



사용자 가이드

연구 및 엔지니어링 스튜디오



연구 및 엔지니어링 스튜디오: 사용자 가이드

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 관련하여 고객에게 혼동을 일으킬 수 있는 방식이나 Amazon 브랜드 이미지를 떨어뜨리는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

개요	1
기능 및 이점	1
개념 및 정의	2
아키텍처 개요	4
아키텍처 다이어그램	4
AWS이 제품의 서비스	5
데모 환경	8
원클릭 데모 스택을 만드세요.	8
사전 조건	8
리소스 생성 및 매개 변수 입력	9
배포 후 단계	10
배포 계획	12
비용	12
보안	12
IAM 역할	12
보안 그룹	13
데이터 암호화	13
지원됨 AWS 리전	13
할당량	14
이 제품의 서비스 할당량 AWS	14
AWS CloudFormation 할당량	14
복원력 계획	14
제품 배포	16
사전 조건	16
관리자 AWS 계정 사용자로 생성	16
Amazon EC2 SSH 키 페어 생성	17
서비스 할당량 증가	17
퍼블릭 도메인 생성 (선택 사항)	17
도메인 생성 (GovCloud 전용)	18
외부 리소스 제공	19
사용자 환경에 LDAPS 구성 (선택 사항)	19
프라이빗 VPC 구성 (선택 사항)	20
외부 리소스 생성	31
1단계: 제품 실행	35

2단계: 처음 로그인	43
제품 업데이트	44
메이저 버전 업데이트	44
마이너 버전 업데이트	44
제품 제거	46
사용 AWS Management Console	46
사용 AWS Command Line Interface	46
삭제 중 shared-storage-security-group	46
Amazon S3 버킷 삭제	47
구성 가이드	48
사용자 및 그룹 관리	48
IAM ID 센터를 통한 SSO 설정	48
싱글 사인온 (SSO) 을 위한 ID 공급자 구성	52
사용자 비밀번호 설정	62
하위 도메인 생성	62
ACM 인증서 생성	63
아마존 CloudWatch 로그	64
사용자 지정 권한 범위 설정	65
RES 지원 AMI를 구성합니다.	69
RES 환경에 액세스하기 위한 IAM 역할 준비	70
EC2 Image Builder 구성 요소 생성	71
EC2 Image Builder 레시피 준비	75
EC2 Image Builder 인프라 구성	77
Image Builder 이미지 파이프라인 설정	78
Image Builder 이미지 파이프라인 실행	79
RES에 새 소프트웨어 스택 등록	79
관리자 가이드	80
세션 관리	80
대시보드	81
세션	82
소프트웨어 스택 (AMI)	85
권한 프로필	89
디버깅	92
데스크톱 설정	92
환경 매니지먼트	93
프로젝트	94

사용자	100
그룹	101
파일 시스템	102
환경 상태	106
스냅샷 관리	107
환경 설정	114
보안 암호 관리	115
비용 모니터링 및 제어	117
권한	122
제품 사용	124
가상 데스크톱	124
지원되는 운영 체제	125
새 데스크톱 시작	125
데스크톱에 액세스	125
데스크톱 상태 제어	127
가상 데스크톱 수정	128
세션 정보 검색	128
가상 데스크톱 예약	129
공유 데스크톱	131
데스크톱 공유	131
공유 데스크톱에 액세스	132
파일 브라우저	132
파일 업로드	133
파일 삭제	133
즐거찾기 관리	133
파일 편집	134
파일 전송	134
SSH 액세스	135
문제 해결	136
설치 문제	136
AWS CloudFormation 스택 생성에 실패했습니다. “WaitCondition 수신 실패 메시지” 메시지가 표시됩니다. 오류: 상태. TaskFailed”	136
AWS CloudFormation 스택이 성공적으로 생성된 후 이메일 알림을 받지 못했습니다.	137
장애 상태의 인스턴스 순환 또는 vdc-controller	137
종속 객체 오류로 인해 환경 CloudFormation 스택을 삭제하지 못했습니다.	140
환경 생성 중에 CIDR 블록 매개변수에서 오류가 발생했습니다.	141

CloudFormation 환경 생성 중 스택 생성 실패	141
CREATE_FAILED로 AdDomainAdminNode 인해 외부 리소스 (데모) 스택 생성이 실패합니 다.	141
ID 관리 문제	142
환경에 로그인하면 즉시 로그인 페이지로 돌아갑니다.	142
로그인하려고 할 때 “사용자를 찾을 수 없음” 오류	143
Active Directory에 사용자가 추가되었지만 RES에서 누락되었습니다.	144
세션 생성 시 사용자 사용 불가	144
클러스터 관리자 로그의 크기 제한 초과 오류 CloudWatch	144
고지 사항	145
개정	146
.....	cxlvii

개요

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

관리자는 특정 사용자 집합이 공유 리소스에 액세스하고 협업할 수 있도록 프로젝트라고 하는 가상 협업 공간을 만들 수 있습니다. 관리자는 자체 애플리케이션 소프트웨어 스택 (AMI) 을 구축하여 RES 사용자가 Windows 또는 Linux 가상 데스크톱을 시작하도록 허용하고 공유 파일 시스템을 통해 프로젝트 데이터에 액세스할 수 있도록 할 수 있습니다. 관리자는 소프트웨어 스택과 파일 시스템을 할당하고 해당 프로젝트 사용자로만 액세스를 제한할 수 있습니다. 관리자는 내장된 원격 분석을 사용하여 환경 사용을 모니터링하고 사용자 문제를 해결할 수 있습니다. 또한 리소스의 과소비를 방지하기 위해 개별 프로젝트의 예산을 설정할 수 있습니다. 제품이 오픈 소스이기 때문에 고객은 RES 포털의 사용자 경험을 자신의 필요에 맞게 사용자 지정할 수도 있습니다.

RES는 추가 비용 없이 사용할 수 있으며 애플리케이션을 실행하는 데 필요한 AWS 리소스에 대해서만 비용을 지불하면 됩니다.

이 안내서는 Research and Engineering Studio on AWS, 참조 아키텍처 및 구성 요소, 배포 계획을 위한 고려 사항, Amazon Web Services (AWS) 클라우드에 RES를 배포하기 위한 구성 단계에 대한 개요를 제공합니다.

기능 및 이점

연구 및 엔지니어링 스튜디오 AWS on은 다음과 같은 기능을 제공합니다.

웹 기반 사용자 인터페이스

RES는 관리자, 연구원, 엔지니어가 연구 및 엔지니어링 작업 공간에 액세스하고 관리하는 데 사용할 수 있는 웹 기반 포털을 제공합니다. 과학자와 엔지니어는 RES를 사용하기 위해 전문 지식 AWS 계정 또는 클라우드 전문 지식이 없어도 됩니다.

프로젝트 기반 구성

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

애플리케이션) 과 스토리지 리소스를 프로젝트에 할당합니다. 프로젝트별로 지출을 모니터링하고 관리합니다.

협업 도구

과학자와 엔지니어는 프로젝트의 다른 구성원을 초대하여 함께 협업하도록 할 수 있으며, 동료에게 부여하고 싶은 권한 수준을 설정할 수 있습니다. 이러한 개인은 RES에 로그인하여 해당 데스크톱에 연결할 수 있습니다.

기존 ID 관리 인프라와의 통합

기존 ID 관리 및 디렉터리 서비스 인프라와 통합하여 사용자의 기존 기업 ID를 사용하여 RES 포털에 연결하고 기존 사용자 및 그룹 멤버십을 사용하여 프로젝트에 권한을 할당할 수 있습니다.

연구 저장 및 공유 데이터에 대한 액세스

사용자가 가상 데스크톱 세션에서 공유 데이터에 액세스할 수 있도록 하려면 기존 파일 시스템에 연결하거나 RES에서 새 파일 시스템을 생성하십시오. 지원되는 스토리지 서비스에는 리눅스 데스크톱용 Amazon Elastic File System과 윈도우 및 리눅스 NetApp 데스크톱용 ONTAP용 Amazon FSx가 포함됩니다.

모니터링 및 보고

분석 대시보드를 사용하여 인스턴스 유형, 소프트웨어 스택, 운영 체제 유형에 대한 리소스 사용량을 모니터링할 수 있습니다. 또한 대시보드는 보고를 위해 프로젝트별 리소스 사용량을 분류하여 제공합니다.

예산 및 비용 관리

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

개념 및 정의

이 섹션에서는 주요 개념을 설명하고 이 제품과 관련된 용어를 정의합니다.

파일 브라우저

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

파일 시스템

파일 시스템은 프로젝트 데이터 (종종 데이터셋이라고 함) 를 저장하는 컨테이너 역할을 합니다. 프로젝트 경계 내에서 스토리지 솔루션을 제공하고 협업 및 데이터 액세스 제어를 개선합니다.

글로벌 관리자

RES 환경 전체에서 공유되는 RES 리소스에 액세스할 수 있는 관리 대리인. 범위와 권한은 여러 프로젝트에 걸쳐 있습니다. 프로젝트를 만들거나 수정하고 프로젝트 소유자를 할당할 수 있습니다. 프로젝트 소유자 및 프로젝트 구성원에게 권한을 위임하거나 할당할 수 있습니다. 조직의 규모에 따라 같은 사람이 RES 관리자 역할을 하는 경우도 있습니다.

프로젝트

프로젝트는 데이터와 컴퓨팅 리소스의 구분된 경계 역할을 하는 애플리케이션 내의 논리적 파티션으로, 데이터 흐름에 대한 거버넌스를 보장하고 프로젝트 간 데이터 및 VDI 호스트 공유를 방지합니다.

프로젝트 기반 권한

프로젝트 기반 권한은 여러 프로젝트가 존재할 수 있는 시스템에서 데이터와 VDI 호스트의 논리적 파티션을 설명합니다. 프로젝트 내 데이터 및 VDI 호스트에 대한 사용자의 액세스 권한은 관련 역할에 따라 결정됩니다. 사용자에게 액세스가 필요한 각 프로젝트에 대한 액세스 권한 (또는 프로젝트 멤버십) 을 할당해야 합니다. 그렇지 않으면 멤버십이 부여되지 않은 사용자는 프로젝트 데이터 및 VDI에 액세스할 수 없습니다.

프로젝트 멤버

RES 리소스 (VDI, 스토리지 등) 의 최종 사용자 범위와 권한은 할당된 프로젝트로 제한됩니다. 권한을 위임하거나 할당할 수 없습니다.

프로젝트 소유자

특정 프로젝트에 대한 액세스 권한 및 소유권을 가진 관리 대리인. 범위와 권한은 소유한 프로젝트로 제한됩니다. 소유한 프로젝트의 프로젝트 구성원에게 권한을 할당할 수 있습니다.

소프트웨어 스택

소프트웨어 스택은 사용자가 VDI 호스트에 프로비저닝하기 위해 선택한 운영 체제를 기반으로 하는 RES 전용 메타데이터가 포함된 [Amazon 머신 이미지 \(AMI\)](#) 입니다.

VDI 호스트

가상 데스크톱 인스턴스 (VDI) 호스트를 사용하면 프로젝트 구성원이 프로젝트별 데이터 및 컴퓨팅 환경에 액세스할 수 있으므로 안전하고 격리된 작업 공간이 보장됩니다.

용어에 대한 일반적인 참조는 일반 참조의 AWS [AWS 용어집](#)을 참조하십시오. AWS

아키텍처 개요

이 섹션에서는 이 제품과 함께 배포된 구성 요소의 아키텍처 다이어그램을 제공합니다.

아키텍처 다이어그램

기본 매개 변수와 함께 이 제품을 배포하면 다음 구성 요소가 배포됩니다. AWS 계정

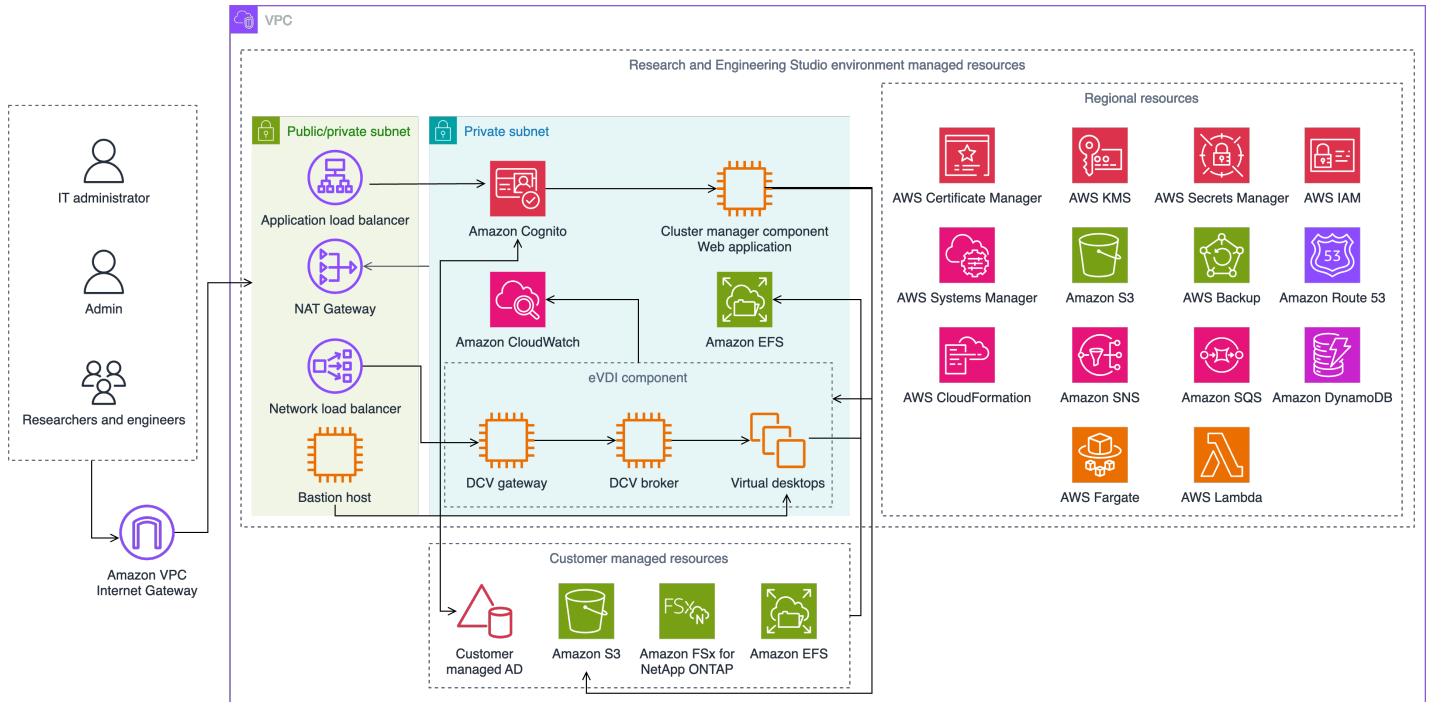


그림 1: AWS 건축 연구 및 엔지니어링 스튜디오

Note

AWS CloudFormation 리소스는 AWS Cloud Development Kit (AWS CDK) 구성을 기반으로 생성됩니다.

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

1. RES는 웹 포털용 구성 요소뿐만 아니라 다음과 같은 구성 요소도 설치합니다.
 - a. 대화형 워크로드를 위한 엔지니어링 가상 데스크톱 (eVDI) 구성 요소

b. 메트릭 구성 요소

Amazon은 eVDi 구성 요소로부터 지표를 CloudWatch 수신합니다.

c. 배스천 호스트 구성 요소

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

2. RES는 NAT 게이트웨이 뒤의 프라이빗 서브넷에 구성 요소를 설치합니다. 관리자는 애플리케이션 로드 밸런서 (ALB) 또는 배스천 호스트 구성 요소를 통해 프라이빗 서브넷에 액세스합니다.
3. Amazon DynamoDB는 환경 구성을 저장합니다.
4. AWS Certificate Manager(ACM) 은 애플리케이션 로드 밸런서 (ALB) 용 공개 인증서를 생성하고 저장합니다.

Note

도메인용 신뢰할 수 있는 인증서를 AWS Certificate Manager 생성하려면 를 사용하는 것이 좋습니다.

5. Amazon Elastic File System (EFS) 은 모든 해당 인프라 호스트와 eVDI Linux 세션에 마운트된 기본 /home 파일 시스템을 호스팅합니다.
6. RES는 Amazon Cognito를 사용하여 clusteradmin이라는 초기 부트스트랩 사용자를 생성하고 설치 중에 제공된 이메일 주소로 임시 자격 증명을 보냅니다. 클러스터 관리자는 처음 로그인할 때 비밀번호를 변경해야 합니다.
7. Amazon Cognito는 권한 관리를 위해 조직의 액티브 디렉터리 및 사용자 ID와 통합됩니다.
8. 보안 영역을 통해 관리자는 권한에 따라 제품 내 특정 구성 요소에 대한 액세스를 제한할 수 있습니다.

AWS이 제품의 서비스

AWS 서비스	설명
Amazon Elastic Compute Cloud	Core. 선택한 운영 체제 및 소프트웨어 스택으로 가상 데스크톱을 만들 수 있는 기본 컴퓨팅 서비스를 제공합니다.

AWS 서비스	설명
Elastic Load Balancing	Core. 배스천, 클러스터 관리자 및 VDI 호스트는 로드 밸런서 뒤의 Auto Scaling 그룹에서 생성됩니다. ELB는 웹 포털의 트래픽을 RES 호스트 간에 밸런싱합니다.
Amazon Virtual Private Cloud	Core. 모든 핵심 제품 구성 요소는 VPC 내에서 생성됩니다.
Amazon Cognito	Core. 사용자 ID 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 호스트를 위한 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.
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 위해 애플리케이션 바이너리를 저장합니다.
AWS Key Management Service	지원. Amazon SQS 대기열, DynamoDB 테이블 및 Amazon SNS 주제를 사용하여 저장된 데이터를 암호화하는 데 사용됩니다.

AWS 서비스	설명
AWS Secrets Manager	지원. Active Directory에 서비스 계정 자격 증명을 저장하고 VDI용 자체 서명된 인증서를 저장합니다.
AWS CloudFormation	지원. 제품의 배포 메커니즘을 제공합니다.
AWS Identity and Access Management	지원. 호스트의 액세스 수준을 제한합니다.
Amazon Route 53	지원. 내부 로드 밸런서와 배스천 호스트 도메인 이름을 확인하기 위한 프라이빗 호스팅 영역을 생성합니다.
Amazon Simple Queue Service	지원. 비동기 실행을 지원하는 작업 대기열을 생성합니다.
Amazon Simple Notification Service	지원. 컨트롤러 및 호스트와 같은 VDI 구성 요소 간의 게시-구독자 모델을 지원합니다.
AWS Fargate	지원. Fargate 작업을 사용하여 환경을 설치, 업데이트 및 삭제합니다.
아마존 FSx 파일 게이트웨이	선택 사항. 외부 공유 파일 시스템을 제공합니다.
ONTAP용 아마존 NetApp FSx	선택 사항. 외부 공유 파일 시스템을 제공합니다.
AWS Certificate Manager	선택 사항. 사용자 지정 도메인의 신뢰할 수 있는 인증서를 생성합니다.
AWS Backup	선택 사항. Amazon EC2 호스트, 파일 시스템 및 DynamoDB를 위한 백업 기능을 제공합니다.

데모 환경 만들기

이 섹션의 단계에 따라 리서치 앤 엔지니어링 스튜디오를 사용해 보세요. AWS이 데모는 [Research and Engineering Studio on AWS 데모 환경 스택 템플릿을 사용하여 최소한의 매개 변수로 비프로덕션 환경을 배포](#)합니다. SSO용 Keycloak 서버를 사용합니다.

스택을 배포한 후에는 로그인하기 전에 [배포 후 단계](#) 아래 단계에 따라 환경에 사용자를 설정해야 합니다.

원클릭 데모 스택을 만드세요.

이 AWS CloudFormation 스택은 연구 및 엔지니어링 스튜디오에 필요한 모든 구성 요소를 생성합니다.

배포 시간: ~90분

사전 조건

주제

- [관리자 AWS 계정 사용자로 광고 만들기](#)
- [Amazon EC2 SSH 키 페어 생성](#)
- [서비스 할당량 증가](#)

관리자 AWS 계정 사용자로 광고 만들기

관리자가 AWS 계정 있는 사용자가 있어야 합니다.

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

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

에 AWS 계정가입하면 AWS 계정 루트 사용자a가 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 작업](#)을 수행하는 것입니다.

Amazon EC2 SSH 키 페어 생성

Amazon EC2 SSH 키 페어가 없는 경우 키 페어를 생성해야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 [Amazon EC2를 사용하여 키 페어 생성을](#) 참조하십시오.

서비스 할당량 증가

다음에 [대한 서비스 할당량을 늘리는](#) 것이 좋습니다.

- [아마존 VPC](#)
 - NAT 게이트웨이당 엘라스틱 IP 주소 할당량을 5개에서 8개로 늘립니다.
 - 가용 영역당 NAT 게이트웨이를 5개에서 10개로 늘립니다.
- [아마존 EC2](#)
 - EC2-VPC 엘라스틱 IP를 5개에서 10개로 늘리십시오.

AWS 계정에는 각 서비스에 대한 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 다르게 표시 되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다. 자세한 정보는 [the section called “이 제품의 서비스 할당량 AWS”](#)을 참조하십시오.

리소스 생성 및 매개 변수 입력

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/cloudformation> 에서 AWS CloudFormation 콘솔을 엽니다.

Note

관리자 계정으로 로그인했는지 확인하세요.

2. [콘솔에서 템플릿을](#) 실행합니다.
3. 매개 변수에서 이 제품 템플릿의 매개 변수를 검토하고 필요에 따라 수정합니다.

파라미터	기본값	설명
EnvironmentName	< <i>res-demo</i> >	res-로 시작하고 11자 이하로 시작하는 RES 환경에 부여되는 고유한 이름입니다.

파라미터	기본값	설명
AdministratorEmail		제품 설정을 완료하는 사용자의 이메일 주소입니다. Active Directory 싱글 사인온 통합이 실패할 경우 이 사용자는 브레이크-글래스 사용자 역할도 수행합니다.
KeyPair		인프라 호스트에 연결하는 데 사용되는 키 쌍입니다.
클라이언트 IP IDR	<0.0.0.0/0>	시스템 연결을 제한하는 IP 주소 필터. 배포 ClientIpCidr 후 업데이트할 수 있습니다.
InboundPrefixList		(선택 사항) 배스천 호스트에 웹 UI 및 SSH에 직접 액세스할 수 있도록 허용된 IP의 관리 접두사 목록을 제공하십시오.

배포 후 단계

- 에서 사용자 암호 재설정 AWS Directory Service - 데모 스택은 사용 가능한 사용자 이름 (admin1,, user1admin2,) 을 가진 사용자 4명을 생성합니다. user2
 - 디렉터리 서비스 콘솔로 이동합니다.
 - 환경에 맞는 디렉터리 ID를 선택합니다. <StackName>*DirectoryService*스택의 출력에서 디렉터리 ID를 가져올 수 있습니다.
 - 오른쪽 상단의 작업 드롭다운 메뉴에서 사용자 암호 재설정을 선택합니다.
 - 사용하려는 모든 사용자에게 사용자 이름을 입력하고 원하는 비밀번호를 입력한 다음 비밀번호 재설정을 선택합니다.
- 사용자 암호를 재설정 한 후에는 Research and Engineering Studio가 환경의 사용자를 동기화할 때까지 기다려야 합니다. 연구 및 엔지니어링 스튜디오는 xx.00에 매시간 사용자를 동기화합니다.

그런 일이 발생할 때까지 기다리거나 에 나와 있는 단계에 따라 사용자를 즉시 [Active Directory에 사용자가 추가되었지만 RES에서 누락되었습니다](#). 동기화할 수 있습니다.

이제 배포가 준비되었습니다. 이메일로 받은 EnvironmentUrl 것을 사용하여 UI에 액세스하거나 배포된 스택의 출력에서 동일한 URL을 가져올 수도 있습니다. 이제 Active Directory에서 암호를 재설정 한 사용자 및 암호를 사용하여 연구 및 엔지니어링 스튜디오 환경에 로그인할 수 있습니다.

배포 계획

비용

Research and Engineering Studio AWS on은 추가 비용 없이 이용할 수 있으며 애플리케이션을 실행하는 데 필요한 리소스에 대한 비용만 지불하면 됩니다. AWS 자세한 정보는 [AWS이 제품의 서비스를](#) 참조하세요.

Note

이 제품을 실행하는 동안 사용되는 AWS 서비스 비용은 사용자 부담입니다. 비용 관리에 도움이 되도록 [예산을 AWS Cost Explorer](#)세우는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은 이 제품에 사용되는 각 AWS 서비스의 가격 책정 웹페이지를 참조하십시오.

보안

AWS 인프라를 기반으로 시스템을 구축하면 사용자와 AWS사용자 간에 보안 책임이 분담됩니다. 이 [공동 책임 모델](#)은 호스트 운영 체제, 가상화 계층, 서비스가 AWS 운영되는 시설의 물리적 보안을 비롯한 구성 요소를 운영, 관리 및 제어하므로 운영 부담을 줄여줍니다. AWS 보안에 대한 자세한 내용은 [AWS 클라우드 보안을](#) 참조하십시오.

IAM 역할

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

RES는 IAM 내에서 ID 기반 정책을 지원합니다. RES는 배포 시 관리자 권한 및 액세스를 정의하는 정책을 생성합니다. 제품을 구현하는 관리자는 RES와 통합된 기존 고객인 Active Directory 내에서 최종 사용자와 프로젝트 리더를 생성하고 관리합니다. 자세한 내용은 AWS ID 및 Access Management 사용 설명서의 [IAM 정책 생성](#)을 참조하십시오.

조직의 관리자는 Active Directory를 사용하여 사용자 액세스를 관리할 수 있습니다. 최종 사용자가 RES 사용자 인터페이스에 액세스하면 RES는 [Amazon Cognito](#)를 사용하여 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. 제품이 배포된 후에는 보안 그룹을 검토하고 필요에 따라 액세스를 추가로 제한하는 것이 좋습니다.

데이터 암호화

기본적으로 Research and Engineering Studio on AWS (RES) 은 RES 소유 키를 사용하여 저장 및 전송 중인 고객 데이터를 암호화합니다. RES를 배포할 때 지정할 수 있습니다. AWS KMS key RES는 사용자 자격 증명을 사용하여 키 액세스 권한을 부여합니다. 고객이 소유하고 관리하는 AWS KMS key 서비스를 제공하는 경우 저장된 고객 데이터는 해당 키를 사용하여 암호화됩니다.

RES는 SSL/TLS를 사용하여 전송 중인 고객 데이터를 암호화합니다. TLS 1.2가 필요하지만 TLS 1.3을 사용하는 것이 좋습니다.

지원됨 AWS 리전

이 제품은 현재 전혀 제공되지 않는 서비스를 사용합니다 AWS 리전. 모든 서비스를 이용할 수 있는 AWS 리전 곳에서 이 제품을 출시해야 합니다. 지역별 최신 AWS 서비스 가용성은 [AWS 리전모든 서비스 목록](#)을 참조하십시오.

리서치 및 엔지니어링 스튜디오 AWS on은 AWS 리전다음과 같은 분야에서 지원됩니다.

지역명	
미국 동부(오하이오)	캐나다(중부)
미국 동부(버지니아 북부)	유럽(프랑크푸르트)
미국 서부(캘리포니아 북부)	유럽(아일랜드)
미국 서부(오레곤)	유럽(런던)
아시아 태평양(뭄바이)	유럽(밀라노)
아시아 태평양(서울)	유럽(파리)
아시아 태평양(싱가포르)	이스라엘(텔아비브)

지역명	
아시아 태평양(시드니)	AWS GovCloud (미국 서부)
아시아 태평양(도쿄)	

할당량

서비스 할당량은 AWS 계정계정의 최대 서비스 리소스 또는 작업 수입니다.

이 제품의 AWS 서비스 할당량

[이 제품에 구현된 각 서비스의 할당량](#)이 충분한지 확인하십시오. 자세한 내용은 [AWS 서비스 할당량](#)을 참조하십시오.

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 요청](#)을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 [한도 증가 양식](#)을 사용합니다.

AWS CloudFormation 할당량

AWS 계정 Your에는 이 제품의 [스택을 실행할 때 알아두어야 할 AWS CloudFormation 할당량이 있습니다](#). 이러한 할당량을 이해하면 이 제품을 성공적으로 배포하는 데 방해가 되는 제한 오류를 피할 수 있습니다. 자세한 내용은 사용자 [AWS CloudFormation 안내서의 할당량](#)을 참조하십시오. AWS CloudFormation

복원력 계획

이 제품은 시스템을 운영하기 위한 Amazon EC2 인스턴스의 수와 크기를 최소화한 기본 인프라를 배포합니다. 대규모 프로덕션 환경에서 복원력을 개선하려면 인프라의 Auto Scaling 그룹 (ASG) 내에서 기본 최소 용량 설정을 늘리는 것이 좋습니다. 인스턴스 1개에서 인스턴스 2개로 값을 늘리면 다중 가용 영역 (AZ) 의 이점을 얻을 수 있으며 예상치 못한 데이터 손실 시 시스템 기능을 복원하는 시간이 단축됩니다.

ASG 설정은 Amazon EC2 콘솔 <https://console.aws.amazon.com/ec2/> 내에서 사용자 지정할 수 있습니다. 이 제품은 기본적으로 각 이름이 로 끝나는 4개의 ASG를 생성합니다. -asg 최소값과 원하는 값을 프로덕션 환경에 적합한 양으로 변경할 수 있습니다. 수정하려는 그룹을 선택한 다음 작업 및 편집을 선택합니다. ASG에 대한 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling [그룹 크기](#) 조정을 참조하십시오.

제품 배포

Note

이 제품은 [AWS CloudFormation 템플릿과 스택](#)을 사용하여 배포를 자동화합니다. CloudFormation 템플릿은 이 제품에 포함된 AWS 리소스와 해당 속성을 설명합니다. CloudFormation 스택은 템플릿에 설명된 리소스를 제공합니다.

제품을 출시하기 전에 이 가이드의 앞부분에서 설명한 [비용](#), [아키텍처](#), [네트워크 보안](#) 및 기타 고려 사항을 검토하십시오.

주제

- [사전 조건](#)
- [외부 리소스 생성](#)
- [1단계: 제품 출시](#)
- [2단계: 처음으로 로그인하기](#)

사전 조건

주제

- [관리자 AWS 계정 사용자로 생성](#)
- [Amazon EC2 SSH 키 페어 생성](#)
- [서비스 할당량 증가](#)
- [퍼블릭 도메인 생성 \(선택 사항\)](#)
- [도메인 생성 \(GovCloud 전용\)](#)
- [외부 리소스 제공](#)
- [사용자 환경에 LDAPS를 구성합니다 \(선택 사항\).](#)
- [프라이빗 VPC 구성 \(선택 사항\)](#)

관리자 AWS 계정 사용자로 생성

관리자가 AWS 계정 있는 사용자가 있어야 합니다.

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

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

에 AWS 계정가입하면 AWS 계정 루트 사용자a가 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 것](#)입니다.

Amazon EC2 SSH 키 페어 생성

Amazon EC2 SSH 키 페어가 없는 경우 키 페어를 생성해야 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 [Amazon EC2를 사용하여 키 페어 생성을](#) 참조하십시오.

서비스 할당량 증가

다음에 [대한 서비스 할당량을 늘리는](#) 것이 좋습니다.

- [Amazon VPC](#)
 - NAT 게이트웨이당 엘라스틱 IP 주소 할당량을 5개에서 8개로 늘립니다.
 - 가용 영역당 NAT 게이트웨이를 5개에서 10개로 늘립니다.
- [Amazon EC2](#)
 - EC2-VPC 엘라스틱 IP를 5개에서 10개로 늘리십시오.

AWS 계정에는 각 서비스에 대한 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 다르게 표시 되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다. 자세한 정보는 [the section called “이 제품의 서비스 할당량 AWS”](#)을 참조하십시오.

퍼블릭 도메인 생성 (선택 사항)

사용자에게 친숙한 URL을 만들려면 제품에 사용자 지정 도메인을 사용하는 것이 좋습니다. Amazon Route 53 또는 다른 공급자를 사용하여 도메인을 등록하고 를 사용하여 도메인에 대한 인증서를 가져 와야 AWS Certificate Manager합니다. 이미 퍼블릭 도메인과 인증서가 있는 경우 이 단계를 건너뛰어도 됩니다.

1. 지침에 따라 Route53에 [도메인을 등록하십시오](#). 확인 이메일을 받게 됩니다.
2. 도메인의 호스팅 영역을 검색하십시오. 이는 Route53에 의해 자동으로 생성됩니다.
 - a. Route53 콘솔을 엽니다.
 - b. 왼쪽 탐색창에서 호스팅 영역을 선택합니다.
 - c. 도메인 이름용으로 생성된 호스팅 영역을 열고 호스팅 영역 ID를 복사합니다.
3. [도메인 인증서를 AWS Certificate Manager 열고 다음 단계에 따라 요청하세요](#). 솔루션을 배포할 계획이 있는 지역에 있는지 확인하십시오.
4. 탐색에서 인증서 목록을 선택하고 인증서 요청을 찾으십시오. 요청이 보류 중이어야 합니다.
5. 인증서 ID를 선택하여 요청을 여십시오.
6. 도메인 섹션에서 Route53에서 레코드 생성을 선택합니다. 요청을 처리하는 데 약 10분이 소요됩니다.
7. 인증서가 발급되면 인증서 상태 섹션에서 ARN을 복사합니다.

도메인 생성 (GovCloud 전용)

AWS GovCloud (미국 서부) 지역에 배포하는 경우 다음 사전 필수 단계를 완료해야 합니다.

1. 퍼블릭 호스팅 도메인이 생성된 상업용 파티션 AWS 계정에 [인증서 AWS CloudFormation 스택을](#) 배포합니다.
2. 인증서 CloudFormation 출력에서 `및` 를 찾아 기록해 둡니다. `CertificateARN`
`PrivateKeySecretARN`
3. GovCloud 파티션 계정에서 `CertificateARN` 출력 값으로 시크릿을 생성합니다. 새 시크릿 ARN을 기록하고 시크릿 값에 접근할 `vdc-gateway` 수 있도록 시크릿에 태그 두 개를 추가한다.
 - a. `res: = ModuleName virtual-desktop-controller`
 - b. `res: EnvironmentName = [환경 이름]` (이것은 res-데모일 수 있습니다.)
4. GovCloud 파티션 계정에서 출력 값으로 시크릿을 생성합니다. `PrivateKeySecretArn` 새 시크릿 ARN을 기록하고 시크릿 값에 접근할 `vdc-gateway` 수 있도록 시크릿에 태그 두 개를 추가한다.
 - a. `res: = ModuleName virtual-desktop-controller`
 - b. `res: EnvironmentName = [환경 이름]` (이것은 res-데모일 수 있습니다.)

외부 리소스 제공

연구 및 엔지니어링 스튜디오를 에 AWS배포하는 경우 제품에서 사용하는 외부 리소스가 필요합니다. RES는 배포 시 이러한 리소스가 존재할 것으로 예상합니다.

- 네트워킹 (VPC, 퍼블릭, 프라이빗 서브넷)

여기에서 환경을 호스팅하는 데 사용되는 EC2 인스턴스, Active Directory (AD) 및 공유 스토리지를 실행할 수 있습니다.

- 스토리지 (아마존 EFS)

스토리지 볼륨에는 가상 데스크톱 인프라 (VDI) 에 필요한 파일 및 데이터가 포함되어 있습니다.

- 디렉터리 서비스 ()AWS Directory Service for Microsoft Active Directory

디렉터리 서비스는 환경 페이지에 대해 사용자를 인증합니다.

- 서비스 계정 비밀번호가 포함된 시크릿

Research and Engineering Studio는 서비스 계정 비밀번호를 포함하여 사용자가 제공하는 [비밀에](#) 액세스합니다. [AWS Secrets Manager](#)

Tip

데모 환경을 배포하고 있는데 이러한 외부 리소스를 사용할 수 없는 경우 AWS 고성능 컴퓨팅 레시피를 사용하여 외부 리소스를 생성할 수 있습니다. 계정에 리소스를 [외부 리소스 생성](#) 배포하려면 다음 섹션을 참조하십시오.

AWS GovCloud (미국 서부) 지역에 데모를 배포하려면 의 사전 필수 단계를 완료해야 합니다. [도메인 생성 \(GovCloud 전용\)](#)

사용자 환경에 LDAPS를 구성합니다 (선택 사항).

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

1. [서버측 LDAPS를 활성화하는 방법에](#) 제공된 단계를 따르십시오. AWS Managed Microsoft AD이 미 LDAPS를 활성화한 경우 이 단계를 건너뛰어도 됩니다.
2. AD에 LDAPS가 구성되어 있는지 확인한 후 AD 인증서를 내보냅니다.

- a. 액티브 디렉터리 서버로 이동합니다.
 - b. 관리자 PowerShell 권한으로 엽니다.
 - c. certmgr.msc를 실행하여 인증서 목록을 엽니다.
 - d. 먼저 신뢰할 수 있는 루트 인증 기관을 연 다음 인증서를 열어 인증서 목록을 엽니다.
 - e. AD 서버와 이름이 같은 인증서를 선택하여 보류 (또는 마우스 오른쪽 단추로 클릭) 하고 모든 작업을 선택한 다음 내보내기를 선택합니다.
 - f. Base-64로 인코딩된 X.509 (.CER) 를 선택하고 다음을 선택합니다.
 - g. 디렉터리를 선택한 후 다음을 선택합니다.
3. 시크릿 생성 AWS Secrets Manager:
- Secrets Manager에서 보안 암호를 생성할 때, 보안 암호 유형에서 다른 유형의 보안 암호를 선택하고 PEM으로 인코딩된 인증서를 일반 텍스트 필드에 붙여넣습니다.
4. 생성된 ARN을 기록하고 DomainTLSCertificateSecretARN 파라미터로 입력합니다. [the section called “1단계: 제품 실행”](#)

프라이빗 VPC 구성 (선택 사항)

Research and Engineering Studio를 격리된 VPC에 배포하면 조직의 규정 준수 및 거버넌스 요구 사항을 충족하는 향상된 보안을 제공합니다. 하지만 표준 RES 배포에서는 종속성 설치를 위한 인터넷 액세스를 사용합니다. 프라이빗 VPC에 RES를 설치하려면 다음 사전 요구 사항을 충족해야 합니다.

주제

- [아마존 머신 이미지 \(AMI\) 준비](#)
- [VPC 엔드포인트 설정](#)
- [VPC 엔드포인트 없이 서비스에 연결](#)
- [프라이빗 VPC 배포 파라미터 설정](#)

아마존 머신 이미지 (AMI) 준비


1. 다운로드 [종속성](#). 격리된 VPC에 배포하려면 공용 인터넷 액세스 없이 RES 인프라를 사용할 수 있어야 합니다.
2. Amazon S3 읽기 전용 액세스 및 Amazon EC2와 같은 신뢰할 수 있는 ID를 사용하여 IAM 역할을 생성합니다.

- a. <https://console.aws.amazon.com/iam/>에서 IAM 콘솔을 엽니다.
 - b. 역할에서 역할 생성을 선택합니다.
 - c. 신뢰할 수 있는 엔티티 선택 페이지에서:
 - 신뢰할 수 있는 엔티티 유형에서 선택합니다 AWS 서비스.
 - 서비스 또는 사용 사례의 사용 사례에서 EC2를 선택하고 다음을 선택합니다.
 - d. 권한 추가에서 다음 권한 정책을 선택하고 다음을 선택합니다.
 - AmazonS3 ReadOnlyAccess
 - 아마존 SSM ManagedInstanceCore
 - EC2 InstanceProfileForImageBuilder
 - e. 역할 이름과 설명을 추가한 다음 역할 생성을 선택합니다.
3. EC2 이미지 빌더 구성 요소 생성:
- a. 에서 EC2 Image Builder 콘솔을 <https://console.aws.amazon.com/imagebuilder> 엽니다.
 - b. 저장된 리소스에서 구성 요소를 선택하고 구성 요소 생성을 선택합니다.
 - c. 구성 요소 생성 페이지에서 다음 세부 정보를 입력합니다.
 - 구성 요소 유형에서 빌드를 선택합니다.
 - 구성 요소 세부 정보를 보려면 다음을 선택하세요.

파라미터	사용자 입력
이미지 운영 체제 (OS)	Linux
호환되는 OS 버전	Amazon Linux 2
구성 요소 이름	다음과 같은 이름을 선택합니다. <i>< research-and-engineering-studio -###>#</i> 같은 이름 선택
구성 요소 버전입니다.	1.0.0부터 시작하는 것이 좋습니다.
설명	선택적 사용자 입력.

- d. 구성 요소 만들기 페이지에서 문서 내용 정의를 선택합니다.

- i. 정의 문서 내용을 입력하기 전에 tar.gz 파일의 파일 URI가 필요합니다. RES에서 제공한 tar.gz 파일을 Amazon S3 버킷에 업로드하고 버킷 속성에서 파일의 URI를 복사합니다.
- ii. 다음을 입력합니다.

 Note

AddEnvironmentVariables 선택 사항이며 인프라 호스트에 사용자 지정 환경 변수가 필요하지 않은 경우 제거할 수 있습니다.

https_proxy 환경 변수를 설정하는 http_proxy 경우, 인스턴스가 프록시를 사용하여 localhost, 인스턴스 메타데이터 IP 주소 및 VPC 엔드포인트를 지원하는 서비스를 쿼리하지 못하도록 하려면 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 만들기 페이지에서 다음을 입력합니다.

섹션	파라미터	사용자 입력
레시피 세부 정보	이름	적절한 이름 (예: res-recipe-linux-x 86) 을 입력합니다.
	버전	일반적으로 1.0.0부터 시작하는 버전을 입력합니다.
	설명	선택적 설명을 추가합니다.
기본 이미지	이미지 선택	관리 이미지를 선택합니다.
	OS	Amazon Linux
	이미지 출처	퀵 스타트 (아마존 관리)
	이미지 이름	아마존 리눅스 2 x86
	자동 버전 관리 옵션	사용 가능한 최신 OS 버전을 사용하세요.

섹션	파라미터	사용자 입력
인스턴스 구성	-	모든 항목을 기본 설정으로 유지하고, 파이프라인 실행 후 SSM 에이전트 제거가 선택되지 않았는지 확인하세요.
작업 디렉터리	작업 디렉토리 경로	/루트/부트스트랩/res_dependencies
구성 요소	빌드 컴포넌트	다음을 검색하고 선택합니다. <ul style="list-style-type: none"> • 아마존 매니지드: -2-리눅스 aws-cli-version • 아마존 관리: amazon-cloudwatch-agent-linux • 본인 소유: 이전에 생성한 Amazon EC2 구성 요소. 필드에 AWS 계정 ID와 현재 AWS 리전 정보를 입력합니다.
	테스트 구성 요소	검색 및 선택: <ul style="list-style-type: none"> • 아마존 관리: simple-bot-test-linux

b. 레시피 생성을 선택합니다.

5. Image Builder 인프라 구성을 생성합니다.

a. 저장된 리소스에서 인프라 구성을 선택합니다.

b. 인프라 구성 생성을 선택합니다.

c. 인프라 구성 생성 페이지에서 다음을 입력합니다.

섹션	파라미터	사용자 입력
일반	이름	적절한 이름을 입력합니다 (예: res-infra-linux-x 86).
	설명	선택적 설명을 추가합니다.
	IAM 역할	이전에 생성한 IAM 역할을 선택합니다.
AWS 인프라	인스턴스 유형	t3.medium을 선택하세요.
	VPC, 서브넷, 보안 그룹	<p>인터넷 액세스 및 Amazon S3 버킷에 대한 액세스를 허용하는 옵션을 선택합니다. 보안 그룹을 생성해야 하는 경우 Amazon EC2 콘솔에서 다음과 같이 입력하여 보안 그룹을 생성할 수 있습니다.</p> <ul style="list-style-type: none"> • VPC: 인프라 구성에 사용되는 것과 동일한 VPC를 선택합니다. 이 VPC는 인터넷에 액세스할 수 있어야 합니다. • 인바운드 규칙: <ul style="list-style-type: none"> • 유형: SSH • 소스: 사용자 지정 • CIDR 블록: 0.0.0.0/0

d. 인프라 구성 생성을 선택합니다.

6. 새 EC2 Image Builder 파이프라인을 생성하십시오.

a. 이미지 파이프라인으로 이동하여 이미지 파이프라인 생성을 선택합니다.

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

- 파이프라인 이름 및 선택적 설명
 - 빌드 일정에서 일정을 설정하거나 AMI 베이킹 프로세스를 수동으로 시작하려면 수동을 선택합니다.
- c. 레시피 선택 페이지에서 기존 레시피 사용을 선택하고 이전에 생성한 레시피 이름을 입력합니다. 다음을 선택합니다.
 - d. 이미지 프로세스 정의 페이지에서 기본 워크플로를 선택하고 다음을 선택합니다.
 - e. 인프라 구성 정의 페이지에서 기존 인프라 구성 사용을 선택하고 이전에 만든 인프라 구성의 이름을 입력합니다. 다음을 선택합니다.
 - f. 배포 설정 정의 페이지에서 선택 사항에 대해 다음 사항을 고려하십시오.
 - RES가 해당 환경에서 인프라 호스트 인스턴스를 제대로 시작할 수 있도록 출력 이미지는 배포된 RES 환경과 동일한 지역에 있어야 합니다. 서비스 기본값을 사용하면 EC2 Image Builder 서비스가 사용되는 지역에 출력 이미지가 생성됩니다.
 - 여러 지역에 RES를 배포하려면 새 배포 설정 생성을 선택하고 해당 지역에 지역을 더 추가할 수 있습니다.
 - g. 선택 항목을 검토하고 파이프라인 생성을 선택합니다.
7. EC2 Image Builder 파이프라인을 실행합니다.
 - a. 이미지 파이프라인에서 생성한 파이프라인을 찾아 선택합니다.
 - b. 액션을 선택하고 파이프라인 실행을 선택합니다.

파이프라인에서 AMI 이미지를 생성하는 데 약 45분에서 1시간이 걸릴 수 있습니다.
 8. 생성된 AMI의 AMI ID를 적어두고 에서 InfrastructureHost AMI 파라미터의 입력으로 사용하십시오 [the section called “1단계: 제품 실행”](#).

VPC 엔드포인트 설정

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

1. 엔드포인트가 이전에 구성되지 않은 경우 [액세스 및 인터페이스 VPC 엔드포인트 AWS 서비스 사용에](#) 제공된 지침을 따르십시오.
2. 두 가용 영역 각각에서 프라이빗 서브넷을 하나씩 선택합니다.

AWS 서비스	서비스 이름
Application Auto Scaling	com.amazonaws. <i>region</i> .application-autoscaling
AWS CloudFormation	com.amazonaws. <i>region</i> .cloudformation
아마존 CloudWatch	com.amazonaws. <i>region</i> .monitoring
아마존 CloudWatch 로그	com.amazonaws. <i>region</i> .logs
Amazon DynamoDB	com.amazonaws. <i>.dynamodb ##</i> (게이트웨이 엔드포인트 필요)
Amazon EC2	com.amazonaws. <i>region</i> .ec2
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api com.amazonaws. <i>region</i> .ecr.dkr
Amazon Elastic File System	com.amazonaws. <i>region</i> .elasticfilesystem
Elastic Load Balancing	com.amazonaws. <i>region</i> .elasticloadbalancing
아마존 EventBridge	com.amazonaws. <i>region</i> .events
Amazon FSx	com.amazonaws. <i>region</i> .fsx
AWS Key Management Service	com.amazonaws. <i>region</i> .kms
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-streams
Amazon S3	com.amazonaws. <i>.s3 ##</i> (RES에서 기본적으로 생성되는 게이트웨이 엔드포인트가 필요합니다.)
AWS Secrets Manager	com.amazonaws. <i>region</i> .secretsmanager
Amazon SES	com.amazonaws. <i>.email-smtp ##</i> (use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az4, cac1-az4, cac1-az4 등의 가용 영역에서는 지원되지 않음)

AWS 서비스	서비스 이름
AWS Security Token Service	com.amazonaws. <i>region</i> .sts
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
AWS Systems Manager	com.amazonaws. <i>region</i> .ec2messages
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> .ssmmessages

VPC 엔드포인트 없이 서비스에 연결

VPC 엔드포인트를 지원하지 않는 서비스와 통합하려면 VPC의 퍼블릭 서브넷에 프록시 서버를 설정하면 됩니다. AWS Identity Center를 ID 공급자로 사용하여 Research and Engineering Studio 배포에 필요한 최소한의 액세스 권한을 가진 프록시 서버를 만들려면 다음 단계를 따르십시오.

1. RES 배포에 사용할 VPC의 퍼블릭 서브넷에서 Linux 인스턴스를 시작합니다.
 - 리눅스 제품군 — 아마존 리눅스 2 또는 아마존 리눅스 3
 - 아키텍처 — x86
 - 인스턴스 유형 — t2.micro 이상
 - 보안 그룹 — 0.0.0.0/0의 포트 3128에 대한 TCP
2. 인스턴스에 연결하여 프록시 서버를 설정합니다.
 - a. http 연결을 엽니다.
 - b. 모든 관련 서브넷에서 다음 도메인으로의 연결을 허용합니다.
 - .amazonaws.com (일반 서비스용) AWS
 - .amazoncognito.com (아마존 코그니토용)
 - .awsapps.com (아이덴티티 센터용)
 - .signin.aws (아이덴티티 센터용)
 - .amazonaws-us-gov.com (고브 클라우드용)
 - c. 다른 모든 연결을 거부하세요.

- d. 프록시 서버를 활성화하고 시작합니다.
 - e. 프록시 서버가 수신하는 포트를 기록해 둡니다.
3. 프록시 서버에 대한 액세스를 허용하도록 라우팅 테이블을 구성하십시오.
 - a. VPC 콘솔로 이동하여 인프라 호스트 및 VDI 호스트에 사용할 서브넷의 라우팅 테이블을 확인합니다.
 - b. 라우팅 테이블을 편집하여 들어오는 모든 연결이 이전 단계에서 만든 프록시 서버 인스턴스로 이동할 수 있도록 하십시오.
 - c. 인프라/VDI에 사용할 모든 서브넷 (인터넷 액세스 불가) 의 라우팅 테이블에 대해 이 작업을 수행하십시오.
 4. 프록시 서버 EC2 인스턴스의 보안 그룹을 수정하고 프록시 서버가 수신하는 포트에서 인바운드 TCP 연결을 허용하는지 확인하십시오.

프라이빗 VPC 배포 파라미터 설정

[the section called “1단계: 제품 실행”](#)에서는 AWS CloudFormation 템플릿에 특정 파라미터를 입력해야 합니다. 방금 구성한 프라이빗 VPC에 성공적으로 배포하려면 다음 파라미터를 명시된 대로 설정해야 합니다.

파라미터	Input
InfrastructureHostAMI	에서 생성한 인프라 AMI ID를 사용합니다. the section called “아마존 머신 이미지 (AMI) 준비” .
IsLoadBalancerInternetFacing	false로 설정합니다.
LoadBalancerSubnets	인터넷에 접속할 수 없는 사설 서브넷을 선택합니다.
InfrastructureHostSubnets	인터넷에 접속할 수 없는 사설 서브넷을 선택하십시오.
VdiSubnets	인터넷에 접속할 수 없는 사설 서브넷을 선택하십시오.
[ClientIP]	VPC CIDR을 선택하여 모든 VPC IP 주소에 대한 액세스를 허용할 수 있습니다.

외부 리소스 생성

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

배포 전에 [레시피 템플릿을 다운로드](#)할 수 있습니다.

배포 시간: 약 40~90분

1. <https://console.aws.amazon.com/cloudformation> 에서 AWS Management Console 로그인하고 AWS CloudFormation 콘솔을 엽니다.

Note

관리자 계정인지 확인하세요.

2. [콘솔에서 템플릿을 실행](#)합니다.

AWS GovCloud (미국 서부) 지역에 배포하는 경우 GovCloud 파티션 계정에서 [템플릿을 실행하십시오](#).

3. 템플릿 매개 변수를 입력합니다.

파라미터	기본값	설명
DomainName	corp.res.com	액티브 디렉터리에 사용되는 도메인입니다. 기본값은 부트스트랩 사용자를 설정하는 LDIF 파일에 제공됩니다. 기본 사용자를 사용하려면 값을 기본값으로 두십시오. 값을 변경하려면 별도의 LDIF 파일을 업데이트하여 제공하십시오. 액티브 디렉터리에 사용되는 도메인과 일치하지 않아도 됩니다.

파라미터	기본값	설명
SubDomain (GovCloud 전용)		<p>이 매개변수는 상업 지역의 경우 선택사항이지만 지역에는 GovCloud 필수입니다.</p> <p>SubDomaina를 입력하면 DomainName 제공된 매개변수 앞에 매개변수 접두사가 붙습니다. 제공된 Active Directory 도메인 이름은 하위 도메인이 됩니다.</p>
AdminPassword		<p>액티브 디렉터리 관리자의 암호 (사용자 이름Admin). 이 사용자는 초기 부트스트랩 단계에서 Active Directory에 생성되며 이후에는 사용되지 않습니다.</p> <p>참고: 이 사용자의 암호는 Active Directory의 암호 복잡성 요구 사항을 충족해야 합니다.</p>

파라미터	기본값	설명
ServiceAccountPassword		<p>서비스 계정을 만드는 데 사용되는 암호 (ReadOnlyUser) 이 계정은 동기화에 사용됩니다.</p> <p>중요: 리서치 앤 엔지니어링 스튜디오 릴리스 2024.06부터는 의 일반 텍스트 비밀번호가 포함된 비밀 ARN을 제공해야 합니다. ServiceAccount</p> <p>참고: 이 사용자의 암호는 Active Directory의 암호 복잡성 요구 사항을 충족해야 합니다.</p>
키페어		<p>SSH 클라이언트를 사용하여 관리 인스턴스를 연결합니다.</p> <p>참고:AWS Systems Manager 세션 관리자를 사용하여 인스턴스에 연결할 수도 있습니다.</p>

파라미터	기본값	설명
LDIFS3Path	aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif	<p>액티브 디렉터리 설정의 부트스트랩 단계에서 가져온 LDIF 파일의 Amazon S3 경로입니다. 자세한 내용은 LDIF 지원을 참조하십시오. 이 매개 변수는 Active Directory에 여러 사용자를 생성하는 파일로 미리 채워집니다.</p> <p>파일을 보려면 에서 사용할 수 있는 res.ldif 파일을 참조하십시오. GitHub</p>
ClientIpCidr		<p>사이트에 액세스하는 데 사용할 IP 주소. 예를 들어 IP 주소를 선택하고 호스트의 액세스만 허용하는 [IPADDRESS]/32 데 사용할 수 있습니다. 배포 후 이 정보를 업데이트할 수 있습니다.</p>
ClientPrefixList		<p>Active Directory 관리 노드에 대한 액세스를 제공하는 접두사 목록을 입력합니다. 관리형 접두사 목록을 만드는 방법에 대한 자세한 내용은 고객 관리 접두사 목록 사용을 참조하십시오.</p>

파라미터	기본값	설명
EnvironmentName	res- <i>[environment name]</i>	PortalDomainName 가 제공되는 경우 이 매개 변수를 사용하여 생성된 암호에 태그를 추가하여 환경 내에서 사용할 수 있습니다. 이는 RES 스택을 생성할 때 사용된 EnvironmentName 매개 변수와 일치해야 합니다. 계정에 여러 환경을 배포하는 경우 이 환경은 고유해야 합니다.
PortalDomainName		GovCloud 배포의 경우 이 파라미터를 입력하지 마십시오. 인증서와 암호는 사전 요구 사항 중에 수동으로 생성되었습니다. Amazon Route 53에 있는 해당 계정의 도메인 이름. 이 정보가 제공되면 공개 인증서와 키 파일이 생성되어 업로드됩니다 AWS Secrets Manager. 자체 도메인과 인증서가 있는 경우 이 매개 변수를 비워 둘 EnvironmentName 수 있습니다.

4. [기능] 의 모든 체크박스를 확인하고 [Create stack] 을 선택합니다.

1단계: 제품 출시

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

배포 시간: 약 60분

이 제품을 배포하기 전에 이 제품의 [CloudFormation 템플릿을 다운로드](#)할 수 있습니다.

AWS GovCloud (미국 서부) 에 배포하는 경우 이 템플릿을 사용하십시오.

res-stack - 이 템플릿을 사용하여 제품 및 모든 관련 구성 요소를 시작할 수 있습니다. 기본 구성은 RES 메인 스택과 인증, 프론트엔드 및 백엔드 리소스를 배포합니다.

Note

AWS CloudFormation 리소스는 AWS Cloud Development Kit (AWS CDK) ()AWS CDK구조에서 생성됩니다.

AWS CloudFormation 템플릿은 연구 및 엔지니어링 스튜디오를 AWS 에 배포합니다. AWS 클라우드 스택을 시작하기 전에 [사전 요구](#) 사항을 충족해야 합니다.

1. <https://console.aws.amazon.com/cloudformation> 에서 **AWS Management Console 로그인**하고 **AWS CloudFormation 콘솔을 엽니다.**
2. **템플릿을 실행**합니다.

AWS GovCloud (미국 서부) 에 배포하려면 이 [템플릿을 실행](#)하세요.

3. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전곳에서 솔루션을 실행하려면 콘솔 탐색 표시줄의 지역 선택기를 사용하십시오.

Note

이 제품은 Amazon Cognito 서비스를 사용하며, 현재는 이 서비스를 전혀 사용할 수 없습니다. AWS 리전 Amazon Cognito를 사용할 수 있는 AWS 리전 곳에서 이 제품을 시작해야 합니다. 지역별 최신 가용성은 [AWS 리전 ai 서비스 목록](#)을 참조하십시오.

4. 매개 변수에서 이 제품 템플릿의 매개 변수를 검토하고 필요에 따라 수정하십시오. 자동화된 외부 리소스를 배포한 경우 외부 리소스 스택의 출력 탭에서 이러한 매개변수를 찾을 수 있습니다.

파라미터	기본값	설명
EnvironmentName	< <i>res-demo</i> >	res-로 시작하고 11자 이하로 시작하는 RES 환경에 부여되는 고유한 이름입니다.

파라미터	기본값	설명
AdministratorEmail		제품 설정을 완료하는 사용자의 이메일 주소입니다. Active Directory 싱글 사인온 통합이 실패할 경우 이 사용자는 브레이크-글래스 사용자 역할도 추가로 수행합니다.
InfrastructureHostAMI	ami- <i>[## ## ###]</i>	(선택 사항) 모든 인프라 호스트에 사용할 사용자 지정 AMI ID를 제공할 수 있습니다. 현재 지원되는 기본 OS는 아마존 리눅스 2입니다. 자세한 정보는 다시 사용할 수 있는 AMI를 구성합니다 를 참조하세요.
SSH KeyPair		인프라 호스트에 연결하는 데 사용되는 키 페어.
[ClientIP]	<i>x.x.x .0/24 ##</i> <i>x.x.x .0/32</i>	시스템 연결을 제한하는 IP 주소 필터. 배포 ClientIpCidr 후 업데이트할 수 있습니다.
ClientPrefixList		(선택 사항) 바스천 호스트에 웹 UI 및 SSH에 직접 액세스할 수 있도록 허용된 IP의 관리 접두사 목록을 제공하십시오.
IAM PermissionBoundary		(선택 사항) RES에서 생성한 모든 역할에 권한 경계로 연결되는 관리형 정책 ARN을 제공할 수 있습니다. 자세한 정보는 사용자 지정 권한 범위 설정 을 참조하세요.

파라미터	기본값	설명
VpcId		인스턴스가 시작될 VPC의 IP.
IsLoadBalancerInternetFacing		인터넷 연결 로드 밸런서를 배포하려면 true를 선택합니다 (로드 밸런서에는 퍼블릭 서브넷 필요). 제한된 인터넷 액세스가 필요한 배포의 경우 false를 선택하십시오.
LoadBalancerSubnets		로드 밸런서가 실행될 서로 다른 가용 영역에 있는 서브넷을 두 개 이상 선택하십시오. 제한된 인터넷 액세스가 필요한 배포의 경우 프라이빗 서브넷을 선택하십시오. 인터넷 액세스가 필요한 배포의 경우 퍼블릭 서브넷을 선택하십시오. 외부 네트워킹 스택에서 2개 이상을 생성한 경우 생성된 스택을 모두 선택하십시오.
InfrastructureHostSubnets		인프라 호스트가 시작될 서로 다른 가용 영역에서 최소 두 개의 프라이빗 서브넷을 선택합니다. 외부 네트워킹 스택에서 2개 이상을 생성한 경우, 생성된 스택을 모두 선택하십시오.

파라미터	기본값	설명
VdiSubnets		VDI 인스턴스가 시작될 서로 다른 가용 영역에서 두 개 이상의 프라이빗 서브넷을 선택합니다. 외부 네트워킹 스택에서 2개 이상을 생성한 경우 생성된 것을 모두 선택하십시오.
ActiveDirectoryName	<i>corp.res.com</i>	액티브 디렉터리의 도메인. 포털 도메인 이름과 일치하지 않아도 됩니다.
AD ShortName	<i>corp</i>	액티브 디렉터리의 약칭. 이를 NetBIOS 이름이라고도 합니다.
LDAP 베이스	<i>DC=corp,DC=res,DC=com</i>	LDAP 계층 구조 내의 베이스에 대한 LDAP 경로입니다.
LDAP 연결 URI		액티브 디렉터리의 호스트 서버가 도달할 수 있는 단일 ldap://경로. 기본 AD 도메인을 사용하여 자동화된 외부 리소스를 배포한 경우 ldap://corp.res.com을 사용할 수 있습니다.
ServiceAccountUserName	ServiceAccount	AD에 연결하는 데 사용되는 서비스 계정의 사용자 이름입니다. 이 계정에는 ComputerSOU 내에서 컴퓨터를 만들 수 있는 액세스 권한이 있어야 합니다.

파라미터	기본값	설명
ServiceAccountPasswordSecretArn		에 대한 일반 텍스트 암호가 포함된 보안 ARN을 제공하십시오. ServiceAccount
사용자: Ou		동기화할 사용자를 위한 AD 내 조직 단위.
GroupSOU		동기화할 그룹을 위한 AD 내 조직 단위.
SudoerSou		전 세계 사용자를 위한 AD 내 조직 단위.
SudoersGroupName	RES 관리자	설치 시 인스턴스에 sudoer 액세스 권한이 있고 RES에서 관리자 액세스 권한을 가진 모든 사용자를 포함하는 그룹 이름입니다.
컴퓨터/SOU		인스턴스가 가입할 AD 내 조직 단위.
도메인 TLS ARN CertificateSecret		(선택 사항) AD와의 TLS 통신을 가능하게 하는 도메인 TLS 인증서 암호 ARN을 제공합니다.

파라미터	기본값	설명
EnableLdapID 매핑		UID 및 GID 번호가 SSSD에서 생성되는지 또는 AD에서 제공한 번호를 사용하는지를 결정합니다. SSSD에서 생성한 UID 및 GID를 사용하려면 True로 설정하고 AD에서 제공하는 UID 및 GID를 사용하려면 False로 설정합니다. 대부분의 경우 이 파라미터를 True로 설정해야 합니다.
애드조인 비활성화	False	Linux 호스트가 디렉터리 도메인에 가입하지 못하게 하려면 True로 변경하십시오. 그렇지 않으면 기본 설정인 False를 그대로 두십시오.
ServiceAccountUserDN		디렉터리에 서비스 계정 사용자의 DN (고유 이름) 을 입력합니다.
SharedHomeFilesystemID		Linux VDI 호스트의 공유 홈 파일 시스템에 사용할 EFS ID입니다.
CustomDomainNameforWebApp		(선택 사항) 웹 포털에서 시스템의 웹 부분에 대한 링크를 제공하는 데 사용하는 하위 도메인.
CustomDomainNameforVDI		(선택 사항) 웹 포털에서 시스템의 VDI 부분에 대한 링크를 제공하는 데 사용하는 하위 도메인.

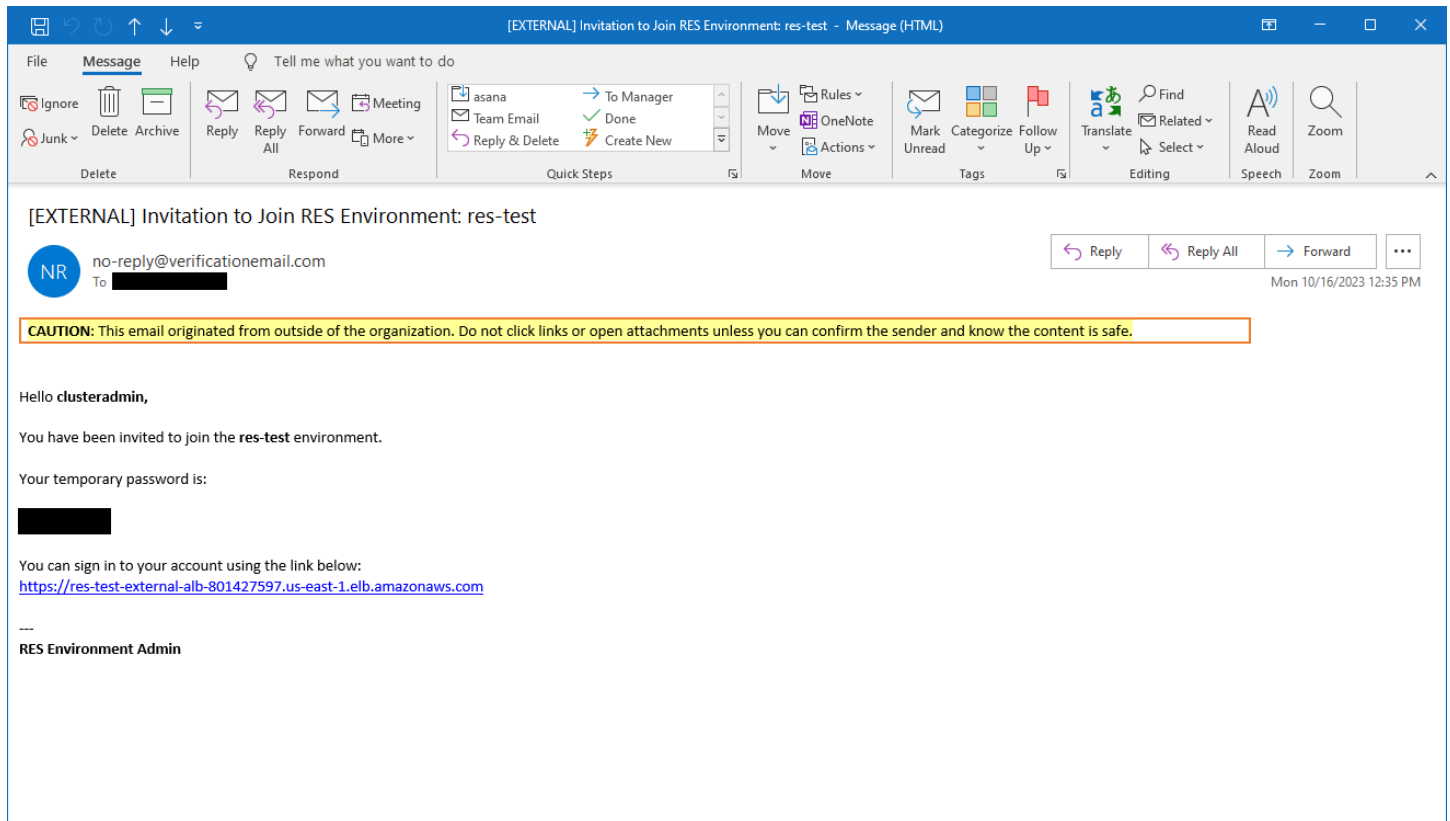
파라미터	기본값	설명
ACM 인증서 EAR NforWebApp		(선택 사항) 기본 구성을 사용하는 경우 제품은 amazonaws.com 도메인에서 웹 애플리케이션을 호스팅합니다. 도메인에서 제품 서비스를 호스팅할 수 있습니다. 자동화된 외부 리소스를 배포한 경우 이 리소스는 자동으로 생성되었으며 res-bi 스택의 출력에서 해당 정보를 찾을 수 있습니다. 웹 애플리케이션용 인증서를 생성해야 하는 경우 을 참조하십시오. 구성 가이드
CertificateSecretARNForVDI		(선택 사항) 이 ARN 암호는 웹 포털의 공개 인증서용 공개 인증서를 저장합니다. 자동화된 외부 리소스에 포털 도메인 이름을 설정하는 경우 res-bi 스택의 Outputs 탭에서 이 값을 찾을 수 있습니다.
PrivateKeySecretARNForVDI		(선택 사항) 이 ARN 암호는 웹 포털 인증서의 개인 키를 저장합니다. 자동화된 외부 리소스에 포털 도메인 이름을 설정하는 경우 res-bi 스택의 Outputs 탭에서 이 값을 찾을 수 있습니다.

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

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

2단계: 처음으로 로그인하기

제품 스택이 계정에 배포되면 자격 증명이 포함된 이메일을 받게 됩니다. URL을 사용하여 계정에 로그인하고 다른 사용자를 위한 작업 영역을 구성하십시오.



처음으로 로그인한 후에는 SSO 공급자에 연결하도록 웹 포털에서 설정을 구성할 수 있습니다. 배포 후 구성 정보는 를 참조하십시오. [구성 가이드](#)

제품 업데이트

Research and Engineering Studio (RES)에서는 버전 업데이트가 메이저 버전인지 마이너 버전인지에 따라 두 가지 방법으로 제품을 업데이트할 수 있습니다.

RES는 날짜 기반 버전 관리 체계를 사용합니다. 메이저 릴리스는 연도와 월을 사용하고, 마이너 릴리스는 필요한 경우 시퀀스 번호를 추가합니다. 예를 들어 버전 2024.01은 2024년 1월에 메이저 릴리스로 릴리스되었고 버전 2024.01.01은 해당 버전의 마이너 릴리스 업데이트입니다.

주제

- [메이저 버전 업데이트](#)
- [마이너 버전 업데이트](#)

메이저 버전 업데이트

Research and Engineering Studio는 스냅샷을 사용하여 환경 설정을 그대로 유지하면서 이전 RES 환경에서 최신 RES 환경으로 마이그레이션할 수 있도록 지원합니다. 또한 사용자를 온보딩하기 전에 이 프로세스를 사용하여 환경 업데이트를 테스트하고 확인할 수 있습니다.

최신 버전의 RES로 환경을 업데이트하려면:

1. 현재 환경의 스냅샷을 만드세요. [the section called “스냅샷 생성”](#)를 참조하세요.
2. 새 버전으로 RES를 재배포하십시오. [the section called “1단계: 제품 실행”](#)를 참조하세요.
3. 업데이트된 환경에 스냅샷을 적용합니다. [the section called “스냅샷 적용”](#)를 참조하세요.
4. 모든 데이터가 새 환경으로 성공적으로 마이그레이션되었는지 확인하십시오.

마이너 버전 업데이트

RES에 대한 마이너 버전 업데이트의 경우 새로 설치할 필요가 없습니다. AWS CloudFormation 템플릿을 업데이트하여 기존 RES 스택을 업데이트할 수 있습니다. 업데이트를 AWS CloudFormation 배포하기 전에 현재 RES 환경의 버전을 확인하십시오. 템플릿 시작 부분에서 버전 번호를 찾을 수 있습니다.

예: "Description": "RES_2024.1"

마이너 버전을 업데이트하려면:

1. 에서 최신 AWS CloudFormation 템플릿을 다운로드하십시오 [the section called “1단계: 제품 실행”](#).
2. <https://console.aws.amazon.com/cloudformation> 에서 AWS CloudFormation 콘솔을 엽니다.
3. 스택에서 기본 스택을 찾아 선택합니다. 다음과 같이 *<stack-name>* 표시되어야 합니다.
4. 업데이트를 선택합니다.
5. 현재 템플릿 바꾸기를 선택합니다.
6. 템플릿 소스로 템플릿 파일 업로드를 선택합니다.
7. 파일 선택을 선택하고 다운로드한 템플릿을 업로드합니다.
8. 스택 세부 정보 지정에서 다음을 선택합니다. 파라미터를 업데이트할 필요는 없습니다.
9. 스택 옵션 구성에서 다음을 선택합니다.
10. [검토] 에서 *<stack-name>*[제출] 을 선택합니다.

제품 제거

또는 를 사용하여 제품의 연구 및 엔지니어링 스튜디오를 제거할 수 있습니다. AWS AWS Management Console AWS Command Line Interface이 제품에서 생성한 Amazon Simple Storage 서비스 (Amazon S3) 버킷을 수동으로 삭제해야 합니다. 보존할 데이터를 저장한 shared-storage-security-group 경우 이 제품은 < EnvironmentName >-를 자동으로 삭제하지 않습니다.

사용 AWS Management Console

1. [AWS CloudFormation 콘솔](#)에 로그인합니다.
2. 스택 페이지에서 이 제품의 설치 스택을 선택합니다.
3. 삭제를 선택합니다.

사용 AWS Command Line Interface

사용자 환경에서 AWS Command Line Interface (AWS CLI) 를 사용할 수 있는지 확인하십시오. 설치 지침은 사용 [설명서의 AWS Command Line Interface내용](#)을 참조하십시오. AWS CLI 제품이 배포된 지역의 관리자 계정에서 를 사용할 수 있고 구성되었는지 확인한 후 다음 명령을 실행합니다. AWS CLI

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

삭제 shared-storage-security-group

Warning

제품은 의도하지 않은 데이터 손실을 방지하기 위해 기본적으로 이 파일 시스템을 보존합니다. 보안 그룹 및 관련 파일 시스템을 삭제하기로 선택하면 해당 시스템에 보관된 모든 데이터가 영구적으로 삭제됩니다. 데이터를 백업하거나 새 보안 그룹에 데이터를 재할당하는 것이 좋습니다.

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/efs/> 에서 Amazon EFS 콘솔을 엽니다.

2. <RES-stack-name>-와 관련된 모든 파일 시스템을 삭제합니다 shared-storage-security-group. 또는 이러한 파일 시스템을 다른 보안 그룹에 재할당하여 데이터를 유지할 수도 있습니다.
3. AWS Management Console [로그인하고 https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/) 에서 Amazon EC2 콘솔을 엽니다.
4. *shared-storage-security-group*<RES-stack-name>-를 삭제합니다.

Amazon S3 버킷 삭제

이 제품은 우발적인 데이터 손실을 방지하기 위해 AWS CloudFormation 스택을 삭제하기로 결정한 경우 제품에서 생성한 Amazon S3 버킷 (옵트인 지역에 배포용) 을 보존하도록 구성되어 있습니다. 제품을 제거한 후 데이터를 보존할 필요가 없다면 이 S3 버킷을 수동으로 삭제할 수 있습니다. 다음 단계에 따라 Amazon S3 버킷을 삭제합니다.

1. AWS Management Console 로그인하고 <https://console.aws.amazon.com/s3/> 에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 버킷을 선택합니다.
3. stack-nameS3 버킷을 찾습니다.
4. 각 Amazon S3 버킷을 선택한 다음 비우기를 선택합니다. 각 버킷을 비워야 합니다.
5. S3 버킷을 선택하고 [Delete] 를 선택합니다.

를 사용하여 AWS CLI S3 버킷을 삭제하려면 다음 명령을 실행합니다.

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

Note

이 --force 명령은 버킷의 내용을 비웁니다.

구성 가이드

이 구성 안내서는 기술 담당자를 대상으로 제품의 Research and Engineering Studio를 추가로 사용자 지정하고 통합하는 방법에 대한 배포 후 지침을 제공합니다. AWS

주제

- [사용자 및 그룹 관리](#)
- [하위 도메인 생성](#)
- [ACM 인증서 생성](#)
- [아마존 CloudWatch 로그](#)
- [사용자 지정 권한 범위 설정](#)
- [다시 사용할 수 있는 AMI를 구성합니다](#)

사용자 및 그룹 관리

연구 및 엔지니어링 스튜디오는 모든 SAML 2.0 준수 ID 공급자를 사용할 수 있습니다. 외부 리소스를 사용하여 RES를 배포했거나 IAM ID 센터를 사용할 계획이라면 을 참조하십시오. [the section called “IAM ID 센터를 통한 SSO 설정”](#) SAML 2.0을 준수하는 자체 ID 공급자가 있는 경우 을 참조하십시오. [the section called “싱글 사인온 \(SSO\) 을 위한 ID 공급자 구성”](#)

주제

- [IAM 아이덴티티 센터를 통한 SSO 설정](#)
- [싱글 사인온 \(SSO\) 을 위한 ID 공급자 구성](#)
- [사용자 암호 설정](#)

IAM 아이덴티티 센터를 통한 SSO 설정

ID 센터가 관리형 액티브 디렉터리에 아직 연결되어 있지 않다면 다음으로 시작하십시오. [the section called “ID 센터 설정”](#) ID 센터가 이미 관리형 액티브 디렉터리에 연결되어 있다면 다음으로 시작하십시오. [the section called “ID 센터에 연결”](#).

Note

AWS GovCloud (미국 서부) 지역에 배포하는 경우 Research and Engineering Studio를 배포한 AWS GovCloud (US) 파티션 계정에 SSO를 설정하십시오.

1단계: ID 센터 설정

ID 센터 활성화

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/iam/> 에서 IAM 콘솔을 엽니다.
2. 아이덴티티 센터를 엽니다.
3. 활성화를 선택합니다.
4. 다음으로 활성화를 선택합니다 AWS Organizations.
5. 계속을 선택합니다.

Note

관리형 액티브 디렉터리가 있는 지역과 동일한 지역에 있는지 확인하세요.

ID 센터를 관리형 액티브 디렉터리에 연결

ID 센터를 활성화한 후 다음 권장 설정 단계를 완료하십시오.

1. 탐색에서 설정을 선택합니다.
2. ID 소스에서 작업을 선택하고 ID 소스 변경을 선택합니다.
3. 기존 디렉터리에서 디렉터리를 선택합니다.
4. 다음을 선택합니다.
5. 변경 내용을 검토하고 확인 **ACCEPT** 상자에 입력합니다.
6. ID 소스 변경을 선택합니다.

사용자 및 그룹을 ID 센터에 동기화

변경이 [the section called “ID 센터를 관리형 액티브 디렉터리에 연결”](#) 완료되면 녹색 배너가 나타납니다.

1. 확인 배너에서 가이드 설정 시작을 선택합니다.
2. 속성 매핑 구성에서 다음을 선택합니다.
3. 사용자 섹션에서 동기화할 사용자를 입력합니다.
4. 추가를 선택합니다.
5. 다음을 선택합니다.
6. 변경 내용을 검토하고 구성 저장을 선택합니다.
7. 동기화 프로세스는 몇 분 정도 걸릴 수 있습니다. 동기화되지 않는 사용자에게 대한 경고 메시지가 표시되면 동기화 재개를 선택합니다.

사용자 활성화

1. 메뉴에서 사용자를 선택합니다.
2. 액세스를 활성화하려는 사용자를 선택합니다.
3. 사용자 액세스 활성화를 선택합니다.

2단계: ID 센터에 연결

ID 센터에서 애플리케이션 설정

1. 에 AWS Management Console 로그인하고 <https://console.aws.amazon.com/singlesignon/> 에서 IAM 아이덴티티 센터를 엽니다.
2. [Applications]를 선택합니다.
3. 애플리케이션 추가를 선택합니다.
4. 설정 기본 설정에서 설정하려는 애플리케이션이 있습니다를 선택합니다.
5. 애플리케이션 유형에서 SAML 2.0을 선택합니다.
6. 다음을 선택합니다.
7. 사용하려는 디스플레이 이름과 설명을 입력합니다.
8. IAM ID 센터 메타데이터에서 IAM ID 센터 SAML 메타데이터 파일의 링크를 복사합니다. RES 포털에서 SSO를 구성할 때 필요합니다.

9. 애플리케이션 속성에서 애플리케이션 시작 URL을 입력합니다. 예: < your-portal-domain >/sso
10. 애플리케이션 ACS URL에서 RES 포털의 리디렉션 URL을 입력합니다. 이를 찾으려면:
 - a. 환경 관리에서 일반 설정을 선택합니다.
 - b. ID 제공자 탭을 선택합니다.
 - c. 싱글 사인온에서 SAML 리디렉션 URL을 찾을 수 있습니다.
11. 애플리케이션 SAML 오디언스에서 Amazon Cognito URN을 입력합니다. URN을 생성하려면:
 - a. RES 포털에서 일반 설정을 엽니다.
 - b. ID 제공자 탭에서 사용자 풀 ID를 찾습니다.
 - c. 사용자 풀 ID를 다음 문자열에 추가합니다.

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

12. 제출을 선택합니다.

애플리케이션의 속성 매핑 구성

1. ID 센터에서 생성한 애플리케이션의 세부 정보를 엽니다.
2. 작업을 선택하고 속성 매핑 편집을 선택합니다.
3. 제목에 \$ {user:email} 를 입력합니다.
4. 형식에서 이메일 주소를 선택합니다.
5. 새 속성 매핑 추가를 선택합니다.
6. 애플리케이션의 사용자 속성에 이메일을 입력합니다.
7. IAM ID 센터의 이 문자열 값 또는 사용자 속성에 매핑하기 아래에 \$ {user:email} 을 입력합니다.
8. 형식에 지정되지 않음을 입력합니다.
9. 변경 사항 저장를 선택합니다.

ID 센터에서 응용 프로그램에 사용자 추가

1. ID 센터에서 생성한 애플리케이션에 할당된 사용자를 열고 사용자 할당을 선택합니다.
2. 애플리케이션 액세스 권한을 할당하려는 사용자를 선택합니다.
3. 사용자 배정을 선택합니다.

RES 환경 내에서 SSO 설정

1. 연구 및 엔지니어링 스튜디오 환경에서 환경 관리에서 일반 설정을 엽니다.
2. ID 제공자 탭을 엽니다.
3. SSO (Single Sign-On) 에서 상태 옆의 편집 버튼을 선택합니다.
4. 다음 정보를 포함하여 양식을 작성하십시오.
 - a. SAML을 선택합니다.
 - b. 제공자 이름 아래 사용자에게 친숙한 이름을 입력합니다.
 - c. 메타데이터 문서 엔드포인트 URL 입력을 선택합니다.
 - d. 중에 복사한 URL을 입력합니다. [the section called “ID 센터에서 애플리케이션 설정”](#)
 - e. 제공업체 이메일 속성에 이메일을 입력합니다.
 - f. 제출을 선택합니다.
5. 페이지를 새로 고치고 상태가 활성화된 것으로 표시되는지 확인합니다.

싱글 사인온 (SSO) 을 위한 ID 공급자 구성

연구 및 엔지니어링 스튜디오는 모든 SAML 2.0 ID 공급자와 통합하여 RES 포털에 대한 사용자 액세스를 인증합니다. 이 단계는 선택한 SAML 2.0 ID 공급자와 통합하기 위한 지침을 제공합니다. IAM ID 센터를 사용하려는 경우 을 참조하십시오. [the section called “IAM ID 센터를 통한 SSO 설정”](#)

Note

사용자의 이메일은 IDP SAML 어설션과 액티브 디렉터리에서 일치해야 합니다. ID 공급자를 Active Directory에 연결하고 정기적으로 사용자를 동기화해야 합니다.

주제

- [ID 공급자를 구성하십시오.](#)
- [ID 공급자를 사용하도록 RES를 구성하십시오.](#)
- [비프로덕션 환경에서 ID 제공자 구성](#)
- [SAML IdP 문제 디버깅](#)

ID 공급자를 구성하십시오.

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

1. RES는 RES 포털 및 프로젝트에 액세스할 수 있는 사용자 ID가 포함된 AD (AWS 관리형 AD 또는 자체 프로비저닝 AD)가 있다고 가정합니다. AD를 ID 서비스 공급자에 연결하고 사용자 ID를 동기화합니다. ID 제공업체의 설명서를 확인하여 AD를 연결하고 사용자 ID를 동기화하는 방법을 알아보세요. 예를 들어 [사용 설명서의 Active Directory를 ID 소스로 사용을 참조하십시오](#). AWS IAM Identity Center
2. ID 공급자 (IdP) 에서 RES용 SAML 2.0 애플리케이션을 구성합니다. 이 구성에는 다음과 같은 매개 변수가 필요합니다.
 - SAML 리디렉션 URL — IdP가 서비스 공급자에게 SAML 2.0 응답을 보내는 데 사용하는 URL입니다.

Note

IdP에 따라 SAML 리디렉션 URL의 이름이 다를 수 있습니다.

- 애플리케이션 URL
- 어설션 컨슈머 서비스 (ACS) URL
- ACS POST 바인딩 URL

URL을 가져오려면

1. 관리자 또는 클러스터 관리자로 RES에 로그인합니다.
2. 환경 관리 → 일반 설정 → ID 제공자로 이동합니다.
3. SAML 리디렉션 URL을 선택합니다.

- SAML 오디언스 URI — 서비스 제공자 측 SAML 오디언스 엔티티의 고유 ID입니다.

Note

IdP에 따라 SAML 오디언스 URI의 이름이 다를 수 있습니다.

- ClientID

- 애플리케이션 SAML 오디언스
- SP 개체 ID

다음 형식으로 입력을 제공합니다.

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

SAML 오디언스 URI를 찾으려면

1. 관리자 또는 클러스터 관리자로 RES에 로그인합니다.
 2. 환경 관리 → 일반 설정 → ID 제공자로 이동합니다.
 3. 사용자 풀 ID를 선택합니다.
3. RES에 게시된 SAML 어설션에는 사용자의 이메일 주소로 다음 필드/클레임이 설정되어 있어야 합니다.
- SAML 제목 또는 네임ID
 - SAML 이메일
4. IdP는 구성에 따라 SAML 어설션에 필드/클레임을 추가합니다. RES에는 다음 필드가 필요합니다. 대부분의 공급자는 기본적으로 이 필드를 자동으로 채웁니다. 구성해야 하는 경우 다음 필드 입력 및 값을 참조하십시오.
- AudienceRestriction — 로 설정합니다. `urn:amazon:cognito:sp:user-pool-id`. Amazon Cognito 사용자 풀의 *user-pool-id* ID로 바꾸십시오.

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

- 응답 — InResponseTo 로 설정합니다. `https://user-pool-domain/saml2/idpresponse` Amazon Cognito 사용자 풀의 도메인 *user-pool-domain* 이름으로 바꾸십시오.

```
<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 Recipient InResponseTo ID로 설정합니다.

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

- AuthnStatement— 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 이 필드를 다음과 같이 설정합니다.
`<domain-url>/saml2/logout`

도메인 URL을 가져오려면

1. 관리자 또는 클러스터 관리자로 RES에 로그인합니다.
 2. 환경 관리 ⇒ 일반 설정 ⇒ ID 제공자로 이동합니다.
 3. 도메인 URL을 선택합니다.
6. IdP가 Amazon Cognito와의 신뢰를 구축하기 위한 서명 인증서를 수락하는 경우 Amazon Cognito 서명 인증서를 다운로드하여 IdP에 업로드하십시오.

서명 인증서를 받으려면

1. [시작하기](#) 섹션에서 Amazon Cognito 콘솔을 엽니다. AWS Management Console

2. 사용자 풀을 선택합니다. 사용자 풀은 다음과 같아야 `res-<environment name>-user-pool` 합니다.
3. [로그인 환경(Sign-in experience)] 탭을 선택합니다.
4. 페더레이션 ID 제공자 로그인 섹션에서 서명 인증서 보기를 선택합니다.

Cognito user pool sign-in Info

Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

Cognito user pool sign-in options

User name
Email

User name requirements

User names are not case sensitive

Federated identity provider sign-in (1) Info
Refresh Delete Add identity provider View signing certificate

Your app users can sign-in through external social identity providers like Facebook, Google, Amazon, or Apple, and through your on-prem directories via SAML or Open ID Connect.

Identity provider	Identity provider type	Created time	Last updated time
<input type="radio"/> idc	SAML	2 weeks ago	3 hours ago

이 인증서를 사용하여 Active Directory IDP를 설정하고, 추가하고, 이 신뢰 당사자에 대한 SAML 지원을 활성화할 수 있습니다. relying party trust

Note

이는 키클로크 및 IDC에는 적용되지 않습니다.

5. 애플리케이션 설정이 완료되면 SAML 2.0 애플리케이션 메타데이터 XML 또는 URL을 다운로드합니다. 다음 섹션에서 사용할 수 있습니다.

ID 공급자를 사용하도록 RES를 구성하십시오.

RES용 싱글 사인온 설정을 완료하려면

1. 관리자 또는 클러스터 관리자로 RES에 로그인합니다.
2. 환경 관리 ⇒ 일반 설정 ⇒ ID 제공자로 이동합니다.

Environment Settings

View and manage environment settings. [View Environment Status](#)

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

[General](#) | [Network](#) | **[Identity Provider](#)** | [Directory Service](#) | [Analytics](#) | [Metrics](#) | [CloudWatch Logs](#) | [SES](#) | [EC2](#) | [Back](#)

Identity Provider

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

Single Sign-On

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

- SSO (Single Sign-On) 에서 상태 표시기 옆에 있는 편집 아이콘을 선택하여 SSO (Single Sign-On) 구성 페이지를 엽니다.

Single Sign On Configuration ✕

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

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

OIDC
Configure trust between Cognito and an OIDC identity provider,

Provider Name
Name used for the provider in cognito

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

Upload metadata document

Enter metadata document endpoint URL

Metadata document

📎 **Choose file**

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

Refresh Token Expiration (hours)
Must be between 1 and 87600 (10 years)

12

Cancel

Submit

- a. ID 공급자의 경우 SAML을 선택합니다.
- b. 제공자 이름에는 ID 공급자의 고유한 이름을 입력합니다.

Note

다음 이름은 허용되지 않습니다.

- Cognito
- IdentityCenter

- c. 메타데이터 문서 소스에서 적절한 옵션을 선택하고 메타데이터 XML 문서를 업로드하거나 ID 제공자의 URL을 제공합니다.
 - d. 제공자 이메일 속성에 텍스트 값을 입력합니다email.
 - e. 제출을 선택합니다.
4. 환경 설정 페이지를 다시 로드하십시오. 구성이 올바르면 SSO (Single Sign-On) 가 활성화됩니다.

비프로덕션 환경에서 ID 제공자 구성

제공된 [외부 리소스](#)를 사용하여 비프로덕션 RES 환경을 만들고 IAM Identity Center를 ID 공급자로 구성한 경우 Okta와 같은 다른 ID 공급자를 구성하는 것이 좋습니다. RES SSO 활성화 양식에서는 다음과 같은 세 가지 구성 매개변수를 요청합니다.

1. 제공자 이름 - 수정할 수 없음
2. 메타데이터 문서 또는 URL — 수정 가능
3. 제공자 이메일 속성 — 수정 가능

메타데이터 문서 및 제공자 이메일 속성을 수정하려면 다음과 같이 하십시오.

1. Amazon Cognito 콘솔로 이동합니다.
2. 탐색에서 사용자 풀을 선택합니다.
3. 사용자 풀을 선택하면 사용자 풀 개요를 볼 수 있습니다.
4. 로그인 경험 탭에서 페더레이션 ID 제공자 로그인으로 이동하여 구성된 ID 공급자를 엽니다.
5. 일반적으로 메타데이터만 변경하고 속성 매핑은 변경하지 않고 그대로 두면 됩니다. 속성 매핑을 업데이트하려면 편집을 선택합니다. 메타데이터 문서를 업데이트하려면 메타데이터 바꾸기를 선택합니다.

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

View, add, and edit attribute mappings between SAML and your user pool. < 1 > ⚙

User pool attribute	SAML attribute
email	email

Metadata document [Info](#) Replace metadata

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

<p>Metadata document source Enter metadata document endpoint URL</p>	<p>Metadata document endpoint URL https://portal.sso.us-west-2.amazonaws.com/saml/metadata/MDg4ODM3NTczNjY0X2lucy04M2EyYTYyMGUzZTFiMDI4</p>
---	--

6. 속성 매핑을 편집한 경우 DynamoDB에서 <environment name>.cluster-settings 테이블을 업데이트해야 합니다.
 - a. DynamoDB 콘솔을 열고 탐색에서 테이블을 선택합니다.
 - b. <environment name>.cluster-settings 테이블을 찾아 선택한 다음 작업 메뉴에서 항목 탐색을 선택합니다.
 - c. 스캔 또는 쿼리 항목에서 필터로 이동하여 다음 매개 변수를 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 찾은 다음 편집을 선택하여 Amazon Cognito의 변경 사항에 맞게 문자열을 수정합니다.

▼ **Scan or query items**

Scan
 Query

Select a table or index: Table - res-jan19.cluster-settings
 Select attribute projection: All attributes

▼ **Filters** 6

Attribute name	Type	Condition	Value	
<input type="text" value="key"/>	String	Equal to	identity-provider	Remove

Add filter

Run Reset

✔ Completed. Read capacity units consumed: 13
✕

Items returned (1)

Item	Actions
<input type="checkbox"/> key (String)	
<input type="checkbox"/> identity-provider.cognito.ss	<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> <p>Edit String ✕</p> <p><input type="text" value="email"/></p> <p>Enter any string value.</p> <p>Cancel Save</p> </div>

8
< 1 >
⚙️
✕

version
1

SAML IdP 문제 디버깅

SAML 추적기 — Chrome 브라우저용 이 확장 프로그램을 사용하여 SAML 요청을 추적하고 SAML 어설션 값을 확인할 수 있습니다. [자세한 내용은 Chrome 웹 스토어의 SAML-트레이서를 참조하십시오.](#)

SAML 개발자 도구 - SAML로 인코딩된 값을 디코딩하고 SAML 어설션의 필수 필드를 확인하는 데 사용할 수 있는 도구를 OneLogin 제공합니다. 자세한 내용은 웹 사이트의 [Base 64 디코드 + 팽창](#)을 참조하십시오. OneLogin

Amazon CloudWatch Logs — 로그에서 RES CloudWatch 로그에서 오류나 경고를 확인할 수 있습니다. 로그는 이름 형식의 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 추가](#)를 참조하십시오.

사용자 암호 설정

1. [AWS Directory Service 콘솔에서](#) 생성된 스택의 디렉토리를 선택합니다.
2. 작업 메뉴에서 사용자 암호 재설정을 선택합니다.
3. 사용자를 선택하고 새 비밀번호를 입력합니다.
4. 비밀번호 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) 지역에 배포하는 경우 도메인 퍼블릭 호스팅 영역을 호스팅하는 상업용 파티션 계정에서 웹 애플리케이션과 VDI 하위 도메인을 설정하십시오.

1. AWS Management Console [로그인하고 https://console.aws.amazon.com/route53/](https://console.aws.amazon.com/route53/) 에서 Route 53 콘솔을 엽니다.
2. 생성한 도메인을 찾아 레코드 생성을 선택합니다.
3. 레코드 이름으로 web을 입력합니다.
4. 레코드 유형으로 CNAME을 선택합니다.
5. Value에는 초기 이메일에서 받은 링크를 입력합니다.
6. 레코드 생성을 선택합니다.
7. VDC에 대한 레코드를 생성하려면 NLB 주소를 검색하십시오.
 - a. [에 AWS Management Console 로그인하고 https://console.aws.amazon.com/cloudformation](https://console.aws.amazon.com/cloudformation/) 에서 AWS CloudFormation 콘솔을 엽니다.
 - b. <environment-name>-vdc를 선택합니다.
 - c. 리소스를 선택하고 엽니다<environmentname>-vdc-external-nlb.

- d. NLB에서 DNS 이름을 복사합니다.
8. <https://console.aws.amazon.com/route53/> 에서 Route 53 콘솔에 **AWS Management Console** 로 **그인하고 여십시오.**
9. 도메인을 찾아 레코드 생성을 선택합니다.
10. 레코드 이름 아래에 를 입력합니다vdc.
11. 레코드 유형(Record type)에서 CNAME을 선택합니다.
12. NLB의 경우 DNS를 입력합니다.
13. Create Record Set(레코드 세트 생성)를 선택합니다.

ACM 인증서 생성

기본적으로 RES는 amazonaws.com 도메인을 사용하는 애플리케이션 로드 밸런서에서 웹 포털을 호스팅합니다. 자체 도메인을 사용하려면 사용자가 제공하거나 ACM에서 요청한 퍼블릭 SSL/TLS 인증서를 구성해야 합니다. AWS Certificate Manager ACM을 사용하는 경우 클라이언트와 웹 서비스 호스트 간의 SSL/TLS 채널을 암호화하기 위한 매개변수로 제공해야 하는 AWS 리소스 이름을 받게 됩니다.

Tip

외부 리소스 데모 패키지를 배포하는 경우 외부 리소스 스택을 배포할 PortalDomainName 때 선택한 도메인을 입력해야 합니다. [the section called “외부 리소스 생성”](#)

커스텀 도메인용 인증서를 만들려면:

1. 콘솔에서 [AWS Certificate Manager](#) 열어 공개 인증서를 요청합니다. AWS GovCloud (미국 서부)에 배포하는 경우 GovCloud 파티션 계정에서 인증서를 생성하십시오.
2. 공개 인증서 요청을 선택하고 다음을 선택합니다.
3. 도메인 이름에서 *.PortalDomainName 및 모두에 대한 인증서를 PortalDomainName 요청합니다.
4. 검증 방법에서 DNS 검증을 선택합니다.
5. 요청을 선택합니다.
6. 인증서 목록에서 요청한 인증서를 엽니다. 각 인증서는 검증 보류 중 상태로 표시됩니다.

Note

인증서가 보이지 않으면 목록을 새로 고치세요.

7. 다음 중 하나를 수행하십시오.
 - 상업용 배포: 요청된 각 인증서의 인증서 세부 정보에서 Route 53에 레코드 생성을 선택합니다. 인증서 상태가 발급됨으로 변경되어야 합니다.
 - GovCloud 배포: AWS GovCloud (미국 서부) 에 배포하는 경우 CNAME 키와 값을 복사하십시오. 상업용 파티션 계정에서 값을 사용하여 퍼블릭 호스팅 영역에 새 레코드를 생성합니다. 인증서 상태가 Issued로 변경되어야 합니다.
8. 파라미터로 입력할 새 인증서 ARN을 복사합니다. ACMCertificateARNforWebApp

아마존 CloudWatch 로그

리서치 앤 엔지니어링 스튜디오는 설치 CloudWatch 중에 다음과 같은 로그 그룹을 생성합니다. 기본 보존에 대해서는 다음 표를 참조하십시오.

CloudWatch 로그 그룹	Retention
/aws/lambda/ < >-클러스터 엔드포인트 installation-stack-name	만료되지 않음
/AWS/람다/ < >-sync installation-stack-name cluster-manager-scheduled-ad	만료되지 않음
/aws/lambda/ < >-클러스터 설정 installation-stack-name	만료되지 않음
/AWS/람다/ < >-oauth-자격 증명 installation-stack-name	만료되지 않음
/AWS/람다/ < >- installation-stack-name self-signed-certificate	만료되지 않음
/AWS/람다/ < >- installation-stack-name update-cluster-prefix-list	만료되지 않음

CloudWatch 로그 그룹	Retention
/AWS/람다/ < >- installation-stack-name vdc-scheduled-event-transformer	만료되지 않음
/aws/lambda/ < >-클라이언트 범위 installation-stack-name vdc-update-cluster-manager	만료되지 않음
/< >/클러스터 관리자 installation-stack-name	3개월
/< installation-stack-name >/vdc/컨트롤러	3개월
/< installation-stack-name >/vdc/dcv-broker	3개월
/< installation-stack-name >/vdc/ dcv-connection-gateway	3개월

로그 그룹의 기본 보존을 변경하려면 <https://console.aws.amazon.com/cloudwatch/> **CloudWatch** 콘솔로 이동하여 로그에서 로그 데이터 보존 [변경의](#) 지침을 따를 수 있습니다. CloudWatch

사용자 지정 권한 범위 설정

2024.04부터는 사용자 지정 권한 경계를 추가하여 RES에서 생성한 역할을 선택적으로 수정할 수 있습니다. IAM PermissionBoundary 파라미터의 일부로 권한 경계의 ARN을 제공하여 사용자 지정 권한 경계를 RES AWS CloudFormation 설치의 일부로 정의할 수 있습니다. 이 매개변수를 비워 두면 모든 RES 역할에 권한 경계가 설정되지 않습니다. 다음은 RES 역할이 작동하는 데 필요한 작업 목록입니다. 사용하려는 모든 권한 경계가 다음 작업을 명시적으로 허용하는지 확인하십시오.

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

```

다시 사용할 수 있는 AMI를 구성합니다

RES 지원 AMI를 사용하면 사용자 지정 AMI에 가상 데스크톱 인스턴스 (VDI)에 대한 RES 종속성을 사전 설치할 수 있습니다. RES-Ready AMI를 사용하면 사전 베이킹된 이미지를 사용하는 VDI 인스턴스의 부팅 시간이 개선됩니다. EC2 Image Builder를 사용하면 AMI를 새 소프트웨어 스택으로 구축하고 등록할 수 있습니다. Image Builder에 대한 자세한 내용은 [Image Builder 사용 설명서](#)를 참조하십시오.

시작하기 전에 [최신 버전의 RES를 배포해야](#) 합니다.

주제

- [RES 환경에 액세스할 수 있도록 IAM 역할을 준비하십시오.](#)
- [EC2 Image Builder 구성 요소 생성](#)
- [EC2 Image Builder 레시피 준비](#)
- [EC2 Image Builder 인프라 구성](#)

- [Image Builder 이미지 파이프라인 설정](#)
- [Image Builder 이미지 파이프라인 실행](#)
- [RES에 새 소프트웨어 스택을 등록합니다.](#)

RES 환경에 액세스할 수 있도록 IAM 역할을 준비하십시오.

EC2 Image Builder에서 RES 환경 서비스에 액세스하려면 RES-EC2 라는 IAM 역할을 생성하거나 수정해야 합니다. InstanceProfileForImageBuilder Image Builder에서 사용할 수 있도록 IAM 역할을 구성하는 방법에 대한 자세한 내용은 Image Builder 사용 설명서의 [AWS Identity and Access Management \(IAM\)](#) 을 참조하십시오.

역할에 필요한 사항은 다음과 같습니다.

- 신뢰할 수 있는 관계에는 Amazon EC2 서비스가 포함됩니다.
- 아마존/SSM ManagedInstanceCore 및 EC2 정책 InstanceProfileForImageBuilder
- 배포된 RES 환경에 대한 DynamoDB 및 Amazon S3 액세스가 제한된 사용자 지정 RES 정책

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

신뢰할 수 있는 관계 주체:

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

RES 정책:

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

```

"Statement": [
  {
    "Sid": "RES DynamoDB Access",
    "Effect": "Allow",
    "Action": "dynamodb:GetItem",
    "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-EnvironmentName}.cluster-settings",
    "Condition": {
      "ForAllValues:StringLike": {
        "dynamodb:LeadingKeys": [
          "global-settings.gpu_settings.*",
          "global-settings.package_config.*"
        ]
      }
    }
  },
  {
    "Sid": "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/*"
  }
]
}

```

EC2 Image Builder 구성 요소 생성

Image Builder 사용 [안내서의 Image Builder 콘솔을 사용하여 구성 요소를 생성하는](#) 지침을 따르십시오.

구성 요소 세부 정보를 입력합니다.

1. 유형에서 빌드를 선택합니다.
2. 이미지 운영 체제 (OS) 의 경우 Linux 또는 Windows를 선택합니다.
3. 구성 요소 이름에는 다음과 같은 의미 있는 이름을 입력합니다 **research-and-engineering-studio-vdi-<operating-system>**.
4. 구성 요소의 버전 번호를 입력하고 필요에 따라 설명을 추가합니다.
5. 정의 문서의 경우 다음 정의 파일을 입력합니다. 오류가 발생하는 경우 YAML 파일은 공백을 구분하므로 원인일 가능성이 높습니다.

Linux

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

phases:
  - name: build
    steps:
      - name: PrepareRESBootstrap
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - 'mkdir -p /root/bootstrap/logs'
```

```

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

```

Windows

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

phases:
  - name: build
    steps:
      - name: CreateRESBootstrapFolder
        action: CreateFolder
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - path: 'C:\Users\Administrator\RES\Bootstrap'
            overwrite: true
```



```

- name: DownloadRESWindowsInstallPackage
  action: S3Download
  onFailure: Abort
  maxAttempts: 3
  inputs:
    - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
      {{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
      res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
      destination:
        '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvReleaseVersion }}'
      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 만들고 구성 요소 만들기를 선택합니다.

EC2 Image Builder 레시피 준비

Note

CentOS 7은 현재 2024년 6월 end-of-life 30일에 출시될 예정입니다. 연구 및 엔지니어링 스튜디오 버전 2024.06은 CentOS 7을 지원하는 마지막 버전이 될 것입니다.

EC2 Image Builder 레시피는 새 이미지를 생성하기 위한 출발점으로 사용할 기본 이미지를 정의합니다. 새 이미지를 정의하는 동시에 이미지를 사용자 정의하고 모든 것이 예상대로 작동하는지 확인하기

위해 사용자가 추가하는 구성 요소 집합도 정의합니다. 필요한 RES 소프트웨어 종속성을 사용하여 대상 AMI를 구성하려면 레시피를 만들거나 수정해야 합니다. 레시피에 대한 자세한 내용은 [레시피 관리](#)를 참조하십시오.

RES는 다음 이미지 운영 체제를 지원합니다.

- 아마존 리눅스 2 (x86 및 ARM64)
- 센토스 7 (x86 및 ARM64)
- RHEL 7 (x86), 8 (x86), 9 (x86)
- 우분투 22.04.3 (x86)
- 윈도우 2019, 2022년 (x86)

Create a new recipe

1. 에서 EC2 Image Builder 콘솔을 <https://console.aws.amazon.com/imagebuilder> 엽니다.
2. 저장된 리소스에서 이미지 레시피를 선택합니다.
3. 이미지 레시피 생성을 선택합니다.
4. 고유한 이름과 버전 번호를 입력합니다.
5. RES에서 지원하는 기본 이미지를 선택합니다.
6. SSM 에이전트가 사전 설치되어 있지 않은 경우 인스턴스 구성에서 SSM 에이전트를 설치합니다. 사용자 데이터 및 기타 필요한 사용자 데이터에 정보를 입력합니다.

Note

SSM 에이전트 설치 방법에 대한 자세한 내용은 다음을 참조하십시오.

- [Linux용 EC2 인스턴스에 SSM 에이전트를 수동으로 설치](#)
- [Windows 서버용 EC2 인스턴스에서 SSM 에이전트를 수동으로 설치 및 제거](#)

7. Linux 기반 레시피의 경우 Amazon 관리 `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.
8. Linux 또는 Windows 환경용으로 만든 EC2 Image Builder 구성 요소를 추가하고 필요한 파라미터 값을 입력합니다. 필수 입력 파라미터는 AWSAccountID, RES EnvNameEnvRegion, RES 및 RES입니다EnvReleaseVersion.

⚠ Important

Linux 환경에서는 `aws-cli-version-2-linux` 빌드 구성 요소를 먼저 추가한 후 이러한 구성 요소를 순서대로 추가해야 합니다.

9. (권장) Amazon 관리 `simple-boot-test-<linux-or-windows>` 테스트 구성 요소를 추가하여 AMI를 시작할 수 있는지 확인합니다. 이는 최소 권장 사항입니다. 요구 사항을 충족하는 다른 테스트 구성 요소를 선택할 수 있습니다.
10. 필요한 경우 옵션 섹션을 모두 작성하고 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 관리 `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 환경용으로 만든 EC2 Image Builder 구성 요소를 추가하고 필요한 파라미터 값을 입력합니다. 필수 입력 파라미터는 `AWSAccountID`, `RES EnvNameEnvRegion`, `RES` 및 `RES입니다EnvReleaseVersion`.

⚠ Important

Linux 환경에서는 `aws-cli-version-2-linux` 빌드 구성 요소를 먼저 추가한 후 이러한 구성 요소를 순서대로 추가해야 합니다.

3. 필요한 경우 옵션 섹션을 모두 작성하고 원하는 다른 구성 요소를 추가한 다음 레시피 만들기를 선택합니다.

EC2 Image Builder 인프라 구성

인프라 구성을 사용하여 Image Builder가 Image Builder 이미지를 구축하고 테스트하는 데 사용하는 Amazon EC2 인프라를 지정할 수 있습니다. RES와 함께 사용하려면 새 인프라 구성을 생성하거나 기존 인프라 구성을 사용할 수 있습니다.

- 새 인프라 구성을 만들려면 인프라 구성 [만들기](#)를 참조하십시오.

- 기존 인프라 구성을 사용하려면 인프라 구성을 [업데이트하세요](#).

Image Builder 인프라를 구성하려면:

1. IAM 역할의 경우 이전에 구성한 역할을 입력합니다. [the section called “RES 환경에 액세스하기 위한 IAM 역할 준비”](#)
2. 인스턴스 유형에서는 메모리가 4GB 이상이고 선택한 기본 AMI 아키텍처를 지원하는 유형을 선택합니다. [Amazon EC2 인스턴스](#) 유형을 참조하십시오.
3. VPC, 서브넷, 보안 그룹의 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 설정

Image Builder 이미지 파이프라인은 기본 이미지, 빌드 및 테스트용 구성 요소, 인프라 구성, 배포 설정을 조합합니다. RES 지원 AMI용 이미지 파이프라인을 구성하려면 새 파이프라인을 생성하거나 기존 파이프라인을 사용할 수 있습니다. 자세한 내용은 [Image Builder 사용 설명서의 AMI 이미지 파이프라인 생성 및 업데이트](#)를 참조하십시오.

Create a new Image Builder pipeline

1. 에서 Image Builder 콘솔을 엽니다 <https://console.aws.amazon.com/imagebuilder>.
2. 탐색에서 이미지 파이프라인을 선택합니다.
3. 이미지 파이프라인 생성을 선택합니다.
4. 고유한 이름, 선택적 설명, 일정, 빈도를 입력하여 파이프라인 세부 정보를 지정합니다.
5. 레시피 선택에서 기존 레시피 사용을 선택하고 에서 생성한 레시피를 선택합니다 [the section called “EC2 Image Builder 레시피 준비”](#). 레시피 세부 정보가 정확한지 확인하세요.
6. 이미지 생성 프로세스 정의의 경우 사용 사례에 따라 기본 또는 사용자 지정 워크플로를 선택합니다. 대부분의 경우 기본 워크플로로도 충분합니다. 자세한 내용은 [EC2 Image Builder 파이프라인의 이미지 워크플로 구성](#)을 참조하십시오.
7. 인프라 구성 정의에서 기존 인프라 구성 선택을 선택하고 에서 [the section called “EC2 Image Builder 인프라 구성”](#) 생성한 인프라 구성을 선택합니다. 인프라 세부 정보가 정확한지 확인하십시오.

8. 배포 설정 정의에서 서비스 기본값을 사용하여 배포 설정 생성을 선택합니다. 출력 이미지는 RES 환경과 AWS 리전 같아야 합니다. 서비스 기본값을 사용하면 Image Builder가 사용되는 지역에 이미지가 생성됩니다.
9. 파이프라인 세부 정보를 검토하고 파이프라인 생성을 선택합니다.

Modify an existing Image Builder pipeline

1. 기존 파이프라인을 사용하려면 에서 만든 레시피를 사용하도록 세부 정보를 [the section called “EC2 Image Builder 레시피 준비”](#) 수정하세요.
2. 변경 사항 저장을 선택합니다.

Image Builder 이미지 파이프라인 실행

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

이미지 파이프라인을 실행하려면:

1. 이미지 파이프라인에서 에서 [the section called “Image Builder 이미지 파이프라인 설정”](#) 만든 파이프라인을 선택합니다.
2. 액션에서 파이프라인 실행을 선택합니다.

RES에 새 소프트웨어 스택을 등록합니다.

1. 의 지침에 따라 소프트웨어 [the section called “소프트웨어 스택 \(AMI\)”](#) 스택을 등록하십시오.
2. AMI ID의 경우 내장된 출력 이미지의 AMI ID를 입력합니다 [the section called “Image Builder 이미지 파이프라인 실행”](#).

관리자 가이드

이 관리자 안내서는 기술 담당자를 위해 AWS 제품을 추가로 사용자 지정하고 Research and Engineering Studio와 통합하는 방법에 대한 추가 지침을 제공합니다.

주제

- [세션 관리](#)
- [환경 관리](#)
- [보안 암호 관리](#)
- [비용 모니터링 및 제어](#)
- [권한](#)

세션 관리

세션 관리는 세션 개발 및 테스트를 위한 유연한 대화형 환경을 제공합니다. 관리자는 사용자가 프로젝트 환경 내에서 대화형 세션을 만들고 관리하도록 허용할 수 있습니다.

주제

- [대시보드](#)
- [세션](#)
- [소프트웨어 스택 \(AMI\)](#)
- [권한 프로필](#)
- [디버깅](#)
- [데스크톱 설정](#)


대시보드

Research and Engineering Studio
demoadmin1 ▾

RES > Virtual Desktop > Dashboard
7 C 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.

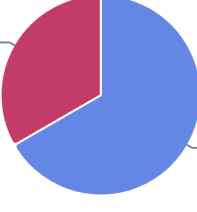


STOPPING

■ STOPPING

Base OS 3

Summary of all virtual desktop sessions by Base OS.

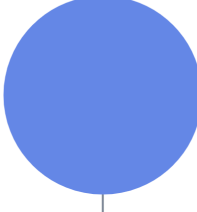


Windows
Amazon Linu...

■ Amazon Linux 2
■ Windows

Project 4

Summary of all virtual desktop sessions by Project Code.

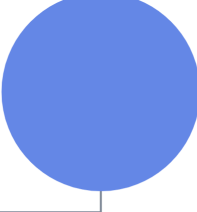


project1

■ project1

Availability Zones 5

Summary of all virtual desktop sessions by Availability Zone.



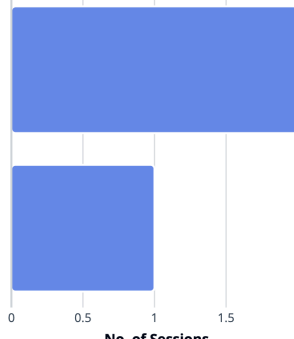
us-west-2a

■ us-west-2a

Software Stacks 6

Summary of all virtual desktop sessions by Software Stack.

Software Stacks



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

■ Sessions

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

세션 관리 대시보드를 통해 관리자는 다음을 빠르게 확인할 수 있습니다.

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 업데이트하십시오.
8. 세션 보기를 선택하여 세션으로 이동합니다.

세션

세션에는 연구 및 엔지니어링 스튜디오 내에서 만든 모든 가상 데스크톱이 표시됩니다. 세션 페이지에서 세션 정보를 필터링 및 보거나 새 세션을 생성할 수 있습니다.

RES > Virtual Desktops > Sessions

Sessions (2)

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

Created ▾ Last 1 month Actions ▾ Create Session

Search All States All Operating Systems

Session Name	Owner	Base OS	Instance Ty...	State	Project	Created On
<input checked="" type="checkbox"/> demoadmin1aml21	demoadmin1	Amazon Linux 2	m6a.large	Stopped	project1	9/27/2023, 8:31:50 AM
<input type="checkbox"/> demoadmin1windows1	demoadmin1	Windows	m6a.large	Stopped	project1	9/27/2023, 8:38:23 AM

1. 메뉴를 사용하여 지정된 기간 내에 생성되거나 업데이트된 세션별로 결과를 필터링할 수 있습니다.
2. 세션을 선택하고 Actions 메뉴를 사용하여 다음을 수행하십시오.
 - a. 세션 재개
 - b. 세션 중지/하이버네이트

- c. 강제 중지/하이버네이트 세션
 - d. 세션 종료
 - e. 세션 강제 종료
 - f. 세션 (들) 건강
 - g. 소프트웨어 스택 생성
3. 세션 생성을 선택하여 새 세션을 생성합니다.
 4. 이름으로 세션을 검색하고 상태 및 운영 체제별로 필터링합니다.
 5. 자세한 내용을 보려면 세션 이름을 선택하십시오.

세션 생성

1. [세션 생성] 을 선택합니다. 새 가상 데스크톱 시작 모달이 열립니다.
2. 새 세션의 세부 정보를 입력합니다.
3. (선택 사항) 고급 옵션 표시를 켜서 서브넷 ID 및 DCV 세션 유형과 같은 추가 세부 정보를 제공하십시오.
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

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

세션 세부 정보

세션 목록에서 세션 이름을 선택하여 세션 세부 정보를 확인합니다.

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

Session: demoadmin1aml21

General Information

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

< **Details** Server Software Stack Project Permissions Schedule Monitoring Session >

Session Details

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

소프트웨어 스택 (AMI)

📘 Note

제공된 CentSO7 소프트웨어 스택을 실행하려면 [연결된](#) 표준 계정을 AWS Marketplace 사용하여 AMI를 구독해야 합니다. AWS GovCloud (US)

소프트웨어 스택 페이지에서 Amazon 머신 이미지 (AMI) 를 구성하고 기존 AMI를 관리할 수 있습니다.

Software Stacks

Manage your Virtual Desktop Software Stacks

Search All Operating Systems ▼

Name	Description	AMI ID	Base OS	Root Volume Size	Min RAM	GPU Manufacturer	Created On
<input type="radio"/> CentOS7 - ARM64	CentOS7 - ARM64	ami-07f692d95b2b9c8c5	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> CentOS7 - x86_64	CentOS7 - x86_64	ami-00f8e2c955f7ffa9b	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> RHEL8 - x86_64	RHEL8 - x86_64	ami-0b530377951178d6b	RedHat Enterprise Linux 8	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> UBUNTU2204 - x86_64	UBUNTU2204 - x86_64	ami-073ffe13d826b7f8	Ubuntu 22.04	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> RHEL7 - x86_64	RHEL7 - x86_64	ami-0bb2449c2217c9b0	RedHat Enterprise Linux 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Windows - x86_64	Windows - x86_64	ami-0667133d0dc6089e1	Windows	30GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Windows -AMD	Windows -AMD	ami-05df91be1d294f195	Windows	30GB	4GB	AMD	6/7/2024, 11:25:20 AM
<input type="radio"/> Windows -NVIDIA	Windows -NVIDIA	ami-00d7af9d003819a90	Windows	30GB	4GB	NVIDIA	6/7/2024, 11:25:20 AM
<input type="radio"/> RHEL9 - x86_64	RHEL9 - x86_64	ami-099f85fc24d27c2a7	RedHat Enterprise Linux 9	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Amazon Linux 2 - ARM64	Amazon Linux 2 - ARM64	ami-04ed2b27d86c17f09	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
<input type="radio"/> Amazon Linux 2 - x86_64	Amazon Linux 2 - x86_64	ami-0ee5c62243ab25259	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM

1. 기존 소프트웨어 스택을 검색하려면 운영 체제 드롭다운을 사용하여 OS별로 필터링하십시오.
2. 소프트웨어 스택의 이름을 선택하면 스택에 대한 세부 정보를 볼 수 있습니다.
3. 소프트웨어 스택을 선택한 후 Actions 메뉴를 사용하여 스택을 편집하고 스택을 프로젝트에 할당합니다.
4. 소프트웨어 스택 등록 버튼을 사용하면 새 스택을 만들 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

GPU Manufacturer

Select the GPU Manufacturer for the software stack

Min. Storage Size (GB)

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

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

Projects

Select applicable projects for the software stack

프로젝트에 소프트웨어 스택 할당

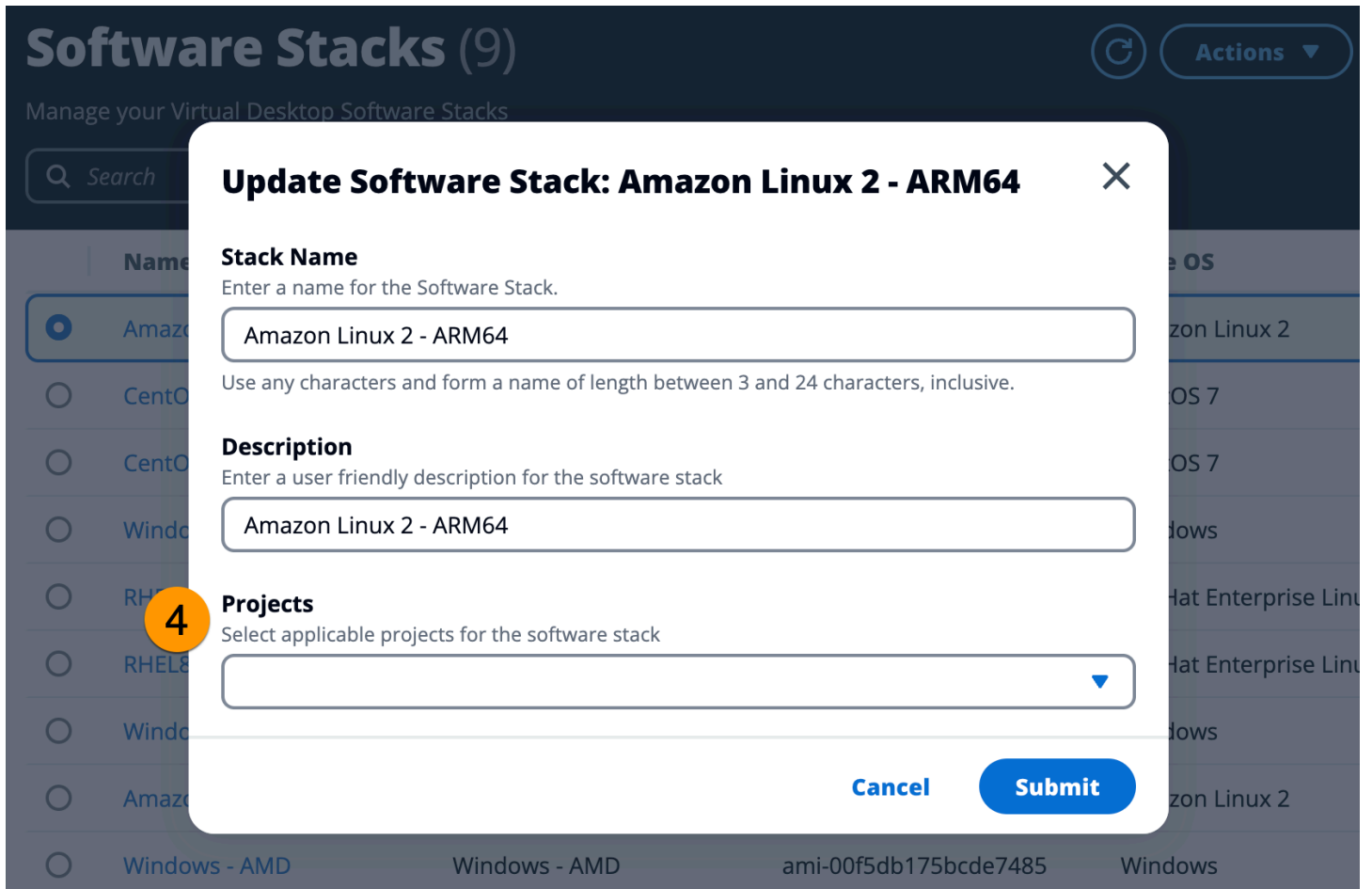
새 소프트웨어 스택을 생성할 때 스택을 프로젝트에 할당할 수 있습니다. 초기 생성 후 프로젝트에 스택을 추가해야 하는 경우 다음을 수행하십시오.

Note

자신이 멤버로 속해 있는 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.

권한 프로필

권한 프로필을 사용하여 권한에 대한 재사용 가능한 프로필을 만들고 관리할 수 있습니다.

Research and Engineering Studio

RES > Virtual Desktops > Permission Profiles

Permission Profiles

Manage your Virtual Desktop Permission Profiles

1

3 Actions Create Permission Profile

4

Profile ID	Title	Description	Created On
<input checked="" type="radio"/> observer_profile	View Only Profile	This profile grants view only access on the DCV Session. Can see screen only. Can not control session	10/3/2023, 2:27:32 PM
<input type="radio"/> admin_profile	Admin Profile	This profile grants the same access as the Admin on the DCV Session	10/3/2023, 2:27:32 PM
<input type="radio"/> collaborator_profile	Collaboration Profile	This profile grants certain access on the DCV Session. Can see screen, control mouse and keyboard.	10/3/2023, 2:27:32 PM
<input type="radio"/> owner_profile	Owner Profile	This profile grants the same access as the Session Owner on the DCV Session	10/3/2023, 2:27:32 PM

1. 권한 프로필을 검색합니다.
2. 세부 정보를 보려면 프로필 ID를 선택합니다.
3. 프로필을 선택하면 작업 메뉴를 사용하여 프로필을 편집합니다.
4. 권한 프로필 만들기를 선택하여 새 프로필을 생성합니다.

권한 프로필 생성

1. 권한 프로필 생성을 선택합니다.
2. 새 프로필의 세부 정보를 입력하고 권한 토글을 사용하여 프로필에 대한 권한을 선택합니다.
3. 제출을 선택합니다.

Register new Permission Profile



Profile ID

Enter a Unique Profile ID for the Permission Profile

Title

Enter a user friendly Title for the Permission Profile

Description

Enter a user friendly description for the Permission Profile

Built In

All features

Display

Receive visual data from the NICE DCV server

Pointer

View NICE DCV server mouse position events and pointer shapes

Mouse

Input from the client mouse to the NICE DCV server

Keyboard

Input from the client keyboard to the NICE DCV server

Audio In

Send audio from the client to the NICE DCV server

Audio Out

Receive audio from the NICE DCV server to the client

Clipboard Copy

Copy data from the NICE DCV server to the client clipboard

Clipboard Paste

Copy data to the NICE DCV server from the client clipboard

File Upload

Upload files to the session storage

File Download

Download files from the session storage

USB

Use USB devices from the client

Printer

Create PDFs or XPS files from the NICE DCV server to the client

Smartcard

Read the smart card from the client

Stylus

Input from specialized USB devices, such as 3D pointing devices or graphic tablets

Keyboard SAS

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

Web Camera

Use the Web Camera connected to a client device in a session

Touch

Use native touch events from the client device

Screenshot

Save a screenshot of the remote desktop

Gamepad

Use gamepads connected to a client computer in a session

Unsupervised Access

Allow a user to connect to session without supervision

Cancel

Submit

권한 프로필 편집

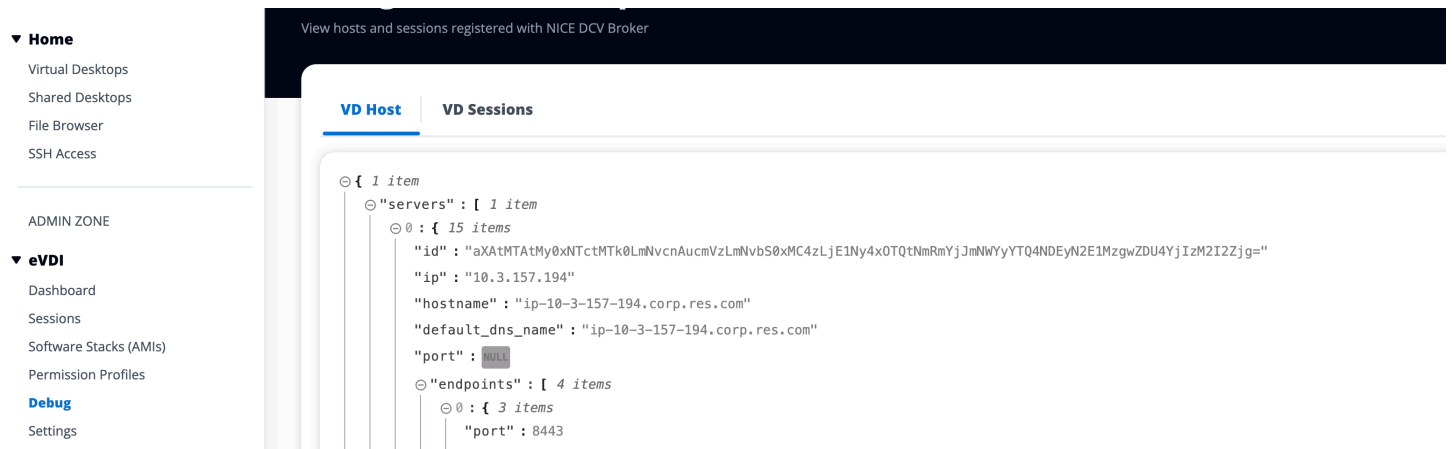
1. 권한 프로필 페이지에서 편집해야 하는 권한 프로필을 선택합니다.
2. 작업을 선택합니다.
3. 권한 프로필 편집을 선택합니다.
4. 프로필을 편집합니다.
5. 제출을 선택합니다.

권한 프로필 세부 정보 보기

권한 프로필 목록에서 프로필 ID를 선택하여 세부 정보를 확인합니다. 세부 정보 페이지에서 편집을 선택하여 권한 프로필을 편집할 수도 있습니다.

디버깅

디버깅 패널에는 가상 데스크톱과 관련된 메시지 트래픽이 표시됩니다. 이 패널을 사용하여 호스트 간 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 관련된 리소스를 구성할 수 있습니다. 서버 탭에서는 다음과 같은 설정에 액세스할 수 있습니다.

- DCV 세션 유효 제한 시간
- 유효 타임아웃 경고
- CPU 사용률 임계값

- 사용자당 허용된 세션

The screenshot displays the configuration page for the 'virtual-desktop-controller' module. The interface includes a left-hand navigation menu with sections for Home, eVDI, and Environment Management. The main content area is divided into tabs: General, Notifications, Server, Controller, Broker, Connection Gateway, Backup, and CloudWatch Logs. The 'General' tab is active, showing settings for QUIC (Disabled), Subnet AutoRetry (Enabled), eVDI Subnets (two subnets: subnet-0706342f7d6fa0082 and subnet-023f50062d2b46030), and Randomize Subnets (Disabled). Below this, the 'OpenAPI Specification' section provides links to the eVDI API Spec and the Swagger Editor.

환경 관리

RES의 환경 관리 섹션에서 관리자는 연구 및 엔지니어링 프로젝트를 위해 격리된 환경을 만들고 관리할 수 있습니다. 이러한 환경에는 컴퓨팅 리소스, 스토리지 및 기타 필수 구성 요소가 모두 보안 환경 내에 포함될 수 있습니다. 사용자는 프로젝트의 특정 요구 사항에 맞게 이러한 환경을 구성하고 사용자 지정할 수 있으므로 다른 프로젝트 또는 환경에 영향을 주지 않고 솔루션을 쉽게 실험, 테스트 및 반복할 수 있습니다.

주제

- [프로젝트](#)
- [사용자](#)
- [그룹](#)
- [파일 시스템](#)
- [환경 상태](#)
- [스냅샷 관리](#)
- [환경 설정](#)

프로젝트

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

주제

- [프로젝트 보기](#)
- [프로젝트 생성](#)
- [프로젝트 편집](#)
- [프로젝트에 태그 추가 또는 제거](#)
- [프로젝트와 관련된 파일 시스템 보기](#)
- [시작 템플릿 추가](#)

프로젝트 보기

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

프로젝트 대시보드는 사용할 수 있는 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 비용 할당을 추적하는 데 사용할 수 있는 리소스 AWS Cost Explorer Service태그입니다. 자세한 내용은 [사용자 정의 비용 할당 태그 활성화](#)를 참조하십시오.

Important

프로젝트 ID를 만든 후에는 변경할 수 없습니다.

고급 옵션에 대한 자세한 내용은 [을 참조하십시오](#) [시작 템플릿 추가](#).

3. (선택 사항) 프로젝트 예산을 설정합니다. 예산에 대한 자세한 내용은 [을 참조하십시오](#). [비용 모니터링 및 제어](#)
4. 사용자 및/또는 그룹에 적절한 역할 (“프로젝트 구성원” 또는 “프로젝트 소유자”) 을 할당하십시오. 각 역할이 취할 수 있는 조치는 [권한](#) 참조하십시오.
5. 제출을 선택합니다.

Create new Project

Project Definition

Title

Enter a user friendly project title

Project ID

Enter a project id

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

Description

Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

Add file systems

Select applicable file systems for the Project

home [efs] X

▶ Advanced Options

Team Configurations

Groups

Select applicable ldap groups for the Project

Add group

Role

Choose a role for the group

Remove group

Users

Select applicable users for the Project

Add user

Role

Choose a role for the user

Remove user

Cancel

Submit

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](#) 을 참조하십시오. 고급 옵션에 대한 자세한 내용은 을 참조하십시오 [시작 템플릿 추가](#).
4. 제출을 선택합니다.

Edit Project

Project Definition

Title
Enter a user friendly project title

Project ID
Enter a project-id

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

Description
Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

▼ **Advanced Options**

Add Policies
Select applicable policies for the Project

Add Security Groups
Select applicable security groups for the Project

▶ **Linux**

▶ **Windows**

Team Configurations

<p>Groups Select applicable ldap groups for the Project</p> <input type="text" value="group_1"/> <input type="button" value="Add group"/>	<p>Role Choose a role for the group</p> <input type="text" value="Project Member"/> <input type="button" value="Remove group"/>
<p>Users Select applicable users for the Project</p> <input type="text" value="user1"/> <input type="button" value="Add user"/>	<p>Role Choose a role for the user</p> <input type="text" value="Project Member"/> <input type="button" value="Remove user"/>

프로젝트에 태그 추가 또는 제거

프로젝트 태그는 해당 프로젝트에서 생성된 모든 인스턴스에 태그를 할당합니다.

1. 프로젝트 목록에서 프로젝트를 선택합니다.
2. 작업 메뉴에서 [태그 업데이트] 를 선택합니다.
3. [태그 추가] 를 선택하고 키 값을 입력합니다.
4. 태그를 제거하려면 제거하려는 태그 옆의 제거를 선택합니다.

프로젝트와 관련된 파일 시스템 보기

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

The screenshot shows the 'Projects' management interface. At the top, there's a search bar and a 'Create Project' button. Below is a table with columns: Title, Project Code, Status, Budgets, Groups, and Updated On. One project, 'project-1', is selected. Below the table, a section titled 'File Systems in project-1' is expanded, showing a table with columns: Title, Name, File System ID, Mount Target, Projects, Scope, Provider, and Created through RES?. The table currently shows 'No records'.

시작 템플릿 추가

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

정책 추가

IAM 정책을 추가하여 프로젝트에 배포된 모든 인스턴스에 대한 VDI 액세스를 제어할 수 있습니다. 정책을 온보딩하려면 다음 키값 쌍으로 정책에 태그를 지정하십시오.

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

IAM 역할에 대한 자세한 내용은 IAM의 [정책 및 권한](#)을 참조하십시오.

보안 그룹 추가

보안 그룹을 추가하여 프로젝트 내 모든 VDI 인스턴스의 송신 및 수신 데이터를 제어할 수 있습니다. 보안 그룹을 온보딩하려면 다음 키값 쌍으로 보안 그룹에 태그를 지정하십시오.


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

보안 그룹에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [보안 그룹을 사용한 AWS 리소스 트래픽 제어를](#) 참조하십시오.

시작 스크립트 추가

프로젝트 내 모든 VDI 세션에서 시작되는 시작 스크립트를 추가할 수 있습니다. RES는 Linux 및 Windows용 스크립트 시작을 지원합니다. 스크립트 시작의 경우 다음 중 하나를 선택할 수 있습니다.

VDI가 시작될 때 스크립트 실행

이 옵션은 RES 구성 또는 설치가 실행되기 전에 VDI 인스턴스의 시작 부분에서 스크립트를 시작합니다.

VDI가 구성되면 스크립트를 실행합니다.

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/sample
로컬 파일	파일: ///user/scripts/example.sh

인수의 경우 모든 인수를 쉼표로 구분하여 제공하십시오.

▼ Linux

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

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="https://sample.samplecontent.com/sample"/>	<input type="text"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="file:///root/bootstrap/latest/launch/script"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

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

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

▼ Windows

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

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

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

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

프로젝트 구성 예제

사용자

Active Directory에서 동기화된 모든 사용자는 사용자 페이지에 표시됩니다. 사용자는 제품 구성 중에 클러스터 관리자 사용자에게 의해 동기화됩니다. 초기 사용자 구성에 대한 자세한 내용은 [구성 가이드](#)를 참조하십시오.

Note

관리자는 활성 사용자를 위한 세션만 생성할 수 있습니다. 기본적으로 모든 사용자는 제품 환경에 로그인할 때까지 비활성 상태가 됩니다. 사용자가 비활성 상태인 경우 해당 사용자를 위한 세션을 생성하기 전에 로그인하도록 요청하세요.

Research and Engineering Studio | demoadmin4

RES > Environment Management > Users

Users

Environment user management

1

2 **Actions**

- Set as Admin User
- Disable User

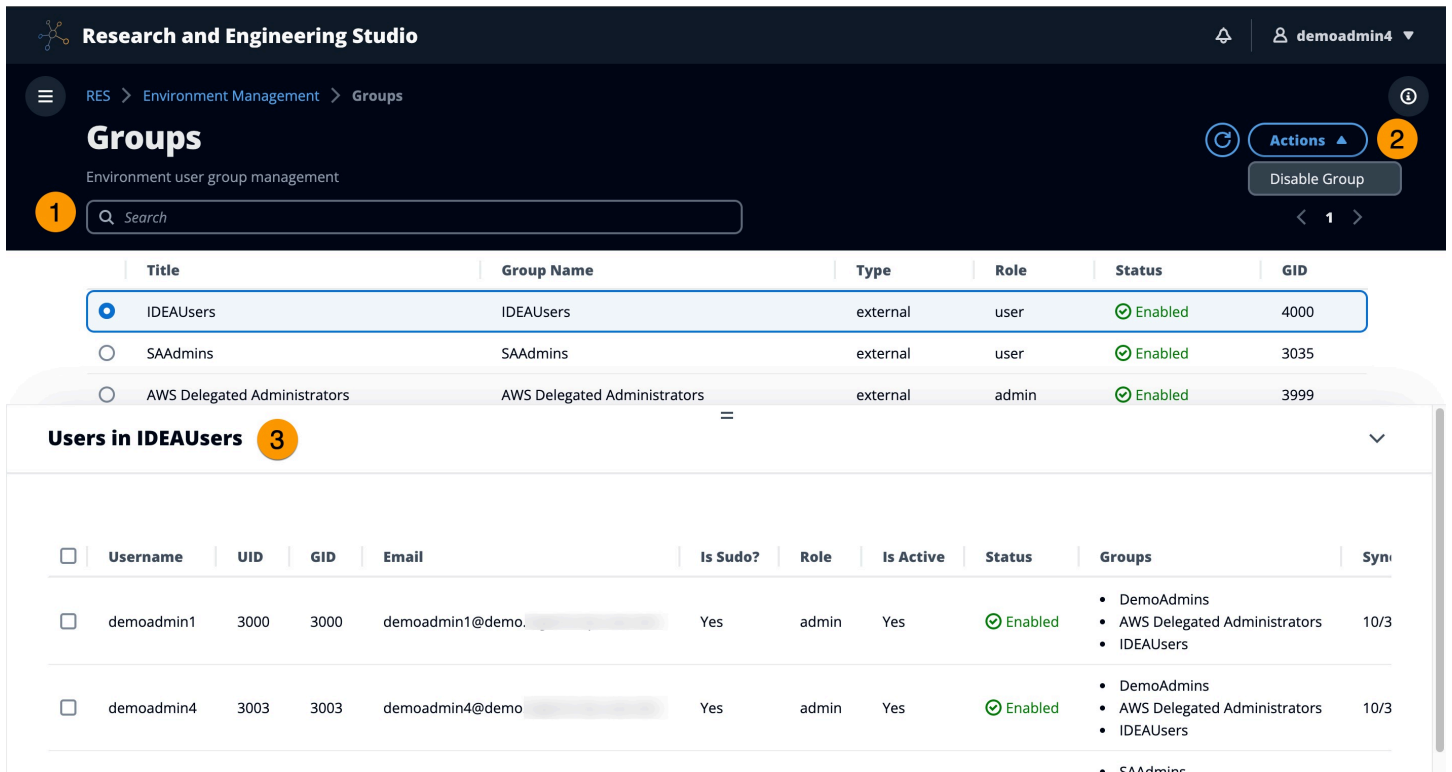
Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
<input checked="" type="radio"/> demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	• IDEAUUsers • DemoUsers
<input type="radio"/> sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	• SAUsers
<input type="radio"/> demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	• DemoAdmins • AWS Delegated Administrators • IDEAUUsers
<input type="radio"/> pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	• ProductUsers

사용자 페이지에서 다음을 수행할 수 있습니다.

1. 사용자를 검색합니다.
2. 사용자 이름을 선택한 경우 작업 메뉴를 사용하여 다음을 수행할 수 있습니다.
 - a. 관리자로 설정
 - b. 사용자 비활성화

그룹

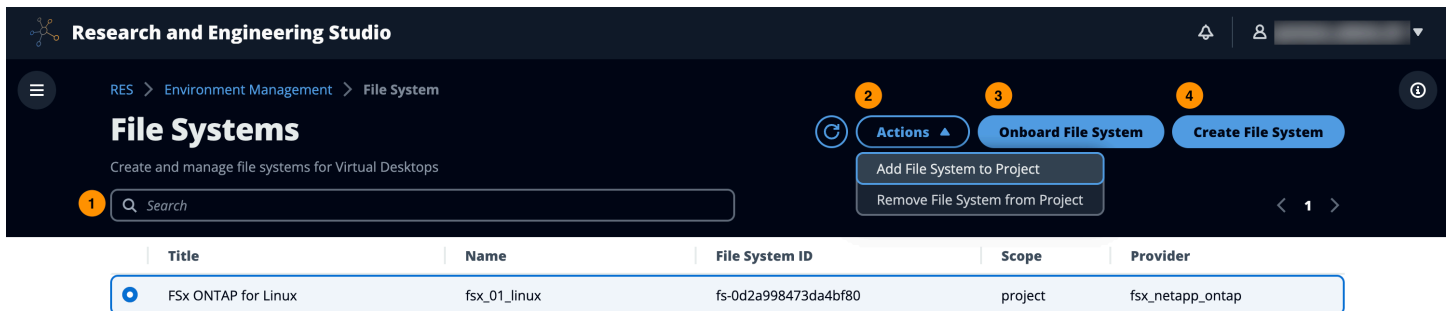
활성 디렉터리에서 동기화된 모든 그룹이 그룹 페이지에 표시됩니다. 그룹 구성 및 관리에 대한 자세한 내용은 [그룹 구성 가이드](#)를 참조하십시오.



그룹 페이지에서 다음을 수행할 수 있습니다.

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

파일 시스템



파일 시스템 페이지에서 다음을 수행할 수 있습니다.

1. 파일 시스템을 검색합니다.
2. 파일 시스템을 선택한 경우 작업 메뉴를 사용하여 다음을 수행할 수 있습니다.

- a. 프로젝트에 파일 시스템 추가
 - 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.

파일 시스템 생성

1. 파일 시스템 생성을 선택합니다.
2. 새 파일 시스템의 세부 정보를 입력합니다.
3. VPC의 서브넷 ID를 제공합니다. ID는 환경 관리 > 설정 > 네트워크 탭에서 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

Projects

Select applicable project



Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

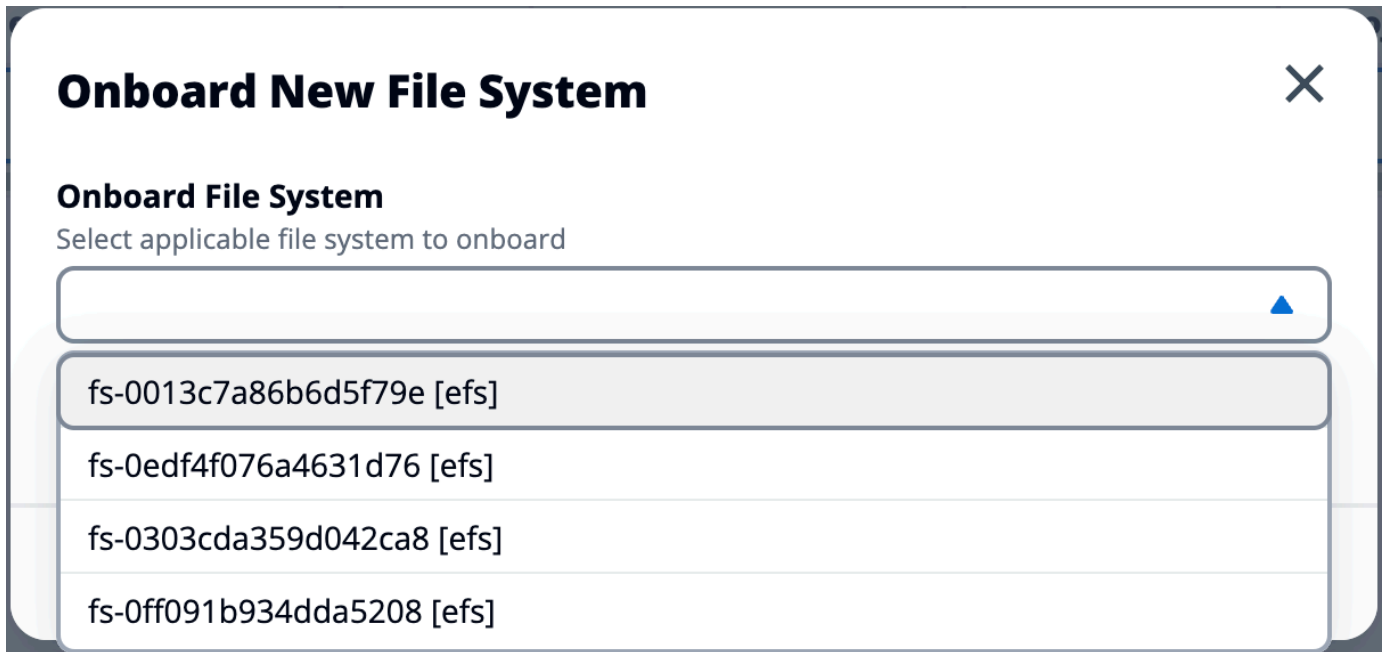
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

Enter directory to mount the file system

파일 시스템 온보딩

1. 온보드 파일 시스템을 선택합니다.
2. 드롭다운에서 파일 시스템을 선택합니다. 추가 세부 정보가 입력되면서 모달이 확장됩니다.




3. 파일 시스템 세부 정보를 입력합니다.
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

환경 상태

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

Research and Engineering Studio
demoadmin4

RES > Environment Management > Status
View Environment Settings

Environment Status

Modules

Environment modules and status

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

Infrastructure Hosts

Cluster hosts and status

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

스냅샷 관리

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

Snapshot Management

Created Snapshots 1


[Create Snapshot](#) 2

Snapshots created from the environment

 < 1 >

S3 Bucket Name	Snapshot Path	Status	Created On
----------------	---------------	--------	------------

No records

Applied Snapshots 3


[Apply Snapshot](#) 4

Snapshots applied to the environment

 < 1 >

S3 Bucket Name	Snapshot Path	Status	Created On
----------------	---------------	--------	------------

No records

스냅샷 관리 페이지에서 다음을 수행할 수 있습니다.

1. 생성된 모든 스냅샷과 상태를 볼 수 있습니다.
2. 스냅샷 생성. 스냅샷을 만들려면 먼저 적절한 권한이 있는 버킷을 만들어야 합니다.
3. 적용된 모든 스냅샷과 상태를 볼 수 있습니다.
4. 스냅샷 적용.

스냅샷 생성

스냅샷을 생성하려면 먼저 Amazon S3 버킷에 필요한 권한을 제공해야 합니다. 버킷 생성에 대한 자세한 내용은 [버킷 생성](#)을 참조하세요. 버킷 버전 관리 및 서버 액세스 로깅을 활성화하는 것이 좋습니다. 프로비저닝 후 버킷의 속성 탭에서 이러한 설정을 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 명령문을 추가합니다. 이 값들을 사용자의 값으로 대체합니다.
 - AWS_ACCOUNT_ID
 - RES_환경_이름
 - AWS_REGION
 - S3_버킷_이름

Important

에서 지원하는 버전 문자열은 제한되어 있습니다. AWS자세한 정보는 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html 섹션을 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 만들려면:

1. [스냅샷 생성(Create Snapshot)]을 클릭합니다.
2. 생성한 Amazon S3 버킷의 이름을 입력합니다.
3. 버킷 내에 스냅샷을 저장하려는 경로를 입력합니다. 예를 들어 **october2023/23**입니다.
4. 제출을 선택합니다.

Create New Snapshot ✕

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

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

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

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

Cancel
Submit

5. 5~10분 후 스냅샷 페이지에서 [Refresh] 를 선택하여 상태를 확인합니다. 상태가 IN_PROGRESS 에서 COMPLETED (완료됨) 로 변경될 때까지 스냅샷은 유효하지 않습니다.

스냅샷 적용

환경의 스냅샷을 만든 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 프로필, 파일 시스템 등의 데이터가 새 환경에 연결된 상태로 복사됩니다. 사용자 세션은 복제되지 않습니다. 스냅샷이 적용되면 각 리소스 레코드의 기본 정보를 검사하여 해당 레코드가 이미 존재하는지 확인합니다. 레코드가 중복되는 경우 스냅샷은 새 환경에서 리소스 생성을 건너뛰게 됩니다. 이름이나 키를 공유하는 것과 같이 비슷하지만 다른 기본 리소스 정보가 다른 레코드의 경우 다음 RecordName_SnapshotRESVersion_ApplySnapshotID 규칙에 따라 수정된 이름과 키가 있는 새 레코드가 생성됩니다. 타임스탬프처럼 ApplySnapshotID 보이며 스냅샷을 적용하려는 각 시도를 식별합니다.

스냅샷을 적용하는 동안 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 리소스가 생성됩니다.

새 환경이 예상과 다르거나 실패할 경우 CloudWatch 로그 그룹에 /res-<env-name>/cluster-manager 있는 로그에서 세부 정보를 확인할 수 있습니다. 각 로그에는 [스냅샷 적용] 태그가 있습니다. 스냅샷을 적용한 후에는 [the section called “스냅샷 관리”](#) 페이지에서 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 명령문을 추가합니다. 이 값들을 사용자의 값으로 대체합니다.

- AWS_ACCOUNT_ID
- RES_환경_이름
- AWS_REGION
- S3_버킷_이름

```
{
  "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 내 스냅샷의 파일 경로를 입력합니다.
4. 제출을 선택합니다.

Apply a Snapshot ✕

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

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

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

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

Cancel
Submit

5. 5~10분 후 스냅샷 관리 페이지에서 [Refresh] 를 선택하여 상태를 확인합니다.

환경 설정

환경 설정에는 다음과 같은 제품 구성 세부 정보가 표시됩니다.

- 일반

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

- ID 제공업체

싱글 사인온 상태와 같은 정보를 표시합니다.

- 네트워크

액세스를 위한 VPC ID, 접두사 목록 ID를 표시합니다.

- Directory Service

사용자 이름 및 암호에 대한 Active Directory 설정 및 서비스 계정 암호 관리자 ARN을 표시합니다.

Research and Engineering Studio

RES > Environment Management > Settings

Environment Settings View Environment Status

View and manage environment settings.

Environment Name: res-demo2 | AWS Region: us-east-2 | S3 Bucket: res-demo2-cluster-us-east-2-930513735672

General Settings

- Administrator Username: clusteradmin
- Administrator Email: [redacted]
- Home Directory: /internal/res-demo2
- Locale: en_US
- Timezone: America/New_York
- Default Encoding: utf-8

Web Portal

- Title: Research and Engineering Studio
- Subtitle: -
- Copyright Text: Copyright {year} Amazon Inc. or its affiliates. All Rights Reserved.

OpenAPI Specification [Info](#)

- Environment Manager API Spec: <https://res.demo.ingenio.hpc.aws.dev/cluster-manager/api/v1/openapi.yml>
- Swagger Editor: <https://editor.swagger.io?url=https://res.demo.ingenio.hpc.aws.dev/cluster-manager/api/v1/openapi.yml>

보안 암호 관리

리서치 앤 엔지니어링 스튜디오는 를 사용하여 다음과 같은 비밀을 유지합니다 AWS Secrets Manager. RES는 환경 생성 중에 자동으로 비밀을 생성합니다. 환경 생성 중에 관리자가 입력한 암호는 매개변수로 입력됩니다.

비밀 이름	설명	RES 생성	관리자 입력
<envname>- sso-client-secret	환경을 위한 싱글 사인 온 OAuth2 클라이언트 시크릿	✓	
<envname>- vdc-client-secret	vdc ClientSecret	✓	

비밀 이름	설명	RES 생성	관리자 입력
<envname>- vdc-client-id	vdc ClientId	✓	
<envname>- -키 vdc-gateway-certificate-private	도메인용 자체 서명 인증서 개인 키	✓	
<envname>- vdc-gateway-certificate-certificate	도메인용 자체 서명 인증서	✓	
<envname>- cluster-manager-client-secret	클러스터 매니저 ClientSecret	✓	
<envname>- cluster-manager-client-id	클러스터 매니저 ClientId	✓	
<envname>- external-private-key	도메인용 자체 서명 인증서 개인 키	✓	
<envname>-외부 인증서	도메인용 자체 서명 인증서	✓	
<envname>- internal-private-key	도메인용 자체 서명 인증서 개인 키	✓	
<envname>-내부 인증서	도메인용 자체 서명 인증서	✓	
<envname>-디렉토리 서비스- ServiceAccountUsername			✓
<envname>-디렉토리 서비스- ServiceAccountPassword			✓

DynamoDB의 <envname>-cluster-settings 테이블에는 다음과 같은 비밀 ARN 값이 포함되어 있습니다.

키	소스
ID 제공자.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	스택
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	스택
클러스터.로드_밸런서.internal_alb.certificates.private_key_secret_arn	스택
디렉터리 서비스.root_사용자 이름_secret_arn	
vdc.client_secret	스택
클러스터.로드_밸런서.external_alb.certificates.certificate_certificate_secret_arn	스택
클러스터.로드_밸런서.internal_alb.certificates.certificate_certificate_secret_arn	스택
디렉터리 서비스.root_password_secret_arn	
클러스터.secretsmanager.kms_key_id	
클러스터.로드_밸런서.external_alb.certificates.private_key_secret_arn	스택
클러스터 관리자. 클라이언트_시크릿	

비용 모니터링 및 제어

Note

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

[AWS 비용 관리에 도움이 되도록 Cost Explorer](#)를 통해 [예산을](#) 작성하는 것이 좋습니다. 요금은 변경될 수 있습니다. 자세한 내용은 각 요금제 웹페이지를 참조하십시오. [the section called “AWS이 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. AWS Management Console 로그인하고 <https://console.aws.amazon.com/billing/> 에서 AWS Billing 콘솔을 엽니다.
2. 비용 할당 태그를 선택합니다.
3. `res:Project` 및 `res:EnvironmentName` 태그를 검색하여 선택합니다.
4. 활성화를 선택합니다.

The screenshot shows the AWS Billing console interface for 'Cost allocation tags'. On the left is a navigation menu with 'Billing' selected. The main content area is titled 'Cost allocation tags' and shows 'User-defined cost allocation tags (2/47)'. A search bar contains 'res' and shows '11 matches'. Below the search bar is a table of tags. The 'res:EnvironmentName' tag is selected and highlighted in blue, with a yellow circle containing the number '3' next to it. The 'res:Project' tag is also highlighted in blue, with a yellow circle containing the number '4' next to it. The table has columns for 'Tag key', 'Status', 'Last updated date', and 'Last used month'. All tags shown are 'Inactive'.

Tag key	Status	Last updated date	Last used month
<input type="checkbox"/> res:BackupPlan	Inactive	-	November 2023
<input type="checkbox"/> res:ClusterName	Inactive	-	November 2023
<input type="checkbox"/> res:DCVSessionUUID	Inactive	-	November 2023
<input type="checkbox"/> res:EndpointName	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:EnvironmentName	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleId	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleName	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleVersion	Inactive	-	November 2023
<input type="checkbox"/> res:NodeType	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:Project	Inactive	-	November 2023

Note

배포 후 RES 태그가 표시되는 데 최대 하루가 걸릴 수 있습니다.

RES 리소스에 대한 예산을 세우는 방법:

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

- 예산 유형에서 비용 예산 - 권장을 선택합니다.
- 다음을 선택합니다.

- 계정의 다른 예산과 구분할 수 있도록 세부 정보에 의미 있는 예산 이름을 입력합니다. 예: [EnvironmentName] - [ProjectName] - [BudgetName]
- 예산 금액 설정에 프로젝트 예산 금액을 입력합니다.
- 예산 범위에서 특정 AWS 비용 측정기준 필터링을 선택합니다.
- [Add filter]를 선택합니다.
- 측정기준에서 태그를 선택합니다.
- 태그에서 Res:Project를 선택합니다.

Note

태그와 값을 사용할 수 있게 되려면 최대 2일이 걸릴 수 있습니다. 프로젝트 이름을 사용할 수 있게 되면 예산을 만들 수 있습니다.

12. 값에서 프로젝트 이름을 선택합니다.
13. 필터 적용을 선택하여 프로젝트 필터를 예산에 연결합니다.
14. 다음을 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 X

Cancel

Apply filter

Add filter

▼ Advanced options

Aggregate costs by

Unblended costs

Supported charge types

Upfront reservation fees X

Recurring reservation charges X

Other subscription costs X

Taxes X

Support charges X

Discounts X

Cancel

Previous

Next

15. (선택 사항) 알림 임계값 추가.
16. 다음을 선택합니다.
17. (선택 사항) 알림이 구성된 경우 작업 첨부를 사용하여 알림과 함께 원하는 작업을 구성하십시오.
18. 다음을 선택합니다.
19. 예산 구성을 검토하고 추가 예산 매개 변수에 올바른 태그가 설정되었는지 확인합니다.
20. 예산 생성을 선택합니다.

이제 예산이 생성되었으므로 프로젝트 예산을 활성화할 수 있습니다. 프로젝트 예산을 활성화하려면 [the section called “프로젝트 편집”](#)을 참조하십시오. 예산을 초과할 경우 가상 데스크톱을 시작할 수 없습니다. 데스크톱을 시작하는 동안 예산을 초과하더라도 데스크톱은 계속 운영됩니다.

Title	Project Code	Status	Budgets	Groups	Updated On
project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 ⊗ Budget Exceeded Limit: 500.00 USD, Forecasted: 3945.34 USD	<ul style="list-style-type: none"> DemoUsers DemoAdmins ProductUsers 	10/31/2023, 12:44:12 PM

예산을 변경해야 하는 경우 콘솔로 돌아가서 예산 금액을 편집하세요. 변경 사항이 RES 내에서 적용되는 데 최대 15분이 걸릴 수 있습니다. 또는 프로젝트를 편집하여 예산을 사용하지 않도록 설정할 수도 있습니다.

권한

	프로젝트 멤버	프로젝트 소유자	글로벌 관리자	범위
사용자를 프로젝트 멤버/프로젝트 소유자로 추가		X	X	프로젝트 소유자: 소유한 프로젝트 글로벌 관리자: 모든 프로젝트
그룹을 프로젝트 멤버/프로젝트 소유자로 추가		X	X	프로젝트 소유자: 소유한 프로젝트

	프로젝트 멤버	프로젝트 소유자	글로벌 관리자	범위
				글로벌 관리자: 모든 프로젝트
사용자 제거		X	X	프로젝트 소유자: 소유한 프로젝트 글로벌 관리자: 모든 프로젝트
그룹 제거		X	X	프로젝트 소유자: 소유한 프로젝트 글로벌 관리자: 모든 프로젝트
VDI 인스턴스 시 작/중지	X	X	X	프로젝트 멤버/프 로젝트 소유자: 프로젝트의 일부 일 때 소유하는 VDI 인스턴스입 니다. 글로벌 관리자: 모든 VDI 인스턴 스.

제품 사용

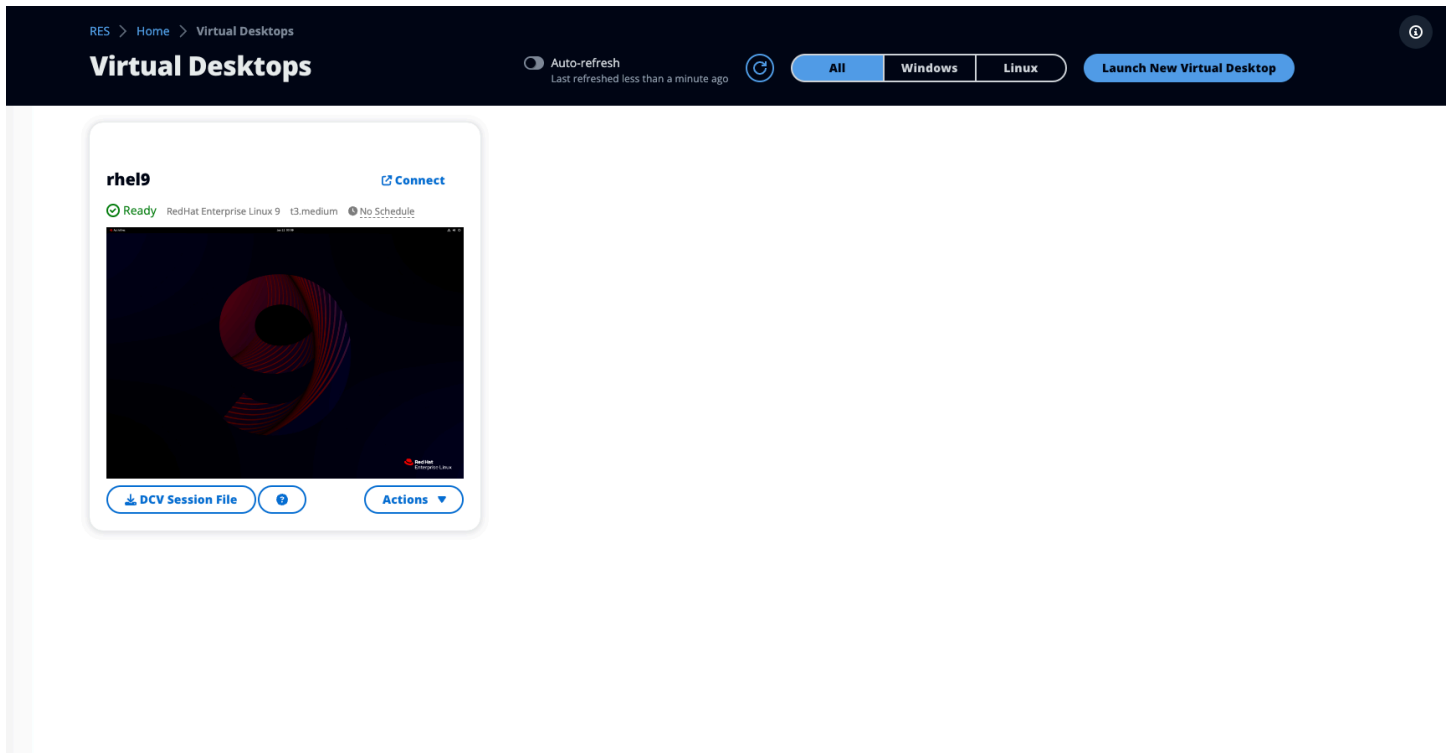
이 섹션에서는 가상 데스크톱을 사용하여 다른 사용자와 협업하는 방법에 대한 지침을 제공합니다.

주제

- [가상 데스크톱](#)
- [공유 데스크톱](#)
- [파일 브라우저](#)
- [SSH 액세스](#)

가상 데스크톱

가상 데스크톱 인터페이스 (VDI) 모듈을 사용하면 Windows 또는 Linux 가상 데스크톱을 만들고 관리할 수 있습니다. AWS사용자는 선호하는 도구와 애플리케이션을 사전 설치 및 구성하여 Amazon EC2 인스턴스를 시작할 수 있습니다.



지원되는 운영 체제

Note

CentOS 7은 현재 2024년 6월 end-of-life 30일에 출시될 예정입니다. 연구 및 엔지니어링 스튜디오 버전 2024.06은 CentOS 7을 지원하는 마지막 버전이 될 것입니다.

RES는 현재 다음 운영 체제를 사용하여 가상 데스크톱을 시작하는 것을 지원합니다.

- 아마존 리눅스 2 (x86 및 ARM64)
- 센토스 7 (x86 및 ARM64)
- RHEL 7 (x86), 8 (x86), 9 (x86)
- 우분투 22.04.03 (x86)
- 윈도우 2019, 2022년 (x86)

새 데스크톱 실행

1. 메뉴에서 내 가상 데스크톱을 선택합니다.
2. 새 가상 데스크톱 시작을 선택합니다.
3. 새 데스크톱의 세부 정보를 입력합니다.
4. 제출을 선택합니다.

데스크톱 정보가 포함된 새 카드가 즉시 나타나고 10~15분 내에 데스크톱을 사용할 수 있습니다. 시작 시간은 선택한 이미지에 따라 달라집니다. RES는 GPU 인스턴스를 탐지하고 관련 드라이버를 설치합니다.

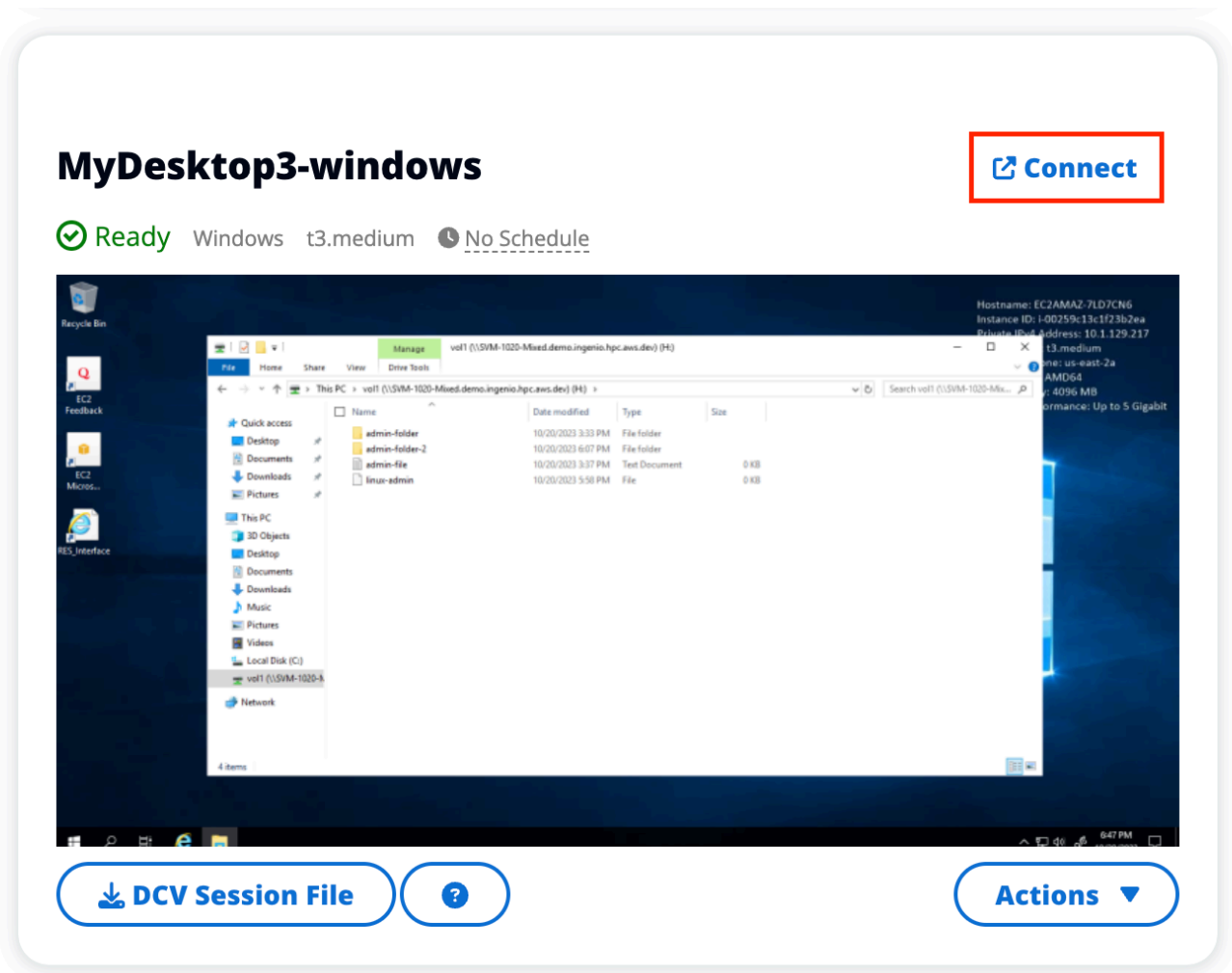
데스크톱에 액세스

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

Web connection

웹 브라우저를 통해 데스크톱에 액세스하는 것이 가장 쉬운 연결 방법입니다.

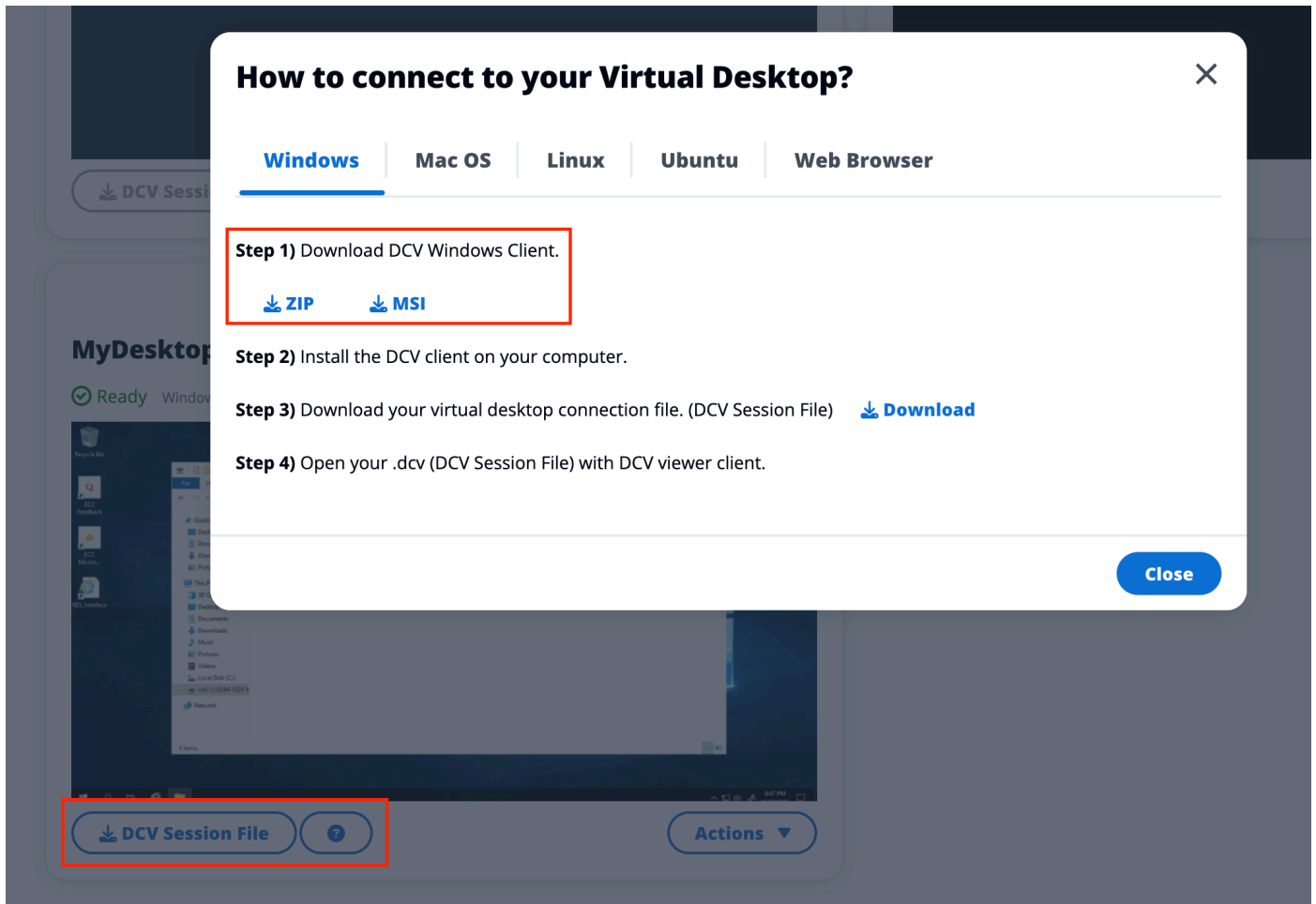
- Connect를 선택하거나 썸네일을 선택하여 브라우저를 통해 데스크톱에 직접 액세스합니다.



DCV connection

DCV 클라이언트를 통해 데스크톱에 액세스하면 최상의 성능을 얻을 수 있습니다. DCV를 통해 액세스하려면:

1. DCV 세션 파일을 선택하여 다운로드하십시오. dcv파일. 시스템에 DCV 클라이언트가 설치되어 있어야 합니다.
2. 설치 지침을 보려면? 를 선택하십시오. 아이콘.



데스크톱 상태 제어

데스크톱 상태를 제어하려면:

1. 작업을 선택합니다.
2. 가상 데스크톱 상태를 선택합니다. 다음 네 가지 상태 중에서 선택할 수 있습니다.

- 중지

중지된 세션에서는 데이터가 손실되지 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 데이터를 RES 파일 시스템에 백업해야 합니다.


- 최대 절전 모드

데스크톱 상태가 메모리에 저장됩니다. 데스크톱을 다시 시작하면 애플리케이션이 다시 시작되지만 원격 연결이 끊길 수 있습니다. 모든 인스턴스가 하이버네이션을 지원하는 것은 아니며, 이 옵션은 인스턴스 생성 중에 하이버네이션을 활성화한 경우에만 사용할 수 있습니다. 인스턴스가 이 상태를 지원하는지 확인하려면 [하이버네이션](#) 사전 요구 사항을 참조하십시오.

가상 데스크톱 수정

가상 데스크톱의 하드웨어를 업데이트하거나 세션 이름을 변경할 수 있습니다.

1. 인스턴스 크기를 변경하기 전에 세션을 중지해야 합니다.
 - a. 작업을 선택합니다.
 - b. 가상 데스크톱 상태를 선택합니다.
 - c. 중지를 선택합니다.

 Note

최대 절전 모드로 전환된 세션의 데스크톱 크기는 업데이트할 수 없습니다.

2. 데스크톱이 중지된 것을 확인한 후 작업을 선택한 다음 [세션 업데이트] 를 선택합니다.
3. 세션 이름을 변경하거나 원하는 데스크톱 크기를 선택합니다.
4. 제출을 선택합니다.
5. 인스턴스가 업데이트되면 데스크톱을 다시 시작합니다.
 - a. 작업을 선택합니다.
 - b. 가상 데스크톱 상태를 선택합니다.
 - c. 시작을 선택합니다.

세션 정보 검색

1. 작업을 선택합니다.

2. [정보 보기] 를 선택합니다.

가상 데스크톱 예약

기본적으로 가상 데스크톱에는 일정이 없으며 세션을 중지하거나 종료할 때까지 활성 상태를 유지합니다. 또한 데스크톱이 유휴 상태인 경우 예기치 않게 중지되는 것을 방지하기 위해 데스크톱이 중지됩니다. 유휴 상태는 활성 연결이 없고 최소 15분 동안 CPU 사용량이 15% 미만일 때 결정됩니다. 데스크톱을 자동으로 시작하고 중지하도록 일정을 구성할 수 있습니다.

1. 작업을 선택합니다.
2. 일정을 선택합니다.
3. 매일 일정을 설정하세요.
4. 저장을 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

공유 데스크톱

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

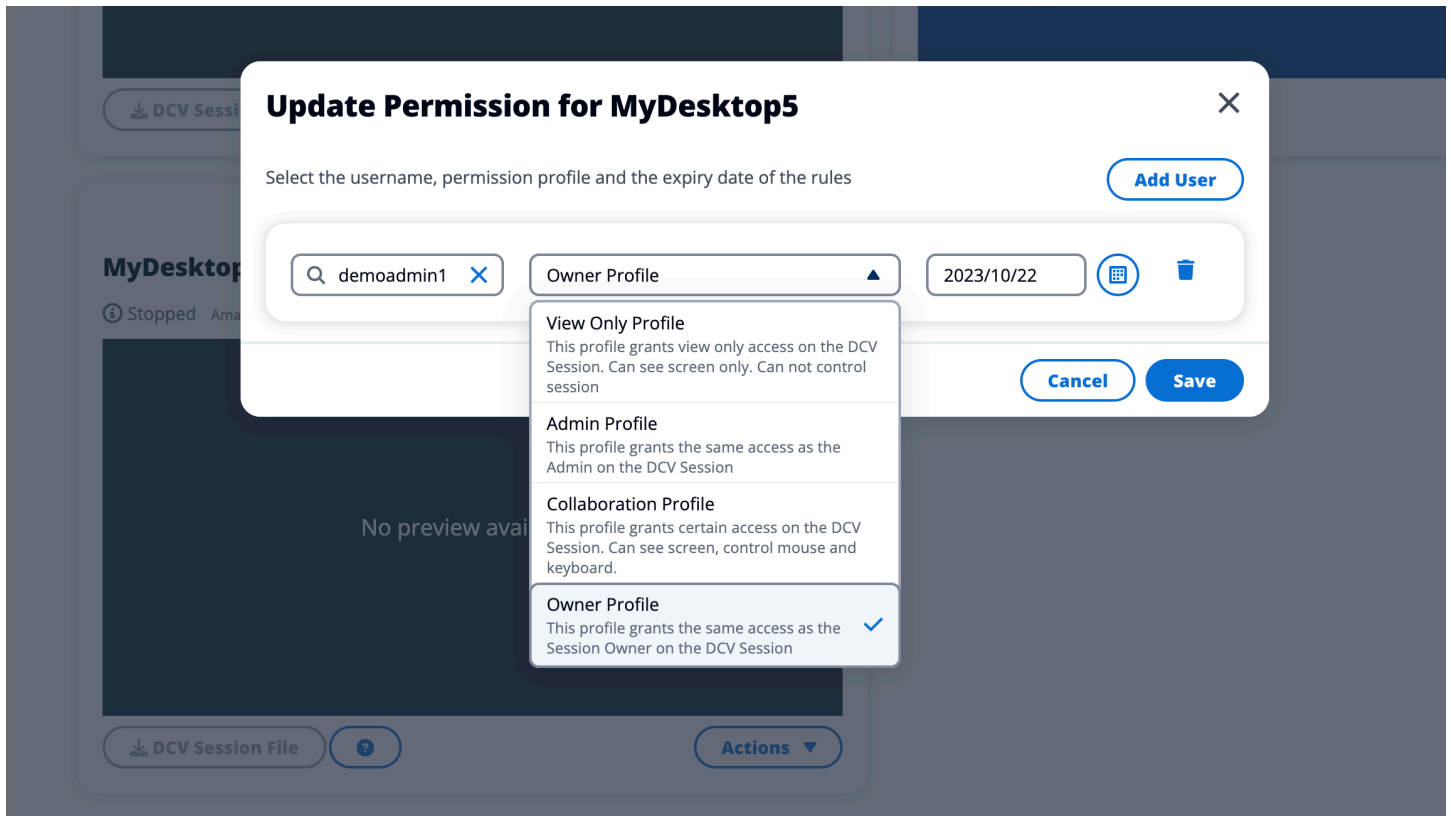
The screenshot shows the 'Shared Desktops' interface. At the top, there's a breadcrumb 'RES > Home > Shared Desktops' and a title 'Shared Desktops (2)'. Below the title is a subtitle: 'List of Virtual Desktops shared with you. Unless user has Admin or Owner profile, session owner must be connected in order for them to connect.' There are filters for 'Session Created' (Last 1 month) and a search bar. Below the filters is a table with columns: Name, Session Owner, Base OS, Instance Type, State, Permission Expiry, Download DCV File, and Join Session. Two desktops are listed: 'DemoSession' and 'MyDesktop6-linux-gs'. Both are in a 'Ready' state. At the bottom right of the table, there are pagination controls showing '< 1 >'.

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

세션을 공유하는 동안 협력자의 권한을 구성할 수 있습니다. 예를 들어 공동 작업 중인 팀원에게 읽기 전용 액세스 권한을 부여할 수 있습니다.

데스크톱을 공유하세요.

1. 데스크톱 세션에서 Actions를 선택합니다.
2. 세션 권한을 선택합니다.
3. 사용자 및 권한 수준을 선택합니다. 만료 시간을 설정할 수도 있습니다.
4. 저장을 선택합니다.



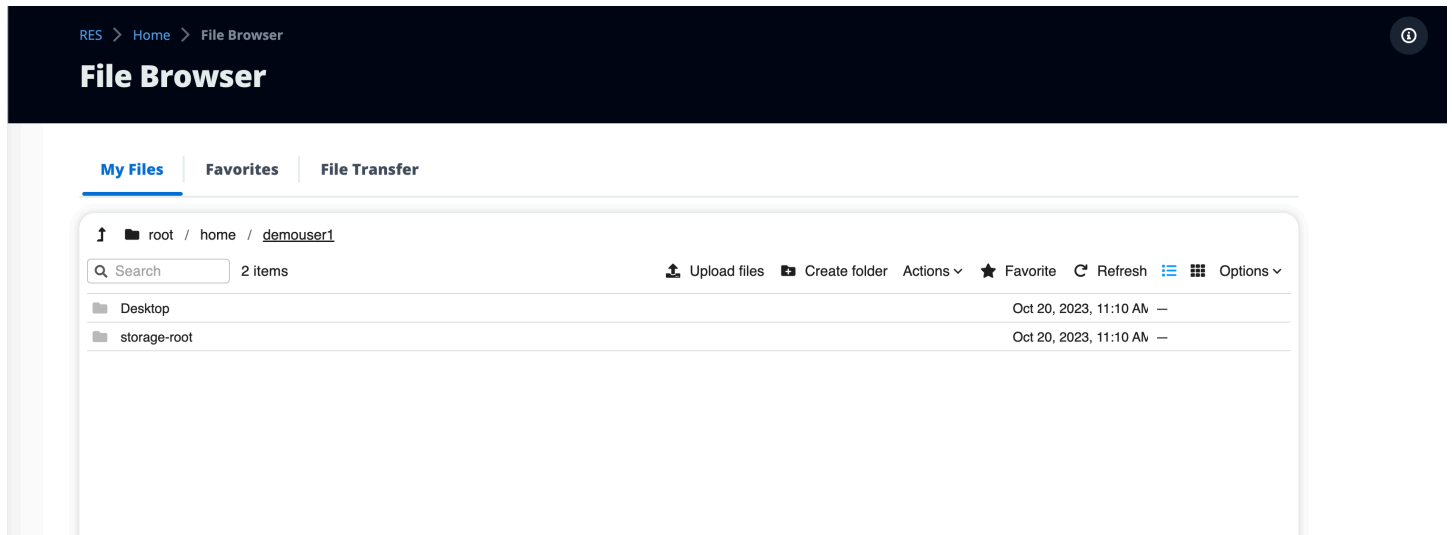
권한에 대한 자세한 내용은 [이 섹션을 참조하십시오](#) [the section called “권한 프로파일”](#).

공유 데스크톱에 액세스

공유 데스크톱에서 공유된 데스크톱을 보고 인스턴스에 연결할 수 있습니다. 웹 브라우저 또는 DCV로 가입할 수 있습니다. 연결하려면 [의 안내를 따르세요](#). [the section called “데스크톱에 액세스”](#)

파일 브라우저

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



파일 업로드

1. 파일 업로드를 선택합니다.
2. 파일을 드롭하거나 업로드할 파일을 찾아보세요.
3. 파일 업로드 (n) 개를 선택합니다.

파일 삭제

1. 삭제하려는 파일을 선택합니다.
2. 작업을 선택합니다.
3. 파일 삭제를 선택합니다.

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

즐거찾기 관리

중요한 파일 및 폴더를 고정하려면 즐겨찾기에 추가할 수 있습니다.

1. 파일 또는 폴더를 선택합니다.
2. 즐겨찾기를 선택합니다.

또는 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하고 즐겨찾기를 선택할 수도 있습니다.

Note

즐거찾기는 로컬 브라우저에 저장됩니다. 브라우저를 변경하거나 캐시를 지운 경우 즐겨찾기를 다시 고정해야 합니다.

파일 편집

웹 포털 내에서 텍스트 기반 파일의 콘텐츠를 편집할 수 있습니다.

1. 업데이트하려는 파일을 선택합니다. 파일 내용이 포함된 모달이 열립니다.
2. 업데이트하고 [Save] 를 선택합니다.

파일 전송

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

- FileZilla (윈도우, 맥OS, 리눅스)
- 원SCP (윈도우)
- AWS Transfer for FTP (아마존 EFS)

RES > Home > File Browser

File Browser

My Files | Favorites | **File Transfer**

File Transfer Method

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

 FileZilla

Available for download on Windows, MacOS and Linux

 WinSCP

Available for download on Windows Only

 AWS Transfer

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

FileZilla

Step 1: Download FileZilla

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

Step 2: Download Key File

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

[Download Key File \[*.ppk\] \(Windows\)](#)

Step 3: Configure FileZilla

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

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

Save the settings and click **Connect**

Step 4: Connect and transfer file to FileZilla

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

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

SSH 액세스

SSH를 사용하여 배스천 호스트에 액세스하려면:

1. RES 메뉴에서 SSH 액세스를 선택합니다.
2. 화면 지침에 따라 SSH 또는 PuTTY를 사용하여 액세스하십시오.

문제 해결

이 문서에는 시스템을 모니터링하는 방법과 발생할 수 있는 특정 문제를 해결하는 방법에 대한 정보가 포함되어 있습니다. 문제에 대한 해결 방법을 찾을 수 없는 경우 [에서 GitHub 추가 문제 해결 항목을 찾을 수 있습니다.](#)

주제

- [설치 문제](#)
- [ID 관리 문제](#)

설치 문제

주제

- [AWS CloudFormation 스택 생성에 실패했습니다. “WaitCondition 수신 실패 메시지” 메시지가 표시됩니다. 오류: 상태. TaskFailed”](#)
- [AWS CloudFormation 스택이 성공적으로 생성된 후 이메일 알림을 받지 못했습니다.](#)
- [장애 상태의 인스턴스 순환 또는 vdc-controller](#)
- [종속 객체 오류로 인해 환경 CloudFormation 스택을 삭제하지 못했습니다.](#)
- [환경 생성 중에 CIDR 블록 매개변수에서 오류가 발생했습니다.](#)
- [CloudFormation 환경 생성 중 스택 생성 실패](#)
- [CREATE_FAILED로 AdDomainAdminNode 인해 외부 리소스 \(데모\) 스택 생성이 실패합니다.](#)

AWS CloudFormation 스택 생성에 실패했습니다. “WaitCondition 수신 실패 메시지” 메시지가 표시됩니다. 오류: 상태. TaskFailed”

문제를 식별하려면 이름이 지정된 Amazon CloudWatch 로그 그룹을 <stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce> 검토하십시오. 이름이 같은 로그 그룹이 여러 개 있는 경우 먼저 사용할 수 있는 로그 그룹을 살펴보십시오. 로그 내의 오류 메시지는 문제에 대한 자세한 정보를 제공합니다.

Note

파라미터 값에 공백이 없는지 확인하십시오.

AWS CloudFormation 스택이 성공적으로 생성된 후 이메일 알림을 받지 못했습니다.

이메일 초대를 성공적으로 AWS CloudFormation 만든 후에도 이메일 초대장을 받지 못한 경우 다음 사항을 확인하세요.

1. 이메일 주소 매개변수가 올바르게 입력되었는지 확인합니다.

이메일 주소가 잘못되었거나 액세스할 수 없는 경우 연구 및 엔지니어링 스튜디오 환경을 삭제하고 재배포하십시오.

2. Amazon EC2 콘솔에서 순환 인스턴스의 증거를 확인하십시오.

<envname>접두사가 종료된 것으로 나타나는 Amazon EC2 인스턴스가 있다가 새 인스턴스로 교체되는 경우 네트워크 또는 Active Directory 구성에 문제가 있을 수 있습니다.

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

파라미터가 잘못된 경우 RES 환경을 삭제하고 재배포해야 할 수 있습니다. 자세한 정보는 [제품 제거](#)를 참조하세요.

4. 자체 외부 리소스를 사용하여 제품을 배포한 경우 네트워킹 및 Active Directory가 예상 구성과 일치하는지 확인하십시오.

인프라 인스턴스가 Active Directory에 성공적으로 가입되었는지 확인하는 것이 중요합니다. 다음 단계를 따라 문제를 [the section called “장애 상태의 인스턴스 순환 또는 vdc-controller”](#) 해결해 보십시오.

장애 상태의 인스턴스 순환 또는 vdc-controller

이 문제의 가장 가능성 있는 원인은 리소스가 Active Directory에 연결하거나 Active Directory에 연결할 수 없기 때문입니다.

문제를 확인하려면:

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

상태가 비활성 또는 실패이거나 로그에 오류가 표시되면 인스턴스가 Active Directory에 가입할 수 없는 것입니다.

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

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

Might see errors highlighted in RED here

SSM 오류 로그

문제를 해결하려면:

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

이 문제는 세 가지 가능한 근본 원인 중 하나일 수 있습니다.

근본 원인 1: 잘못된 LDAP 연결 세부 정보가 입력되었습니다.

로그를 검토합니다. 다음과 같은 상황이 여러 번 반복되는 경우 인스턴스가 Active Directory에 가입하지 못한 것입니다.

```
+ 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 확인하십시오.
 - directoryservice ldap_connection_uri
 - 디렉토리 서비스 ldap_base
 - directoryservice.users.ou
 - 디렉토리서비스.groups.ou
 - 디렉터리 서비스.sudoers.ou
 - 디렉터리 서비스.computers.ou
 - 디렉터리 서비스 이름
2. DynamoDB 테이블의 잘못된 값을 모두 업데이트하십시오. 테이블은 DynamoDB 콘솔의 테이블 아래에 있습니다. 테이블 이름은 다음과 같아야 합니다. **[stack name].cluster-settings**
3. 테이블을 업데이트한 후 현재 환경 인스턴스를 실행 중인 클러스터 관리자 및 vdc-controller를 삭제하십시오. Auto Scaling은 DynamoDB 테이블의 최신 값을 사용하여 새 인스턴스를 시작합니다.

근본 원인 2: 잘못된 ServiceAccount 사용자 이름을 입력했습니다.

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

1. AWS 콘솔에서 Secrets Manager를 엽니다.
2. `directoryserviceServiceAccountUsername`를 찾습니다. 비밀은 다음과 같아야 **[stack name]-directoryservice-ServiceAccountUsername**입니다.
3. 시크릿을 열면 세부 정보 페이지를 볼 수 있습니다. [보안 값]에서 [암호 값 검색]을 선택하고 [일반 텍스트]를 선택합니다.
4. 값이 업데이트된 경우 해당 환경에서 현재 실행 중인 클러스터 관리자 및 vdc-controller 인스턴스를 삭제하십시오. 오토 스케일링은 Secrets Manager의 최신 값을 사용하여 새 인스턴스를 시작합니다.

근본 원인 3: 잘못된 ServiceAccount 비밀번호를 입력했습니다.

로그가 표시되는 `Invalid credentials` 경우 스택 생성 중에 입력한 ServiceAccount 암호가 올바르지 않을 수 있습니다.

1. AWS 콘솔에서 Secrets Manager를 엽니다.
2. `directoryserviceServiceAccountPassword`를 찾습니다. 비밀은 다음과 같아야 **[stack name]-directoryservice-ServiceAccountPassword** 합니다.
3. 시크릿을 열면 세부 정보 페이지를 볼 수 있습니다. [보안 값] 에서 [암호 값 검색] 을 선택하고 [일반 텍스트] 를 선택합니다.
4. 암호를 잊어버렸거나 입력한 암호가 정확한지 확실하지 않은 경우 Active Directory 및 Secrets Manager에서 암호를 재설정할 수 있습니다.
 - a. 에서 비밀번호를 재설정하려면: AWS Managed Microsoft AD
 - i. AWS 콘솔을 열고 으로 이동합니다 AWS Directory Service.
 - ii. RES 디렉터리의 디렉터리 ID를 선택하고 작업을 선택합니다.
 - iii. 사용자 암호 재설정을 선택합니다.
 - iv. ServiceAccount 사용자 이름을 입력합니다.
 - v. 새 비밀번호를 입력하고 비밀번호 재설정을 선택합니다.
 - b. Secrets Manager에서 비밀번호를 재설정하려면:
 - i. AWS 콘솔을 열고 Secrets Manager로 이동합니다.
 - ii. `directoryserviceServiceAccountPassword`를 찾습니다. 비밀은 다음과 같아야 **[stack name]-directoryservice-ServiceAccountPassword** 합니다.
 - iii. 시크릿을 열면 세부 정보 페이지를 볼 수 있습니다. [보안 값] 에서 [암호 값 검색] 을 선택하고 [일반 텍스트] 를 선택합니다.
 - iv. 편집을 선택합니다.
 - v. ServiceAccount 사용자의 새 비밀번호를 설정하고 [Save] 를 선택합니다.
5. 값이 업데이트된 경우 해당 환경에서 현재 실행 중인 클러스터 관리자 및 `vdc-controller` 인스턴스를 삭제하십시오. Auto Scaling은 최신 값을 사용하여 새 인스턴스를 시작합니다.

종속 객체 오류로 인해 환경 CloudFormation 스택을 삭제하지 못했습니다.

와 같은 종속 객체 오류로 인해 **[env-name]-vdc** CloudFormation 스택 삭제가 실패하는 경우 `vdcvhostsecuritygroup`, 이는 콘솔을 사용하여 RES에서 생성한 서브넷 또는 보안 그룹에서 Amazon EC2 인스턴스를 실행했기 때문일 수 있습니다. AWS

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

환경 생성 중에 CIDR 블록 매개변수에서 오류가 발생했습니다.

환경을 생성할 때 응답 상태가 [FAILED] 인 CIDR 블록 매개 변수에 오류가 나타납니다.

오류 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.
```

이 문제를 해결하는 데 필요한 형식은 x.x.x.0/24 또는 x.x.x.0/32입니다.

CloudFormation 환경 생성 중 스택 생성 실패

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

이 경우 환경을 삭제하고 생성을 다시 시도하세요. 다른 지역에서 생성을 다시 시도할 수도 있습니다.

CREATE_FAILED로 AdDomainAdminNode 인해 외부 리소스 (데모) 스택 생성이 실패합니다.

데모 환경 스택 생성이 실패하고 다음 오류가 발생하는 경우, 인스턴스 시작 후 프로비저닝 중에 Amazon EC2 패치가 예기치 않게 발생했기 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 구성되었는지, 모든 인스턴스에 대해 패치가 구성되어 있는지 확인합니다.
2. RunCommandSSM/Automation 실행 기록에서 패치 관련 SSM 문서의 실행이 인스턴스 시작과 일치하는지 확인합니다.
3. 환경의 Amazon EC2 인스턴스 로그 파일에서 로컬 인스턴스 로깅을 검토하여 프로비저닝 중에 인스턴스가 재부팅되었는지 확인합니다.

패치 적용으로 인해 문제가 발생한 경우, 시작 후 최소 15분 후에 RES 인스턴스에 대한 패치 적용을 연기하십시오.

ID 관리 문제

싱글 사인온 (SSO) 및 ID 관리와 관련된 대부분의 문제는 잘못된 구성으로 인해 발생합니다. SSO 구성 설정에 대한 자세한 내용은 다음을 참조하십시오.

- [the section called “IAM ID 센터를 통한 SSO 설정”](#)
- [the section called “싱글 사인온 \(SSO\) 을 위한 ID 공급자 구성”](#)

ID 관리와 관련된 다른 문제를 해결하려면 다음 문제 해결 항목을 참조하십시오.

주제

- [환경에 로그인하면 바로 로그인 페이지로 돌아갑니다.](#)
- [로그인을 시도할 때 “사용자를 찾을 수 없음” 오류가 발생합니다.](#)
- [Active Directory에 사용자가 추가되었지만 RES에서 누락되었습니다.](#)
- [세션을 생성할 때는 사용자를 사용할 수 없습니다.](#)
- [CloudWatch 클러스터 관리자 로그의 크기 제한 초과 오류](#)

환경에 로그인하면 바로 로그인 페이지로 돌아갑니다.

이 문제는 SSO 통합이 잘못 구성되었을 때 발생합니다. 문제를 확인하려면 컨트롤러 인스턴스 로그를 확인하고 구성 설정에 오류가 있는지 검토하십시오.

로그를 확인하려면:

1. <https://console.aws.amazon.com/cloudwatch/> 에서 CloudWatch 콘솔을 엽니다.
2. 로그 그룹에서 이름이 지정된 그룹을 찾습니다/*<environment-name>*/cluster-manager.
3. 로그 그룹을 열어 로그 스트림의 오류를 검색합니다.

구성 설정을 확인하려면:

1. <https://console.aws.amazon.com/dynamodb/>에서 DynamoDB 콘솔을 엽니다.
2. 테이블에서 이름이 지정된 테이블을 찾으십시오 *<environment-name>*.cluster-settings.

3. 테이블을 열고 테이블 항목 탐색을 선택합니다.
4. 필터 섹션을 펼치고 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 False로 변경하십시오.

Edit item

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

Attributes

Attribute name	Value
key - Partition key	identity-provider.cognito.sso_enabled
value	<input type="radio"/> True <input checked="" type="radio"/> False 

7. RES 사용자 인터페이스로 돌아가 SSO를 재구성하십시오.

로그인을 시도할 때 “사용자를 찾을 수 없음” 오류가 발생합니다.

RES 인터페이스에 로그인할 때 “사용자를 찾을 수 없음” 오류가 표시되면 Active Directory에는 사용자가 있지만 RES에는 없는 것입니다. 최근에 AD에 사용자를 추가한 경우 해당 사용자는 RES에 동기화되지 않을 수 있습니다. RES는 매시간 동기화되므로 다음 동기화 후 사용자가 추가되었는지 잠시 기다려야 할 수 있습니다. 즉시 동기화하려면 [the section called “Active Directory에 사용자가 추가되었지만 RES에서 누락되었습니다.”](#) 단계를 따르세요.

사용자가 RES에 있는 경우:

1. 속성 매핑이 올바르게 구성되었는지 확인하십시오. 자세한 설명은 [the section called “싱글 사인온 \(SSO\)을 위한 ID 공급자 구성”](#) 섹션을 참조하세요.
2. SAML 제목과 SAML 이메일이 모두 사용자의 이메일 주소에 매핑되는지 확인하십시오.

Active Directory에 사용자가 추가되었지만 RES에서 누락되었습니다.

Active Directory에 사용자를 추가했지만 RES에 없는 경우 AD 동기화를 트리거해야 합니다. AD 동기화는 Lambda 함수에 의해 매시간 수행되어 AD 항목을 RES 환경으로 가져옵니다. 새 사용자 또는 그룹을 추가한 후 다음 동기화 프로세스가 실행될 때까지 지연되는 경우가 있습니다. Amazon 심플 큐 서비스에서 수동으로 동기화를 시작할 수 있습니다.

동기화 프로세스를 수동으로 시작하십시오.

1. <https://console.aws.amazon.com/sqs/>에서 Amazon SQS 콘솔을 엽니다.
2. 대기열에서 을 선택합니다. <environment-name>-cluster-manager-tasks.fifo
3. [메시지 전송 및 수신(Send and receive messages)]을 선택합니다.
4. 메시지 본문에 다음을 입력합니다.

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

5. 메시지 그룹 ID에 다음을 입력합니다. **adsync.sync-from-ad**
6. 메시지 중복 제거 ID에는 임의의 영숫자 문자열을 입력합니다. 이 항목은 5분 이내의 모든 통화와 달라야 합니다. 그렇지 않으면 요청이 무시됩니다.

세션을 생성할 때는 사용자를 사용할 수 없습니다.

세션을 만드는 관리자이지만 세션을 만들 때 Active Directory에 있는 사용자를 사용할 수 없는 경우 사용자는 처음으로 로그인해야 할 수 있습니다. 활성 사용자에 대한 세션만 생성할 수 있습니다. 활성 사용자는 환경에 한 번 이상 로그인해야 합니다.

CloudWatch 클러스터 관리자 로그의 크기 제한 초과 오류

```
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 표시되면 LDAP 검색에서 너무 많은 사용자 레코드가 반환된 것일 수 있습니다. 이 문제를 해결하려면 IDP의 ldap 검색 결과 한도를 늘리십시오.

고지 사항

각 Amazon EC2 인스턴스에는 관리 목적의 원격 데스크톱 서비스 (터미널 서비스) 라이선스 2개가 함께 제공됩니다. 이 [정보는](#) 관리자를 위해 이러한 라이선스를 프로비저닝하는 데 도움이 됩니다. 또한 이를 사용하면 RDP 및 RDP 라이선스 없이도 Amazon EC2 인스턴스로 원격 전송할 수 있습니다. [AWS Systems Manager Session Manager](#) 추가 원격 데스크톱 서비스 라이선스가 필요한 경우 Microsoft 또는 Microsoft 라이선스 리셀러로부터 원격 데스크톱 사용자 CAL을 구입해야 합니다. Software Assurance가 활성화된 원격 데스크톱 사용자 CAL은 라이선스 이동성 혜택을 제공하며 AWS 기본 (공유) 테넌트 환경으로 전환할 수 있습니다. 소프트웨어 보증 또는 라이선스 이동성 혜택 없이 라이선스를 가져오는 방법에 대한 자세한 내용은 FAQ의 [이 섹션을](#) 참조하십시오.

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 (a) 정보 제공만을 목적으로 하고, (b) 사전 통지 없이 변경될 수 있는 AWS 현재 제품 제공 및 관행을 나타내며, (c) 해당 계열사, 공급업체 또는 라이선스 제공자로부터 AWS 어떠한 약정이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 “있는 그대로” 제공됩니다. AWS 고객에 대한 책임과 책임은 AWS 계약에 의해 통제되며, 본 문서는 고객과 체결한 계약의 일부가 아니며 수정하지도 않습니다. AWS

Research and Engineering Studio AWS on은 아파치 소프트웨어 재단에서 제공하는 Apache 라이선스 버전 2.0의 조건에 따라 라이선스가 [부여됩니다](#).

개정

[자세한 내용은 저장소의 ChangeLog.md 파일을 참조하십시오.](#) GitHub

날짜	변경 사항
2023년 11월	최초 릴리스
2023년 12월	GovCloud 길찾기 및 템플릿 추가
2024년 1월	릴리스 버전: 2024.01
2024년 2월	릴리스 버전 2024.01.01 — 업데이트된 배포 템플릿
2024년 3월	추가 문제 해결 주제, CloudWatch 로그 보존, 마이너 버전 제거
2024년 4월	릴리스 버전 2024.04 — RES 지원 AMI 및 프로젝트 시작 템플릿
2024년 6월	<ul style="list-style-type: none"> 릴리스 버전 2024.06 — 우분투 지원, 프로젝트 소유자 권한. 사용 설명서: 추가됨 데모 환경 만들기

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.