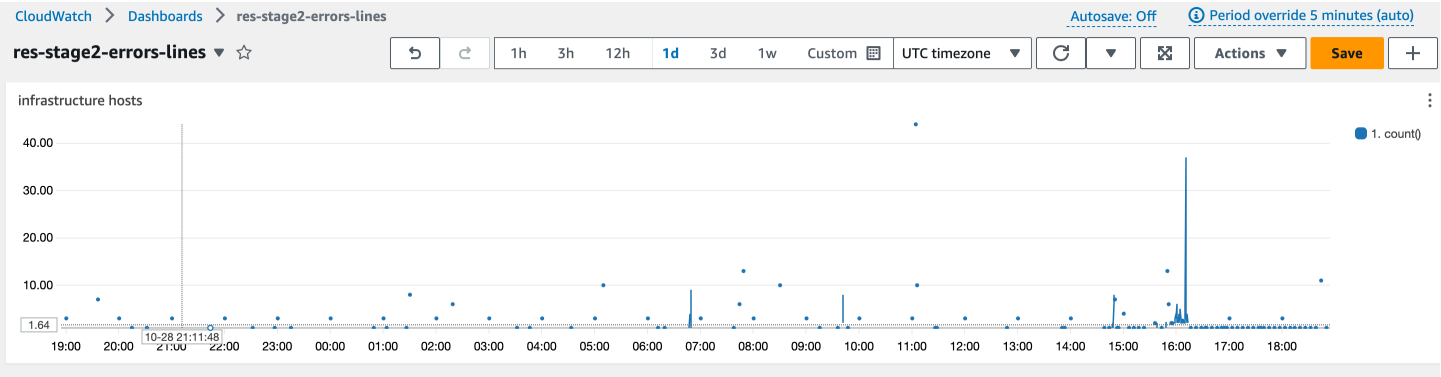
예를 들어 문자열 오류 발생을 계산ERROR하고 이를 선으로 그래프화하는 위젯을 생성합니다. 이 방법을 사용하면 패턴 변경이 발생했음을 나타내는 잠재적 문제 또는 추세의 발생을 더 쉽게 감지할 수 있습니다.

다음은 인프라 호스트의 예제입니다. 이를 사용하려면 쿼리 라인을 연결하고 <envname> 및 <region> 속성을 적절한 값으로 바꿉니다.

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

대시보드의 예는 다음과 같습니다.



CloudFormation 스택

환경 생성 중에 생성된 CloudFormation 스택에는 환경 구성과 관련된 리소스, 이벤트 및 출력 정보가 포함됩니다.

각 스택에 대해 이벤트, 리소스 및 출력 탭을 참조하여 스택에 대한 정보를 확인할 수 있습니다.

RES 스택:

- <envname>-bootstrap
- <envname>-클러스터
- <envname>-메트릭
- <envname>-디렉터리서비스
- <envname>-identity-provider
- <envname>-shared-storage
- <envname>-cluster-manager
- <envname>-vdc

- <envname>-bastion-host

데모 환경 스택(데모 환경을 배포하고 이러한 외부 리소스를 사용할 수 없는 경우 AWS 고성능 컴퓨팅 레시피를 사용하여 데모 환경을 위한 리소스를 생성할 수 있습니다.)

- <envname>
- <envname>-네트워킹
- <envname>-DirectoryService
- <envname>-스토리지
- <envname>-WindowsManagementHost

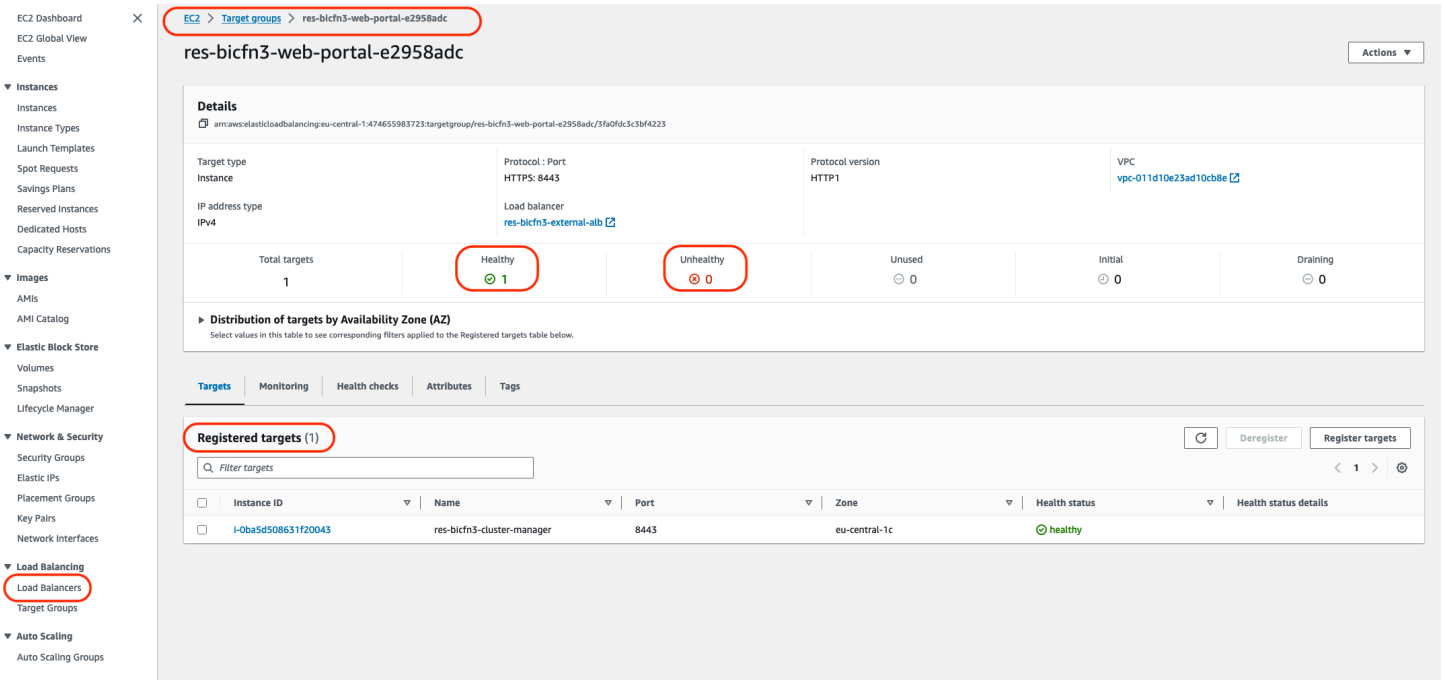
문제로 인한 시스템 실패로 Amazon EC2 Auto Scaling Group Activity에 반영됨

가 서버 오류를 RES UIs 나타내는 경우 원인은 애플리케이션 소프트웨어 또는 기타 문제일 수 있습니다.

각 인프라 Amazon EC2 인스턴스 Autoscaling 그룹(ASGs)에는 인스턴스의 조정 활동을 감지하는 데 유용할 수 있는 활동 탭이 포함되어 있습니다. UI 페이지에 오류가 있거나 액세스할 수 없는 경우 Amazon EC2 콘솔에서 종료된 인스턴스가 여러 개 있는지 확인하고 Auto Scaling Group Activity 탭에서 관련 를 확인하여 Amazon EC2 인스턴스가 순환 중인지 ASG 확인합니다.

그렇다면 인스턴스에 대한 관련 Amazon CloudWatch 로그 그룹을 사용하여 문제의 원인을 나타낼 수 있는 오류가 기록되고 있는지 확인합니다. SSM 세션 콘솔을 사용하여 해당 유형의 실행 중인 인스턴스에 대한 세션을 열고 인스턴스가 비정상으로 표시되고 에 의해 종료되기 전에 인스턴스의 로그 파일을 검사하여 원인을 확인할 수도 있습니다ASG.

이 문제가 발생하는 경우 ASG 콘솔에 다음과 유사한 활동이 표시될 수 있습니다.

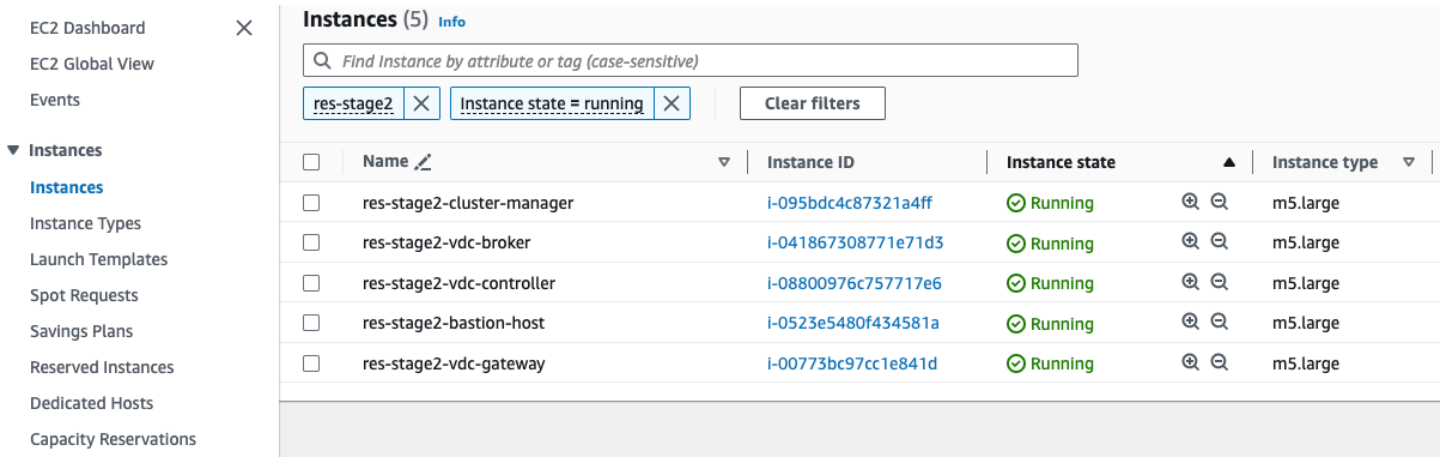


일반적인 Amazon EC2 콘솔 모양

이 섹션에는 다양한 상태에서 작동하는 시스템의 스크린샷이 포함되어 있습니다.

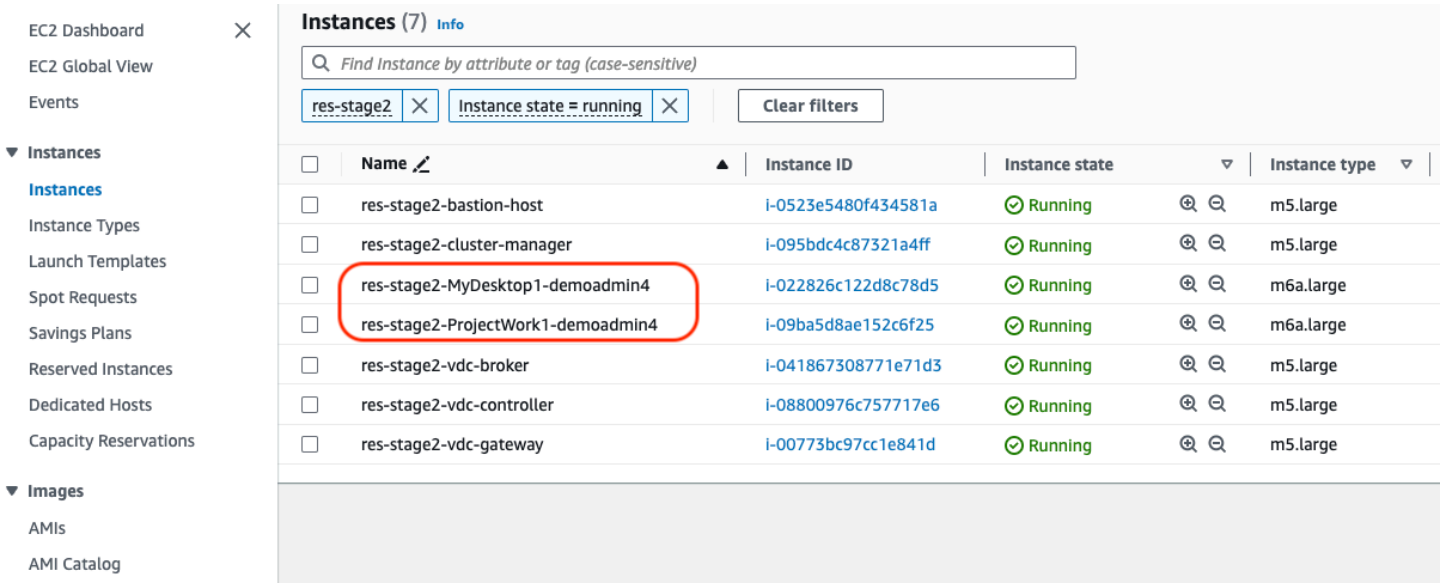
인프라 호스트

Amazon EC2 콘솔은 실행 중인 데스크톱이 없는 경우 일반적으로 다음과 비슷합니다. 표시된 인스턴스는 Amazon이 EC2 호스팅하는 RES 인프라입니다. 인스턴스 이름의 접두사는 RES 환경 이름입니다.



인프라 호스트 및 가상 데스크톱

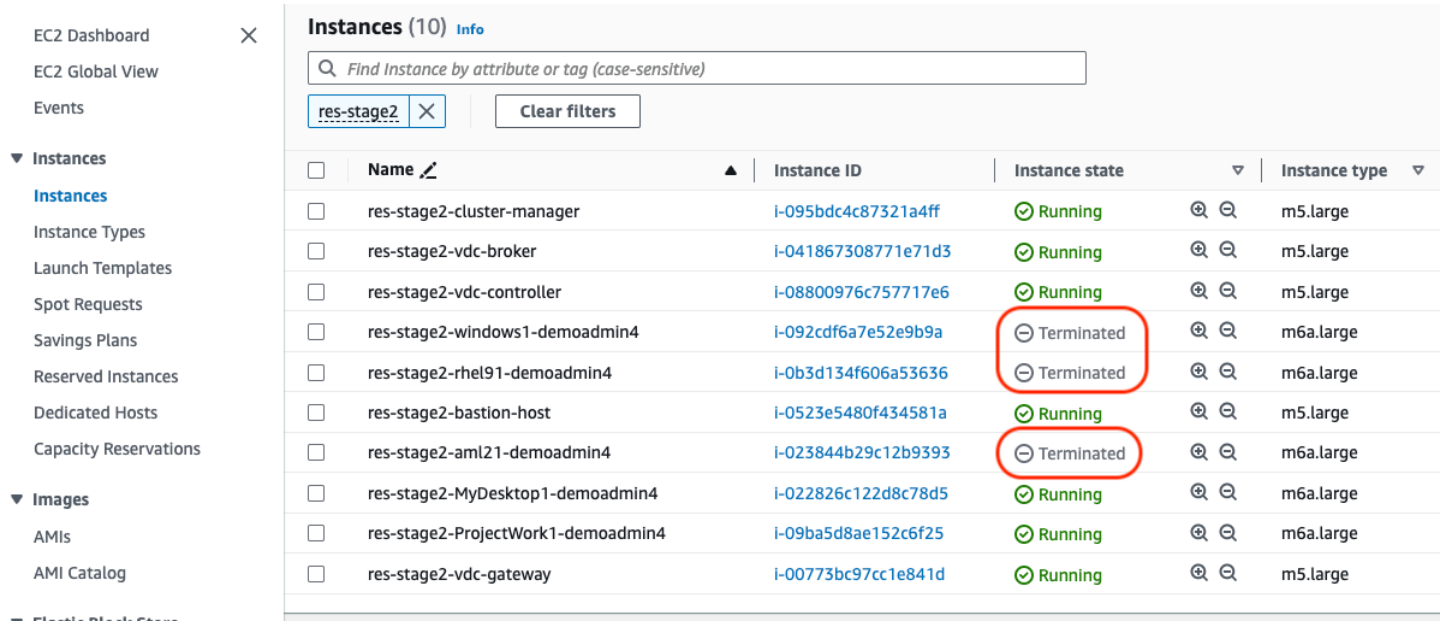
Amazon EC2 콘솔에서 가상 데스크톱이 실행 중일 때 다음과 비슷하게 나타납니다. 이 경우 가상 데스크톱은 빨간색으로 표시됩니다. 인스턴스 이름의 접미사는 데스크톱을 생성한 사용자입니다. 중앙의 이름은 시작 시 설정된 세션 이름이며 기본 'MyDesktop' 또는 사용자가 설정한 이름입니다.



종료된 상태의 호스트

Amazon EC2 콘솔에 종료된 인스턴스가 표시되면 일반적으로 종료된 데스크톱 호스트입니다. 콘솔에 종료된 상태의 인프라 호스트가 포함된 경우, 특히 동일한 유형이 여러 개 있는 경우, 이는 시스템 문제가 진행 중임을 나타낼 수 있습니다.

다음 이미지는 종료된 데스크톱 인스턴스를 보여줍니다.



참조를 위한 유용한 Active Directory(AD) 관련 명령

다음은 AD 구성 관련 정보를 보기 위해 인프라 호스트에 입력할 수 있는 LDAP 관련 명령의 예입니다. 사용된 도메인 및 기타 파라미터는 환경 생성 시 입력한 파라미터를 반영해야 합니다.

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

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

Windows DCV 디버깅

Windows 데스크톱에서는 다음을 사용하여 연결된 세션을 나열할 수 있습니다.

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

Amazon DCV 버전 정보 찾기

AmazonDCV은 가상 데스크톱 세션에 사용됩니다. AWS Amazon DCV. 다음 예제에서는 설치된 DCV 소프트웨어의 버전을 확인하는 방법을 보여줍니다.

Linux

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

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

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

Windows

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

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

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

문제 RunBooks

다음 섹션에는 발생할 수 있는 문제, 이를 감지하는 방법, 문제 해결 방법에 대한 제안이 포함되어 있습니다.

- 설치 문제
  - 설치 후 사용자 지정 도메인을 설정하고 싶습니다. RES
  - AWS CloudFormation “실패 메시지를 수신했습니다”WaitCondition 라는 메시지로 스택을 생성하지 못했습니다. 오류:상태.TaskFailed'
  - 스택이 성공적으로 생성된 후 AWS CloudFormation 이메일 알림이 수신되지 않음
  - 실패한 상태의 인스턴스 사이클링 또는 vdc 컨트롤러

설치 문제

주제

- CloudFormation 환경 생성 중 스택 생성 실패
- AdDomainAdminNode CREATE_에서 외부 리소스(데모) 스택 생성 실패FAILED

.....

설치 후 사용자 지정 도메인을 설정하고 싶습니다. RES

> **Note**
>
> 사전 조건 : 이러한 단계를 수행하기 전에 Secrets Manager 보안 암호에 인증서와 PrivateKey 콘텐츠를 저장해야 합니다.

웹 클라이언트에 인증서 추가

1. 외부-alb 로드 밸런서의 리스너에 연결된 인증서를 업데이트합니다.
   a. AWS 콘솔의 EC2 > 로드 밸런싱 > 로드 밸런서 에서 RES 외부 로드 밸런서로 이동합니다.
   b. 명명 규칙 을 따르는 로드 밸런서를 검색합니다*<env-name>*`-external-alb`.
   c. 로드 밸런서에 연결된 리스너를 확인합니다.
   d. 기본 SSL/TLS 인증서가 새 인증서 세부 정보와 연결된 리스너를 업데이트합니다.
   e. 변경 내용을 저장합니다.
2. 클러스터 설정 테이블에서:
   a. DynamoDB -> 테이블 -> 에서 클러스터 설정 테이블을 찾습니다*<env-name>*`.cluster-settings`.
   b. 항목 탐색 및 속성별 필터링 - 이름 '키', 유형 '문자열', 조건 '포함', 값 '외부_alb'로 이동합니다.
   c. True`cluster.load_balancers.external_alb.certificates.provided`로 설정합니다.
   d. 값을 업데이트합니다`cluster.load_balancers.external_alb.certificates.custom_dns_name`. 웹 사용자 인터페이스의 사용자 지정 도메인 이름입니다.
   e. 값을 업데이트합니다`cluster.load_balancers.external_alb.certificates.acm_certificate_arn`. Amazon Certificate Manager(ARN)에 저장된 해당 인증서의 Amazon 리소스 이름()입니다 ACM.

3. 웹 클라이언트에 대해 생성한 해당 Route53 하위 도메인 레코드를 외부 alb 로드 밸런서 의 DNS 이름을 가리키도록 업데이트합니다`<env-name>-external-alb`.
4. SSO 가 환경에서 이미 구성된 경우 RES 웹 포털의 일반 설정 > 자격 증명 공급자 > Single Sign On > 상태 > 편집 버튼에서 처음 사용한 것과 동일한 입력SSO으로 다시 구성합니다.

에 인증서 추가 VDIs

1. 보안 암호에 다음 태그를 추가하여 보안 암호에 대한 GetSecret 작업을 수행할 수 있는 권한을 RES 애플리케이션에 부여합니다.
   - `res:EnvironmentName` : *`<env-name>`*
   - `res:ModuleName` : `virtual-desktop-controller`
2. 클러스터 설정 테이블에서:
   a. DynamoDB -> 테이블 -> 에서 클러스터 설정 테이블을 찾습니다*`<env-name>`*`.cluster-settings`.
   b. 항목 탐색 및 속성별 필터링 - 이름 '키', 유형 '문자열', 조건 '포함' 및 값 'dcv_connection_gateway'로 이동합니다.
   c. True`vdc.dcv_connection_gateway.certificate.provided`로 설정합니다.
   d. 값을 업데이트합니다`vdc.dcv_connection_gateway.certificate.custom_dns_name`. VDI 액세스에 사용되는 사용자 지정 도메인 이름입니다.
   e. 값을 업데이트합니다`vdc.dcv_connection_gateway.certificate.certificate_secret_arn`. 인증서 콘텐츠를 보유한 ARN 보안 암호의 입니다.
   f. 값을 업데이트합니다`vdc.dcv_connection_gateway.certificate.private_key_secret_arn`. 프라이빗 키 콘텐츠를 보유한 ARN 보안 암호의 입니다.
3. 게이트웨이 인스턴스에 사용되는 시작 템플릿을 업데이트합니다.
   a. AWS 콘솔의 EC2 > Auto Scaling > Auto Scaling Groups에서 Auto Scaling 그룹을 엽니다.
   b. RES 환경에 해당하는 게이트웨이 자동 조정 그룹을 선택합니다. 이름은 명명 규칙 을 따릅니다*`<env-name>`*`-vdc-gateway-asg`.
   c. 세부 정보 섹션에서 시작 템플릿을 찾아 엽니다.
   d. 세부 정보 > 작업 > 템플릿 수정(새 버전 생성)을 선택합니다.

e. 아래로 스크롤하여 고급 세부 정보 로 이동합니다.

f. 맨 아래로 스크롤하여 사용자 데이터 로 이동합니다.

g. CERTIFICATE_SECRET_ARN 및 단어를 찾습니다PRIVATE_KEY_SECRET_ARN. 이러한 값을 인증서(2.c단계 참조) 및 프라이빗 키(2.d단계 참조) 콘텐츠를 보유한 보안 암호에 ARNs 지정된 로 업데이트합니다.

h. Auto Scaling 그룹이 최근에 생성된 버전의 시작 템플릿을 사용하도록 구성되어 있는지 확인합니다(Auto Scaling 그룹 페이지에서).

4. 가상 데스크톱에 대해 생성한 해당 Route53 하위 도메인 레코드를 외부 nlb 로드 밸런서의 DNS 이름을 가리키도록 업데이트합니다*<env-name>*-external-nlb.

5. 기존 dcv-gateway 인스턴스를 종료*<env-name>*-vdc-gateway하고 새 인스턴스가 스핀업될 때까지 기다립니다.

.....

AWS CloudFormation “실패 메시지를 수신했습니다”WaitCondition 라는 메시지로 스택을 생성하지 못했습니다. 오류:상태.TaskFailed'

문제를 식별하려면 라는 Amazon CloudWatch 로그 그룹을 검사합니다<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>. 이름이 같은 로그 그룹이 여러 개 있는 경우 사용 가능한 첫 번째 로그 그룹을 검사합니다. 로그 내의 오류 메시지는 문제에 대한 자세한 정보를 제공합니다.

> **Note**
>
> 파라미터 값에 공백이 없는지 확인합니다.

.....

스택이 성공적으로 생성된 후 AWS CloudFormation 이메일 알림이 수신되지 않음

AWS CloudFormation 스택이 성공적으로 생성된 후 이메일 초대를 받지 못한 경우 다음을 확인합니다.

1. 이메일 주소 파라미터가 올바르게 입력되었는지 확인합니다.

   이메일 주소가 잘못되었거나 액세스할 수 없는 경우 Research and Engineering Studio 환경을 삭제하고 재배포합니다.

2. Amazon EC2 콘솔에서 순환 인스턴스의 증거를 확인하세요.

   <envname> 접두사가 인 Amazon EC2 인스턴스가 종료됨으로 표시된 다음 새 인스턴스로 교체되는 경우 네트워크 또는 Active Directory 구성에 문제가 있을 수 있습니다.

3. AWS 고성능 컴퓨팅 레시피를 배포하여 외부 리소스를 생성한 경우 스택에서 VPC, 프라이빗 및 퍼블릭 서브넷 및 기타 선택한 파라미터가 생성되었는지 확인합니다.

   파라미터 중 하나라도 잘못된 경우 RES 환경을 삭제하고 재배포해야 할 수 있습니다. 자세한 내용은 제품 제거 단원을 참조하십시오.

4. 자체 외부 리소스와 함께 제품을 배포한 경우 네트워킹 및 Active Directory가 예상 구성과 일치하는지 확인합니다.

   인프라 인스턴스가 Active Directory에 성공적으로 가입되었는지 확인하는 것이 중요합니다. 의 단계를 수행하여 문제를 the section called “실패한 상태의 인스턴스 사이클링 또는 vdc 컨트롤러” 해결하세요.

.....

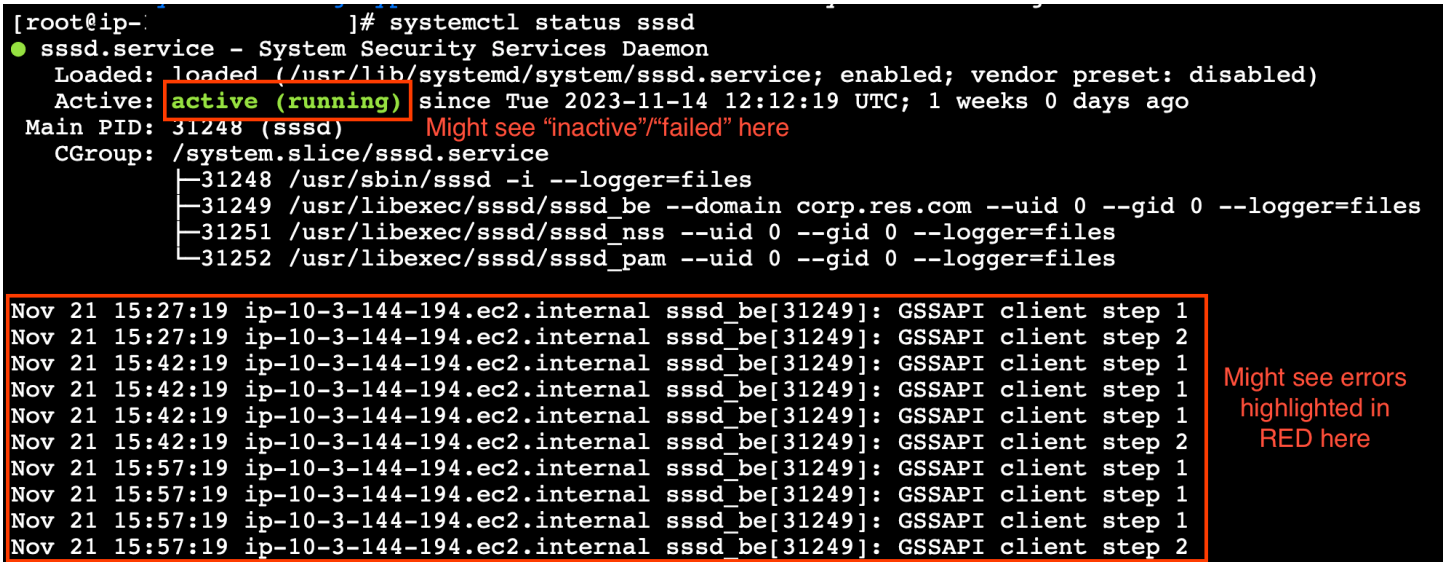
실패한 상태의 인스턴스 사이클링 또는 vdc 컨트롤러

이 문제의 가장 가능한 원인은 리소스(들)가 Active Directory에 연결하거나 조인할 수 없기 때문입니다.

문제를 확인하려면:

1. 명령줄에서 vdc 컨트롤러의 실행 중인 인스턴스SSM에서 를 사용하여 세션을 시작합니다.
2. `sudo su -`를 실행합니다.
3. `systemctl status sssd`를 실행합니다.

상태가 비활성이거나 실패하거나 로그에 오류가 표시되면 인스턴스가 Active Directory에 조인할 수 없는 것입니다.



SSM 오류 로그

문제를 해결하려면:

- 동일한 명령줄 인스턴스에서 를 실행`cat /root/bootstrap/logs/userdata.log`하여 로그를 조사합니다.

이 문제에는 세 가지 가능한 근본 원인 중 하나가 있을 수 있습니다.

근본 원인 1: 잘못된 LDAP 연결 세부 정보가 입력됨

로그를 검토합니다. 다음과 같이 여러 번 반복되는 경우 인스턴스가 Active Directory에 조인할 수 없습니다.

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

1. RES 스택 생성 중에 다음에 대한 파라미터 값이 올바르게 입력되었는지 확인합니다.

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

2. DynamoDB 테이블에서 잘못된 값을 업데이트합니다. 테이블은 DynamoDB 콘솔의 테이블 에서 찾을 수 있습니다. 테이블 이름은 여야 합니다`<stack name>`.cluster-settings.
3. 테이블을 업데이트한 후 현재 환경 인스턴스를 실행 중인 클러스터 관리자 및 vdc 컨트롤러를 삭제합니다. Auto Scaling은 DynamoDB 테이블의 최신 값을 사용하여 새 인스턴스를 시작합니다.

근본 원인 2: 잘못된 ServiceAccount 사용자 이름이 입력됨

로그가 `Insufficient permissions to modify computer account`를 반환하면 스택 생성 중에 입력한 ServiceAccount 이름이 올바르지 않을 수 있습니다.

1. AWS 콘솔에서 Secrets Manager를 엽니다.
2. `directoryserviceServiceAccountUsername`를 찾습니다. 보안 암호는 여야 합니다`<stack name>`-directoryservice-ServiceAccountUsername.
3. 보안 암호를 열어 세부 정보 페이지를 봅니다. 보안 암호 값에서 보안 암호 값 검색을 선택하고 일반 텍스트 를 선택합니다.
4. 값이 업데이트된 경우 현재 실행 중인 환경의 클러스터 관리자 및 vdc 컨트롤러 인스턴스를 삭제합니다. Auto Scaling은 Secrets Manager의 최신 값을 사용하여 새 인스턴스를 시작합니다.

근본 원인 3: 잘못된 ServiceAccount 암호 입력

로그에 이 표시되면 스택 생성 중에 입력한 ServiceAccount 암호`Invalid credentials`가 올바르지 않을 수 있습니다.

1. AWS 콘솔에서 Secrets Manager를 엽니다.
2. `directoryserviceServiceAccountPassword`를 찾습니다. 보안 암호는 여야 합니다`<stack name>`-directoryservice-ServiceAccountPassword.

3. 보안 암호를 열어 세부 정보 페이지를 봅니다. 보안 암호 값에서 보안 암호 값 검색을 선택하고 일반 텍스트 를 선택합니다.
4. 암호를 잊었거나 입력한 암호가 올바른지 확실하지 않은 경우 Active Directory 및 Secrets Manager에서 암호를 재설정할 수 있습니다.

   a. 에서 암호를 재설정하려면 AWS Managed Microsoft AD:

      i. AWS 콘솔을 열고 로 이동합니다 AWS Directory Service.
      ii. 디렉터리의 디렉터리 ID를 선택하고 작업 을 선택합니다. RES
      iii. 사용자 암호 재설정을 선택합니다.
      iv. ServiceAccount 사용자 이름을 입력합니다.
      v. 새 암호를 입력하고 암호 재설정을 선택합니다.

   b. Secrets Manager에서 암호를 재설정하려면:

      i. AWS 콘솔을 열고 Secrets Manager로 이동합니다.
      ii. `directoryserviceServiceAccountPassword`를 찾습니다. 보안 암호는 여야 합니다`<stack name>-directoryservice-ServiceAccountPassword`.
      iii. 보안 암호를 열어 세부 정보 페이지를 봅니다. 보안 암호 값에서 보안 암호 값 검색을 선택한 다음 일반 텍스트 를 선택합니다.
      iv. 편집을 선택합니다.
      v. ServiceAccount 사용자의 새 암호를 설정하고 저장을 선택합니다.
5. 값을 업데이트한 경우 현재 실행 중인 환경의 클러스터 관리자 및 vdc 컨트롤러 인스턴스를 삭제합니다. Auto Scaling은 최신 값을 사용하여 새 인스턴스를 시작합니다.

.....

종속 객체 오류로 인해 환경 CloudFormation 스택이 삭제되지 않음

와 같은 종속 객체 오류로 인해 `<env-name>-vdc` CloudFormation 스택 삭제가 실패하는 경우`vdcdcvhostsecuritygroup`, 이는 콘솔을 사용하여 RES AWS 생성된 서브넷 또는 보안 그룹으로 시작된 Amazon EC2 인스턴스 때문일 수 있습니다.

문제를 해결하려면 이러한 방식으로 시작된 모든 Amazon EC2 인스턴스를 찾아 종료합니다. 그런 다음 환경 삭제를 재개할 수 있습니다.

.....

환경 생성 중 CIDR 블록 파라미터에 오류가 발생했습니다.

환경을 생성할 때 응답 상태가 []인 CIDR 블록 파라미터에 대한 오류가 나타납니다FAILED.

오류의 예:

```
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.
```

문제를 해결하려면 예상 형식은 x.x.x.0/24 또는 x.x.x.0/32입니다.

.....

CloudFormation 환경 생성 중 스택 생성 실패

환경을 생성하려면 일련의 리소스 생성 작업이 필요합니다. 일부 리전에서는 용량 문제가 발생하여 CloudFormation 스택 생성이 실패할 수 있습니다.

이 경우 환경을 삭제하고 생성을 다시 시도합니다. 또는 다른 리전에서 생성을 다시 시도할 수 있습니다.

.....

AdDomainAdminNode CREATE_에서 외부 리소스(데모) 스택 생성 실패FAILED

다음 오류로 데모 환경 스택 생성에 실패하는 경우 인스턴스 시작 후 프로비저닝 중에 예기치 않게 발생하는 Amazon EC2 패치 때문일 수 있습니다.

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

실패 원인을 확인하려면:

1. SSM 상태 관리자에서 패치가 구성되어 있는지, 모든 인스턴스에 구성되어 있는지 확인합니다.
2. SSM RunCommand/Automation 실행 기록에서 패치 관련 SSM 문서의 실행이 인스턴스 시작과 일치하는지 확인합니다.
3. 환경의 Amazon EC2 인스턴스에 대한 로그 파일에서 로컬 인스턴스 로깅을 검토하여 프로비저닝 중에 인스턴스가 재부팅되었는지 확인합니다.

패치 적용으로 인해 문제가 발생한 경우 RES 인스턴스에 대한 패치 적용은 시작 후 최소 15분 후에 지연합니다.

.....

자격 증명 관리 문제

Single Sign-On(SSO) 및 자격 증명 관리와 관련된 대부분의 문제는 잘못된 구성으로 인해 발생합니다. SSO 구성 설정에 대한 자세한 내용은 다음을 참조하세요.

- the section called “IAM Identity CenterSSO로 설정”
- the section called “에 대한 자격 증명 공급자 구성 SSO”

자격 증명 관리와 관련된 기타 문제를 해결하려면 다음 문제 해결 주제를 참조하세요.

주제

- iam을 수행할 권한이 없습니다.PassRole
- 내 AWS 계정 외부의 사람들이 리소스에서 내 Research and Engineering Studio에 AWS 액세스하도록 허용하고 싶습니다.
- 환경에 로그인할 때 즉시 로그인 페이지로 돌아갑니다.
- 로그인을 시도할 때 “사용자를 찾을 수 없음” 오류 발생
- Active Directory에 추가되었지만 에서 누락된 사용자 RES
- 세션을 생성할 때 사용자를 사용할 수 없음
- CloudWatch 클러스터 관리자 로그의 크기 제한이 오류를 초과했습니다.

.....

iam을 수행할 권한이 없습니다.PassRole

iam:PassRole action을 수행할 권한이 없다는 오류가 발생하면 역할을 에 전달할 수 있도록 정책을 업데이트해야 합니다RES.

일부 AWS 서비스를 사용하면 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 에서 작업을 수행하려고 할 때 발생합니다RES. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

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

이 경우 Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다. 도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

.....

내 AWS 계정 외부의 사람들이 리소스에서 내 Research and Engineering Studio에 AWS 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACLs)을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 소유한 AWS 계정에서 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사 AWS 계정에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 소유 AWS 계정에 대한 액세스 권한 제공을 참조하세요.
- 자격 증명 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부 인증 사용자에게 액세스 제공(자격 증명 페더레이션)을 참조하세요.
- 교차 계정 액세스에 역할 및 리소스 기반 정책을 사용하는 차이점을 알아보려면 IAM 사용 설명서의 리소스 기반 정책과 IAM 역할이 어떻게 다른지 참조하세요.

.....

환경에 로그인할 때 즉시 로그인 페이지로 돌아갑니다.

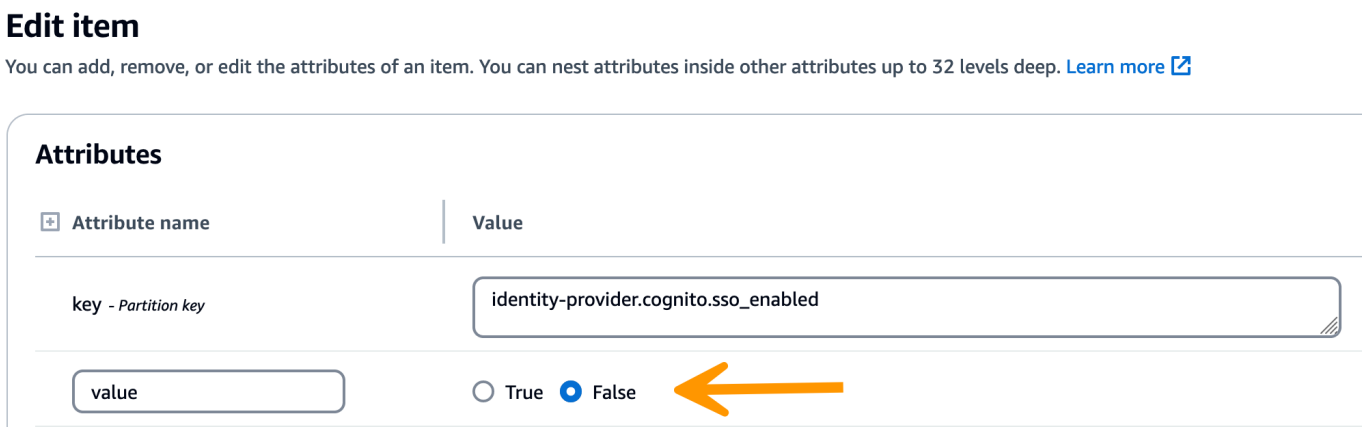
이 문제는 SSO 통합이 잘못 구성된 경우 발생합니다. 문제를 확인하려면 컨트롤러 인스턴스 로그를 확인하고 구성 설정에 오류가 있는지 검토합니다.

로그를 확인하려면:

1. CloudWatch 콘솔 을 엽니다.
2. 로그 그룹 에서 이름이 인 그룹을 찾습니다/*<environment-name>*/cluster-manager.
3. 로그 그룹을 열어 로그 스트림에서 오류를 검색합니다.

구성 설정을 확인하려면:

1. DynamoDB 콘솔 열기
2. 테이블 에서 라는 테이블을 찾습니다*<environment-name>*.cluster-settings.
3. 테이블을 열고 테이블 항목 탐색을 선택합니다.
4. 필터 섹션을 확장하고 다음 변수를 입력합니다.
   - 속성 이름 - 키
   - 조건 - 포함
   - 값 - sso
5. Run(실행)을 선택합니다.
6. 반환된 문자열에서 SSO 구성 값이 올바른지 확인합니다. 잘못된 경우 sso_enabled 키의 값을 False 로 변경합니다.



7. RES 사용자 인터페이스로 돌아가 를 재구성합니다SSO.

.....

로그인을 시도할 때 “사용자를 찾을 수 없음” 오류 발생

사용자가 RES 인터페이스에 로그인하려고 할 때 '사용자를 찾을 수 없음'이라는 오류가 수신되고 사용자가 Active Directory에 있는 경우:

- 사용자가 에 없고 RES 최근에 AD에 사용자를 추가한 경우
  - 사용자가 아직 에 동기화되지 않았을 수 있습니다RES. RES 는 매시간 동기화되므로 기다린 후 다음 동기화 후 사용자가 추가되었는지 확인해야 할 수 있습니다. 즉시 동기화하려면 의 단계를 따릅니다Active Directory에 추가되었지만 에서 누락된 사용자 RES.
- 사용자가 에 있는 경우RES:
  1. 속성 매핑이 올바르게 구성되었는지 확인합니다. 자세한 내용은 Single Sign-On을 위한 자격 증명 공급자 구성(SSO) 단원을 참조하십시오.
  2. SAML 제목과 SAML 이메일이 모두 사용자의 이메일 주소에 매핑되어 있는지 확인합니다.

.....

Active Directory에 추가되었지만 에서 누락된 사용자 RES

Active Directory에 사용자를 추가했지만 에 누락된 경우 AD 동기화RES를 트리거해야 합니다. AD 동기화는 RES 환경으로 AD 항목을 가져오는 Lambda 함수에 의해 매시간 수행됩니다. 경우에 따라 새 사용자 또는 그룹을 추가한 후 다음 동기화 프로세스가 실행될 때까지 지연이 발생할 수 있습니다. Amazon Simple Queue Service에서 수동으로 동기화를 시작할 수 있습니다.

동기화 프로세스를 수동으로 시작합니다.

1. Amazon SQS 콘솔 을 엽니다.
2. 대기열 에서 를 선택합니다`<environment-name>-cluster-manager-tasks.fifo`.
3. [메시지 전송 및 수신(Send and receive messages)]을 선택합니다.
4. 메시지 본문 에 다음을 입력합니다.

   ```
   { "name": "adsync.sync-from-ad", "payload": {} }
   ```

5. 메시지 그룹 ID 에 다음을 입력합니다. **`adsync.sync-from-ad`**
6. 메시지 중복 제거 ID 에 임의의 영숫자 문자열을 입력합니다. 이 항목은 이전 5분 이내에 수행된 모든 통화와 달라야 합니다. 그렇지 않으면 요청이 무시됩니다.

.....

세션을 생성할 때 사용자를 사용할 수 없음

세션을 생성하는 관리자이지만 세션을 생성할 때 Active Directory에 있는 사용자를 사용할 수 없는 경우 사용자가 처음으로 로그인해야 할 수 있습니다. 세션은 활성 사용자에 대해서만 생성할 수 있습니다. 활성 사용자는 환경에 한 번 이상 로그인해야 합니다.

.....

CloudWatch 클러스터 관리자 로그의 크기 제한이 오류를 초과했습니다.

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

CloudWatch 클러스터 관리자 로그에서 이 오류가 발생하면 LDAP 검색에서 너무 많은 사용자 레코드가 반환되었을 수 있습니다. 이 문제를 해결하려면 IDP의 ldap 검색 결과 제한을 늘리세요.

.....

스토리지

주제

.....

를 통해 파일 시스템을 생성RES했지만 VDI 호스트에 탑재되지 않음

파일 시스템을 VDI 호스트에서 탑재하려면 먼저 '사용 가능' 상태여야 합니다. 아래 단계에 따라 파일 시스템이 필수 상태인지 확인합니다.

Amazon EFS

1. Amazon EFS 콘솔 로 이동합니다.

2. 파일 시스템 상태가 사용 가능 인지 확인합니다.
3. 파일 시스템 상태를 사용할 수 없는 경우 VDI 호스트를 시작하기 전에 기다립니다.

Amazon FSx ONTAP

1. Amazon FSx 콘솔 로 이동합니다.
2. 상태가 사용 가능한지 확인합니다.
3. 상태를 사용할 수 없는 경우 VDI 호스트를 시작하기 전에 기다립니다.

.....

를 통해 파일 시스템을 온보딩RES했지만 VDI 호스트에 탑재되지 않음

온보딩된 파일 시스템에는 VDI 호스트가 파일 시스템을 탑재할 수 있도록 구성된 필수 보안 그룹 규칙이 RES 있어야 합니다. 이러한 파일 시스템은 외부에서 생성되므로 RESRES는 연결된 보안 그룹 규칙을 관리하지 않습니다.

온보딩된 파일 시스템과 연결된 보안 그룹은 다음과 같은 인바운드 트래픽을 허용해야 합니다.

- NFS Linux VDC 호스트의 트래픽(포트: 2049)
- SMB Windows VDC 호스트의 트래픽(포트: 445)

.....

VDI 호스트에서 읽기/쓰기할 수 없음

ONTAP 는 볼륨에 대해 및 UNIX NTFS MIXED 보안 스타일을 지원합니다. 보안 스타일은 가 데이터 액세스를 제어하는 데 ONTAP 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형을 결정합니다.

예를 들어 볼륨이 UNIX 보안 스타일을 사용하는 경우 SMB 클라이언트는 의 다중 프로토콜 특성으로 인해 여전히 데이터에 액세스할 수 있습니다(적절하게 인증하고 권한을 부여한 경우). ONTAP 그러나는 UNIX 클라이언트만 기본 도구를 사용하여 수정할 수 있는 UNIX 권한을 ONTAP 사용합니다.

권한 처리 사용 사례 예

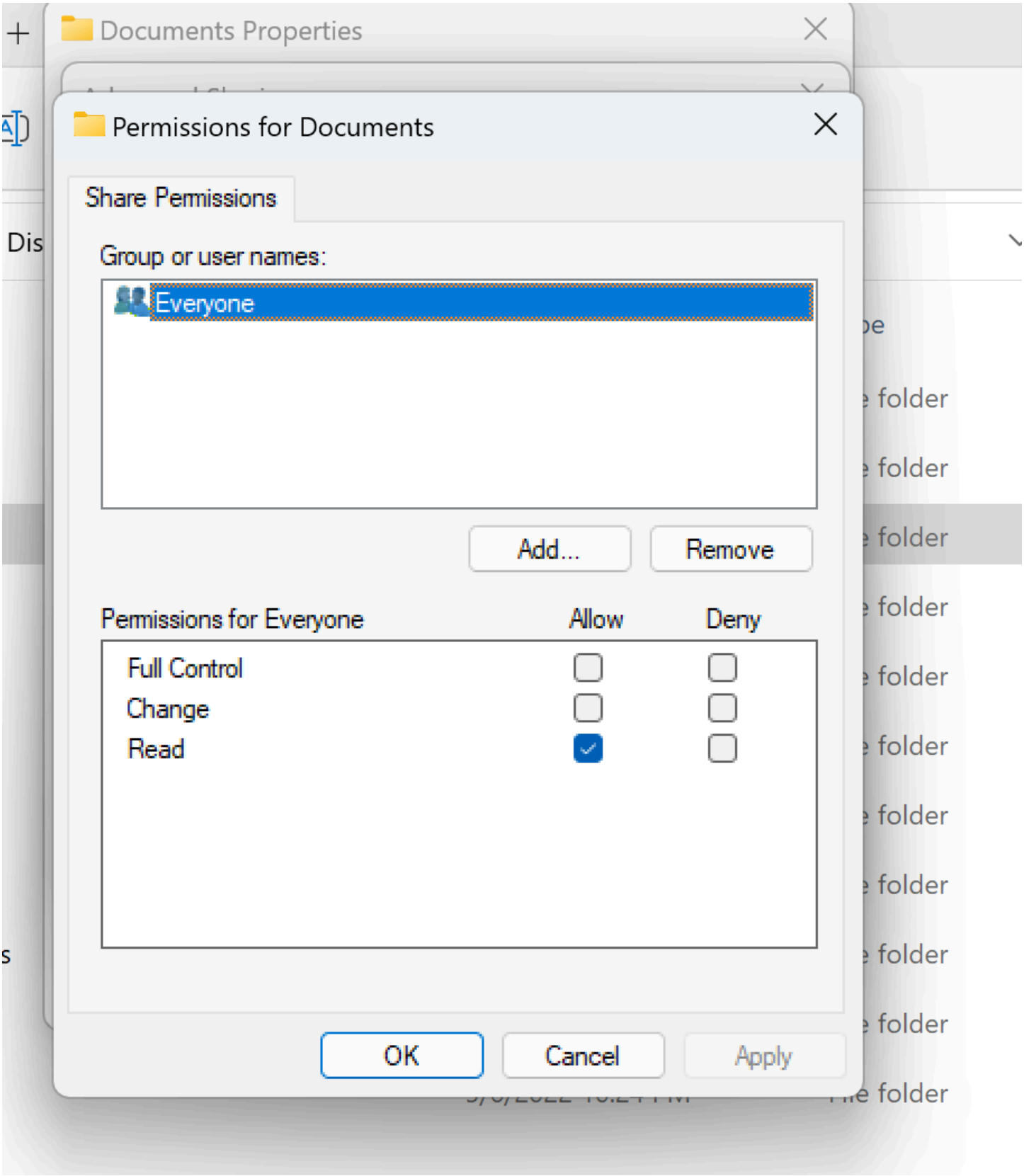
Linux 워크로드에서 UNIX 스타일 볼륨 사용

권한은 다른 사용자에 대해 수도자가 구성할 수 있습니다. 예를 들어, 다음은 /<project-name> 디렉터리에 대한 <group-ID> 전체 읽기/쓰기 권한을 모든 멤버에게 부여합니다.

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

Linux 및 Windows 워크로드에서 NTFS 스타일 볼륨 사용

공유 권한은 특정 폴더의 공유 속성을 사용하여 구성할 수 있습니다. 예를 들어 사용자 user_01 및 폴더 를 지정하면 myfolder, Change또는 의 권한을 Allow 또는 Full ControlRead로 설정할 수 있습니다Deny.


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

볼륨을 Linux 클라이언트와 Windows 클라이언트 모두에서 사용할 경우 Linux 사용자 이름을 동일한 사용자 이름과 domain\username의 NetBIOS 도메인 이름 형식과 SVM 연결하는 이름 매핑을 에 설정해야 합니다. 이는 Linux 사용자와 Windows 사용자 간에 번역하는 데 필요합니다. 자세한 내용은 Amazon FSx for 에서 멀티프로토콜 워크로드 활성화 NetApp ONTAP를 참조하세요.

.....

에서 FSx에 대한 NetApp ONTAP Amazon을 생성RES했지만 도메인에 가입하지 않았습니다.

현재 RES 콘솔에서 FSx 용 NetApp ONTAP Amazon을 생성하면 파일 시스템이 프로비저닝되지만 도메인에 가입되지 않습니다. 생성된 ONTAP 파일 시스템을 도메인SVM에 조인하려면 Microsoft Active Directory에 조인SVMs을 참조하고 Amazon FSx 콘솔의 단계를 따릅니다. 필요한 권한이 AD의 Amazon FSx Service 계정에 위임되었는지 확인합니다. 가 도메인에 성공적으로 SVM 조인되면 SVM 요약 > 엔드포인트 > SMB DNS 이름으로 이동하여 나중에 필요하므로 DNS 이름을 복사합니다.

도메인에 조인된 후 클러스터 설정 DynamoDB 테이블에서 SMB DNS 구성 키를 편집합니다.

1. Amazon DynamoDB 콘솔 로 이동합니다.
2. 테이블 을 선택한 다음 를 선택합니다`<stack-name>-cluster-settings`.
3. 테이블 항목 탐색에서 필터 를 확장하고 다음 필터를 입력합니다.
   - 속성 이름 - 키
   - 조건 - 같음
   - 값 - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. 반환된 항목을 선택한 다음 작업 , 항목 편집 을 선택합니다.
5. 이전에 복사한 SMB DNS 이름으로 값을 업데이트합니다.
6. [Save and close]를 선택합니다.

또한 파일 시스템과 연결된 보안 그룹이 Amazon 을 사용한 파일 시스템 액세스 제어VPC에서 권장하는 대로 트래픽을 허용하는지 확인합니다. 파일 시스템을 사용하는 새 VDI 호스트는 이제 조인된 도메인SVM과 파일 시스템을 탑재할 수 있습니다.

또는 RES 온보드 파일 시스템 기능을 사용하여 도메인에 이미 가입된 기존 파일 시스템을 온보딩할 수 있습니다. Environment Management에서 파일 시스템 , 온보드 파일 시스템 을 선택합니다.

.....

스냅샷

주제

- 스냅샷의 상태는 실패입니다.
- 스냅샷이 테이블을 가져올 수 없음을 나타내는 로그와 함께 적용되지 않습니다.

.....

스냅샷의 상태는 실패입니다.

RES 스냅샷 페이지에서 스냅샷의 상태가 실패인 경우 오류가 발생한 시간 동안 클러스터 관리자에 대한 Amazon CloudWatch 로그 그룹으로 이동하여 원인을 확인할 수 있습니다.

```
[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
```

.....

스냅샷이 테이블을 가져올 수 없음을 나타내는 로그와 함께 적용되지 않습니다.

이전 env에서 가져온 스냅샷이 새 env에 적용되지 않는 경우 클러스터 관리자가 문제를 식별할 수 있도록 CloudWatch 로그를 살펴봅니다. 문제에서 필요한 테이블 클라우드를 가져올 수 없다고 언급하는 경우 스냅샷이 유효한 상태인지 확인합니다.

1. metadata.json 파일을 다운로드하고 다양한 테이블의 ExportStatus 에 상태가 인지 확인합니다 COMPLETED. 다양한 테이블에 `ExportManifest` 필드 세트가 있는지 확인합니다. 위의 필드 세트를 찾을 수 없는 경우 스냅샷은 유효하지 않은 상태이므로 스냅샷 적용 기능과 함께 사용할 수 없습니다.
2. 스냅샷 생성을 시작한 후 스냅샷 상태가 에서 COMPLETED 로 바뀌는지 확인합니다RES. 스냅샷 생성 프로세스에는 최대 5~10분이 소요됩니다. 스냅샷 관리 페이지를 다시 로드하거나 다시 방문하여 스냅샷이 성공적으로 생성되었는지 확인합니다. 이렇게 하면 생성된 스냅샷이 유효한 상태가 됩니다.

.....

인프라

주제

- 정상 인스턴스가 없는 로드 밸런서 대상 그룹

.....

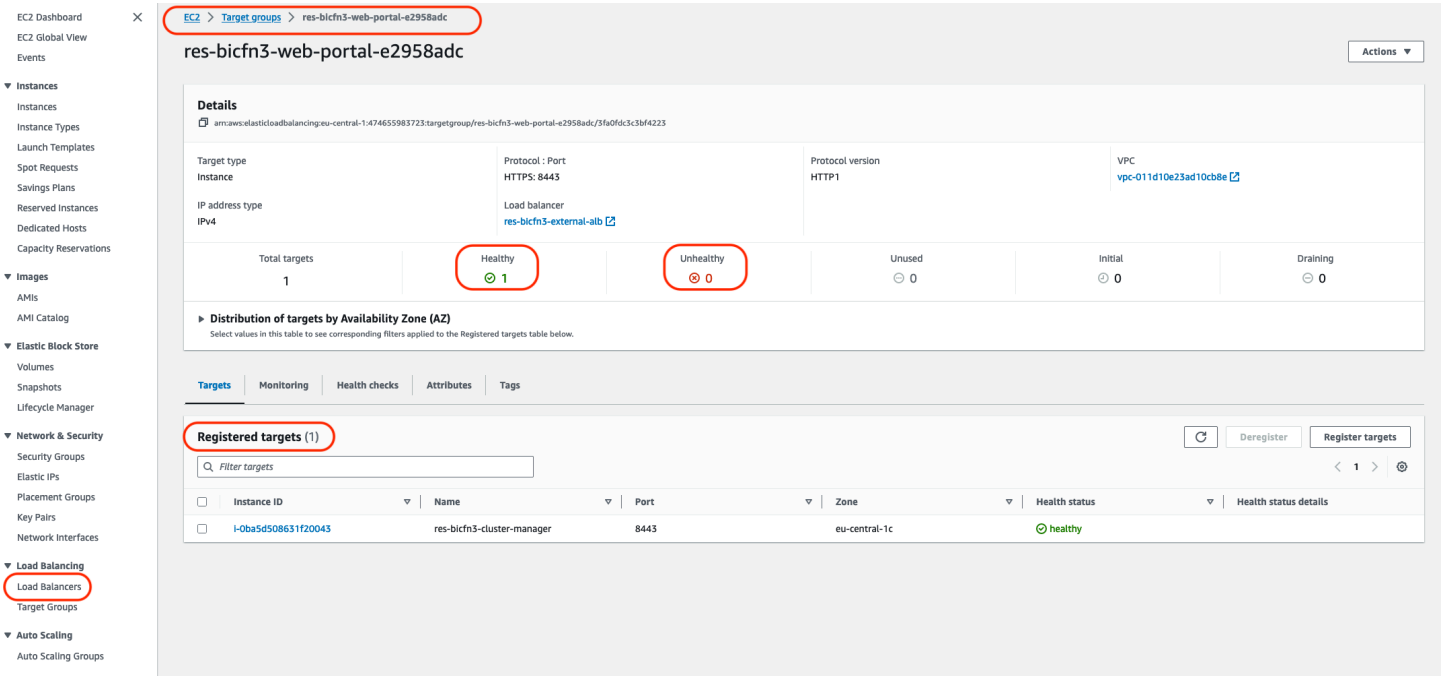
정상 인스턴스가 없는 로드 밸런서 대상 그룹

UI 또는 데스크톱 세션에 서버 오류 메시지와 같은 문제가 나타나는 경우, 이는 인프라 Amazon EC2 인스턴스에 문제가 있음을 나타낼 수 있습니다.

문제의 원인을 확인하는 방법은 먼저 Amazon EC2 콘솔에서 반복적으로 종료되고 새 EC2 인스턴스로 교체되는 것으로 보이는 Amazon 인스턴스가 있는지 확인하는 것입니다. 이 경우 Amazon CloudWatch 로그를 검사하여 원인을 확인할 수 있습니다.

또 다른 방법은 시스템의 로드 밸런서를 확인하는 것입니다. Amazon EC2 콘솔에서 발견된 로드 밸런서가 등록된 정상 인스턴스를 표시하지 않는 경우 시스템 문제가 발생할 수 있음을 나타냅니다.

일반적인 외관의 예는 다음과 같습니다.



상태 항목이 0이면 요청을 처리할 수 있는 Amazon EC2 인스턴스가 없음을 나타냅니다.

비정상 항목이 0이 아닌 경우, 이는 Amazon EC2 인스턴스가 순환 중일 수 있음을 나타냅니다. 이는 설치된 애플리케이션 소프트웨어가 상태 확인을 통과하지 못했기 때문일 수 있습니다.

정상 항목과 비정상 항목이 모두 0이면 네트워크 구성이 잘못되었을 수 있음을 나타냅니다. 예를 들어 퍼블릭 및 프라이빗 서브넷에 해당 이 없을 수 있습니다AZs. 이 조건이 발생하면 콘솔에 네트워크 상태가 존재함을 나타내는 추가 텍스트가 있을 수 있습니다.

.....

Virtual Desktops 시작

주제

- 이전에 작동하던 가상 데스크톱이 더 이상 성공적으로 연결할 수 없음
- 5개의 가상 데스크톱만 시작할 수 있습니다.
- “연결이 닫혔습니다. 전송 오류'
- VDIs 프로비저닝 상태 중단됨
- VDIs 시작 후 오류 상태로 전환

.....

이전에 작동하던 가상 데스크톱이 더 이상 성공적으로 연결할 수 없음

데스크톱 연결이 닫히거나 더 이상 연결할 수 없는 경우, 기본 Amazon EC2 인스턴스가 실패했거나 Amazon EC2 인스턴스가 RES 환경 외부에서 종료 또는 중지되었기 때문일 수 있습니다. 관리자 UI 상태는 준비 상태를 계속 표시할 수 있지만 연결 시도가 실패합니다.

Amazon EC2 콘솔을 사용하여 인스턴스가 종료 또는 중지되었는지 확인해야 합니다. 중지된 경우 다시 시작해 보세요. 상태가 종료되면 다른 데스크톱을 생성해야 합니다. 새 인스턴스가 시작될 때 사용자 홈 디렉터리에 저장된 모든 데이터를 계속 사용할 수 있어야 합니다.

이전에 실패한 인스턴스가 관리자 UI에 계속 표시되는 경우 관리자 UI를 사용하여 종료해야 할 수 있습니다.

.....

5개의 가상 데스크톱만 시작할 수 있습니다.

사용자가 시작할 수 있는 가상 데스크톱 수의 기본 제한은 5입니다. 다음과 같이 관리자 UI를 사용하여 관리자가 변경할 수 있습니다.

- 데스크톱 설정 으로 이동합니다.
- 서버 탭을 선택합니다.
- DCV 세션 패널에서 오른쪽에 있는 편집 아이콘을 클릭합니다.
- 사용자당 허용된 세션의 값을 원하는 새 값으로 변경합니다.
- 제출을 선택합니다.
- 페이지를 새로 고쳐 새 설정이 적용되었는지 확인합니다.

.....

“연결이 닫혔습니다. 전송 오류'

UI 오류 “연결이 닫혔습니다. 전송 오류', 원인은 Windows 인스턴스에서 인증서 생성과 관련된 DCV 서버 소프트웨어의 문제로 인한 것일 수 있습니다.

Amazon CloudWatch 로그 그룹은 다음과 유사한 메시지로 연결 시도 오류를 기록할 `<envname>/vdc/dcv-connection-gateway` 수 있습니다.

```
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)
```

이 경우 SSM Session Manager를 사용하여 Windows 인스턴스에 대한 연결을 열고 다음 2개의 인증서 관련 파일을 제거하는 것이 해결 방법일 수 있습니다.

```
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
```

파일은 자동으로 다시 생성되어야 하며 후속 연결 시도가 성공할 수 있습니다.

이 방법으로 문제를 해결하고 Windows 데스크톱을 새로 시작하면 동일한 오류가 발생하는 경우 소프트웨어 스택 생성 함수를 사용하여 재생성된 인증서 파일을 사용하여 고정된 인스턴스의 새 Windows 소프트웨어 스택을 생성합니다. 이로 인해 성공적인 시작 및 연결에 사용할 수 있는 Windows 소프트웨어 스택이 생성될 수 있습니다.

.....

VDIs 프로비저닝 상태 중단됨

데스크톱 시작이 관리자 UI의 프로비저닝 상태로 유지되는 경우 여러 가지 이유가 있을 수 있습니다.

원인을 확인하려면 데스크톱 인스턴스의 로그 파일을 검사하고 문제를 일으킬 수 있는 오류가 있는지 확인합니다. 이 문서에는 유용한 로그 및 이벤트 정보 소스 라는 제목의 섹션에 관련 정보가 포함된 로그 파일 및 Amazon 로그 CloudWatch 그룹 목록이 포함되어 있습니다.

다음은 이 문제의 잠재적 원인입니다.

- 사용된 AMI ID는 소프트웨어 스택으로 등록되었지만 에서는 지원되지 않습니다RES.

  Amazon Machine Image(AMI)에 필요한 예상 구성 또는 도구가 없으므로 부트스트랩 프로비저닝 스크립트를 완료하지 못했습니다. Linux 인스턴스와 같은 인스턴스/root/bootstrap/logs/의 로그 파일에는 이와 관련된 유용한 정보가 포함될 수 있습니다. AMIs AWS Marketplace에서 가져온 ID는 RES 데스크톱 인스턴스에서 작동하지 않을 수 있습니다. 지원되는지 확인하기 위해 테스트가 필요합니다.
- 사용자 지정 에서 Windows 가상 데스크톱 인스턴스를 시작할 때는 사용자 데이터 스크립트가 실행되지 않습니다AMI.

  기본적으로 사용자 데이터 스크립트는 Amazon EC2 인스턴스가 시작될 때 한 번 실행됩니다. 기존 가상 데스크톱 인스턴스AMI에서 를 생성한 다음 에 소프트웨어 스택을 등록AMI하고 이 소프트웨어

스택으로 다른 가상 데스크톱을 시작하려고 하면 새 가상 데스크톱 인스턴스에서 사용자 데이터 스크립트가 실행되지 않습니다.

문제를 해결하려면 를 생성하는 데 사용한 원래 가상 데스크톱 인스턴스에서 관리자로 PowerShell 명령 창을 열고 다음 명령을 AMI실행합니다.

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

그런 다음 인스턴스AMI에서 새 을 생성합니다. 새 를 사용하여 소프트웨어 스택AMI을 등록하고 나중에 새 가상 데스크톱을 시작할 수 있습니다. 프로비저닝 상태로 유지되는 인스턴스에서 동일한 명령을 실행하고 인스턴스를 재부팅하여 가상 데스크톱 세션을 수정할 수도 있지만 잘못 구성된 에서 다른 가상 데스크톱을 시작할 때 동일한 문제가 다시 발생합니다AMI.

.....

VDIs 시작 후 오류 상태로 전환

가능한 문제 1: 홈 파일 시스템에는 다른 POSIX 권한을 가진 사용자를 위한 디렉터리가 있습니다.

다음 시나리오가 참인 경우 이 문제가 발생할 수 있습니다.

1. 배포된 RES 버전이 2024.01 이상입니다.
2. RES 스택을 배포하는 동안 에 대한 속성이 로 설정`EnableLdapIDMapping`되었습니다`True`.
3. RES 스택 배포 중에 지정된 홈 파일 시스템은 RES 2024.01 이전 버전에서 사용되었거나 로 `EnableLdapIDMapping` 설정된 이전 환경에서 사용되었습니다`False`.

해결 단계 : 파일 시스템에서 사용자 디렉터리를 삭제합니다.

1. SSM 클러스터 관리자 호스트로.
2. `cd /home`.
3. `ls - admin1`는 , `admin2`.. 등과 같이 사용자 이름과 일치하는 디렉터리 이름을 사용하여 디렉터리를 나열해야 합니다.
4. 디렉터리 를 삭제합니다`sudo rm -r 'dir_name'`. ssm-user 및 ec2-user 디렉터리를 삭제하지 마세요.
5. 사용자가 이미 새 env에 동기화된 경우 사용자 DDB 테이블에서 사용자를 삭제합니다(clusteradmin 제외).
6. AD 동기화 시작 - 클러스터 관리자 Amazon `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad`에서 실행합니다EC2.

7. RES 웹 페이지에서 Error 상태의 VDI 인스턴스를 재부팅합니다. 가 약 20분 후에 Ready 상태로 VDI 전환되는지 확인합니다.

.....

가상 데스크톱 구성 요소

주제

- Amazon EC2 인스턴스가 콘솔에서 종료를 반복적으로 표시하고 있습니다.
- AD 가입 실패로 인해 vdc 컨트롤러 인스턴스가 순환 중입니다. / eVDI 모듈에 API 상태 확인 실패가 표시됩니다.
- 프로젝트를 추가하기 위해 소프트웨어 스택을 편집할 때 풀다운에 프로젝트가 표시되지 않습니다.
- cluster-manager Amazon CloudWatch 로그에 “<user-home-init> 계정을 아직 사용할 수 없습니다. 사용자가 동기화될 때까지 대기”(계정이 사용자 이름인 경우)가 표시됩니다.
- 로그인 시도 시 Windows 데스크톱에 “계정이 비활성화되었습니다. 관리자에게 문의하세요.”
- DHCP 외부/고객 AD 구성의 옵션 문제
- Firefox 오류 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

.....

Amazon EC2 인스턴스가 콘솔에서 종료를 반복적으로 표시하고 있습니다.

Amazon EC2 콘솔에서 인프라 인스턴스가 반복적으로 종료된 것으로 표시되는 경우 원인은 구성과 관련이 있을 수 있으며 인프라 인스턴스 유형에 따라 달라집니다. 다음은 원인을 확인하는 방법입니다.

Amazon EC2 콘솔에서 vdc 컨트롤러 인스턴스가 반복적으로 종료된 상태를 표시하는 경우 잘못된 Secret 태그 때문일 수 있습니다. 에서 관리하는 보안 암호에는 인프라 Amazon EC2 인스턴스에 연결된 IAM 액세스 제어 정책의 일부로 사용되는 태그가 RES 있습니다. vdc 컨트롤러가 순환 중이고 CloudWatch 로그 그룹에 다음 오류가 나타나는 경우, 보안 암호에 태그가 올바르게 지정되지 않았기 때문일 수 있습니다. 보안 암호에 다음 태그를 지정해야 합니다.

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

이 오류에 대한 Amazon CloudWatch 로그 메시지는 다음과 비슷하게 표시됩니다.

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

Amazon EC2 인스턴스의 태그를 확인하고 위 목록과 일치하는지 확인합니다.

.....

AD 가입 실패로 인해 vdc 컨트롤러 인스턴스가 순환 중입니다. / eVDI 모듈에 API 상태 확인 실패가 표시됩니다.

eVDI 모듈이 상태 확인에 실패하면 환경 상태 섹션에 다음이 표시됩니다.

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

이 경우 디버깅의 일반적인 경로는 클러스터 관리자 CloudWatch 로그를 살펴보는 것입니다. (이라는 로그 그룹을 찾습니다`<env-name>/cluster-manager`.)

가능한 문제:

- 로그에 텍스트 가 포함된 경우 res 스택이 생성될 때 지정된 ServiceAccount 사용자 이름의 철자가 올바른지 `Insufficient permissions`확인합니다.

  로그 라인 예:

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

  - SecretsManager 콘솔 에서 RES 배포 중에 제공된 ServiceAccount 사용자 이름에 액세스할 수 있습니다. Secrets 관리자에서 해당 보안 암호를 찾고 일반 텍스트 검색을 선택합니다. 사용자 이름이 잘못된 경우 편집을 선택하여 보안 암호 값을 업데이트합니다. 현재 클러스터 관리자 및 vdc 컨트롤러 인스턴스를 종료합니다. 새 인스턴스는 안정적인 상태로 표시됩니다.
  - 제공된 외부 리소스 스택 에서 생성한 리소스를 사용하는 경우 사용자 이름은 “ServiceAccount”여야 합니다. 를 배포하는 동안 `DisableADJoin` 파라미터가 False로 설정된 경우 “ServiceAccount” 사용자에게 AD에서 컴퓨터 객체를 생성할 수 있는 권한이 있는지 RES확인합니다.
- 사용된 사용자 이름이 정확했지만 로그에 텍스트가 포함된 `Invalid credentials`경우 입력한 암호가 잘못되었거나 만료되었을 수 있습니다.

  로그 라인 예:

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

  - Secrets Manager 콘솔에 암호를 저장하는 보안 암호에 액세스하여 env 생성 중에 입력한 암호를 읽을 수 있습니다. 보안 암호(예: `<env_name>directoryserviceServiceAccountPassword`)를 선택하고 일반 텍스트 검색을 선택합니다.
  - 보안 암호의 암호가 잘못된 경우 편집을 선택하여 보안 암호의 값을 업데이트합니다. 현재 클러스터 관리자 및 vdc 컨트롤러 인스턴스를 종료합니다. 새 인스턴스는 업데이트된 암호를 사용하고 안정적인 상태로 나타납니다.
  - 암호가 올바른 경우 연결된 Active Directory에서 암호가 만료되었을 수 있습니다. 먼저 Active Directory에서 암호를 재설정한 다음 보안 암호를 업데이트해야 합니다. 디렉터리 서비스 콘솔 에서 Active Directory의 사용자 암호를 재설정할 수 있습니다.

1. 적절한 디렉터리 ID 선택
2. 작업 , 사용자 암호 재설정을 선택한 다음 사용자 이름(예: “ServiceAccount”)과 새 암호로 양식을 작성합니다.
3. 새로 설정한 암호가 이전 암호와 다른 경우 해당 Secret Manager 암호(예: `<env_name>directoryserviceServiceAccountPassword`.
4. 현재 클러스터 관리자 및 vdc 컨트롤러 인스턴스를 종료합니다. 새 인스턴스는 안정적인 상태로 표시됩니다.

.....

프로젝트를 추가하기 위해 소프트웨어 스택을 편집할 때 풀다운에 프로젝트가 표시되지 않습니다.

이 문제는 사용자 계정을 AD와 동기화하는 것과 관련된 다음 문제와 관련이 있을 수 있습니다. 이 문제가 나타나면 클러스터 관리자 Amazon CloudWatch 로그 그룹에서 오류 “`<user-home-init> account not available yet. waiting for user to be synced`”를 확인하여 원인이 동일한지 또는 관련이 있는지 확인합니다.

.....

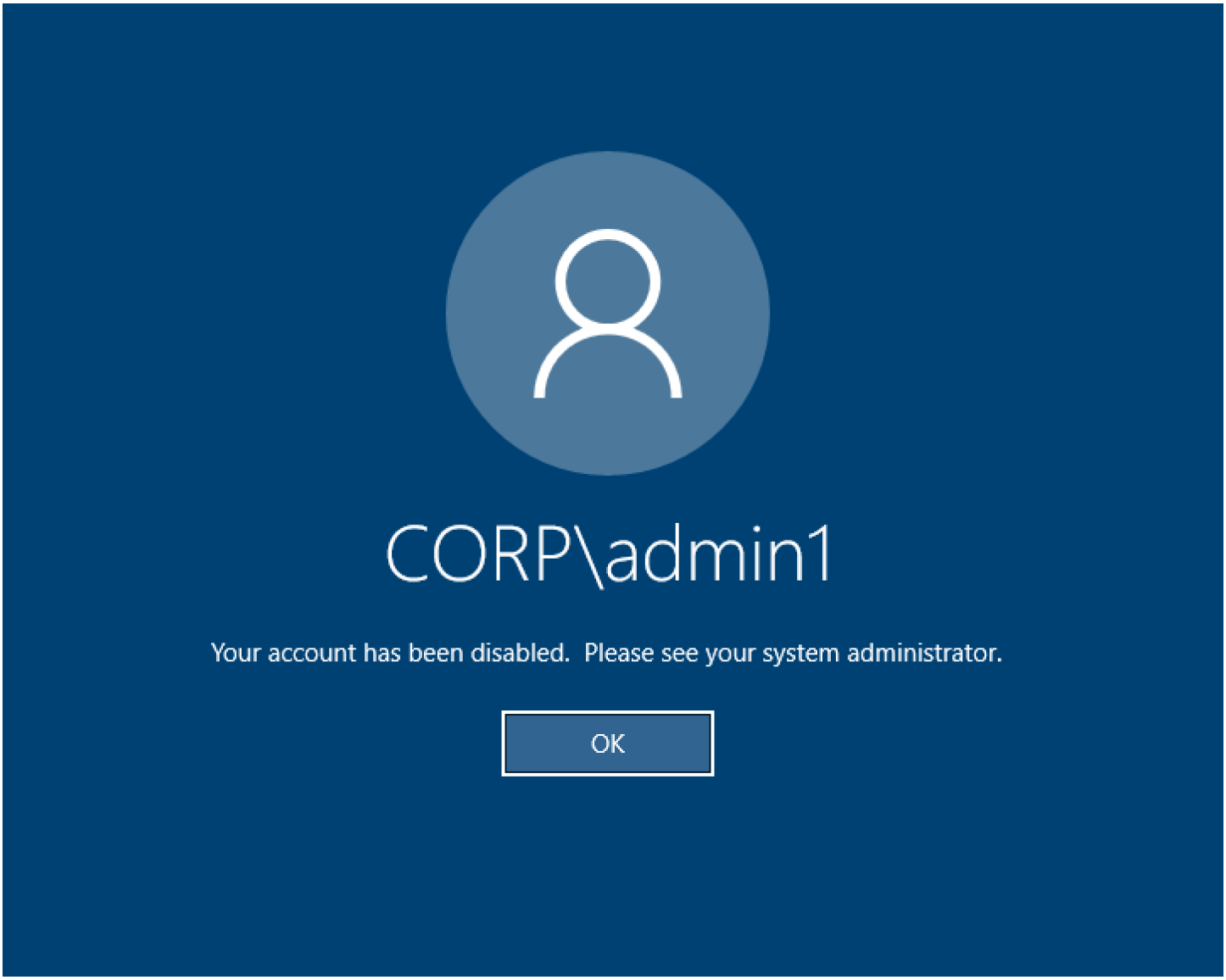
cluster-manager Amazon CloudWatch 로그에 “<user-home-init> 계정을 아직 사용할 수 없습니다. 사용자가 동기화될 때까지 대기”(계정이 사용자 이름인 경우)가 표시됩니다.

SQS 구독자는 사용자 계정에 연결할 수 없으므로 사용 중이며 무한 루프에 갇혀 있습니다. 이 코드는 사용자 동기화 중에 사용자를 위한 홈 파일 시스템을 생성하려고 할 때 트리거됩니다.

사용자 계정에 가져올 수 없는 이유는 사용 중인 AD에 대해 올바르게 구성되지 RES 않았기 때문일 수 있습니다. 예를 들어 BI/RES환경 생성에 사용된 `ServiceAccountCredentialsSecretArn` 파라미터가 올바른 값이 아니었을 수 있습니다.

.....

로그인 시도 시 Windows 데스크톱에 “계정이 비활성화되었습니다. 관리자에게 문의하세요.”



사용자가 잠긴 화면에 다시 로그인할 수 없는 경우 를 통해 성공적으로 로그인한 RES 후 사용자가 에 구성된 AD에서 비활성화되었음을 나타낼 수 있습니다SSO.

AD에서 사용자 계정이 비활성화된 경우 SSO 로그인이 실패합니다.

.....

DHCP 외부/고객 AD 구성의 옵션 문제

자체 Active Directory"The connection has been closed. Transport error"와 함께 를 사용할 때 Windows 가상 데스크톱RES에서 라는 오류가 발생하면 Amazon CloudWatch 로그에서 dcv-connection-gateway 다음과 유사한 항목을 확인합니다.

```
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
```

자체 의 DHCP 옵션에 AD 도메인 컨트롤러를 사용하는 경우 다음을 VPC수행해야 합니다.

1. 두 도메인 컨트롤러 에 를 추가합니다 AmazonProvidedDNSIPs.
2. 도메인 이름을 ec2.internal로 설정합니다.

여기에 예제가 나와 있습니다. 이 구성이 없으면 RES/DCV에서 ip-10-0-x-xx.ec2.internal 호스트 이름을 찾기 때문에 Windows 데스크톱에서 전송 오류 가 발생합니다.

.....

Firefox 오류 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Firefox 웹 브라우저를 사용하면 가상 데스크톱에 연결을 시도할 때 오류 메시지 유형 MOZILLA_PKIX_ERROR_REQUIREDTLS_FEATURE_가MISSING 발생할 수 있습니다.

원인은 RES 웹 서버가 TLS + Stapling On으로 설정되었지만 Stapling Validation으로 응답하지 않기 때문입니다(https://support.mozilla.org/en-US/questions/ 참조1372483.

https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing의 지침에 따라 이 문제를 해결할 수 있습니다.

.....

Env 삭제

주제

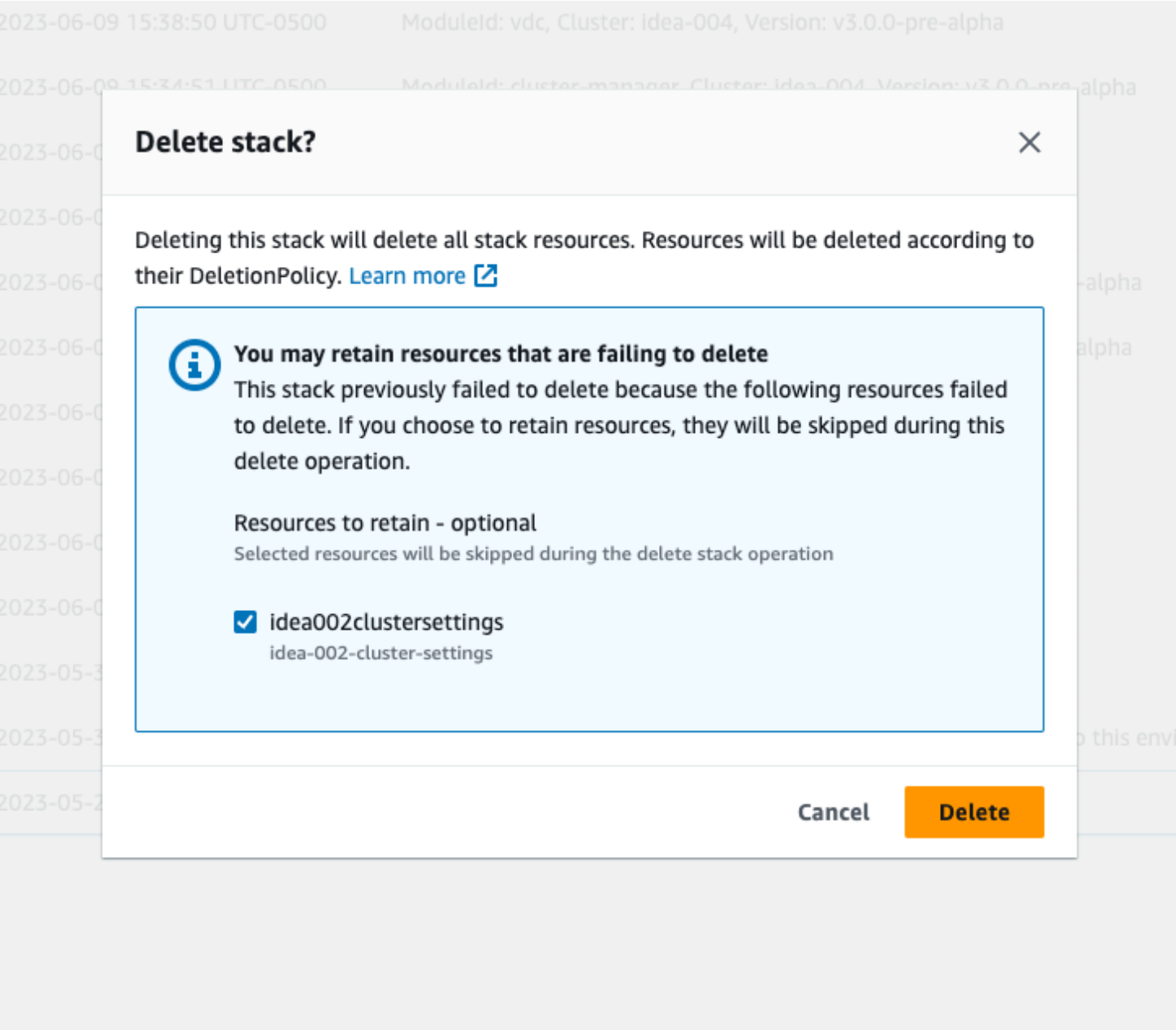
- res-xxx-cluster 스택이 “DELETE_FAILED” 상태이고 “역할이 유효하지 않거나 가정할 수 없음” 오류로 인해 수동으로 삭제할 수 없습니다.
- 로그 수집
- VDI 로그 다운로드
- Linux EC2 인스턴스에서 로그 다운로드
- Windows EC2 인스턴스에서 로그 다운로드
- WaitCondition 오류에 대한 ECS 로그 수집

.....

res-xxx-cluster 스택이 “DELETE_FAILED” 상태이고 “역할이 유효하지 않거나 가정할 수 없음” 오류로 인해 수동으로 삭제할 수 없습니다.

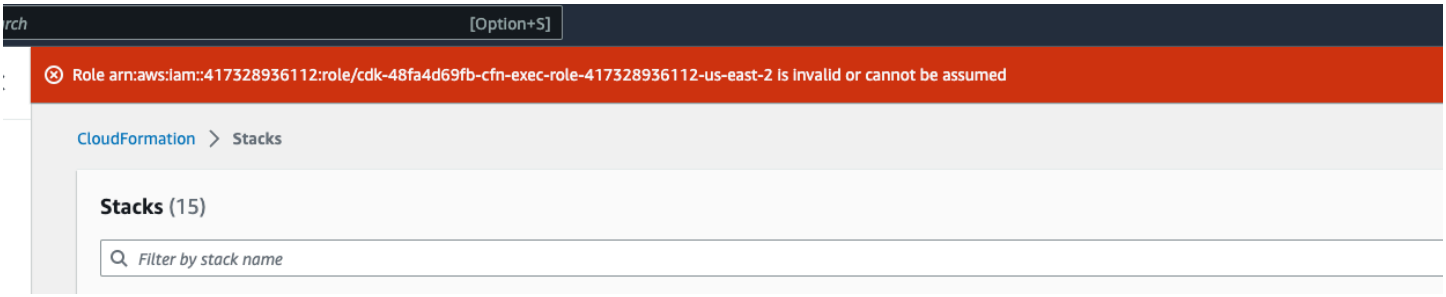
“스택res-xxx-cluster”이 “DELETE_FAILED” 상태이고 수동으로 삭제할 수 없는 경우 다음 단계를 수행하여 삭제할 수 있습니다.

스택이 “DELETE_FAILED” 상태로 표시되면 먼저 수동으로 삭제해 보세요. 스택 삭제를 확인하는 대화 상자가 표시될 수 있습니다. Delete(삭제)를 선택합니다.



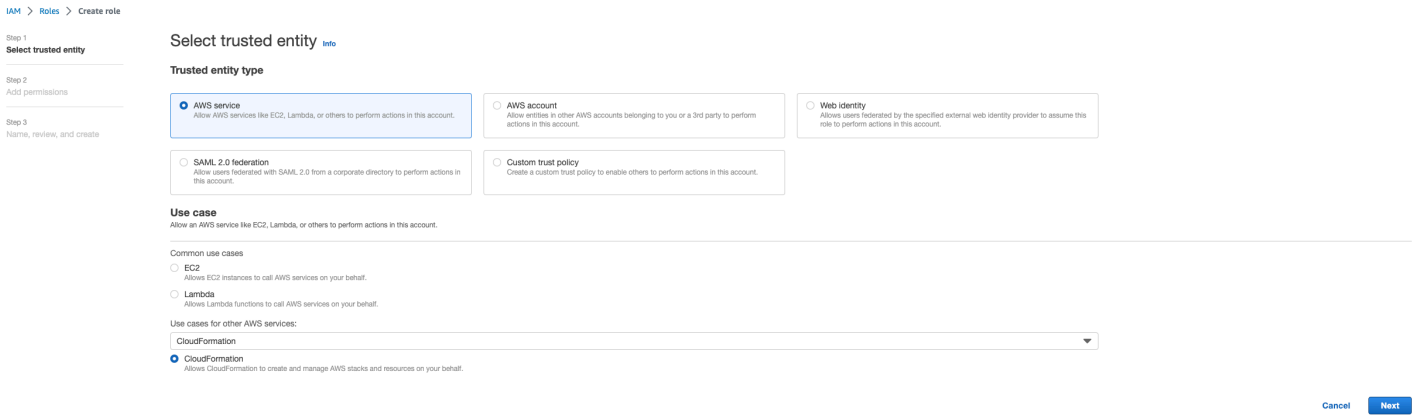
경우에 따라 필요한 스택 리소스를 모두 삭제하더라도 보존할 리소스를 선택하는 메시지가 계속 표시될 수 있습니다. 이 경우 모든 리소스를 '보존할 리소스'로 선택하고 삭제를 선택합니다.

다음과 같은 오류가 표시될 수 있습니다. `Role: arn:aws:iam::... is Invalid or cannot be assumed`

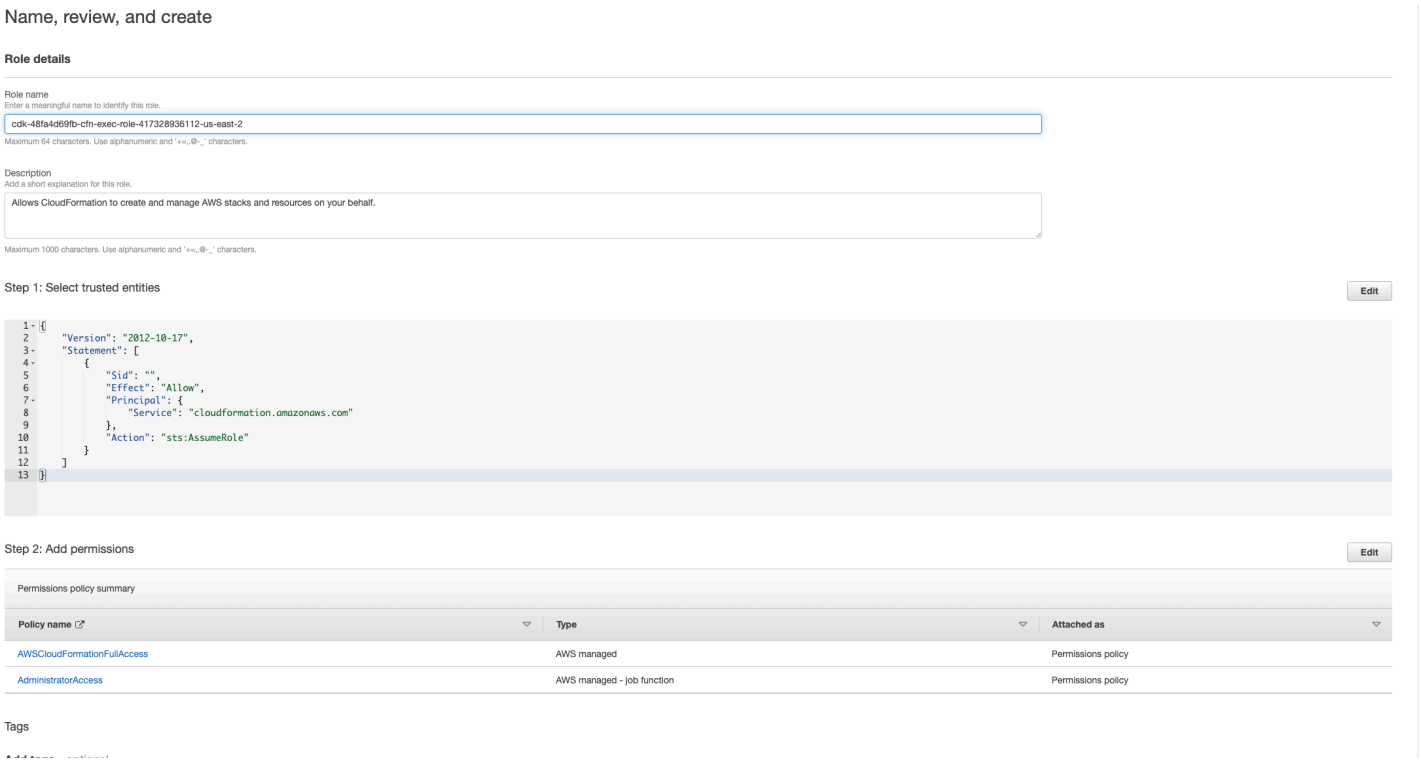


즉, 스택을 삭제하는 데 필요한 역할이 스택 전에 먼저 삭제됩니다. 이를 해결하려면 역할 이름을 복사합니다. IAM 콘솔로 이동하여 다음과 같은 파라미터를 사용하여 해당 이름의 역할을 생성합니다.

- 신뢰할 수 있는 엔터티 유형에서 AWS 서비스 를 선택합니다.
- 사용 사례 에서 를 `Use cases for other AWS services` 선택합니다`CloudFormation`.



Next(다음)를 선택합니다. 역할 'AWSCloudFormationFullAccess' 및 'AdministratorAccess' 권한을 부여해야 합니다. 검토 페이지는 다음과 같아야 합니다.



그런 다음 CloudFormation 콘솔로 돌아가 스택을 삭제합니다. 이제 역할을 생성한 후 삭제할 수 있습니다. 마지막으로 IAM 콘솔로 이동하여 생성한 역할을 삭제합니다.

.....

로그 수집

EC2 콘솔에서 EC2 인스턴스에 로그인

- 다음 지침에 따라 Linux EC2 인스턴스에 로그인합니다.
- 다음 지침에 따라 Windows EC2 인스턴스에 로그인합니다. 그런 다음 Windows PowerShell 를 열어 명령을 실행합니다.

인프라 호스트 로그 수집

1. 클러스터 관리자: 다음 위치에서 클러스터 관리자의 로그를 가져와 티켓에 연결합니다.
   a. 로그 그룹 의 모든 CloudWatch 로그입니다`<env-name>/cluster-manager`.
   b. `<env-name>-cluster-manager` EC2 인스턴스의 `/root/bootstrap/logs` 디렉터리에 있는 모든 로그입니다. 이 섹션의 시작 부분에 있는 “EC2콘솔에서 EC2 인스턴스에 로그인”에서 에 연결된 지침에 따라 인스턴스에 로그인합니다.

2. Vdc 컨트롤러: 다음 위치에서 vdc 컨트롤러의 로그를 가져와 티켓에 연결합니다.

   a. 로그 그룹 의 모든 CloudWatch 로그입니다`<env-name>/vdc-controller`.

   b. `<env-name>-vdc-controller` EC2 인스턴스의 `/root/bootstrap/logs` 디렉터리에 있는 모든 로그입니다. 이 섹션의 시작 부분에 있는 “EC2콘솔에서 EC2 인스턴스에 로그인”에서 에 연결된 지침에 따라 인스턴스에 로그인합니다.

로그를 쉽게 가져오는 방법 중 하나는 Linux EC2 인스턴스에서 로그 다운로드 섹션의 지침을 따르는 것입니다. 모듈 이름은 인스턴스 이름입니다.

VDI 로그 수집

해당 Amazon EC2 인스턴스 식별

사용자가 세션 이름이 VDI 인 를 시작한 경우 Amazon EC2 콘솔에서 인스턴스의 `VDI1`해당 이름은 입니다`<env-name>-VDI1-<user name>`.

Linux VDI 로그 수집

이 섹션의 시작 부분에 있는 “EC2콘솔에서 EC2 인스턴스 로그인”에 연결된 지침에 따라 Amazon EC2 콘솔에서 해당 Amazon EC2 인스턴스에 로그인합니다. VDI Amazon EC2 인스턴스의 `/root/bootstrap/logs` 및 `/var/log/dcv/` 디렉터리에서 모든 로그를 가져옵니다.

로그를 가져오는 방법 중 하나는 s3에 로그를 업로드한 다음 거기서 다운로드하는 것입니다. 이를 위해 다음 단계에 따라 하나의 디렉터리에서 모든 로그를 가져온 다음 업로드할 수 있습니다.

1. `/root/bootstrap/logs` 디렉터리 아래에 dcv 로그를 복사하려면 다음 단계를 따르세요.

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

2. 이제 다음 섹션 -에 나열된 단계에 따라 로그VDI 로그 다운로드를 다운로드합니다.

Windows VDI 로그 수집

이 섹션의 시작 부분에 있는 “EC2콘솔에서 EC2 인스턴스 로그인”에 연결된 지침에 따라 Amazon EC2 콘솔에서 해당 Amazon EC2 인스턴스에 로그인합니다. VDI EC2 인스턴스의 `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` 디렉터리에서 모든 로그를 가져옵니다.

로그를 가져오는 방법 중 하나는 S3에 로그를 업로드한 다음 거기서 다운로드하는 것입니다. 이렇게 하려면 다음 섹션 - 에 나열된 단계를 따릅니다VDI 로그 다운로드.

.....

VDI 로그 다운로드

1. S3 액세스를 허용하도록 VDI EC2 인스턴스 IAM 역할을 업데이트합니다.
2. EC2 콘솔로 이동하여 VDI 인스턴스를 선택합니다.
3. 사용 중인 IAM 역할을 선택합니다.
4. 권한 추가 드롭다운 메뉴의 권한 정책 섹션에서 정책 연결을 선택한 다음 AmazonS3FullAccess 정책을 선택합니다.
5. 권한 추가를 선택하여 해당 정책을 연결합니다.
6. 그런 다음 VDI 유형에 따라 아래 나열된 단계에 따라 로그를 다운로드합니다. 모듈 이름은 인스턴스 이름입니다.
   a. Linux EC2 인스턴스에서 로그 다운로드 Linux용.
   b. Windows EC2 인스턴스에서 로그 다운로드 Windows용.
7. 마지막으로 역할을 편집하여 `AmazonS3FullAccess` 정책을 제거합니다.

> **Note**
>
> 모두 와 동일한 IAM 역할을 VDIs 사용합니다. `<env-name>-vdc-host-role-<region>`

.....

Linux EC2 인스턴스에서 로그 다운로드

로그를 다운로드하려는 EC2 인스턴스에 로그인하고 다음 명령을 실행하여 모든 로그를 s3 버킷에 업로드합니다.

```
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
```

그런 다음 S3 콘솔로 이동하여 이름이 인 버킷을 선택하고 이전에 업로드한 <module_name>_logs.tar.gz 파일을 <environment_name>-cluster-<region>-<aws_account_number> 다운로드합니다.

.....

Windows EC2 인스턴스에서 로그 다운로드

로그를 다운로드하려는 EC2 인스턴스에 로그인하고 다음 명령을 실행하여 모든 로그를 S3 버킷에 업로드합니다.

```
$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
```

그런 다음 S3 콘솔로 이동하여 이름이 인 버킷을 선택하고 이전에 업로드한 <module_name>_logs.zip 파일을 <environment_name>-cluster-<region>-<aws_account_number> 다운로드합니다.

.....

WaitCondition 오류에 대한 ECS 로그 수집

1. 배포된 스택으로 이동하여 리소스 탭을 선택합니다.
2. 배포 → ResearchAndEngineeringStudio → 설치 관리자 → 작업 → CreateTaskDef → CreateContainer → 를 확장LogGroup하고 로그 그룹을 선택하여 CloudWatch 로그를 엽니다.

3. 이 로그 그룹에서 최신 로그를 가져옵니다.

데모 환경

주제

- 자격 증명 공급자에 대한 인증 요청을 처리할 때 데모 환경 로그인 오류 발생

자격 증명 공급자에 대한 인증 요청을 처리할 때 데모 환경 로그인 오류 발생

문제

로그인을 시도하고 '자격 증명 공급자에 대한 인증 요청을 처리할 때 예기치 않은 오류'가 발생하면 암호가 만료될 수 있습니다. 로그인하려는 사용자의 암호 또는 Active Directory 서비스 계정일 수 있습니다.

완화

1. 디렉터리 서비스 콘솔 에서 사용자 및 서비스 계정 암호를 재설정합니다.
2. 위에 입력한 새 암호와 일치하도록 Secrets Manager의 서비스 계정 암호를 업데이트합니다.
   - Keycloak 스택의 경우: PasswordSecret-...-RESExternal-...-DirectoryService... 설명: Microsoft Active Directory용 암호
   - 용RES: res-ServiceAccountPassword-... 설명: Active Directory 서비스 계정 암호
3. EC2 콘솔로 이동하여 클러스터 관리자 인스턴스를 종료합니다. Auto Scaling 규칙은 새 인스턴스 배포를 자동으로 트리거합니다.

알려진 문제

- 알려진 문제 2024.x
  - (2024.08) 가상 데스크톱이 루트 버킷 ARN 및 사용자 지정 접두사로 읽기/쓰기 Amazon S3 버킷을 탑재하지 못함

- (2024.06) AD 그룹 이름에 공백이 포함된 경우 스냅샷 적용 실패
- (2024.04-2024.04.02) VDI 인스턴스 역할에 연결되지 않은 제공된 IAM 권한 경계
- (2024.04.02 이하) ap-southeast-2(Sydney)의 Windows NVIDIA 인스턴스가 시작되지 않음
- (2024.04 및 2024.04.01) 에서 RES 삭제 실패 GovCloud
- (2024년 4월 - 2024.04.02) 재부팅 시 Linux 가상 데스크톱이 “RESUMING” 상태에서 중단될 수 있습니다.
- (2024.04.02 이하) SAMAccountName 속성에 대문자 또는 특수 문자가 포함된 AD 사용자를 동기화하지 못함
- (2024.04.02 이하) Bastion 호스트에 액세스하기 위한 프라이빗 키가 유효하지 않습니다.
- (2024.06 이하) AD 동기화 RES 중에 그룹 멤버가 에 동기화되지 않음
- (2024.06 이하) CVE-2024-6387, R egreSSHion, RHEL9 및 Ubuntu의 보안 취약성 VDIs

알려진 문제 2024.x

.....

(2024.08) 가상 데스크톱이 루트 버킷 ARN 및 사용자 지정 접두사로 읽기/쓰기 Amazon S3 버킷을 탑재하지 못함

버그 설명

Research and Engineering Studio 2024.08은 루트 버킷(즉, VDI) 및 사용자 지정 접두사 ARN(프로젝트 이름 또는 프로젝트 이름 및 사용자 이름)를 사용할 때 가상 데스크톱 인프라(`arn:aws:s3:::example-bucket`) 인스턴스에 읽기/쓰기 S3 버킷을 탑재하지 못합니다.

이 문제의 영향을 받지 않는 버킷 구성은 다음과 같습니다.

- 읽기 전용 버킷
- 버킷의 일부로 접두사가 있는 읽기/쓰기 버킷ARN(즉, `arn:aws:s3:::example-bucket/example-folder-prefix`) 및 사용자 지정 접두사(프로젝트 이름 또는 프로젝트 이름 및 사용자 이름)
- 루트 버킷이 있는 읽기/쓰기 버킷 ARN, 사용자 지정 접두사 없음

VDI 인스턴스를 프로비저닝한 후에는 해당 S3 버킷에 지정된 탑재 디렉터리에 버킷이 탑재되지 않습니다. 의 탑재 디렉터리VDI가 있더라도 디렉터리는 비어 있고 버킷의 현재 내용이 포함되지 않습니다.

터미널을 사용하여 디렉터리에 파일을 쓰면 오류가 `Permission denied, unable to write a file` 발생하고 파일 내용이 해당 S3 버킷에 업로드되지 않습니다.

영향을 받는 버전

2024년 8월

완화

1. 패치 스크립트 및 패치 파일(`patch.py` 및 `s3_mount_custom_prefix_fix.patch`)을 다운로드하려면 다음 명령을 실행하여 패치 스크립트 및 패치 파일을 다운로드할 `<output-directory>` 디렉터리`<environment-name>`와 RES 환경 이름으로 바꿉니다.

   a. 패치는 RES 2024.08에만 적용됩니다.

   b. 패치 스크립트에는 AWS CLI v2, Python 3.9.16 이상 및 Boto3가 필요합니다.

   c. RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 Amazon S3 권한이 있는지 확인합니다RES.

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

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

2. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행합니다.

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. 환경의 Virtual Desktop Controller(vdc-controller) 인스턴스를 종료하려면 다음 명령을 실행합니다. (첫 번째 단계에서 RES 변수를 환경 `ENVIRONMENT_NAME` 이름으로 이미 설정했습니다.)

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
```

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

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

> **Note**
>
> 프라이빗 VPC 설정의 경우 아직 설정하지 않은 경우 `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda` 함수의 경우 이름과 `AWS_STS_REGIONAL_ENDPOINTS` 값이 `Environment variable` 인 를 추가해야 합니다`regional`. 자세한 내용은 격리된 VPC 배포를 위한 Amazon S3 버킷 사전 조건 섹션을 참조하세요.

4. 이름으로 시작하는 대상 그룹이 정상 *<RES-EnvironmentName>*`-vdc-ext` 상태가 되면 루트 버킷ARN과 사용자 지정 접두사가 올바르게 장착된 읽기/쓰기 S3 버킷을 새로 시작해야 VDIs 합니다.

.....

(2024.06) AD 그룹 이름에 공백이 포함된 경우 스냅샷 적용 실패

문제

RES AD 그룹에 이름에 공백이 포함된 경우 2024.06은 이전 버전의 스냅샷을 적용하지 못합니다.

클러스터 관리자 CloudWatch 로그(`<environment-name>/cluster-manager`로그 그룹 아래)에는 AD 동기화 중에 다음 오류가 포함됩니다.

```
[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)$
```

다음 요구 사항을 충족하는 그룹 이름RES만 수락하면 오류가 발생합니다.

- 소문자와 대문자ASCII, 숫자, 대시(-), 마침표(.) 및 밑줄(_)만 포함할 수 있습니다.
- 대시(-)는 첫 번째 문자로 허용되지 않습니다.
- 공백은 포함할 수 없습니다.

영향을 받는 버전

2024년 6월

완화

1. 패치 스크립트 및 패치 파일(patch.py 및 groupname_regex.patch)을 다운로드하려면 다음 명령을 실행하여 파일을 넣을 <output-directory> 디렉터리<environment-name>와 RES 환경 이름으로 바꿉니다.

   a. 패치는 RES 2024.06에만 적용됩니다.

   b. 패치 스크립트에는 AWS CLI v2, Python 3.9.16 이상 및 Boto3가 필요합니다.

   c. RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.

```
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. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행합니다.

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

3. 환경의 Cluster Manager 인스턴스를 다시 시작하려면 다음 명령을 실행합니다. Amazon EC2 Management Console에서 인스턴스를 종료할 수도 있습니다.

```
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**
>
> 패치를 사용하면 AD 그룹 이름에 소문자와 대문자ASCII, 숫자, 대시(-), 마침표(.), 밑줄(_), 총 길이가 1~30인 공백을 포함할 수 있습니다.

.....

(2024.04-2024.04.02) VDI 인스턴스 역할에 연결되지 않은 제공된 IAM 권한 경계

문제

가상 데스크톱 세션이 프로젝트의 권한 경계 구성을 제대로 상속하지 않습니다. 이는 프로젝트 생성 중에 IAMPermissionBoundary 파라미터가 프로젝트에 제대로 할당되지 않아 정의된 권한 경계의 결과입니다.

영향을 받는 버전

2024년 4월 - 2024.04.02

완화

VDIs 가 프로젝트에 할당된 권한 경계를 적절하게 상속하도록 하려면 다음 단계를 따르세요.

1. 패치 스크립트 및 패치 파일(patch.py 및 vdi_host_role_permission_boundary.patch)을 다운로드하려면 다음 명령을 실행하여 파일을 넣을 로컬 디렉터리<output-directory>로 바꿉니다.

   a. 패치는 RES 2024.04.02에만 적용됩니다. 버전 2024.04 또는 2024.04.01을 사용하는 경우 일반 문서에 나열된 단계에 따라 마이너 버전 업데이트를 수행하여 환경을 2024.04.02로 업데이트할 수 있습니다.

   b. 패치 스크립트에는 AWS CLI v2), Python 3.9.16 이상 및 Boto3가 필요합니다.

   c. RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.

```
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. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행<environment-name>하여 를 RES 환경 이름으로 바꿉니다.

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

3. 이 명령을 실행하고 를 환경 이름으로 바꾸어 RES 환경에서 클러스터 관리자 인스턴스<environment-name>를 다시 시작합니다. Amazon EC2 Management Console에서 인스턴스를 종료할 수도 있습니다.

```
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 이하) ap-southeast-2(Sydney)의 Windows NVIDIA 인스턴스가 시작되지 않음

문제

Amazon Machine Images(AMIs)는 특정 구성으로 에서 가상 데스크톱(VDIs)을 스핀 업RES하는 데 사용됩니다. 각 AMI 에는 리전마다 다른 연결된 ID가 있습니다. ap-southeast-2(Sydney)에서 Windows Nvidia 인스턴스를 시작RES하도록 에 구성된 AMI ID가 현재 올바르지 않습니다.

AMI이 유형의 인스턴스 구성에 `ami-0e190f8939a996caf` 대한 -ID가 ap-southeast-2(Sydney)에 잘못 나열되었습니다. AMI 대신 ID를 사용해야 `ami-027cf6e71e2e442f4` 합니다.

사용자는 기본 ami-0e190f8939a996caf 로 인스턴스를 시작하려고 할 때 다음과 같은 오류가 발생합니다AMI.

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

예제 구성 파일을 포함하여 버그를 복제하는 단계:

- ap-southeast-2 리전RES에 배포합니다.
- Windows 기본NVIDIA 소프트웨어 스택(AMI ID)을 사용하여 인스턴스를 시작합니다ami-0e190f8939a996caf.

영향을 받는 버전

모든 RES 버전 2024.04.02 이하가 영향을 받습니다.

완화

버전 RES 2024.01.01에서 다음 완화 조치가 테스트되었습니다.

- 다음 설정을 사용하여 새 소프트웨어 스택 등록
  - AMI ID: ami-027cf6e71e2e442f4
  - 운영 체제: Windows
  - GPU 제조업체: NVIDIA
  - 최소 스토리지 크기(GB): 30
  - 최소 RAM (GB): 4
- 이 소프트웨어 스택을 사용하여 Windows 인스턴스NVIDIA 시작

.....

(2024.04 및 2024.04.01) 에서 RES 삭제 실패 GovCloud

문제

RES 삭제 워크플로 중에 UnprotectCognitoUserPool Lambda는 나중에 삭제될 Cognito 사용자 풀에 대한 삭제 방지를 비활성화합니다. Lambda 실행은 에서 시작합니다InstallerStateMachine.

상용 버전과 GovCloud 리전 간의 기본 AWS CLI 버전 차이로 인해 Lambda의 update_user_pool 호출은 GovCloud 리전에서 실패합니다.

GovCloud 리전RES에서 삭제를 시도할 때 고객에게 다음과 같은 오류가 발생합니다.

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

버그를 복제하는 단계:

- GovCloud 리전RES에 배포
- RES 스택 삭제

영향을 받는 버전

RES 버전 2024.04 및 2024.04.01

완화

버전 RES 2024.04에서 다음 완화 조치가 테스트되었습니다.

- `UnprotectCognitoUserPool` Lambda 열기
  - 명명 규칙: *`<env-name>`*`-InstallerTasksUnprotectCognitoUserPool-...`
- 런타임 설정 -> 편집 -> 런타임 선택 `Python 3.11` -> 저장 .
- 를 엽니다 CloudFormation.
- RES 스택 삭제 -> 설치 관리자 리소스 유지 UNCHECKED -> 삭제 를 그대로 둡니다.

.....

(2024년 4월 - 2024.04.02) 재부팅 시 Linux 가상 데스크톱이 “RESUMING” 상태에서 중단될 수 있습니다.

문제

Linux 가상 데스크톱은 수동 또는 예약된 중지 후 다시 시작할 때 “RESUMING” 상태로 중단될 수 있습니다.

인스턴스를 재부팅한 후 AWS Systems Manager는 원격 명령을 실행하여 새 DCV 세션을 생성하지 않으며 vdc 컨트롤러 CloudWatch 로그(로그 그룹 아래)에 다음 `<environment-name>/vdc/controller` CloudWatch 로그 메시지가 누락되었습니다.

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

영향을 받는 버전

2024년 4월 - 2024.04.02

완화

“RESUMING” 상태에서 멈춘 가상 데스크톱을 복구하려면:

1. SSH EC2 콘솔에서 문제 인스턴스로 이동합니다.
2. 인스턴스에서 다음 명령을 실행합니다.

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

3. 인스턴스가 재부팅될 때까지 기다립니다.

새 가상 데스크톱이 동일한 문제로 실행되지 않도록 하려면:

1. 패치 스크립트 및 패치 파일(patch.py 및 vdi_stuck_in_resuming_status.patch)을 다운로드하려면 다음 명령을 실행하여 파일을 넣을 디렉터리`<output-directory>`로 바꿉니다.

> **Note**
>
> - 패치는 RES 2024.04.02에만 적용됩니다.
> - 패치 스크립트에는 AWS CLI v2, Python 3.9.16 이상 및 Boto3가 필요합니다.
> - RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.

```
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. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행<environment-name>하여 를 RES 환경 이름 및 가 RES 배포된 리전<aws-region>으로 바꿉니다.

```
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. 환경의 VDC 컨트롤러 인스턴스를 다시 시작하려면 다음 명령을 실행<environment-name>하고 를 RES 환경 이름으로 바꿉니다.

```
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 이하) SAMAccountName 속성에 대문자 또는 특수 문자가 포함된 AD 사용자를 동기화하지 못함

문제

RES SSO가 최소 2시간(AD 동기화 주기 2회) 동안 설정된 후 가 AD 사용자를 동기화하지 못합니다. 클러스터 관리자 CloudWatch 로그(<environment-name>/cluster-manager로그 그룹 아래)에는 AD 동기화 중 다음과 같은 오류가 포함됩니다.

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

이 오류는 다음 요구 사항을 충족하는 SAMAccount 사용자 이름RES만 수락하면 발생합니다.

- 소ASCII문자, 숫자, 마침표(.), 밑줄(_)만 포함할 수 있습니다.
- 마침표 또는 밑줄은 첫 번째 또는 마지막 문자로 허용되지 않습니다.
- 두 개의 연속 마침표 또는 밑줄(예: .., __, ._, _.)을 포함할 수 없습니다.

영향을 받는 버전

2024.04.02 이하

완화

1. 패치 스크립트 및 패치 파일(patch.py 및 samaccountname_regex.patch)을 다운로드하려면 다음 명령을 실행하여 파일을 넣을 디렉터리<output-directory>로 바꿉니다.

   > **Note**
   >
   > - 패치는 RES 2024.04.02에만 적용됩니다.
   > - 패치 스크립트에는 AWS CLI v2, Python 3.9.16 이상 및 Boto3가 필요합니다.
   > - RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.

   ```
   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. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행<environment-name>하여 를 RES 환경 이름으로 바꿉니다.

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

3. 환경의 Cluster Manager 인스턴스를 다시 시작하려면 다음 명령을 실행<environment-name>하고 를 RES 환경 이름으로 바꿉니다. Amazon EC2 Management Console에서 인스턴스를 종료할 수도 있습니다.

```
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 이하) Bastion 호스트에 액세스하기 위한 프라이빗 키가 유효하지 않습니다.

문제

사용자가 프라이빗 키를 다운로드하여 RES 웹 포털에서 Bastion 호스트에 액세스하면 키의 형식이 좋지 않습니다. 여러 줄이 단일 줄로 다운로드되므로 키가 무효화됩니다. 다운로드한 키로 Bastion 호스트에 액세스하려고 하면 사용자에게 다음과 같은 오류가 발생합니다.

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

영향을 받는 버전

2024.04.02 이하

완화

이 브라우저는 영향을 받지 않으므로 Chrome을 사용하여 키를 다운로드하는 것이 좋습니다.

또는 뒤에 새 줄을 생성하고 바로 앞에 `-----BEGIN PRIVATE KEY-----` 다른 새 줄을 생성하여 키 파일을 다시 포맷할 수 있습니다`-----END PRIVATE KEY-----`.

.....

(2024.06 이하) AD 동기화 RES 중에 그룹 멤버가 에 동기화되지 않음

버그 설명

GroupOU 다른 RES 경우 그룹 멤버는 와 제대로 동기화되지 않습니다. UserOU

RES 는 AD 그룹에서 사용자를 동기화하려고 할 때 ldapsearch 필터를 생성합니다. 현재 필터는 GroupOU 파라미터 대신 UserOU 파라미터를 잘못 사용합니다. GroupOU 그 결과 검색에서 사용자를 반환하지 못합니다. 이 동작은 UsersOU와 GroupOU가 다른 인스턴스에서만 발생합니다.

영향을 받는 버전

이 문제는 모든 RES 버전 2024.06 이하에 적용됩니다.

완화

다음 단계에 따라 문제를 해결합니다.

1. patch.py 스크립트 및 group_member_sync_bug_fix.patch 파일을 다운로드하려면 다음 명령을 실행하고 파일을 다운로드하려는 `<output-directory>` 로컬 디렉터리`<res_version>`와 패치 RES하려는 버전으로 바꿉니다.

   > **Note**
   >
   > - 패치 스크립트에는 AWS CLI v2, Python 3.9.16 이상 및 Boto3가 필요합니다.
   > - RES 가 배포된 계정 및 리전에 대해 를 AWS CLI 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.
   > - 패치는 RES 버전 2024.04.02 및 2024.06만 지원합니다. 2024.04 또는 2024.04.01을 사용하는 경우 패치를 적용하기 전에 마이너 버전 업데이트에 나열된 단계에 따라 환경을 2024.04.02로 업데이트할 수 있습니다.
   >   - RES 버전: RES 2024.04.02
   >
   >   패치 다운로드 링크: 2024.04.02_group_member_sync_bug_fix.patch
   >   - RES 버전: RES 2024.06

패치 다운로드 링크: 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. 패치 스크립트와 패치 파일이 다운로드되는 디렉터리로 이동합니다. 다음 패치 명령을 실행<environment-name>하여 를 RES 환경 이름으로 바꿉니다.

```
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. 환경에 대한 클러스터 관리자 인스턴스를 다시 시작하려면 다음 명령을 실행합니다.

```
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 이하) CVE-2024-6387, R egreSSHion, RHEL9 및 Ubuntu의 보안 취약성 VDIs

버그 설명

라는 CVE-2024-6387regreSSHion이 오픈SSH 서버에서 식별되었습니다. 이 취약성을 통해 인증되지 않은 원격 공격자는 대상 서버에서 임의 코드를 실행할 수 있으므로 보안 통신을 위해 OpenSSH을 사용하는 시스템에 심각한 위험을 초래할 수 있습니다.

RES의 경우 표준 구성은 로 베이스 호스트를 통과하여 가상 데스크톱SSH으로 이동하는 것이며, 베이스 호스트는 이 취약성의 영향을 받지 않습니다. 그러나 ALL RES 버전에서 RHEL9 및 Ubuntu2024AMI(가상 데스크톱 인프라)에 대해 제공하는 기본VDIs(Amazon Machine Image)은 보안 위협에 취약한 오픈SSH 버전을 사용합니다.

즉, 기존 RHEL9 및 Ubuntu2024를 악용할 VDIs 수 있지만 공격자는 Bastion 호스트에 액세스해야 합니다.

문제에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

영향을 받는 버전

이 문제는 모든 RES 버전 2024.06 이하에 적용됩니다.

완화

RHEL9 및 Ubuntu 모두 보안 취약성을 수정하는 OpenSSH용 패치를 릴리스했습니다. 플랫폼의 해당 패키지 관리자를 사용하여 이러한 항목을 가져올 수 있습니다.

기존 RHEL9 또는 Ubuntu 가 있는 경우 아래 PATCH EXISTING VDIs 지침을 따르는 VDIs것이 좋습니다. 향후 를 패치하려면 PATCH FUTURE VDIs 지침을 따르는 VDIs것이 좋습니다. 이 지침에서는 스크립트를 실행하여 에 플랫폼 업데이트를 적용하는 방법을 설명합니다VDIs.

PATCH EXISTING VDIs

1. 기존 Ubuntu 및 RHEL9 를 모두 패치하는 다음 명령을 실행합니다VDIs.

   a. 패치 스크립트에는 AWS CLI v2가 필요합니다.

   b. RES 가 배포된 계정 및 리전에 대해 AWS CLI를 구성하고 AWS Systems Manager Run Command를 보낼 수 있는 Systems Manager 권한이 있는지 확인합니다.

```
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. 명령 실행 페이지에서 스크립트가 성공적으로 실행되었는지 확인할 수 있습니다. 명령 기록 탭을 클릭하고 최신 명령 ID를 선택한 다음 모든 인스턴스에 SUCCESS 메시지가 IDs 있는지 확인합니다.

PATCH FUTURE VDIs

1. 패치 스크립트 및 패치 파일(patch.py 및 update_openssh.patch)을 다운로드하려면 다음 명령을 실행하여 파일을 다운로드할 <output-directory> 디렉터리<environment-name>와 RES 환경 이름으로 바꿉니다.

> **Note**
>
> - 패치는 RES 2024.06에만 적용됩니다.
> - 패치 스크립트에는 AWS CLI v2), Python 3.9.16 이상 및 Boto3가 필요합니다.
> - RES 가 배포된 계정 및 리전에 대한 AWS CLI의 사본을 구성하고 에서 생성한 버킷에 쓸 수 있는 S3 권한이 있는지 확인합니다RES.

```
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. 다음 패치 명령을 실행합니다.

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

3. 다음 명령을 사용하여 환경의 VDC 컨트롤러 인스턴스를 다시 시작합니다.

```
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

패치 적용 미래VDIs는 RES 버전 2024.06 이상에서만 지원됩니다. 2024.06 이전 버전의 VDIs RES 환경에서 향후 패치를 적용하려면 먼저 의 지침에 따라 RES 환경을 2024.06으로 업그레이드합니다메이저 버전 업데이트.

.....

고지 사항

각 Amazon EC2 인스턴스에는 관리 목적으로 두 개의 원격 데스크톱 서비스(터미널 서비스) 라이선스가 함께 제공됩니다. 이 정보는 관리자를 위해 이러한 라이선스를 프로비저닝하는 데 도움이 됩니다. 또한 라이선스 없이 또는 RDP 라이선스 RDP 없이 Amazon EC2 인스턴스로 원격 전환할 수 AWS Systems Manager Session Manager있는 를 사용할 수 있습니다. 추가 원격 데스크톱 서비스 라이선스가 필요한 경우 Microsoft 또는 Microsoft 라이선스 리셀러로부터 원격 데스크톱 사용자를 구매CALs 해야 합니다. Software AssuranceCALs가 활성화된 원격 데스크톱 사용자는 License Mobility의 이점을 누릴 수 있으며 기본(공유) 테넌트 환경으로 AWS 가져올 수 있습니다. Software Assurance 또는 License Mobility 혜택 없이 라이선스를 가져오는 방법에 대한 자세한 내용은 의 이 섹션을 참조하세요 FAQ.

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 다음과 같습니다. (a) 정보 제공용이며, (b) 현재 제품 제공 및 관행을 나타냅니다 AWS . 예고 없이 변경될 수 있습니다. 및 (c) 는 AWS 및 그 계열사로부터 약속 또는 보증을 생성하지 않습니다. 공급자 또는 licensors. AWS products 또는 서비스는 보증 없이 “있는 그대로” 제공됩니다. 표현, 또는 모든 종류의 조건, 고객에 대한 명시적 또는 묵시적 AWS 책임과 책임은 AWS 계약에 의해 관리됩니다. 이 문서는 수정하지도 않고 AWS 와 고객 간의 모든 계약.

의 Research and Engineering Studio AWS 는 Apache Software Foundation 에서 사용할 수 있는 Apache 라이선스 버전 2.0의 조건에 따라 라이선스가 부여됩니다.

개정

자세한 내용은 GitHub 리포지토리의 CHANGELOG.md 파일을 참조하세요.

날짜	변경 사항

2024년 10월	• 릴리스 버전 2024.10: 에 대한 지원이 추가되었습니다.
	  • 환경 경계.
	  • 데스크톱 공유 프로필.
	  • 가상 데스크톱 인터페이스 자동 중지.

2024년 8월	• 릴리스 버전 2024.08: 에 대한 지원이 추가되었습니다.
	  • Amazon S3 버킷을 Linux Virtual Desktop Infrastructure(VDI) 인스턴스에 탑재합니다. Amazon S3 버킷을 참조하세요.
	  • 사용자 지정 프로젝트 권한, 기존 역할을 커스터마이징하고 사용자 지정 역할을 추가할 수 있는 향상된 권한 모델입니다. 권한 정책을 참조하세요.
	• 사용 설명서: 문제 해결 섹션을 확장했습니다.

2024년 6월	• 릴리스 버전 2024.06 — Ubuntu 지원, 프로젝트 소유자 권한. • 사용 설명서: 추가됨 데모 환경 생성
2024년 4월	릴리스 버전 2024.04 — RES준비 AMIs 및 프로젝트 시작 템플릿
2024년 3월	추가 문제 해결 주제, CloudWatch 로그 보존, 마이너 버전 제거
2024년 2월	릴리스 버전 2024.01.01 — 배포 템플릿 업데이트

날짜	변경 사항
2024년 1월	릴리스 버전 2024.01
2023년 12월	GovCloud 지침 및 템플릿 추가됨
2023년 11월	최초 릴리스

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.