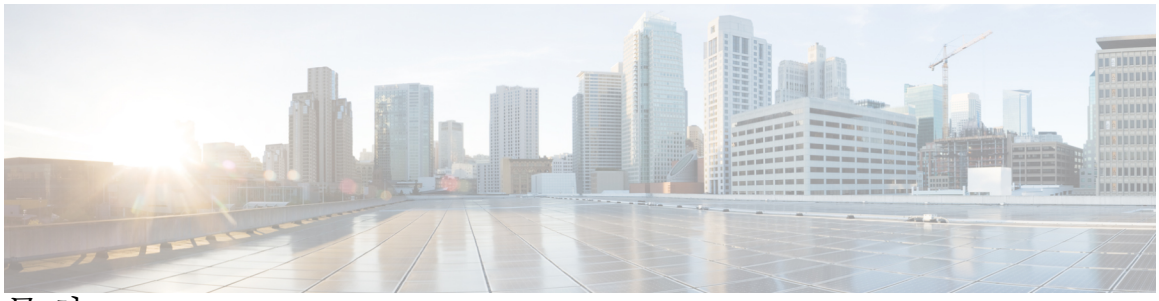
클라우드 플랫폼에 **Cisco Identity Services Engine** 네이티브 구축

최종 변경: 2026년 9월 8일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1

클라우드 기반 **Cisco ISE** 1

- 클라우드 기반 Cisco ISE 1
- 클라우드 플랫폼에서의 Cisco ISE 라이선싱 1
- Cisco ISE 하이브리드 구축 환경 업그레이드 2
  - 온프레미스에 PAN이 설치된 하이브리드 구축 환경 업그레이드 2
  - 클라우드에 PAN이 설치된 하이브리드 구축 환경 업그레이드 2
- 클라우드 플랫폼을 통해 실행된 Cisco ISE 인스턴스의 로그인 자격 증명 3
  - 클라우드 기반 Cisco ISE 의 사용자 이름 3
  - 클라우드 기반 Cisco ISE 비밀번호 3
- 추가 정보 4

장 2

Amazon Web Services의 **Cisco ISE** 5

- Amazon Web Services의 Cisco ISE 개요 5
  - AWS 환경에서 Cisco ISE 실행 방법 5
  - CFT 개요 5
  - AWS 클라우드에 연결된 배포 예시 6
  - Cisco ISE 인스턴스 및 사용 용도 6
  - AWS 환경의 멀티 노드 Cisco ISE 구축 8
- Cisco ISE AWS 인스턴스 생성 사전 요구 사항 8
  - AWS 클라우드 개념 숙지 8
  - 구성 사전 요구 사항 8
  - IP 주소 사전 요구 사항 9
- OCI에서 Cisco ISE 사용 시 알려진 제한 사항 9
  - 지원 제한 사항 9

구성 제한 사항 10
CLI 제한 사항 10
메모리, 디스크 크기 및 볼륨 제한 사항 10
구축 제한 사항 11
업그레이드 제한 사항 11
지연 시간(Latency) 제한 사항 11
사용자 데이터 백업 및 복원 제한 사항 11
AWS Marketplace를 통해 Cisco ISE CFT 실행 12
Cisco ISE 인스턴스 구성 12
Cisco ISE 인스턴스 구성 자동화 13
AWS CloudFormation Designer에서 CFT 보기 13
CFT 실행 및 파라미터 지정 13
Cisco ISE 인스턴스 파라미터 구성 13
다중 DNS 또는 NTP 서버 추가 16
CFT를 사용하여 Cisco ISE 실행 17
Cisco ISE 인스턴스 구성 17
CFT 파일 업로드 및 파라미터 구성 17
Cisco ISE AMI 실행 18
Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동 19
인스턴스 세부 정보 구성 19
고급 세부 정보 구성 20
User data 매개변수 22
스토리지 추가 26
태그 추가 26
보안 그룹 구성 27
검토 및 실행 27
기존 키 쌍 선택 또는 새 키 쌍 생성 27
Cisco ISE AMI 인스턴스 실행 28
설치 후 참고 사항 및 작업 28
인스턴스 실행 상태 확인 30
Cisco ISE GUI 또는 CLI 접속 시점 및 방법 30

키 쌍 다운로드 30
Cisco ISE 프로세스 상태 확인 31
AWS 환경의 Cisco ISE 호환성 정보 32
Cisco Catalyst Center 연동 지원 32
로드 밸런서 연동 지원 32
NIC 점보 프레임 지원 32
AWS 환경에서의 비밀번호 복구 및 재설정 32
비밀번호 재설정 32
AWS 시리얼 콘솔을 통해 Cisco ISE 비밀번호 변경 33
구성된 비밀번호 보기 33
새 퍼블릭 키 쌍 생성 34
AWS 환경에서의 비밀번호 복구 34

장 3

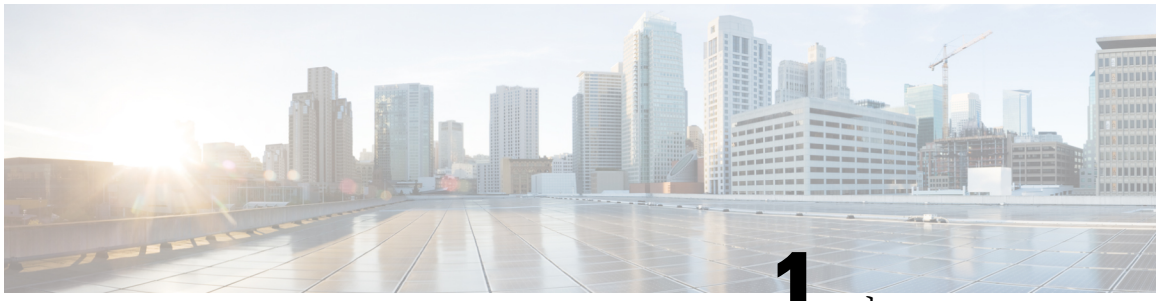
Azure Cloud Services의 Cisco ISE 35
Azure 클라우드 플랫폼의 Cisco ISE 35
Azure 배포 방법 35
Cisco ISE 에서 지원하는 Azure VM 크기 36
Microsoft Azure 클라우드 서비스 환경에서 Cisco ISE의 알려진 제한 사항 38
Azure 내 Cisco ISE 배포 시의 순서가 뒤바뀐 단편화 패킷 제한 사항 39
Azure VM을 사용하여 Cisco ISE 인스턴스 생성 40
Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동 41
인스턴스 세부 정보 구성 41
OS 디스크 크기 구성 42
네트워크 인터페이스 구성 42
사용자 세부 정보 구성 43
태그 구성 45
검토 및 생성 46
디스크 크기 편집 46
Azure 애플리케이션을 사용하여 Cisco ISE 인스턴스 생성 47
Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동 47
인스턴스 세부 정보 추가 47

네트워크 설정 구성 48
서비스 구성 49
사용자 세부 정보 추가 50
User data 매개변수 50
검토 및 생성 53
설치 후 작업 54
Azure 클라우드 기반 Cisco ISE의 호환성 정보 54
로드 밸런서 연동 지원 54
Azure 클라우드 에서 비밀번호 복구 및 재설정 54
시리얼 콘솔을 통한 Cisco ISE GUI 비밀번호 재설정 55
SSH 액세스를 위한 새 퍼블릭 키 쌍 생성 55

장 4

Oracle Cloud Infrastructure의 Cisco ISE 57
Oracle Cloud Infrastructure의 Cisco ISE 57
Cisco ISE가 지원하는 OCI 인스턴스 58
OCI에서 Cisco ISE 사용 시 알려진 제한 사항 59
OCI에서 Cisco ISE 인스턴스 생성 59
OCI 콘솔에서 Cisco ISE 옵션으로 이동 60
인스턴스 세부 정보 구성 60
Cisco ISE 인스턴스 고급 옵션 구성 61
User data 매개변수 64
Terraform Stack 파일을 사용하여 OCI에서 Cisco ISE 인스턴스 생성 68
OCI에서 Cisco ISE 스택 생성 68
Cisco ISE 인스턴스에 대한 변수 구성 69
구성을 검토하고 OCI에서 Cisco ISE 인스턴스 생성 70
설치 후 작업 71
OCI의 Cisco ISE 에 대한 호환성 정보 71
로드 밸런서 연동 지원 71
NIC 점보 프레임 지원 71
OCI 환경의 비밀번호 복구 및 재설정 72
시리얼 콘솔을 통한 Cisco ISE GUI 비밀번호 재설정 72

OCI에서 새 퍼블릭 키 쌍 생성 72
비밀번호 복구 73



1 장

클라우드 기반 Cisco ISE

- 클라우드 기반 Cisco ISE, 1 페이지
- 클라우드 플랫폼에서의 Cisco ISE 라이선싱, 1 페이지
- Cisco ISE 하이브리드 구축 환경 업그레이드, 2 페이지
- 클라우드 플랫폼을 통해 실행된 Cisco ISE 인스턴스의 로그인 자격 증명, 3 페이지
- 추가 정보, 4 페이지

클라우드 기반 Cisco ISE

이제 클라우드 서비스 공급자를 통해 기본적으로 Cisco Identity Services Engine(ISE)을 사용할 수 있으므로, 변화하는 비즈니스 요구 사항에 맞춰 Cisco ISE 구축 환경을 빠르고 쉽게 확장할 수 있습니다. Cisco ISE는 IaaS(Infrastructure as a Service) 솔루션으로 제공되므로, 네트워크 액세스를 신속하게 구축하고 어디에서나 서비스를 제어할 수 있습니다.

온프레미스 네트워크의 Cisco ISE 구축 환경을 다음으로 안전하게 확장할 수 있습니다.

- Cisco ISE 릴리스 3.1 및 이후 버전의 AWS(Amazon Web Services)
- Cisco ISE 릴리스 3.2 및 이후 버전의 Azure Cloud Services(Microsoft Azure) 및
- Cisco ISE 릴리스 3.2 및 이후 버전의 OCI(Oracle Cloud Infrastructure)

클라우드 플랫폼에서의 Cisco ISE 라이선싱

Cisco ISE는 클라우드 플랫폼에서 이용 가능한 BYOL(Bring Your Own License) 솔루션을 활용합니다. 사용하려는 Cisco ISE 기능에 필요한 다른 라이선스 외에도, 클라우드 플랫폼에서 Cisco ISE를 활성화하려면 Common VM License를 사용해야 합니다. Cisco ISE 라이선스에 대한 자세한 내용은 Cisco ISE Licensing Guide를 참조하십시오.

Cisco ISE 하이브리드 구축 환경 업그레이드

AWS, Microsoft Azure, OCI 환경의 Cisco ISE에서는 Cisco ISE 업그레이드 워크플로를 사용할 수 없습니다. Cisco ISE의 신규 설치만 지원됩니다. 그러나 구성 데이터에 대한 백업 및 복원은 가능합니다. Primary Administration Node(PAN)가 클라우드나 온프레미스 어느 곳에 설치되어 있든 관계없이 Cisco ISE 하이브리드 구축 환경을 업그레이드할 수 있습니다.

- 온프레미스에 PAN이 설치된 하이브리드 구축 환경 업그레이드 , 2 페이지.
- 클라우드에 PAN이 설치된 하이브리드 구축 환경 업그레이드 , 2 페이지.

온프레미스에 PAN이 설치된 하이브리드 구축 환경 업그레이드

PAN은 온프레미스에 설치되어 있고 일부 보조 노드는 클라우드에 설치되어 있는 하이브리드 구축 환경을 업그레이드하려면 다음 단계를 따르십시오.

프로시저

단계 **1** Cisco ISE 구축 환경에서 클라우드에 설치된 보조 노드의 등록을 취소합니다.

모든 보조 노드가 클라우드에 설치되어 있는 경우 이로 인해 다운타임이 발생할 수 있습니다.

단계 **2** 온프레미스 구축 환경을 상위 릴리스로 업그레이드합니다.

자세한 내용은 해당 릴리스의 *Cisco Identity Services Engine Upgrade Journey* 내 "Perform the Upgrade" 섹션을 참조하십시오.

단계 **3** 클라우드에 상위 릴리스 버전으로 필요한 수만큼 독립형(Standalone) Cisco ISE 노드를 설치합니다.

네트워크 액세스 디바이스(NAD)의 구성이 변경되는 것을 방지하려면 기존과 동일한 IP 주소로 노드를 설치하고 구성해야 합니다. 설치 프로세스에 대한 자세한 정보는 사용 중인 릴리스의 *Cisco Identity Services Engine Installation Guide*를 참조하십시오.

단계 **4** 이러한 독립형 노드를 업그레이드된 온프레미스 구축 환경에 등록합니다.

Cisco ISE에 새로 구축된 노드로 시스템 인증서를 가져와야 합니다. 시스템 인증서를 Cisco ISE 노드로 가져오는 방법에 대한 자세한 내용은 *Cisco Identity Services Engine Administrator Guide*내 "Basic Setup" 장의 "Import a System Certificate" 섹션을 참조하십시오.

온프레미스에 PAN이 설치된 하이브리드 Cisco ISE 구축 환경의 업그레이드가 완료되었습니다.

클라우드에 PAN이 설치된 하이브리드 구축 환경 업그레이드

다음 단계에 따라 PAN이 클라우드에 설치되어 있는 하이브리드 구축 환경을 업그레이드하십시오.

프로시저

단계 **1** 기존 구축 환경에서 Cisco ISE 구성 설정과 운영 로그를 백업합니다.

단계 **2** 구축 환경 내의 모든 노드를 종료합니다.

단계 **3** 클라우드와 온프레미스 양쪽 모두에 상위 릴리스 버전으로 필요한 수만큼의 독립형(Standalone) Cisco ISE 노드를 설치합니다.

네트워크 액세스 디바이스(NAD)의 구성이 변경되는 것을 방지하려면 기존과 동일한 IP 주소로 노드를 설치하고 구성해야 합니다. 설치 프로세스에 대한 자세한 정보는 사용 중인 릴리스의 *Cisco Identity Services Engine Installation Guide*를 참조하십시오.

단계 **4** 백업 데이터에서 Cisco ISE 설정을 복구합니다. 자세한 정보는 사용 중인 릴리스의 *Cisco Identity Services Engine Upgrade Journey* 내 "Backup and Restore Upgrade Process" 섹션을 참조하십시오.

단계 **5** 모든 노드를 새롭게 업그레이드된 클라우드 구축 환경에 등록합니다.

PAN이 클라우드에 설치되어 있는 하이브리드 Cisco ISE 배포 환경의 업그레이드가 완료되었습니다.

클라우드 플랫폼을 통해 실행된 **Cisco ISE** 인스턴스의 로그인 자격 증명

클라우드 네이티브 이미지를 사용하여 시작하거나 지원되는 클라우드 플랫폼에서 호스팅되는 모든 Cisco ISE 인스턴스의 사용자 이름과 암호는 안전해야 합니다.

클라우드 기반 **Cisco ISE** 의 사용자 이름

클라우드 플랫폼을 통해 실행되는 Cisco ISE 인스턴스의 기본 사용자 이름은 iseadmin입니다. 사용자 데이터에 다른 사용자 이름을 입력하는 경우에도 사용자 이름 iseadmin으로 Cisco ISE 인스턴스가 생성됩니다.

기억	AWS를 통해 시작되는 Cisco ISE 릴리스 3.1 인스턴스의 경우 기본 사용자 이름은 admin입니다.

클라우드 기반 **Cisco ISE** 비밀번호

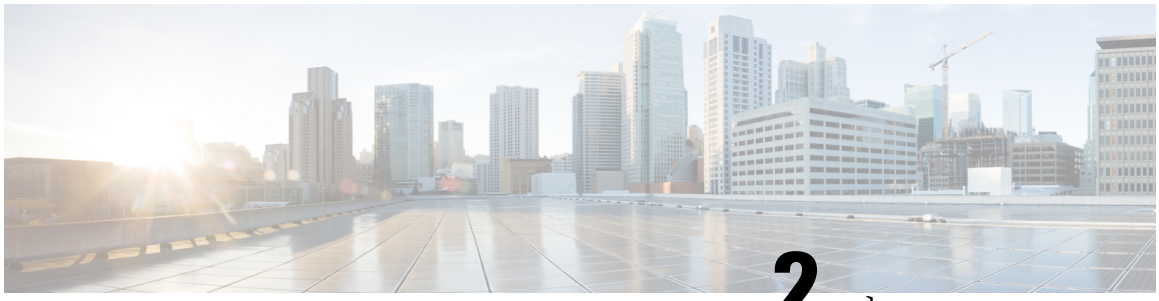
모든 클라우드 플랫폼에서 인스턴스 설정 시 구성한 비밀번호는 평문(Plaintext)으로 저장됩니다. 그러나 평문 비밀번호는 보안 위험을 초래할 수 있습니다. 따라서 클라우드 플랫폼에서 실행된 Cisco ISE 인스턴스의 경우, 처음 Cisco ISE GUI에 액세스할 때 로그인 비밀번호를 재설정해야 합니다. 또한 오류를 방지하기 위해 API 기반 자동화 스크립트 역시 업데이트된 비밀번호로 변경해야 합니다.

클라우드 네이티브 이미지를 사용하여 시작하거나 지원되는 클라우드 플랫폼에서 호스팅되는 모든 Cisco ISE 인스턴스의 사용자 이름과 암호는 안전해야 합니다.

추가 정보

참조:

- 클라우드 플랫폼에서의 Cisco ISE 구축 성능 및 확장성에 대한 정보는 Performance and Scalability Guide for Cisco Identity Services Engine를 참조하십시오.
- Cisco ISE 에 대한 자세한 내용은Cisco Identity Services Engine End-User Documentation을 참조하십시오.



2 장

Amazon Web Services의 Cisco ISE

- Amazon Web Services의 Cisco ISE 개요, 5 페이지
- Cisco ISE AWS 인스턴스 생성 사전 요구 사항 , 8 페이지
- OCI에서 Cisco ISE 사용 시 알려진 제한 사항 , 9 페이지
- AWS Marketplace를 통해 Cisco ISE CFT 실행, 12 페이지
- CFT를 사용하여 Cisco ISE 실행, 17 페이지
- Cisco ISE AMI 실행, 18 페이지
- 설치 후 참고 사항 및 작업, 28 페이지
- AWS 환경의 Cisco ISE 호환성 정보, 32 페이지
- AWS 환경에서의 비밀번호 복구 및 재설정, 32 페이지

Amazon Web Services의 Cisco ISE 개요

AWS 환경에서 Cisco ISE 실행 방법

AWS CloudFormation Templates(CFTs) 또는 Amazon Machine Images(AMIs)를 통해 AWS 환경에 Cisco ISE를 구성하고 실행할 수 있습니다. 다음 목록에 제시된 방법 중 하나를 통해 CFT를 사용하는 것을 권장합니다. AWS 환경에 Cisco ISE를 실행하려면 다음 절차 중 하나를 수행하십시오:

- AWS Marketplace를 통해 Cisco ISE CloudFormation 템플릿 실행
- CloudFormation 템플릿을 사용하여 Cisco ISE 실행
- Cisco ISE AMI 실행

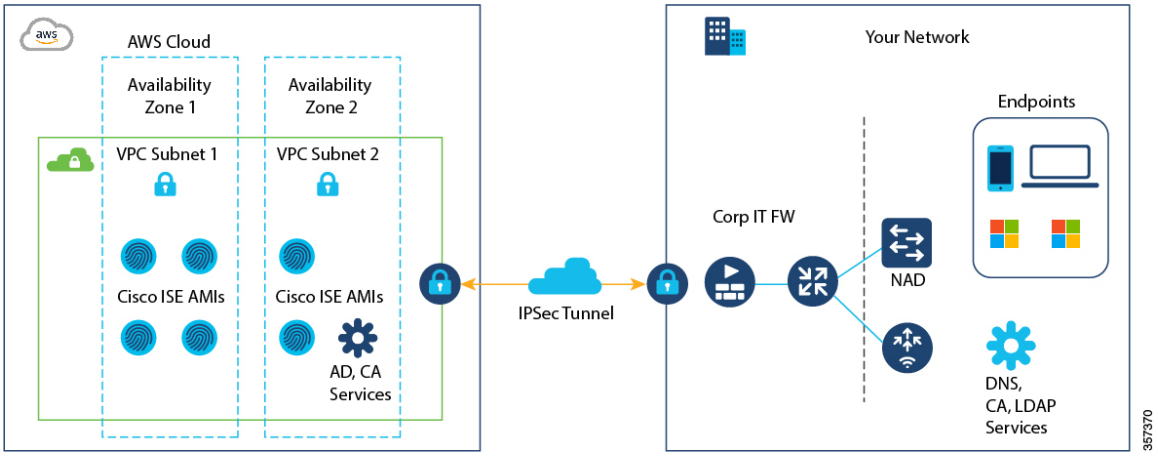
CFT 개요

CFT는 클라우드 구축 환경을 쉽게 생성하고 관리할 수 있도록 해주는 AWS 솔루션입니다. AWS에 Virtual Private Cloud(VPC)를 생성하여 네트워크를 클라우드로 확장하고, IPsec 터널을 통해 조직의 네트워크와 통신할 수 있도록 가상 프라이빗 게이트웨이를 구성합니다.

AWS 클라우드에 연결된 배포 예시

이 그림은 단순 예시입니다. 조직의 요구 사항에 따라 Certificate Authority(CA), Active Directory(AD), Domain Name System(DNS) 서버, Lightweight Directory Access Protocol(LDAP)과 같은 공통 서비스를 온프레미스 또는 AWS 환경에 배치할 수 있습니다.

그림 *1: AWS* 클라우드에 연결된 배포 예시



참조

AWS에서 CFT를 사용하는 방법에 대한 자세한 내용은 AWS CloudFormation User Guide를 참조하십시오.

Cisco ISE 인스턴스 및 사용 용도

이 표에는 현재 사용 가능한 Cisco ISE 인스턴스의 세부 정보가 포함되어 있습니다. 이러한 인스턴스를 사용하려면 Cisco ISE VM 라이선스를 구매해야 합니다. 특정 요구 사항에 대한 EC2 인스턴스 요금에 대한 자세한 내용은 Amazon EC2 On-Demand Pricing을 참조하십시오.

표 *1: Cisco ISE* 인스턴스

Cisco ISE 인스턴스 유형	**CPU** 코어	**RAM(GB)**
t3.xlarge 이 인스턴스는 Cisco ISE 평가 사용 사례를 지원합니다. 100개의 동시 활성 엔드포인트를 지원합니다. Cisco ISE 릴리스 3.5부터는 t3.xlarge 인스턴스 유형이 지원되지 않습니다.	4	16
m5.2.xlarge	8	32
c5.4xlarge	16	32

Cisco ISE 인스턴스 유형	CPU 코어	RAM(GB)
m5.4xlarge Cisco ISE 릴리스 3.3부터는 m5.4xlarge 인스턴스 유형이 지원되지 않습니다.	16	64
c5.9xlarge	36	72
m5.8xlarge	32	128
m5.16xlarge	64	256
c7i.4xlarge*	16	32
m7i.2xlarge*	8	32
m7i.8xlarge*	32	128
m7i.16xlarge*	64	256

* Cisco ISE 릴리스 3.4 패치 4, 3.5 및 이후 버전은 AWS에서 M7i 및 C7i 인스턴스 유형을 지원합니다.

AWS S3 스토리지 서비스를 활용하여 백업 및 복원 파일, 모니터링 및 문제 해결 보고서 등을 쉽게 저장할 수 있습니다.

주의

- 범용 인스턴스(General purpose instance)를 PSN으로 사용하는 경우, 컴퓨팅 최적화 인스턴스(Compute-optimized instance)를 PSN으로 사용할 때보다 성능 수치가 낮게 나타납니다.
- m5.2xlarge 및 m7i.2xlarge 인스턴스는 Extra Small PSN으로만 사용해야 합니다.

특정 인스턴스 유형의 사용 용도

이 표는 일부 인스턴스 유형과 해당 사용 용도를 분류합니다.

표 *2:* 인스턴스 유형 및 사용 용도

인스턴스 범주	인스턴스 유형 예시	사용 용도
컴퓨팅 최적화 인스턴스	c5.4xlarge c5.9xlarge c7i.4xlarge	• 컴퓨팅 집약적 작업 또는 애플리케이션 • Policy Service Node(PSN)

인스턴스 범주	인스턴스 유형 예시	사용 용도
범용 인스턴스	m5.4xlarge (이 인스턴스는 Cisco ISE 릴리스 3.2 및 이전 버전에서만 사용할 수 있습니다.) m5.8xlarge m5.16xlarge m7i.8xlarge m7i.16xlarge	• 데이터 처리 작업 및 데이터베이스 작업 • Policy Administration Node (PAN) 또는 Monitoring and Troubleshooting (MnT) 노드, 혹은 둘 다

참조

AWS 인스턴스의 규모 및 성능 데이터에 대한 자세한 내용은 Cisco ISE Performance and Scale guide를 참조하십시오.

AWS 환경의 멀티 노드 Cisco ISE 구축

앞서 설명한 절차들 외에도, 다음의 Cisco 개발 솔루션을 사용하여 AWS 환경에 멀티 노드 Cisco ISE 배포 환경을 설치하고 자동으로 구성할 수 있습니다.

- 소규모 구축을 위한Cisco ISE AWS Partner Solution.
- 모든 규모의 배포 환경을 위한 Cisco Developed Terraform Script.

Cisco ISE AWS 인스턴스 생성 사전 요구 사항

Cisco ISE AWS 인스턴스를 생성하기 위한 사전 요구 사항은 다음과 같습니다.

AWS 클라우드 개념 숙지

다음 내용을 숙지해야 합니다.

- AWS 서비스 할당량관리
- Amazon Elastic Compute Cloud(EC2) 인스턴스, Amazon Elastic Block Store(EBS) 볼륨과 같은 AWS 솔루션, 그리고 Regions, Availability Zones, Security Groups, Virtual Private Cloud(VPC) 등의 개념

참조

AWS 솔루션에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

구성 사전 요구 사항

Cisco ISE 인스턴스를 구성하기 전에

- 귀하는 AWS에 VPC를 구성하고,
- 암호화된 EBS 볼륨을 생성하며,
- 보안 그룹, 서브넷 및 키 쌍을 생성해야 합니다.

  AWS에서 Cisco ISE를 성공적으로 배포하려면 AWS Identity and Access Management(IAM) 정책에서 Key Management Service(KMS) 리소스에 대한 액세스를 허용해야 합니다. Cisco ISE에 사용할 보안 그룹을 구성할 때, 이용하려는 Cisco ISE 서비스의 모든 포트와 프로토콜에 대한 규칙을 생성해야 합니다. Cisco ISE 릴리스 3.5부터 IPv6 단일 스택 네트워크 환경에 Cisco ISE AWS 인스턴스를 구축하려면, AWS Virtual Private Cloud(VPC) 내에 IPv6용 서브넷이 구성되어 있어야 합니다.

IP 주소 사전 요구 사항

다음은 IP 주소 사전 요건입니다.

- 네트워크 인터페이스에 IPv6 주소를 구성하려면, 서브넷이 AWS에서 활성화된 IPv6 CIDR(Classless Inter-Domain Routing) 풀을 가져야 합니다.
- Cisco ISE CloudFormation 템플릿의 Management Network(관리 네트워크) 필드에 입력하는 IP 주소는 AWS에 네트워크 인터페이스 개체로 이미 존재하고 있는 IP 주소여서는 안 됩니다.
- 구축 환경에서 프라이빗 IP를 정적(Static) IP로 구성할 수 있습니다. 단, 이 정적 IP는 DNS를 통해 확인할 수 있는 호스트 이름과 함께 구성해야 합니다.

OCI에서 Cisco ISE 사용 시 알려진 제한 사항

다음은 AWS에서 Cisco ISE 사용할 때 발생하는 알려진 제한 사항입니다.

지원 제한 사항

- Amazon VPC는 Layer 3 기능만 지원합니다. AWS 인스턴스 상의 Cisco ISE 노드는 Layer 1 및 Layer 2 기능에 의존하는 Cisco ISE 기능을 지원하지 않습니다. 예를 들어, Cisco ISE CLI를 사용하는 DHCP SPAN 프로파일러 프로브 및 CDP 프로토콜 관련 작업은 현재 지원되지 않습니다.

  온프레미스 디바이스에서 VPC로의 통신은 반드시 안전해야 합니다.
- NIC 본딩(NIC bonding)은 지원되지 않습니다.
- 듀얼 NIC는 오직 두 개의 NIC(Gigabit Ethernet 0 및 Gigabit Ethernet 1)로만 지원됩니다. Cisco ISE 인스턴스에 보조 NIC를 구성하려면 다음을 수행해야 합니다:

  1. AWS에서 네트워크 인터페이스 개체를 생성합니다.
  2. Cisco ISE 인스턴스의 전원을 끕니다.
  3. 이 네트워크 인터페이스 개체를 Cisco ISE에 연결합니다.

4. AWS에 Cisco ISE를 설치하고 실행합니다.
5. Cisco ISE CLI를 사용하여 네트워크 인터페이스 개체의 IP 주소를 보조 NIC로 수동 구성합니다.

- Amazon EC2 사용자 데이터 스크립트는 지원되지 않습니다.

구성 제한 사항

다음 사항들은 수행할 수 없습니다:

- Cisco ISE 인스턴스의 Amazon EBS 스냅샷을 생성한 다음 해당 스냅샷으로 다른 EBS 볼륨을 생성하는 작업
- AWS를 통해 Cisco ISE를 실행할 때 IPv6 기반 NTP 서버를 구성하는 작업 Cisco ISE 릴리스 3.5부터는 듀얼 스택 및 순수 IPv6 인스턴스 모두에서 IPv6 기반 NTP 서버 구성이 지원됩니다.
- 성공적으로 생성된 인스턴스의 IP 주소를 변경하는 작업
- 초기 관리자 사용자 계정 이름을 생성하는 작업 초기 관리자 사용자 계정 이름인 iseadmin이 기본으로 생성됩니다. 이 사용자 계정 이름은 설치 프로세스가 완료된 후 Cisco ISE에 SSH 및 GUI로 액세스하는 데 모두 사용됩니다.

Cisco ISE는 인스턴스 세부 정보를 획득하기 위해 IP 주소 169.254.169.254를 통해 AWS 클라우드로 트래픽을 전송합니다. 이는 클라우드 인스턴스인지 여부를 확인하기 위함이며, 온프레미스 배포 환경에서는 이를 무시할 수 있습니다.

CLI 제한 사항

CLI 제한 사항은 다음과 같습니다.

- AWS 환경에서는 비밀번호 기반 인증을 사용하는 Cisco ISE CLI에 대한 SSH 접속이 지원되지 않습니다. 보안 키 쌍을 통해서만 Cisco ISE CLI에 접근할 수 있습니다. 프라이빗 키(또는 PEM) 파일을 사용 중일 때 해당 파일을 분실할 경우, Cisco ISE CLI에 접근할 수 없습니다. 비밀번호 기반 인증 방식을 사용하여 Cisco ISE CLI에 접근하는 모든 연동(Integration)은 지원되지 않습니다(예: Cisco Catalyst Center 릴리스 2.1.2 및 이전 버전).
- Cisco ISE 릴리스 3.1에서는 AWS 환경에서 실행된 Cisco ISE 인스턴스를 통해 show inventory 명령을 실행할 때, 출력 결과에 AWS 환경 내 Cisco ISE의 인스턴스 유형이 표시되지 않습니다. 이 문제는 Cisco ISE 릴리스 3.1 패치 1 및 이후 릴리스에서 해결되었습니다.

메모리, 디스크 크기 및 볼륨 제한 사항

메모리, 디스크 크기 및 볼륨 제한 사항은 다음과 같습니다.

- EC2 인스턴스의 크기는 조정할 수 없습니다.

- Cisco ISE 디스크 EBS 볼륨을 AMI로 변환한 다음 해당 AMI로 다른 EC2 인스턴스를 다시 시작할 수 없습니다.
- 구성한 Cisco ISE CFT에서 볼륨 크기를 GB 단위로 정의합니다. 하지만 AWS는 EBS 스토리지 볼륨을 기비바이트(GiB) 단위로 생성합니다. 따라서 Cisco ISE CFT의 Volume Size(볼륨 크기)에 600을 입력하면 AWS는 600GiB(또는 644.25GB)의 EBS 볼륨을 생성합니다.
- Cisco ISE 유휴 상태일 때 Insufficient *Virtual Machine Resources* 알람을 수신할 수 있습니다. 효과적인 전력 절감을 위해 CPU 주파수가 필수 기준선 주파수(2GHz)보다 낮게 유지되므로 이 알람은 무시해도 됩니다.

구축 제한 사항

지원되는 구축 유형은 두 가지이지만, 노드 간 지연 시간(Latency)이 300밀리초 미만이어야 합니다.

- 일부 Cisco ISE 노드는 온프레미스에 배치하고 나머지 노드는 AWS에 배치하는 하이브리드 구축 환경.
- VPC 피어링 연결을 통한 리전 간(Interregional) 구축 환경.

업그레이드 제한 사항

AWS 환경의 Cisco ISE에서는 Cisco ISE 업그레이드 워크플로를 사용할 수 없습니다. 신규 설치만 지원됩니다. 그러나 구성 데이터에 대한 백업 및 복원은 가능합니다.

참조

Cisco ISE 하이브리드 구축 업그레이드에 대한 자세한 내용은 *Upgrade Guidelines for Hybrid Deployments* 를 참조하십시오.

지연 시간(Latency) 제한 사항

온프레미스에 위치한 외부 ID 소스를 연동할 수 있습니다. 하지만 온프레미스 ID 소스를 사용할 경우 지연 시간으로 인해 AWS 호스팅 ID 소스나 Cisco ISE 내부 사용자 데이터베이스를 사용할 때보다 Cisco ISE의 성능이 떨어질 수 있습니다.

사용자 데이터 백업 및 복원 제한 사항

사용자 데이터 백업 및 복원 제한 사항은 다음과 같습니다.

- 사용자 데이터 검색은 Metadata V1(IMDSv1)에서만 지원되며 V2에서는 동작하지 않습니다.
- Cisco ISE CLI 또는 GUI를 통해 구성 데이터 백업 도중 복원 작업을 실행할 때 ADE-OS 파라미터를 포함해서는 안 됩니다.

AWS Marketplace를 통해 Cisco ISE CFT 실행

이 방법을 사용하여 독립형 Cisco ISE 인스턴스를 실행할 수 있습니다.

Cisco ISE CFT는 범용 SSD(gp2) 볼륨 유형의 인스턴스를 생성합니다.

AWS 시장 통해 Cisco ISE CFT를 실행하려면 다음 단계를 따르십시오.

프로시저

단계 **1** Cisco ISE 인스턴스를 구성합니다.

단계 **2** CFT 실행 및 파라미터 지정

Cisco ISE 인스턴스 구성

다음 단계에 따라 Cisco ISE 인스턴스를 구성하십시오.

프로시저

단계 **1** https://console.aws.amazon.com/ 에서 Amazon Management Console에 로그인합니다.

단계 **2** **AWS Marketplace Subscriptions(AWS** 마켓플레이스 구독**)**을 검색합니다.

단계 **3** **Manage Subscriptions(**구독 관리**)** 화면에서 **Discover Products(**제품 검색**)**를 클릭합니다.

단계 **4** 제품 이름을 클릭합니다.

단계 **5** **Continue with Selected Configuration(**선택한 구성으로 계속**)**을 클릭합니다.

단계 **6** **Configure this Software(**이 소프트웨어 구성**)** 영역에서 **Learn More(**자세히 알아보기**)**를 클릭합니다.

단계 **7** **Download CloudFormation Template(CloudFormation** 템플릿 다운로드**)**를 클릭하여 시스템 로컬에 Cisco ISE CFT를 다운로드합니다.

필요에 따라 다운로드한 CFT를 사용하여 다른 Cisco ISE 인스턴스 구성을 자동화할 수 있습니다.

Learn More(자세히 알아보기**)** 대화 상자에서 **View Template(**템플릿 보기**)**를 클릭하여 AWS CloudFormation Designer에서 CFT를 볼 수 있습니다.

단계 **8** **Software Version(**소프트웨어 버전**)** 및 **AWS Region(AWS** 지역**)** 드롭다운 목록에서 필요한 값을 선택합니다.

단계 **9** **Continue to Launch(**시작으로 계속**))**를 클릭합니다. 자세한 내용은 CFT 실행 및 파라미터 지정, 13 페이지를 참조하십시오.

Cisco ISE 인스턴스 구성 자동화

필요에 따라 다운로드한 CFT를 사용하여 다른 Cisco ISE 인스턴스 구성을 자동화할 수 있습니다.

AWS CloudFormation Designer에서 CFT 보기

Learn More(자세히 알아보기**)** 대화 상자에서 **View Template(**템플릿 보기**)**를 클릭하여 AWS CloudFormation Designer에서 CFT를 볼 수 있습니다.

CFT 실행 및 파라미터 지정

다음 단계에 따라 CFT를 실행하고 파라미터를 구성하십시오.

프로시저

단계 **1** **Action(**작업**)** 드롭다운 목록에서 **Provision(**프로비전**)**을 선택합니다.

단계 **2** **Launch(**실행**)**를 클릭합니다.

단계 **3** **Create Stack(**스택 생성**)** 창에서 **Template Is Ready(**템플릿 준비됨**)** 및 **Amazon S3 URL** 라디오 버튼을 클릭합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **6** **Parameters(**파라미터**)** 영역에 세부 사항을 입력합니다. 파라미터에 대한 자세한 내용은 Cisco ISE 인스턴스 파라미터 구성, 13 페이지를 참조하십시오.

단계 **7** **Next(**다음**)**를 클릭하여 인스턴스 생성 프로세스를 시작합니다.

참조

Cisco ISE 배포 환경 생성에 대한 내용은 사용 중인 릴리스의 *Cisco ISE Administrator Guide* 내 "Deployment" 장을 참조하십시오.

Cisco ISE 인스턴스 파라미터 구성

Cisco ISE 인스턴스에 대해 다음과 같은 매개변수를 구성할 수 있습니다:

필드 이름	필드 설명
호스트 이름	이 필드는 알파벳, 숫자 및 하이픈(-)만 지원합니다. 이름의 길이는 19자를 초과할 수 없습니다.

필드 이름	필드 설명
인스턴스 키 쌍	SSH를 통해 Cisco ISE 인스턴스에 액세스하려면 AWS에서 사용자 이름 iseadmin으로 생성한 PEM 파일을 선택합니다. Cisco ISE 릴리스 3.1의 경우, 사용자 이름은 admin입니다. 아직 구성하지 않았다면 지금 AWS에서 PEM 키 쌍을 생성하십시오. 예: `ssh -i mykey Pair.pem iseadmin#myhostname.compute-1.amazonaws.com`
보안 그룹 관리	드롭다운 목록에서 Security Group(보안 그룹)을 선택합니다. 이 CFT를 구성하기 전에 AWS에서 보안 그룹을 생성해야 합니다. 이 단계에서는 보안 그룹을 하나만 추가할 수 있습니다. 보안 그룹은 설치 후 Cisco ISE 에서 추가할 수 있습니다.
관리 네트워크	Cisco ISE 인터페이스에 사용할 서브넷 을 선택합니다. IPv6 주소를 활성화하려면 IPv6 CIDR 블록을 VPC 및 서브넷과 연결해야 합니다. 아직 서브넷을 구성하지 않았다면 지금 AWS에서 생성하십시오.
관리 프라이빗 IP (Cisco ISE 릴리스 3.5에서는 **Management Interface IPv4 Address(**관리 인터페이스 **IPv4** 주소**)** 로 이름 변경됨)	앞서 선택한 서브넷 의 IPv4 주소를 입력합니다. 이 필드를 비워 두면 AWS DHCP가 IP 주소를 할당합니다. Cisco ISE 인스턴스를 생성한 후 **Instance Summary(**인스턴스 요약**)** 창에서 프라이빗 IP 주소를 복사합니다. 그런 다음 Cisco ISE 구축 환경을 생성하기 전에 DNS 서버에서 IP와 호스트 이름을 매핑합니다.
IPv6 전용 인스턴스 생성 (Cisco ISE 릴리스 3.5부터 적용)	IPv6 전용 인스턴스 생성 여부를 선택합니다. 선택할 경우 IPv4 주소는 할당되지 않습니다.
관리 IPv6 주소 (Cisco ISE 릴리스 3.5부터 적용)	이전에 선택한 서브넷 의 IPv6 주소를 입력합니다. 이 필드를 비워 두면 AWS DHCP가 IPv6 주소를 할당합니다.
표준 시간대	드롭다운 목록에서 표준 시간대를 선택합니다.
인스턴스 유형	드롭다운 목록에서 Cisco ISE 인스턴스 유형을 선택합니다.
암호화	암호화를 활성화하려면 드롭다운 목록에서 **True(**참**)**를 선택합니다. Cisco ISE 3.3 이상 릴리스에서 이 필드의 기본값은 **True(**참**)** 입니다.

필드 이름	필드 설명
(선택 사항) KMS 키	데이터 암호화를 위한 KMS Key 또는 Amazon Resource Name, 혹은 별칭(alias)을 입력합니다. 이 필드는 Cisco ISE 릴리스 3.3 및 이후 버전에 적용되는 선택 사항입니다. • KMS Key가 제공되면 데이터 암호화에 사용됩니다. • KMS Key가 제공되지 않으면 기본 키가 데이터 암호화에 사용됩니다.
볼륨 크기	볼륨 크기를 GB 단위로 지정합니다. 허용되는 범위는 300GB~2400GB입니다. 프로덕션 환경에서는 600GB를 권장합니다. 평가 목적으로만 600GB 미만의 볼륨 크기를 구성하십시오. 인스턴스를 종료하면 볼륨도 함께 삭제됩니다. AWS는 EBS 스토리지 볼륨을 기비바이트(GiB) 단위로 생성합니다. 예를 들어 Volume Size(볼륨 크기) 필드에 600을 입력하면 AWS는 600GiB(또는 644.25GB)의 EBS 볼륨을 생성합니다.
DNS 도메인	이 필드에 허용되는 값은 ASCII 문자, 숫자, 하이픈 (-) 및 마침표(.)입니다.
기본 네임 서버 (Cisco ISE 릴리스 3.4 이전의**Name Server(**네임 서버**)**)	네임 서버의 IP 주소를 입력합니다.
(선택 사항) 보조 네임 서버 (Cisco ISE 릴리스 3.4부터 적용)	Cisco ISE 에 대해 설정할 보조 이름 서버의 IP 주소를 입력합니다.
(선택 사항) 3차 네임 서버 (Cisco ISE 릴리스 3.4부터 적용)	Cisco ISE 에 대해 설정할 3차 네임 서버의 IP 주소를 입력합니다.
기본 NTP 서버 (Cisco ISE 릴리스 3.4 이전의**NTP Server(NTP** 서버**)**)	기본 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다(예: time.nist.gov). 구문이 잘못된 경우 Cisco ISE 서비스가 시작되지 않을 수 있습니다. 여기에 입력한 IP 주소 또는 호스트 이름이 올바르지 않으면 Cisco ISE가 NTP 서버와 동기화할 수 없습니다. SSH 터미널을 사용하여 Cisco ISE에 로그인한 다음, Cisco ISE CLI를 사용하여 올바른 NTP 서버를 구성하십시오.

필드 이름	필드 설명
(선택 사항) 보조 NTP 서버 (Cisco ISE 릴리스 3.4부터 적용)	보조 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다(예: time.nist.gov). 구문이 잘못된 경우 Cisco ISE 서비스가 시작되지 않을 수 있습니다.
(선택 사항) 3차 NTP 서버 (Cisco ISE 릴리스 3.4부터 적용)	3차 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다(예: time.nist.gov). 구문이 잘못된 경우 Cisco ISE 서비스가 시작되지 않을 수 있습니다.
ERS	Cisco ISE 시작 시 ERS 서비스를 활성화하려면 **yes(**예**)**를 입력합니다. 이 필드의 기본값은 **no(**아니요**)**입니다.
OpenAPI	Cisco ISE 시작 시 OpenAPI 서비스를 활성화하려면 **yes(**예**)**를 입력합니다. 이 필드의 기본값은 **no(**아니요**)**입니다. Cisco ISE 릴리스 3.4부터 OpenAPI 서비스는 기본적으로 활성화됩니다.
pxGrid	Cisco ISE 시작 시 pxGrid 서비스를 활성화하려면 **yes(**예**)**를 입력합니다. 이 필드의 기본값은 **no(**아니요**)**입니다.
pxGrid 클라우드	이 필드의 기본값은 **no(**아니요**)**입니다. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI를 통해서만 활성화할 수 있습니다. 따라서 이 필드를 사용할 수 없습니다.
비밀번호	Cisco ISE GUI에 사용할 관리자 비밀번호를 입력합니다. 비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 합니다. 비밀번호는 AWS 콘솔의 인스턴스 설정 창 내 **User Data(**사용자 데이터**)** 영역에 평문(Plain text)으로 표시됩니다.

참조

사용 중인 릴리스의 *Cisco ISE Administrator Guide* 내 "Basic Setup" 장의 "User Password Policy" 섹션을 참조하십시오.

다중 DNS 또는 NTP 서버 추가

Cisco ISE 릴리스 3.4부터는 CFT를 통해 최대 3개의 DNS 또는 NTP 서버를 구성할 수 있지만, 한 번에 하나의 서버만 추가할 수 있습니다. Cisco ISE 인스턴스를 구축한 후 DNS 또는 NTP 서버를 추가하려면 Cisco ISE CLI를 사용해야 합니다.

Cisco ISE 릴리스 3.5부터는 CFT를 통해 IPv6 DNS 및 NTP 서버를 직접 구성할 수 있습니다. 이전 Cisco ISE 릴리스에서 IPv6 서버를 구성하려면 Cisco ISE CLI를 사용하십시오.

CFT를 사용하여 Cisco ISE 실행

이 방법을 사용하여 독립형 Cisco ISE 인스턴스를 실행할 수 있습니다.

Cisco ISE CFT는 범용 SSD(gp2) 볼륨 유형의 인스턴스를 생성합니다.

다음 단계에 따라 CFT를 사용하여 Cisco ISE를 실행하십시오.

시작하기 전에

프로시저

단계 **1** Cisco ISE 인스턴스를 구성합니다.
단계 **2** CFT 파일을 업로드하고 파라미터를 구성합니다.

Cisco ISE 인스턴스 구성

다음 단계에 따라 Cisco ISE 인스턴스를 구성하십시오.

프로시저

단계 **1** https://console.aws.amazon.com/ 에서 Amazon Management Console에 로그인합니다.
단계 **2** **AWS Marketplace Subscriptions(AWS** 마켓플레이스 구독**)**을 검색합니다.
단계 **3** **Manage Subscriptions(**구독 관리**)** 화면에서 **Discover Products(**제품 검색**)**를 클릭합니다.
단계 **4** 검색 창에 Cisco ISE (Cisco Identity Services Engine)를 입력합니다.
단계 **5** 제품 이름을 클릭합니다.
단계 **6** 새 창이 표시되면 **Continue to Subscribe(**구독 진행**)**를 클릭합니다.
단계 **7** **Continue with Selected Configuration(**선택한 구성으로 계속**)**을 클릭합니다.
단계 **8** **Configure this Software(**이 소프트웨어 구성**)** 영역에서 **Learn More(**자세히 알아보기**)**를 클릭합니다.

CFT 파일 업로드 및 파라미터 구성

CFT 파일을 업로드하고 파라미터를 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Download CloudFormation Template(CloudFormation** 템플릿 다운로드**)**를 클릭하여 Cisco ISE CFT를 로컬 시스템에 다운로드합니다.

단계 **2** AWS 검색 창을 사용하여 **CloudFormation**을 검색합니다.

단계 **3** **Create Stack(**스택 생성**)** 드롭다운 목록에서 **With new resources (standard)(**새 리소스 포함**(**표준**))**를 선택합니다.

단계 **4** **Create Stack(**스택 생성**)** 창에서 **Template Is Ready(**템플릿 준비됨**)** 및 **Upload a Template File(**템플릿 파일 업로드**)**을 선택합니다.

단계 **5** **Choose File(**파일 선택**)**을 클릭하고 Cisco ISE 인스턴스 구성 , 17 페이지에서 다운로드한 CFT 파일을 업로드합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** **Stack Name(**스택 이름**)** 필드에 값을 입력합니다.

단계 **8** **Parameters(**파라미터**)** 영역에 필요한 세부 정보를 입력합니다. 파라미터에 대한 자세한 내용은 Cisco ISE 인스턴스 파라미터 구성, 13 페이지를 참조하십시오.

Cisco ISE AMI 실행

다음 단계에 따라 Cisco ISE AMI를 실행하십시오.

1. Amazon EC2 콘솔의 Cisco ISE 옵션으로 이동합니다.
2. 인스턴스 세부 정보 구성
3. 고급 세부 정보 구성
4. 스토리지 추가
5. 태그 추가
6. 보안 그룹 구성
7. 검토 및 실행
8. 기존 키 쌍을 선택하거나 새 키 쌍을 생성
9. Launch Instances(인스턴스 실행)

주의 Simplified Auto Recovery(간소화된 자동 복구)는 시스템 상태 확인 오류가 발생할 경우 기본 인프라의 자동 복구를 수행하는 AWS 기능입니다. 이 프로세스는 AWS에서 관리하며, 서비스 연속성을 보장하기 위해 인스턴스를 자동으로 재부팅합니다.

자동 재부팅 프로세스 중에 발생하는 리소스 프로비저닝 지연으로 인해 간혹 Cisco ISE가 올바르게 초기화되지 않을 수 있습니다.

이 경우 AWS Management Console에 로그인하고 EC2 Dashboard로 이동하여 해당 Cisco ISE 인스턴스를 선택한 후 수동으로 재부팅하여 서비스를 정상 상태로 복구하십시오. EC2 인스턴스 관리에 대한 자세한 지침은 공식 AWS 설명서를 참조하십시오.

Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동

다음 단계에 따라 AWS EC2 콘솔에서 **Cisco Identity Engine(ISE)** 옵션으로 이동하십시오:

프로시저

단계 **1** https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔로 로그인합니다.

단계 **2** 왼쪽 창에서 **Instances(**인스턴스**)**를 클릭합니다.

단계 **3** **Instances(**인스턴스**)** 창에서 **Launch Instances(**인스턴스 시작**)**를 클릭합니다.

단계 **4** **Step 1: Choose AMI(1**단계**: AMI** 선택**)** 창의 왼쪽 메뉴에서 **AWS Marketplace(AWS** 마켓플레이스**)**를 클릭합니다.

단계 **5** 검색 필드에 **Cisco Identity Services Engine**입력합니다.

단계 **6** **Cisco Identity Services Engine (ISE)** 옵션에서 **Select(**선택**)**를 클릭합니다.
AMI의 다양한 세부 정보가 포함된 **Cisco Identity Services Engine (ISE)** 대화 상자가 나타납니다.

단계 **7** 정보를 검토하고 **Continue(**계속**)**을 클릭하여 진행합니다.

인스턴스 세부 정보 구성

AWS EC2 콘솔에서 Cisco ISE 인스턴스 세부 정보를 추가하고 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Step 2: Choose an Instance Type(2**단계**:** 인스턴스 유형 선택**)** 창에서 사용할 인스턴스 유형 옆에 있는 라디오 버튼을 클릭합니다.

단계 **2** **Next: Configure Instance Details(**다음**:** 인스턴스 세부 정보 구성**)**를 클릭합니다.

단계 **3** **Step 3: Configure Instance Details(3**단계**:** 인스턴스 세부 정보 구성**)** 창에서 지침에 설명된 대로 각 필드에 필수 정보를 입력합니다.

표 *3:* 인스턴스 세부 정보에 대한 구성 지침

필드 이름	필드 설명
인스턴스 수	필드에 **1**을 입력합니다.
네트워크	Cisco ISE 인스턴스를 시작할 VPC를 선택합니다.
서브넷	Cisco ISE 인스턴스를 시작할 서브넷 을 선택합니다. 참고 Cisco ISE 릴리스 3.5부터는 IPv6 전용 AWS 서브넷 사용하여 IPv6 전용 네트워크에서 Cisco ISE AWS 인스턴스를 시작할 수 있습니다.
네트워크 인터페이스	드롭다운 목록에는 기본적으로 **New Network Interface(**새 네트워크 인터페이스**)**가 표시되며, 이는 연결된 DHCP 서버에 의해 IP 주소가 Cisco ISE 에 자동 할당됨을 의미합니다. 이 필드에 IP 주소를 입력하여 Cisco ISE 에 고정 IP 주소를 할당할 수 있습니다. **Network Interfaces(**네트워크 인터페이스**)** 드롭다운 목록에서 동일한 서브넷 의 기존 네트워크 인터페이스를 선택할 수도 있습니다. 설정 프로세스 중에는 인터페이스를 하나만 구성할 수 있습니다. Cisco ISE 설치한 후에는 Cisco ISE 통해 인터페이스를 추가할 수 있습니다.

다음에 수행할 작업

정보를 검토하고 *Configure advanced details* 단계로 진행합니다.

고급 세부 정보 구성

AWS EC2 콘솔에서 고급 Cisco ISE 인스턴스 세부 정보를 추가하고 구성하려면 다음 단계를 따르십시오.

프로시저

Advanced Details(고급 세부 정보**)** 영역 내 **User Data(**사용자 데이터**)** 섹션에서 **As Text(**텍스트로**)** 라디오 버튼을 클릭하고 키-값 쌍을 올바른 형식으로 입력합니다. Cisco ISE 릴리스 3.5부터는 IPv6 단일 스택 네트워크에서 Cisco ISE AWS 인스턴스를 실행하려면 **Advanced Details(**고급 세부 정보**)** 에서 **Metadata IPv6 endpoint(**메타데이터 **IPv6** 엔드포인트**)**옵션을 활성화해야 합니다.

User data(사용자 데이터) 입력을 통해 구성하는 각 필드에는 올바른 구문을 사용해야 합니다. **User data(**사용자 데이터**)** 필드에 입력하는 정보는 입력할 때 검증되지 않습니다. 잘못된 구문을 사용하면 이미지를 시작할 때 Cisco ISE 서비스가 시작되지 않을 수 있습니다. 사용자 데이터 필드를 통해 제출하는 설정에 대한 지침은 다음과 같습니다.

표 *4: User data(*사용자 데이터*)* 필드 구성 지침

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
hostname	알파벳과 숫자, 하이픈(-)만 포함된 호스트 이름을 입력합니다. 호스트 이름의 길이는 19자 미만이어야 하며 밑줄(_)을 포함해서는 안 됩니다.	구문은 권장 사항을 충족해야 합니다.
primarynameserver	기본 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	Cisco ISE 릴리스 3.5부터 IPv6 단일 스택 네트워크의 AWS 인스턴스에서 IPv6 기반 이름 서버가 지원됩니다.
dnsdomain	DNS 도메인 의 FQDN을 입력합니다. 이 항목에는 ASCII 문자, 숫자, 하이픈(-), 마침표(.)를 포함할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.
ntpserver	동기화에 사용할 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다(예: time.nist.gov).	Cisco ISE 릴리스 3.5부터는 IPv6 기반 NTP 서버가 듀얼 스택 및 IPv6 단일 스택 네트워크 기반 AWS 인스턴스에 대해 이 필드에서 지원됩니다.
timezone	시간대를 입력합니다(예: Etc/UTC). 특히 Cisco ISE 노드가 분산 구축 환경에 설치된 경우, 모든 Cisco ISE 노드를 협정 세계시(UTC) 표준 시간대로 설정하는 것을 권장합니다. 이를 통해 구축 환경 내 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프를 항상 동기화할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.
username	구성하는 기본 사용자 이름은 **admin**이어야 합니다. **admin**이외의 사용자 이름을 구성하는 경우 AMI를 시작할 때 Cisco ISE CLI에 액세스할 수 없습니다.	Cisco ISE 릴리스 3.2부터 필수 사용자 이름은 **iseadmin**입니다. 따라서 username=<admin> 태그는 지원되지 않습니다.
비밀번호	Cisco ISE의 GUI 기반 로그인에 사용할 비밀번호를 구성합니다. 입력하는 비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 합니다. 비밀번호는 6~25자 사이여야 하며 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 비밀번호 는 사용자 이름 또는 사용자 이름의 역순(iseadmin 또는 nimdaesi), cisco 또는 ocsic과 같거나 이를 포함할 수 없습니다. 허용되는 특수 문자는 @~*!,+=_- 입니다. .	사용 중인 릴리스의 Cisco ISE Administrator Guide 내 "Basic Setup" 장의 "User Password Policy" 섹션을 참조하십시오.

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
ersapi	ERS를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.
openapi	OpenAPI를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	Cisco ISE 릴리스 3.4부터 OpenAPI 서비스는 기본적으로 활성화됩니다. 인스턴스를 시작할 때 OpenAPI 관련 옵션을 지정할 필요가 없습니다.
pxGrid	pxGrid를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.
pxgrid_cloud	pxGrid Cloud 활성화하려면 **yes** 를, pxGrid Cloud 허용하지 않으려면 **no** 를 입력합니다. pxGrid Cloud를 활성화하려면 반드시 pxGrid를 먼저 활성화해야 합니다. pxGrid를 비활성화한 상태에서 pxGrid Cloud를 활성화하면, 실행 시 pxGrid Cloud 서비스가 활성화되지 않습니다.	Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI에서만 활성화할 수 있습니다. 따라서 이 필드는 User data에 포함되지 않습니다.

다음에 수행할 작업

정보를 검토하고 *Add storage* 단계로 진행합니다.

User data 매개변수

필드	형식	**Cisco ISE** 릴리스 **3.1**	**Cisco ISE** 릴리스 **3.2**	**Cisco ISE** 릴리스 **3.3**	**Cisco ISE** 릴리스 **3.4**	**Cisco ISE** 릴리스 **3.5**
hostname	호스트 이름 =<hostname of Cisco ISE>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
primarynameserver	primarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primarynameserver=<IPv6 주소> 지원)	지원됨.	지원됨.	지원됨.	지원됨.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
secondarynameserver	secondarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiarynameserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiarynameserver 필드를사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
tertiarynameserver	tertiarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
dnsdomain	dnsdomain=<example.com>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ntpserver	ntpserver=<NTP FQDN IPv4 또는 서버의 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 ntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원됨.	지원됨.	지원됨.	지원되지 않음. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전부터 primaryntpserver로 대체됩니다. ntpserver를사용하면 Cisco ISE 서비스가 시작되지 않을 수 있습니다.	지원되지 않음. 대신 primaryntpserver를 사용하십시오.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
Primaryntpserver	primaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전에서 ntpserver를 대체합니다.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
secondaryntpserver	secondaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiaryntpserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiaryntpserver 필드를사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
tertiaryntpserver	tertiaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
timezone	timezone=<표준 시간대>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
username	username=<admin>	지원됨 (예: <admin>) Cisco ISE 릴리스 3.1 패치 1부터 지원됨.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.
username	username=iseadmin	필수 아님	필수	필수	필수	필수
비밀번호	password=<비밀번호>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ersapi	ersapi=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
openapi	openapi=<yes/no>	지원됨.	지원됨.	지원됨.	OpenAPI는 기본적으로 활성화되어 있습니다.	OpenAPI는 기본적으로 활성화되어 있습니다.
pxGrid	pxGrid=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
pxgrid_cloud	pxgrid_cloud=<yes/no>	지원되지 않음	지원되지 않음	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원되지 않음. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI를 통해서만 활성화할 수 있습니다.

파라미터 구문 요구 사항

Cisco ISE on Cloud의 User data 파라미터를 지정할 때 속성이나 값을 작은따옴표나 큰따옴표로 묶지 마십시오. 모든 값은 따옴표 없이 평문(Plain text)으로 입력해야 합니다.

잘못된 입력	올바른 입력
hostname="i34a"	hostname=i34a
primarynameserver="9.9.9.9"	primarynameserver="9.9.9.9"
dnsdomain="example.com"	dnsdomain=example.com
primaryntpserver="north-america.pool.ntp.org"	primaryntpserver="north-america.pool.ntp.org"

Cisco ISE 릴리스 3.3부터 시리얼 콘솔에 유효성 검사 결과 메시지가 표시됩니다. 이러한 메시지는 결과가 생성되는 시점에 시리얼 콘솔이 열려 있는 경우에만 볼 수 있습니다.

스토리지 추가

다음 단계에 따라 Cisco ISE 인스턴스에 스토리지를 추가하십시오:

프로시저

단계 **1** **Next: Add Storage(**다음**:** 스토리지 추가**)**를 클릭합니다.

단계 **2** **4**단계**:** 스토리지 추가 창에서 다음을 수행합니다.

a) 크기**(GiB)** 열에 값을 입력합니다.

이 필드의 유효한 범위는 279.4~2235.2GiB입니다. 프로덕션 환경의 경우 스토리지를 558.8 GiB 이상으로 구성해야 합니다. 558.8 GiB 미만의 스토리지는 평가 환경(Evaluation environment)에서만 지원됩니다. 참고로 Cisco ISE는 스토리지를 GB 단위로 정의하여 생성됩니다. 이곳에 입력한 GiB 값은 Cisco ISE 이미지 생성 프로세스 중에 GB 단위 값으로 자동 변환됩니다. GB 단위를 기준으로 할 때 유효한 스토리지 범위는 300~2400 GB이며, 프로덕션 환경에서 Cisco ISE에 허용되는 최솟값은 600 GB입니다.

b) **Volume Type(**볼륨 유형**)** 드롭다운 목록에서 **General** 맞춤형 **SSO (gp2)**를선택합니다.

c) EBS 암호화 활성화하려면 **Encryption(**암호화**)** 드롭다운 목록에서 암호화 키를 선택합니다.

경고**!**
이 창에 표시되는 **Add New Volume(**새 볼륨 추가**)** 버튼을 클릭하지 마십시오.

다음에 수행할 작업

정보를 검토하고 *Add tags(*태그 추가*)* 단계를 진행합니다.

태그 추가

프로시저

단계 **1** **Next: Add Tags(**다음**:** 태그 추가**)**를 클릭합니다.

단계 **2** (선택 사항) **Step 5: Add Tags(5**단계**:** 태그 추가**)** 창에서 **Add Tag(**태그 추가**)**를 클릭하고 **Key(**키**)** 및 **Value(**값**)** 필드에 필요한 정보를 입력합니다. **Instances(**인스턴스**)**, **Volumes(**볼륨**)**및 **Network Interfaces(**네트워크 인터페이스**)** 열의 확인란은 기본적으로 선택되어 있습니다. **Step 3: Configure Instance Details(3**단계**:** 인스턴스 세부 정보 구성**)** 창에서 특정 네트워크 인터페이스를 선택한 경우 이 창에서 추가하는 각 태그에 대한 **Network Interfaces(**네트워크 인터페이스**)** 확인란의 선택을 해제해야 합니다.

다음에 수행할 작업

정보를 검토하고 보안 그룹 구성으로 진행합니다.

보안 그룹 구성

새 보안 그룹을 생성하거나 기존 보안 그룹을 추가하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Next: Configure Security Group(**다음**:** 보안 그룹 구성**)**을 선택합니다.

단계 **2** **Step 6: Configure Security Group(6**단계**:** 보안 그룹 구성**)** 창의 **Assign a security group(**보안 그룹 할당**)** 영역에서 해당 라디오 버튼을 클릭하여 새 보안 그룹을 생성하거나 기존 보안 그룹을 선택할 수 있습니다.

a) **Create a new security group(**새 보안 그룹 생성**)**을선택하는 경우 **Type(**유형**)**, **Protocol(**프로토콜**)**, **Port Range(**포트 범위**)**, **Source(**소스**)**및 **Description(**설명**)** 필드에 필요한 세부 정보를 입력합니다.

b) **Select existing security group(**기존 보안 그룹 선택**)**을 선택하는 경우, 추가할 보안 그룹 옆의 확인란을 선택합니다.

다음에 수행할 작업

정보를 검토하고 *Review and Launch(검토 및 실행)* 단계를 진행합니다.

검토 및 실행

다음 단계에 따라 지금까지 생성한 구성을 검토하고 Cisco ISE AMI를 실행하십시오:

프로시저

단계 **1** **Review and Launch(**검토 및 실행**)**를 클릭합니다.

단계 **2** **Step 7: Review Instance Launch(7**단계**:** 인스턴스 시작 검토**)** 창에서 이 워크플로우 에서 생성한 모든 구성을 검토합니다. 해당 **Edit(**편집**)** 링크를 클릭하여 이러한 섹션의 값을 편집할 수 있습니다.

단계 **3** **Launch(**실행**)**를 클릭합니다.

다음에 수행할 작업

Select an existing key pair or create a new key pair 단계로 진행합니다.

기존 키 쌍 선택 또는 새 키 쌍 생성

기존 키 쌍을 선택하거나 새 키 쌍을 생성하려면 다음 단계를 따르십시오:

프로시저

Select an existing key pair or create a new key pair(기존 키 쌍 선택 또는 새 키 쌍 생성**)** 대화 상자의 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Choose an existing key pair(**기존 키 쌍 선택**)**
- **Create a new key pair(**새 키 쌍 생성**)**

참고
SSH를 사용하여 Cisco ISE 에 로그인하려면 사용자 이름이 **iseadmin**인 키 쌍을 사용합니다. 키 쌍은 그대로 유지해야 합니다. 키 쌍이 손실되거나 손상된 경우 새 키 쌍을 기존 인스턴스에 매핑할 수 없으므로 Cisco ISE 를 복구할 수 없습니다.

다음에 수행할 작업

정보를 검토하고 *Launch instances* 단계로 진행합니다.

Cisco ISE AMI 인스턴스 실행

Cisco ISE AMI 인스턴스를 실행합니다:

프로시저

승인 확인(Acknowledgment statement) 체크박스를 선택한 후 **Launch Instances(**인스턴스 실행**)**를 클릭합니다.

Launch Status(실행 상태**)** 창에는 인스턴스 생성의 진행 상황이 표시됩니다.

다음에 수행할 작업

동일한 절차를 사용하여 추가 Cisco ISE AMI 인스턴스를 생성할 수 있습니다.

설치 후 참고 사항 및 작업

인스턴스 실행 상태를 확인하려면 AWS 콘솔의 왼쪽 창에서 **Instances(**인스턴스**)**를 클릭합니다. 인스턴스가 구성되는 동안 인스턴스의 **Status Check(**상태 확인**)** 열에 **Initializing(**초기화 중**)**이 표시됩니다. 인스턴스가 준비되어 사용할 수 있게 되면 해당 열에 **'x checks done'**이 표시됩니다.

Cisco ISE EC2 인스턴스가 생성되고 약 30분 후부터 Cisco ISE GUI 또는 CLI에 접속할 수 있습니다. AWS가 해당 인스턴스에 할당한 IP 주소를 사용하여 Cisco ISE의 CLI 및 GUI에 접속하고, Cisco ISE 관리 포털 또는 콘솔에 로그인할 수 있습니다.

Cisco ISE 인스턴스가 준비되고 사용할 수 있으면 다음 단계를 수행합니다.

1. AWS에서 키 쌍을 생성하면 키 쌍을 로컬 시스템으로 다운로드하라는 메시지가 표시됩니다. SSH 터미널에서 Cisco ISE 인스턴스에 성공적으로 로그인하려면 특정 권한을 업데이트해야 하므로 키 쌍을 반드시 다운로드하십시오.

   사용하는 운영 체제에 따라 다음 중 하나를 수행합니다.

표 ***5: OS*** 기반 작업

사용 중인 **OS**가...	수행할 작업
Linux 또는 macOS	CLI에서 다음 명령을 실행합니다. `sudo chmod 0400 mykeypair.pem`
Windows	1. 로컬 시스템에서 키 파일을 마우스 오른쪽 버튼으로 클릭합니다. 2. **Properties(**속성**) > Security(**보안**) > Advanced(**고급**)**를 차례로 선택합니다. 3. **Permissions(**권한**)** 탭에서 해당 옵션을 클릭하여 적절한 사용자에게 모든 권한을 할당하고, **Disable Inheritance(**상속 비활성화**)**를 클릭합니다. 4. **Disable Inheritance(**상속 비활성화**)**를 클릭한 다음 **Convert inherited permissions into explicit permissions on this object(**이 개체에 대해 상속된 권한을 명시적 권한으로 변환**)**를 클릭합니다. 5. **Permissions(**권한**)** 탭의 **Permissions entries(**권한 항목**)** 영역에서 해당 항목을 클릭하여 시스템 및 관리자 사용자를 선택한 후 **Remove(**제거**)**를 클릭합니다. 6. **Apply(**적용**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

2. CLI 애플리케이션에서 다음 명령을 실행하여 Cisco ISE CLI에 접속합니다.

   ssh -i mykey Pair.pem iseadmin@<*Cisco ISE Private IP Address*>

3. 로그인 프롬프트에서 사용자 이름에 **iseadmin**을 입력합니다.

4. 시스템 프롬프트에서 **show application version ise**을 입력하고 **Enter**를 누릅니다.

5. Cisco ISE 프로세스의 상태를 확인하려면 **show application status ise**를 입력하고 **Enter**를 누릅니다.

출력 결과에 애플리케이션 서버가 실행 중(Running) 상태라고 표시되면 Cisco ISE를 사용할 준비가 된 것입니다.

6. 그런 다음 Cisco ISE GUI에 로그인할 수 있습니다.
7. 해당 릴리스에 대한 *Cisco ISE 설치 가이드* 의 "설치 확인 및 설치 후 작업" 장의 "설치 후 작업 목록" 항목에 표시된 설치 후 작업을 수행합니다.

인스턴스 실행 상태 확인

인스턴스 실행 상태를 확인하려면 AWS 콘솔의 왼쪽 창에서 **Instances(**인스턴스**)**를 클릭합니다. 인스턴스가 구성되는 동안 인스턴스의 **Status Check(**상태 확인**)** 열에 **Initializing(**초기화 중**)**이 표시됩니다. 인스턴스가 준비되어 사용할 수 있게 되면 해당 열에 '**x checks done**'이 표시됩니다.

Cisco ISE GUI 또는 CLI 접속 시점 및 방법

Cisco ISE EC2 인스턴스가 생성되고 약 30분 후부터 Cisco ISE GUI 또는 CLI에 접속할 수 있습니다. AWS가 해당 인스턴스에 할당한 IP 주소를 사용하여 Cisco ISE의 CLI 및 GUI에 접속하고, Cisco ISE 관리 포털 또는 콘솔에 로그인할 수 있습니다.

키 쌍 다운로드

Cisco ISE 인스턴스가 준비되어 사용할 수 있게 되면 다음 단계를 수행하여 키 쌍을 다운로드합니다:

1. AWS에서 키 쌍을 생성하면 키 쌍을 로컬 시스템으로 다운로드하라는 메시지가 표시됩니다.

   SSH 터미널에서 Cisco ISE 인스턴스에 성공적으로 로그인하려면 특정 권한을 업데이트해야 하므로 키 쌍을 반드시 다운로드하십시오.
2. 사용 중인 운영 체제에 따라 다음 중 하나를 수행하십시오:

표 ***6: OS***에 따라 수행할 작업

사용 중인 **OS**가...	수행할 작업
Linux 또는 macOS	CLI에서 다음 명령을 실행합니다: `sudo chmod 0400 mykeypair.pem`

사용 중인 **OS**가...	수행할 작업
Windows	1. 로컬 시스템에서 키 파일을 마우스 오른쪽 버튼으로 클릭합니다. 2. **Properties(**속성**) > Security(**보안**) > Advanced(**고급**)**를 차례로 선택합니다. 3. **Permissions(**권한**)** 탭에서 해당 옵션을 클릭하여 적절한 사용자에게 모든 권한을 할당하고, **Disable Inheritance(**상속 비활성화**)**를 클릭합니다. 4. **Disable Inheritance(**상속 비활성화**)**를 클릭한 다음 **Convert inherited permissions into explicit permissions on this object(**이 개체에 대해 상속된 권한을 명시적 권한으로 변환**)**를 클릭합니다. 5. **Permissions(**권한**)** 탭의 **Permissions entries(**권한 항목**)** 영역에서 해당 항목을 클릭하여 시스템 및 관리자 사용자를 선택한 후 **Remove(**제거**)**를 클릭합니다. 6. **Apply(**적용**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

Cisco ISE 프로세스 상태 확인

다음 단계에 따라 Cisco ISE 프로세스 상태를 확인하십시오.

프로시저

단계 **1** CLI 애플리케이션에서 다음 명령을 실행하여 Cisco ISE CLI에 접속합니다:

ssh -i mykeypair.pem iseadmin@<*Cisco ISE Private IP Address*>

단계 **2** 로그인 프롬프트에서 사용자 이름으로 **iseadmin**을 입력합니다.

단계 **3** 시스템 프롬프트에서 **show application version ise**을 입력하고 **Enter**를 누릅니다.

단계 **4** Cisco ISE 프로세스의 상태를 확인하려면 **show application status ise**를 입력하고 **Enter**를 누릅니다.

출력 결과에 애플리케이션 서버가 실행 중(Running) 상태라고 표시되면 Cisco ISE를 사용할 준비가 된 것입니다.

다음에 수행할 작업

Cisco ISE GUI에 로그인하여 *Cisco ISE Installation Guide* 내 "Installation Verification and Post-Installation Tasks(설치 확인 및 설치 후 작업)" 장의 "List of Post-Installation Tasks(설치 후 작업 목록)"에 나열된 설치 후 작업을 수행합니다.

AWS 환경의 Cisco ISE 호환성 정보

이 섹션에서는 AWS 환경에 고유하게 적용되는 Cisco ISE 호환성 정보를 제공합니다. Cisco ISE 의 일반 호환성 세부 정보는 Cisco Identity Services Engine Network Component Compatibility를 참조하십시오.

Cisco Catalyst Center 연동 지원

Cisco ISE를 Cisco Catalyst Center 릴리스 2.2.1 및 이후 버전과 연동할 수 있습니다.

로드 밸런서 연동 지원

RADIUS 및 TACACS 트래픽의 로드 밸런싱을 위해 AWS 네이티브 네트워크 로드 밸런서를 Cisco ISE와 연동할 수 있습니다. 하지만 다음과 같은 제한 사항이 적용됩니다.

- Change of Authorization(CoA) 기능은 네트워크 로드 밸런서에서 클라이언트 IP 보존(Client IP preservation) 기능을 활성화한 경우에만 지원됩니다.
- 네트워크 로드 밸런서는 Source IP Affinity만 지원하고 Calling Station ID 기반 Sticky Session을 지원하지 않으므로, 불균등한 로드 밸런싱이 발생할 수 있습니다.
- 네트워크 로드 밸런서는 RADIUS 기반 Health Check를 지원하지 않으므로, 노드에서 RADIUS 서비스가 비활성 상태이더라도 트래픽이 Cisco ISE PSN으로 전송될 수 있습니다.

TACACS 트래픽의 로드 밸런싱을 위해 AWS 네이티브 네트워크 로드 밸런서를 Cisco ISE와 연동할 수 있습니다. 하지만 네트워크 로드 밸런서가 TACACS+ 서비스 기반의 Health Check를 지원하지 않으므로, 노드에서 TACACS 서비스가 비활성 상태이더라도 트래픽이 Cisco ISE PSN으로 전송될 수 있습니다.

NIC 점보 프레임 지원

Cisco ISE는 점보 프레임(Jumbo frames)을 지원합니다. Cisco ISE의 최대 전송 단위(MTU)는 9,001바이트인 반면, 네트워크 액세스 디바이스(NAD)의 MTU는 일반적으로 1,500바이트입니다. Cisco ISE 표준 및 점보 프레임을 모두 문제 없이 지원하고 수신합니다. 구성 모드(Configuration mode)의 Cisco ISE CLI를 통해 필요에 따라 Cisco ISE MTU를 재설정할 수 있습니다.

AWS 환경에서의 비밀번호 복구 및 재설정

비밀번호 재설정

다음 작업을 통해 Cisco ISE 가상 머신 비밀번호를 재설정할 수 있습니다.

- AWS 시리얼 콘솔을 통해 Cisco ISE 비밀번호 변경 , 33 페이지.

• 구성된 비밀번호 보기 , 33 페이지.
• 새 퍼블릭 키 쌍 생성, 34 페이지.

AWS 시리얼 콘솔을 통해 Cisco ISE 비밀번호 변경

AWS 환경에서 시리얼 콘솔을 통해 Cisco ISE GUI 비밀번호를 변경하려면 다음 단계를 따르십시오:

프로시저

단계 **1** AWS 계정에 로그인하고 EC2 대시보드로 이동합니다.

단계 **2** 왼쪽 메뉴에서 **Instances(**인스턴스**)**를 클릭합니다.

단계 **3** 비밀번호를 변경해야 하는 Cisco ISE 인스턴스 ID를 클릭합니다. 비밀번호를 알고 있는 경우 이 작업의 5단계로 건너뜁니다.

단계 **4** 시리얼 콘솔에 로그인하려면 Cisco ISE 인스턴스를 설치할 때 설정했던 초기 비밀번호를 사용해야 합니다. 비밀번호 보려면 View the configured password를 참조하십시오.

단계 **5** **Connect(**연결**)**를 클릭합니다.

EC2 시리얼 콘솔 탭이 표시됩니다.

단계 **6** **Connect(**연결**)**를 클릭합니다.

단계 **7** 새 브라우저 탭이 표시됩니다. 화면이 검은색인 경우 **Enter**를 눌러 로그인 프롬프트를 표시합니다.

단계 **8** 시리얼 콘솔에 로그인합니다. 4단계에서 표시된 비밀번호 작동하지 않으면 Password Recovery 섹션을 참조하십시오.

단계 **9** application **reset-passwd iseadmin** 명령을 사용하여 iseadmin 계정에 사용할 새 웹 UI 비밀번호를 설정합니다. iseadmin 계정의 웹 UI 비밀번호가 재설정됩니다.

구성된 비밀번호 보기

구성된 비밀번호를 확인하려면 다음 단계를 따르십시오.

프로시저

단계 **1** EC2 대시보드에서 **Actions(**작업**)**를 클릭합니다.

단계 **2** **Instance Settings(**인스턴스 설정**)**로 이동합니다.

단계 **3** 현재 비밀번호 보려면 **Edit user data(**사용자 데이터 편집**)**를 선택합니다.

새 퍼블릭 키 쌍 생성

Cisco ISE 인스턴스 구성 시점에 생성했던 기존 키 쌍은 사용자가 새로 생성하는 퍼블릭 키로 교체되지 않습니다.

다음 단계에 따라 새로운 퍼블릭 키 쌍을 생성하십시오:

프로시저

단계 **1** AWS에서 새 퍼블릭 키를 생성합니다. 공개 키 쌍을 생성하는 방법에 대한 자세한 내용은 Create key pairs를 참조하십시오.

단계 **2** 이전 작업에서 설명한 내용을 참고하여 AWS 시리얼 콘솔에 로그인합니다.

단계 **3** 퍼블릭 키를 저장할 새 저장소 생성하려면 Creating a private repository를 참조하십시오.

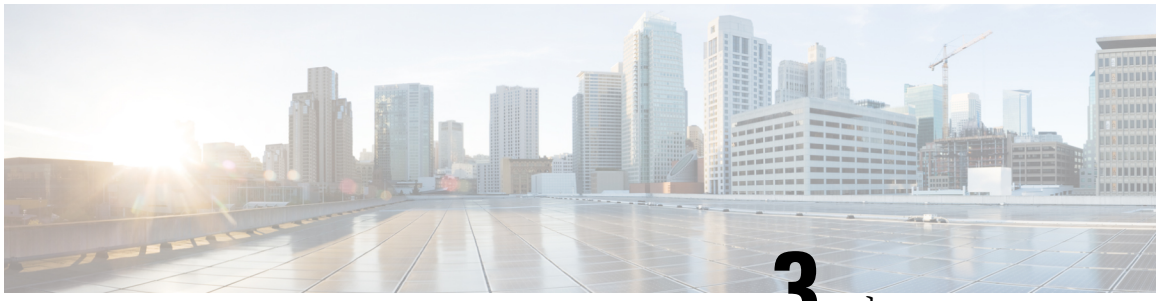
CLI를 통해 액세스할 수 있는 저장소 이미 있는 경우 다음 단계로 건너뜁니다.

단계 **4** 새 퍼블릭 키를 가져오려면 다음 명령을 사용합니다: **crypto key import <public key filename> repository <repository name>**

가져오기가 완료되면 새 퍼블릭 키를 활용하여 SSH를 통해 Cisco ISE에 로그인할 수 있습니다.

AWS 환경에서의 비밀번호 복구

AWS의 Cisco ISE에는 비밀번호 복구 메커니즘이 없습니다. 새로운 Cisco ISE 인스턴스를 생성하고 구성 데이터의 백업 및 복원을 수행해야 할 수 있습니다. 설정 스크립트가 실행되지 않으므로, AWS에서 EC2 인스턴스의 사용자 데이터를 편집하더라도 시리얼 콘솔 로그인에 사용되는 CLI 비밀번호는 변경되지 않습니다. Cisco ISE 가상 인스턴스는 이에 영향을 받지 않습니다.



3 장

Azure Cloud Services의 Cisco ISE

- Azure 클라우드 플랫폼의 Cisco ISE, 35 페이지
- Azure 배포 방법, 35 페이지
- Cisco ISE 에서 지원하는 Azure VM 크기, 36 페이지
- Microsoft Azure 클라우드 서비스 환경에서 Cisco ISE의 알려진 제한 사항, 38 페이지
- Azure 내 Cisco ISE 배포 시의 순서가 뒤바뀐 단편화 패킷 제한 사항, 39 페이지
- Azure VM을 사용하여 Cisco ISE 인스턴스 생성, 40 페이지
- 디스크 크기 편집 , 46 페이지
- Azure 애플리케이션을 사용하여 Cisco ISE 인스턴스 생성, 47 페이지
- 설치 후 작업, 54 페이지
- Azure 클라우드 기반 Cisco ISE의 호환성 정보 , 54 페이지
- Azure 클라우드 에서 비밀번호 복구 및 재설정, 54 페이지

Azure 클라우드 플랫폼의 Cisco ISE

Cisco ISE 는 Azure 클라우드 서비스에서 사용할 수 있습니다. Azure 클라우드 에서 Cisco ISE 구성하고 설치하려면 Azure 클라우드 기능 및 솔루션에 대해 숙지해야 합니다. 시작하기 전에 다음 Azure 클라우드 개념을 숙지하십시오.

- 구독 및 리소스 그룹
- Azure Virtual Machines Instances, Images, SSH Keys, Tags, VM Resizing을 참조하십시오.

Azure 배포 방법

Azure 애플리케이션 또는 Azure VM을 사용하여 Microsoft Azure 환경에 Cisco ISE를 배포할 수 있습니다.

Azure 애플리케이션과 Azure VM 중 어느 것을 사용하여 Cisco ISE를 배포하더라도 비용이나 Cisco ISE 기능 면에서는 차이가 없습니다.

Azure VM 대비 다음과 같은 이점을 제공하는 Azure 애플리케이션의 사용을 권장합니다:

- Azure VM 구성 시의 User Data(사용자 데이터) 필드 대신, Azure 애플리케이션을 사용하면 UI를 통해 직접 Cisco ISE 관련 옵션들을 쉽게 구성할 수 있습니다.
- Azure 애플리케이션 초기 구성 시 300~2400GB 범위 내에서 OS 디스크 볼륨을 선택할 수 있습니다. 하지만 Azure VM의 초기 구성 중에는 OS 디스크 볼륨을 Azure 포털에서 제공하는 고정된 값으로만 변경할 수 있습니다.

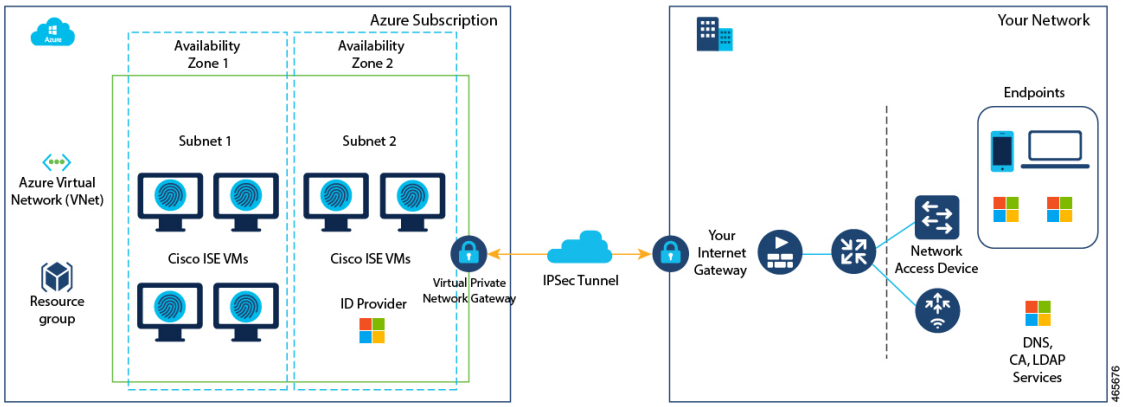
  가상 머신을 재구성하려면 Cisco ISE 설치 및 실행 후에 추가적인 단계를 더 거쳐야 합니다.
- Cisco ISE가 지원하는 특정 Azure VM 크기 목록에서 직접 선택할 수 있습니다.
- 초기 구성 시 정적 프라이빗 IP 주소(Static private IP address)를 구성할 수 있습니다.

다음과 같은 경우 Azure VM을 사용할 수 있습니다:

- Azure 포털 UI를 사용하여 Cisco ISE를 배포하지 않는 경우.
- Azure VM 구성 워크플로에서 사용할 수 있는 추가 설정 중 하나를 이용해야 하는 경우.

아래는 Azure 클라우드에 연결된 배포 환경의 예시입니다.

그림 ***2: Azure*** 클라우드에 연결된 배포 예시



이러한 배포 방법 외에도, Cisco Developed Terraform Script를 사용하여 Azure 환경에 멀티 노드 Cisco ISE 배포 환경을 설치하고 자동으로 생성할 수도 있습니다.

참고 Cisco ISE 인스턴스를 생성하기 위해 기존 Azure 클라우드 이미지를 복제하지 마십시오.

Cisco ISE 에서 지원하는 Azure VM 크기

Cisco ISE 다음 Azure VM 크기 중 하나를 사용하여 설치할 수 있습니다.

표 *7: Cisco ISE* 에서 지원하는 *Azure VM* 크기

Azure VM 크기	vCPU	RAM(GB)
Standard_D64s_v4 이 인스턴스는 Cisco ISE 평가 사용 사례를 지원합니다. 100개의 동시 활성 엔드포인트를 지원합니다.	4	16
Standard_D8s_v4	8	32
Standard_F16s_v2	16	32
Standard_F32s_v2	32	64
Standard_D16s_v4	16	64
Standard_D32s_v4	32	128
Standard_D64s_v4	64	256

Cisco ISE 릴리스 3.5부터는 Standard_D4s_v4 및 Standard_D16s_v4 VM이 지원되지 않습니다.

Fsv2 시리즈 Azure VM 크기는 컴퓨팅에 최적화되어 있으며 컴퓨팅 집약적인 작업 및 애플리케이션의 PSN으로 사용하는 데 가장 적합합니다.

Dsv4 시리즈는 PAN 또는 MnT 노드 또는 둘 다로 사용하는 데 가장 적합한 범용 Azure VM 크기이며 데이터 처리 작업 및 데이터베이스 작업에 사용할 수 있습니다.

범용 인스턴스(General purpose instance)를 PSN으로 사용하는 경우, 컴퓨팅 최적화 인스턴스(Compute-optimized instance)를 PSN으로 사용할 때보다 성능 수치가 낮게 나타납니다.

Standard_D8s_v4 VM 크기는 초대형 PSN으로만 사용해야 합니다.

Azure VM 크기의 규모 및 성능 데이터에 대한 자세한 내용은 *Performance and Scalability Guide for Cisco Identity Services Engine*를 참조하십시오.

참고 시간이 지남에 따라 Microsoft가 Azure VM 크기에 대한 가용성, 예약 구매 또는 예약 갱신 지원을 폐기, 제한 또는 변경할 수 있습니다. Cisco는 Azure 플랫폼 지원 및 Cisco ISE 클라우드 통합이 발전함에 따라 Cisco ISE 에 대해 지원되는 Azure VM 크기 목록을 주기적으로 업데이트합니다.

Azure에서 Cisco ISE 위한 예약을 구축, 크기 조정 또는 구매하기 전에 최신 Microsoft Azure VM 라이프사이클 및 예약 지침을 검토하십시오.

가장 최근의 Microsoft 지침에 따르면 2026년 7월 1일부터 Fsv2 시리즈를 포함한 특정 VM 시리즈의 예약 인스턴스(Reserved VM Instance) 구매 및 갱신과 관련된 변경 사항이 적용될 예정입니다. 이 목록에는 Cisco ISE 에서 지원하는 VM 크기(예: Standard_F16s_v2 및 Standard_F32s_v2)가 포함됩니다.

더 이상 예약 인스턴스 갱신에 사용할 수 없는 Standard_F16s_v2 또는 Standard_F32s_v2를 교체하는 경우, Cisco ISE 에서 지원하는 대체 VM 크기로 Standard_D32s_v4를 사용할 것을 적극 권장합니다. 이러한 인스턴스들은 Microsoft가 지원을 중단하기 전까지는 종량제(Pay-As-You-Go) 방식으로 계속 사용할 수 있습니다.

Microsoft Azure 클라우드 서비스 환경에서 Cisco ISE의 알려진 제한 사항

Microsoft Azure 클라우드 서비스 환경에서 Cisco ISE를 사용할 때 발생하는 알려진 제한 사항은 다음과 같습니다:

- Azure Virtual Machine을 사용하여 Cisco ISE를 생성하는 경우, Microsoft Azure는 기본적으로 DHCP 서버를 통해 VM에 프라이빗 IP 주소를 할당합니다. Microsoft Azure 환경에 Cisco ISE를 배포하기 전에 Microsoft Azure에서 할당한 IP 주소로 정방향 및 역방향 DNS 항목을 먼저 업데이트하십시오.

  Cisco ISE 설치가 완료된 후, Microsoft Azure에서 Network Interface 개체를 업데이트하여 VM에 정적(Static) IP 주소를 할당할 수 있습니다. 이렇게 하려면 다음을 수행합니다.

  1. VM을 중지합니다.
  2. **Private IP address settings(**프라이빗 **IP** 주소 설정**) > Assignment(**할당**) > Static(**정적**)**을 선택합니다.
  3. VM을 재시작합니다.
  4. Cisco ISE 시리얼 콘솔에서 해당 IP 주소를 Gi0 인터페이스에 할당합니다.
  5. Cisco ISE 애플리케이션 서버를 재시작합니다.

- 듀얼 NIC 구성은 단 두 개의 NIC(Gigabit Ethernet 0 및 Gigabit Ethernet 1)로만 지원됩니다. 보조 NIC를 구성하려면 먼저 Azure에서 네트워크 인터페이스 개체를 생성하고, Cisco ISE 인스턴스의 전원을 차단한 다음, 해당 네트워크 인터페이스 개체를 Cisco ISE에 연결하십시오.

Azure 환경에 Cisco ISE 설치 및 실행을 완료한 후, Cisco ISE CLI를 사용하여 수동으로 네트워크 인터페이스 개체의 IP 주소를 보조 NIC로 구성하십시오.

- Microsoft Azure 환경에서는 Cisco ISE 업그레이드를 수행할 수 없습니다. 오직 신규 설치(Fresh installation)만 지원됩니다. 그러나 구성 데이터에 대한 백업 및 복원은 가능합니다. 하이브리드 Cisco ISE 구축 환경 업그레이드와 관련된 사항은 Upgrade Guidelines for Hybrid Deployments를 참조하십시오.
- 퍼블릭 클라우드는 Layer 3 기능만 지원합니다. Microsoft Azure 환경의 Cisco ISE 노드는 Layer 2 기능을 지원하지 않습니다. 일례로, Cisco ISE CLI를 통해 접근하는 DHCP SPAN 프로파일러 프로브와 CDP 프로토콜 기능은 지원되지 않습니다.
- 구성 데이터를 복원하고 백업하려면 먼저 백업 작업을 완료해야 합니다. 그런 다음 CLI를 통해 Cisco ISE를 재시작하고 Cisco ISE GUI에서 복원 작업을 시작하십시오. 상세한 내용은 사용 중인 릴리스의 *Cisco ISE Administrator Guide* 내 "Maintain and Monitor" 장을 참조하십시오.
- Azure 환경에서는 비밀번호 기반 인증을 이용하는 Cisco ISE CLI로의 SSH 접근이 지원되지 않습니다. 안전하게 보관된 보안 키 쌍을 통해서만 Cisco ISE CLI에 접근할 수 있습니다.

  프라이빗 키(또는 PEM) 파일을 사용 중에 해당 파일을 잃어버리면 Cisco ISE CLI에 접근할 수 없게 됩니다.

  비밀번호 기반 인증을 통해 Cisco ISE CLI에 접근하려는 모든 연동 기능은 지원되지 않습니다.
- Azure Cloud 상의 Cisco ISE 배포 환경에서는 Accelerated Networking(가속 네트워킹)이 지원되지 않습니다. 이 기능을 활성화할 경우 노드 등록 및 해제와 같은 작업이 실패할 위험이 있습니다.

Azure 내 Cisco ISE 배포 시의 순서가 뒤바뀐 단편화 패킷 제한 사항

Microsoft Azure의 기본 가상 네트워크 스택은 보안상의 이유(구체적으로는 FragmentSmack 취약성에 대응하기 위해)로 순서가 뒤바뀐 IP 프래그먼트들을 탈락(Drop)시키며, 이는 프래그먼트들이 목적지 가상 머신에 도착하는 것을 원천 차단합니다. 이러한 동작 방식은 Cisco ISE 배포 환경에 악영향을 미칠 수 있습니다. 결과적으로 Cisco ISE와 네트워크 디바이스들이 RADIUS 패킷을 완전한 형태로 수신하지 못하여 인증, 권한 부여 및 DACL(Dynamic Access Control List) 배포 실패로 이어지게 됩니다.

Azure의 기본 VPN Gateway, Azure ExpressRoute, 또는 Azure Virtual WAN을 사용할 경우 모든 버전의 Cisco ISE에서 이 이슈에 직면할 수 있습니다. 이 이슈는 크기가 큰 인증서를 포함한 EAP-TLS 패킷, DACL 푸시, 다수의 속성을 지닌 RADIUS 인증 및 어카운팅 요청과 같이 용량이 큰 RADIUS 패킷에서 특히 자주 발생합니다.

이 문제를 완화하려면 서드파티 VPN 게이트웨이(예: Cisco Catalyst 8000V 또는 Cisco ASAv)를 Azure 가상 머신으로 배포하십시오. 이러한 게이트웨이는 온프레미스 환경에서 들어오는 VPN 터널을 종단시키며 프래그먼트 재조립을 지원합니다. 반면 Azure의 기본 VPN Gateway는 프래그먼트 재조립을 지원하지 않습니다.

서드파티 VPN 게이트웨이를 Azure에 배포하여 온프레미스와 Site-to-site VPN 연결을 구축한 후, 큰 사이즈의 RADIUS 패킷들을 안정적으로 처리하고 Azure 환경의 단편화 문제로 인한 인증 실패를 완화하기 위해 다음 단계를 수행하십시오:

1. 서드파티 VPN 게이트웨이에서 프래그먼트화된 패킷들이 순서가 뒤섞여 도착하더라도 올바르게 재조립될 수 있도록 IP virtual-reassembly를 활성화합니다.

   Catalyst 8000V의 경우 다음 명령을 사용합니다:

   ```
   ip virtual-reassembly-out
   ```

   Cisco ASAv의 경우 다음 명령을 사용합니다:

   ```
   fragment reassembly full outside
   ```

2. 서드파티 VPN 게이트웨이에서는 암호화 이전 단계에서 패킷 단편화를 활성화해야 합니다. Site-to-site VPN의 NAT 트래버설(NAT traversal) 과정이 UDP 4500으로 변환되는 큰 크기의 IPsec 패킷들을 조각낼 수 있기 때문입니다.

   Cisco ASAv의 경우 다음 명령을 사용합니다:

   ```
   crypto ipsec fragmentation before-encryption
   ```

3. Azure 포털을 통해 VPN 게이트웨이 VM의 내부 및 외부 인터페이스 양쪽 모두에서 IP 포워딩을 활성화합니다.

4. 서드파티 VPN 게이트웨이를 경유하는 가상 네트워크 연결을 허용하도록 Azure 라우팅 테이블을 업데이트합니다. 이를 통해 온프레미스 리소스에 원활하게 접근할 수 있습니다.

이러한 설정들을 구성했음에도 간헐적인 인증 실패가 계속 발생한다면, Microsoft 지원 티켓을 생성하여 구독 내 Azure VPN 네트워킹 컴포넌트에 대해 '순서가 뒤바뀐 프래그먼트 허용' 옵션을 활성화해 달라고 요청하십시오.

참고 네트워크 장비(WLC나 스위치 등)와 Cisco ISE의 이그레스(Egress) 구간 모두에서 패킷 단편화를 최소화하려면 네트워크 장비의 RADIUS 소스 인터페이스와 Cisco ISE의 RADIUS 인터페이스 양쪽의 MTU를 낮추는 방안을 고려하십시오. 일반적으로 1400바이트의 MTU 값이 대다수 환경에서 잘 작동하지만, 서브넷 사이의 최적 MTU를 파악하기 위해 PMTUD(Path MTU Discovery) 툴을 활용하면 더 나은 성능을 달성할 수 있습니다.

Azure VM을 사용하여 Cisco ISE 인스턴스 생성

Cisco ISE Azure 인스턴스 생성 사전 요건

- SSH 키 쌍을 생성합니다.
- 가상 네트워크 게이트웨이, 필수 서브넷 및 보안 그룹을 생성합니다.

- Cisco ISE에 사용할 서브넷이 인터넷에 도달할 수 있는지 확인합니다. Microsoft Azure의 Public Route Table(공용 라우팅 테이블) 창에서 서브넷의 다음 홉(Next hop)을 인터넷으로 구성합니다.

Azure VM을 사용하여 Cisco ISE 인스턴스를 생성하려면 다음 단계를 따르십시오.

1. Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동, 41 페이지
2. 인스턴스 세부 정보 구성, 41 페이지
3. OS 디스크 크기 구성, 42 페이지
4. 네트워크 인터페이스 구성, 42 페이지
5. 사용자 세부 정보 구성 , 43 페이지
6. 태그 구성, 45 페이지
7. 검토 및 생성, 46 페이지

Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동

다음 단계에 따라 Azure 콘솔에서 Cisco ISE 옵션으로 이동하십시오.

프로시저

단계 **1** https://portal.azure.com (으)로 이동하여 Microsoft Azure 어카운트에 로그인합니다.

단계 **2** 창 상단에 있는 검색 필드를 Use **Marketplace**를 검색합니다.

단계 **3** **Search the Marketplace(**마켓플레이스 검색**)** 검색 필드를 사용하여 **Cisco Identity Services Engine (ISE)**를 검색합니다.

인스턴스 세부 정보 구성

다음 단계에 따라 Azure 콘솔에서 인스턴스 세부 정보를 구성하십시오.

프로시저

단계 **1** **Virtual Machine(**가상 머신**)**을 클릭합니다.

단계 **2** 표시되는 새 창에서 **Create(**생성**)**를 클릭합니다.

단계 **3** **Basics(**기본 사항**)** 탭에서 다음 작업을 수행합니다.

a) **Basics(**기본 사항**)** 탭의 드롭다운 목록에서 **Subscription(**구독**)** 및 **Resource Group(**리소스 그룹**)**을 선택합니다.

b) **Instance details(**인스턴스 상세정보**)** 영역에서 **Virtual Machine name(**가상 머신 이름**)** 필드에 값을 입력합니다.
c) **Image(**이미지**)** 드롭다운 목록에서 Cisco ISE 이미지를 선택합니다.
d) **Size(**크기**)** 드롭다운 목록에서 Cisco ISE를 설치할 인스턴스 크기를 선택합니다. Cisco ISE에서 지원하는 인스턴스를 선택하십시오.
e) **Administrator account(**관리자 계정**)** > **Authentication type(**인증 유형**)** 영역에서 **SSH Public Key(SSH** 퍼블릭 키**)** 라디오 버튼을 클릭합니다.
f) **Username(**사용자 이름**)** 필드에 **iseadmin**을 입력합니다.

참고
허용되는 유일한 사용자 이름은 **isadmin**입니다. 이외의 다른 사용자 이름은 사용할 수 없습니다.

g) **SSH public key source(SSH** 공개 키 소스**)** 드롭다운 목록에서 **Use existing key Storeed in Azure(Azure**에 저장된 기존 키 사용**)**를 선택합니다.
h) **Stored keys(**저장된 키**)** 드롭다운 목록에서 이 작업의 사전 요구 사항으로 생성해 둔 키 쌍을 선택합니다.
i) **Inbound port rules(**인바운드 포트 규칙**)** 영역에서 **Allow selected ports(**선택한 포트 허용**)** 라디오 버튼을 클릭합니다.
j) **Select inbound ports(**인바운드 포트 선택**)** 드롭다운 목록에서 필요한 프로토콜 포트를 선택합니다.
k) **Licensing(**라이선싱**)** 영역의 **Licensing type(**라이선싱 유형**)** 드롭다운 목록에서 **Other(**기타**)**를선택합니다.

OS 디스크 크기 구성

다음 단계에 따라 OS 디스크 크기를 구성하십시오.

프로시저

단계 **1** **Next: Disks(**다음**:** 디스크**)**를 클릭합니다.
단계 **2** **Disks(**디스크**)** 탭의 **OS Disk Size(OS** 디스크 크기**)** 드롭다운 목록에서 디스크 크기를 선택하거나 기본값을 유지합니다.

참고
Key Management(키 관리**)** 필드에서 디스크 암호화 용으로 고객 관리 키를 사용하는 것이 좋습니다. 기본적으로 Platform-managed key(플랫폼 관리 키)가 사용됩니다. 키 생성에 대한 자세한 내용은 About encryption key management 를 참조하십시오.

나머지 필수 필드는 기본값을 유지하면 됩니다.

네트워크 인터페이스 구성

다음 단계에 따라 네트워크 인터페이스를 구성하십시오.

프로시저

단계 **1** **Next: Networking(**다음**:** 네트워킹**)**을 클릭합니다.

단계 **2** **Network Interface(**네트워크 인터페이스**)** 영역의 **Virtual network(**가상 네트워크**)** 및 **Subnet(**서브넷**)** 드롭다운 목록에서 미리 생성해 둔 가상 네트워크와 서브넷을 선택합니다.

공용(Public) IP 주소가 부여된 서브넷은 온라인 및 오프라인 상태의 포스처 피드(Posture feed) 업데이트를 수신하는 반면, 프라이빗 IP 주소만 부여된 서브넷은 오프라인 포스처 피드 업데이트만 수신합니다.

사용자 세부 정보 구성

사용자 세부 사항을 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **User Management(**사용자 관리**)**를 클릭합니다.

단계 **2** **Management(**관리**)** 탭에서 필수 필드의 기본값을 유지한 후 **Next: Advanced(**다음**:** 고급**)**를 클릭합니다.

단계 **3** **User data(**사용자 데이터**)** 필드에 파라미터를 올바른 형식으로 입력합니다.

User data(사용자 데이터) 입력을 통해 구성하는 각 필드에는 올바른 구문을 사용해야 합니다. **User data(**사용자 데이터**)** 필드에 입력하는 정보는 별도의 유효성 검사를 거치지 않습니다. 잘못된 구문을 사용하면 이미지를 실행할 때 Cisco ISE 서비스가 시작되지 않을 수 있습니다.

User data(사용자 데이터**)** 필드를 통해 제출하는 구성에 대해 다음의 지침을 따르십시오:

표 ***8: User data(***사용자 데이터***)*** 필드 구성 지침

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
hostname	알파벳과 숫자, 하이픈(-)만 포함된 호스트 이름을 입력합니다. 호스트 이름의 길이는 19자 미만이어야 하며 밑줄(_)을 포함해서는 안 됩니다.	구문은 권장 사항을 충족해야 합니다.
primarynameserver	기본 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	Cisco ISE 릴리스 3.4부터: • Cisco ISE 릴리스 3.4부터: 설치 중 **secondarynameserver(**보조 네임 서버**)** 및 **tertiarynameserver(3**차 네임 서버) 필드를 사용하여 보조 및 3차 네임 서버를 구성할 수 있습니다.

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
secondarynameserver (Cisco ISE 릴리스 3.4부터)	보조 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	• **secondarynameserver** 필드를 비워 두고 **tertiarynameserver** 필드만 사용하는 경우 Cisco ISE 서비스가 시작되지 않습니다.
tertiarynameserver (Cisco ISE 릴리스 3.4부터)	3차 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	secondarynameserver 값이 설정된 후에만 사용하십시오.
dnsdomain	DNS 도메인 의 FQDN을 입력합니다. 이 항목에는 ASCII 문자, 숫자, 하이픈(-), 마침표(.)를 포함할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.
ntpserver (Cisco ISE 릴리스 3.4부터 **primaryntpserver**로 이름이 변경됨)	동기화에 사용할 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다(예: time.nist.gov).	Cisco ISE 릴리스 3.4부터: • **ntpserver** 필드 이름이 **primaryntpserver**로 변경되었습니다. **ntpserver**를 사용하면 Cisco ISE 서비스가 시작되지 않습니다.
secondaryntpserver (Cisco ISE 릴리스 3.4부터)	보조 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다.	• **secondaryntpserver** 필드를 비워두고 **tertiaryntpserver** 필드만 사용하는 경우 Cisco ISE 서비스가 시작되지 않습니다.
tertiaryntpserver (Cisco ISE 릴리스 3.4부터)	3차 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다.	secondaryntpserver 값이 설정된 후에만 사용하십시오.
timezone	시간대를 입력합니다(예: Etc/UTC). 특히 Cisco ISE 노드가 분산 구축 환경에 설치된 경우, 모든 Cisco ISE 노드를 협정 세계시(UTC) 표준 시간대로 설정하는 것을 권장합니다. 이를 통해 구축 환경 내 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프를 항상 동기화할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
비밀번호	Cisco ISE의 GUI 기반 로그인에 사용할 비밀번호를 구성합니다. 입력하는 비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 합니다. 비밀번호는 6~25자 사이여야 하며 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 비밀번호 는 사용자 이름 또는 사용자 이름의 역순(iseadmin 또는 nimdaesi), cisco 또는 ocsic과 같거나 이를 포함할 수 없습니다. 허용되는 특수 문자는 @~*!,+=_- 입니다. .	사용 중인 릴리스의 Cisco ISE Administrator Guide 내 "Basic Setup" 장의 "User Password Policy" 섹션을 참조하십시오.
ersapi	ERS를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.
openapi	OpenAPI를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	Cisco ISE 릴리스 3.4부터 OpenAPI 서비스는 기본적으로 활성화됩니다. 인스턴스를 시작할 때 OpenAPI 관련 옵션을 지정할 필요가 없습니다.
pxGrid	pxGrid를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.
pxgrid_cloud	pxGrid Cloud를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	pxGrid Cloud를 활성화하려면 반드시 pxGrid를 먼저 활성화해야 합니다. pxGrid를 비활성화한 상태에서 pxGrid Cloud를 활성화하면, 실행 시 pxGrid Cloud 서비스가 활성화되지 않습니다. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI에서만 활성화할 수 있습니다. 따라서 이 필드는 User data에 포함되지 않습니다.

태그 구성

태그를 구성하려면 다음 단계를 수행합니다.

프로시저

단계 **1** **Next: Tags(**다음**:** 태그**)**를클릭합니다.

단계 **2** 여러 리소스 및 리소스 그룹을 분류하고 통합할 수 있는 이름-값 쌍을 생성하려면 **Name(**이름**)** 및 **Value(**값**)** 필드에 값을 입력합니다.

검토 및 생성

다음 단계에 따라 생성한 구성을 검토하고 Cisco ISE 인스턴스를 생성합니다.

프로시저

단계 **1** **Review+ Create(**검토+ 생성**)**를 클릭합니다.

단계 **2** 지금까지 제공한 정보를 검토하고 **Create(**생성**)**를 클릭합니다.

Deployment is in progress(배포 진행 중**)** 창이 표시됩니다. Cisco ISE 인스턴스를 생성하여 사용할 수 있게 되는 데 30분 정도 걸립니다. Cisco ISE VM 인스턴스가 **Virtual Machines(**가상 머신**)** 창에 표시됩니다(메인 검색 필드를 사용하여 해당 창을 찾으십시오).

디스크 크기 편집

이 섹션은 Cisco ISE VM의 디스크 크기가 300GB인 경우에만 적용됩니다. 다른 디스크 크기를 선택한 경우 이러한 단계를 적용할 수 없습니다.

Microsoft Azure 기본 설정으로 인해 Cisco ISE VM은 300GB의 디스크 크기로 구성됩니다. Cisco ISE 노드에는 일반적으로 300GB 이상의 디스크 크기가 필요합니다. Microsoft Azure에서 Cisco ISE 처음 실행할 때 **Insufficient Virtual Memory(**가상 메모리 부족**)** 알람이 표시될 수 있습니다.

Cisco ISE VM을 생성한 후 Cisco ISE 관리 포털 에 로그인하여 Cisco ISE 올바르게 설정되었는지 확인합니다. 그런 다음 Microsoft Azure 포털의 **Virtual Machines(**가상 머신**)** 페이지에서 다음 단계를 수행하여 디스크 크기를 편집합니다.

프로시저

단계 **1** Cisco ISE 인스턴스를 중지합니다.

단계 **2** 왼쪽 창 에서 **Disk(**디스크**)**를 클릭하고 Cisco ISE 와 함께 사용 중인 디스크를 클릭합니다.

단계 **3** 왼쪽 창 에서 **Size + Performance(**크기 + 성능**)**를 클릭합니다.

단계 **4** **Custom disk size(**사용자 지정 디스크 크기**)** 필드에 원하는 디스크 크기를 GiB 단위로 입력합니다.

Azure 애플리케이션을 사용하여 Cisco ISE 인스턴스 생성

Cisco ISE 인스턴스를 생성하기 전에 Resource Groups, Virtual Networks, Subnets, SSH keys 등 필요한 Azure 리소스들을 미리 생성하십시오.

다음 단계에 따라 Azure 애플리케이션을 사용하여 Cisco ISE 인스턴스를 생성하십시오.

1. Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동, 41 페이지
2. 인스턴스 세부 정보 추가 , 47 페이지
3. 네트워크 설정 구성, 48 페이지
4. 서비스 구성, 49 페이지
5. 사용자 세부 정보 추가, 50 페이지
6. 검토 및 생성, 53 페이지

Amazon EC2 콘솔에서 Cisco ISE 옵션으로 이동

다음 단계에 따라 Azure 콘솔에서 Cisco ISE 옵션으로 이동하십시오.

프로시저

단계 **1** https://portal.azure.com (으)로 이동하여 Microsoft Azure 어카운트에 로그인합니다.

단계 **2** 창 상단에 있는 검색 필드를 Use **Marketplace**를 검색합니다.

단계 **3** **Search the Marketplace(**마켓플레이스 검색**)** 검색 필드를 사용하여 **Cisco Identity Services Engine (ISE)**를 검색합니다.

인스턴스 세부 정보 추가

다음 단계에 따라 Cisco ISE 인스턴스에 대한 기본 구성 세부 정보를 추가합니다.

프로시저

단계 **1** **Azure Application(Azure** 애플리케이션**)**을 클릭합니다.

단계 **2** 표시되는 새 창에서 **Create(**생성**)**를 클릭합니다.
5단계 워크플로우가 표시됩니다.

단계 **3** **Basics(**기본 사항**)** 탭에서 다음을 수행합니다.

a) **Resource Group(**리소스 그룹**)** 드롭다운 목록에서 Cisco ISE 와 연결할 옵션을 선택합니다.

b) **Region(**지역**)** 드롭다운 목록에서 리소스 그룹이 있는 지역을 선택합니다.
c) **Hostname(**호스트 이름**)** 필드에 호스트 이름을 입력합니다.
d) **Time Zone(**표준 시간대**)** 드롭다운 목록에서 표준 시간대를 선택합니다.
e) **VM Size(VM** 크기**)** 드롭다운 목록에서 Cisco ISE 에 사용할 Azure VM 크기를 선택합니다.
f) **Disk Encryption Key(** 디스크 암호화 키) 드롭다운 목록에서 디스크 암호화 에 사용할 키를 선택합니다.

Cisco ISE 릴리스 3.3부터는 **Disk Encryption Key(**디스크 암호화 키**)** 필드에서 디스크 암호화 에 고객이 관리하는 키를 사용하는 것이 좋습니다. 기본적으로 Platform-management key(플랫폼 관리 키)가 사용됩니다. 자세한 내용은 About encryption key management를 참조하십시오.

g) **Disk Storage Type(**디스크 스토리지 유형**)** 드롭다운 목록에서 옵션을 선택합니다.
h) **Volume Size(**볼륨 크기**)** 필드에 Cisco ISE 인스턴스에 할당할 볼륨 크기를 GB 단위로 입력합니다. 기본값은 600GB입니다.

초기에 300GB로 시작하여 나중에 늘릴 계획을 세우는 것보다는, Azure 애플리케이션 템플릿에서 노드를 생성할 때 300GB에서 2400GB 사이의 적절한 디스크 크기를 미리 선택하는 것을 권장합니다.

네트워크 설정 구성

네트워크 설정을 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Next(**다음**)**를 클릭합니다.
단계 **2** **Network Settings(**네트워크 설정**)** 탭에서 다음 세부 정보를 입력합니다.

a) **Virtual Network(**가상 네트워크**)** 드롭다운 목록에서 가상 네트워크를 선택합니다.
b) **Subnet(**서브넷**)** 드롭다운 목록에서 선택한 가상 그룹과 연결된 서브넷 선택합니다.
c) (선택 사항) **Network Security Group(**네트워크 보안 그룹**)** 드롭다운 목록에서 필요한 보안 그룹을 선택합니다.
d) **SSH public key source(SSH** 공개 키 소스**)** 드롭다운 목록에서 해당 옵션을 클릭하여 새 키 쌍을 생성할지 기존 키 쌍을 사용할지 선택합니다.
e) 이전 단계에서 **Use existing key stored in Azure(Azure**에 저장된 기존 키 사용**)** 옵션을 선택한 경우 **Stored Keys(**저장된 키**)** 드롭다운 목록에서 사용할 키를 선택합니다.
f) Cisco ISE 에 고정 IP 주소를 할당하려면 **Private IP address(**프라이빗 **IP** 주소**)** 필드에 IP 주소를 입력합니다. 선택한 서브넷의 다른 리소스에서 해당 IP 주소를 사용하고 있지 않은지 확인합니다.
g) **Public IP address(**공용 **IP** 주소**)**드롭다운 목록에서 Cisco ISE 에서 사용할 주소를 선택합니다. 이 필드를 비워두면 Azure DHCP 서버가 공용 IP 주소를 인스턴스에 할당합니다.
h) **DNS Server(DHCP** 서버**)** 필드에 DNS 서버의 도메인 이름을 입력합니다.

이 단계에서는 하나의 DNS 서버만 추가할 수 있습니다. 설치 후 Cisco ISE CLI를 통해 DNS 서버를 추가할 수 있습니다.

i) **Name Server(**네임 서버**)** 필드에 네임 서버의 IP 주소를 입력합니다.

Cisco ISE 릴리스 3.4부터:

- **Name Server(**네임 서버**)** 필드 이름이 **Primary Name Server(**기본 네임 서버**)**로 변경됩니다.
- 보조 네임 서버의 IP 주소는 **Secondary Name Server(**보조 네임 서버**)** 필드에 입력할 수 있습니다.
- 3차 네임 서버의 IP 주소는 **Tertiary Name Server(3**차 네임 서버**)** 필드에 입력할 수 있습니다. 이 필드를 사용하고 애플리케이션을 성공적으로 실행하려면 **Secondary Name Server(**보조 네임 서버**)** 필드를 비워 두지 않아야 합니다.

j) **NTP Server(NTP** 서버**)** 필드에 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다.

Cisco ISE 릴리스 3.4부터:

- **NTP Server(NTP** 서버**)** 필드 이름이 **Primary NTP Server(**기본 **NTP** 서버**)**로 변경됩니다.
- 보조 NTP 서버의 IP 주소 또는 호스트 이름을 **Secondary NTP Server(**보조 **NTP** 서버**)** 필드에 입력할 수 있습니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다.
- 3차 NTP 서버의 IP 주소 또는 호스트 이름을 **Tertiary NTP Server(3**차 **NTP** 서버**)** 필드에 입력할 수 있습니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다. 이 필드를 사용하고 애플리케이션을 성공적으로 실행하려면 **Secondary NTP Server(**보조 **NTP** 서버**)** 필드를 비워 두면 안 됩니다.

이 단계에서는 하나의 NTP 서버만 추가할 수 있습니다. 설치가 완료된 후 Cisco ISE CLI를 통해 추가 NTP 서버를 등록할 수 있습니다.

참고
입력한 IP 주소가 올바르지 않거나 연결할 수 없는 경우 Cisco ISE 서비스가 실행되지 않을 수 있습니다.

서비스 구성

다음 단계에 따라 서비스를 구성하십시오.

프로시저

Service(서비스**)** 탭에서 다음을 수행합니다.

a) **ERS** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.
b) **Open API** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. Cisco ISE 릴리스 3.4부터는 OpenAPI가 기본적으로 활성화됩니다. 따라서 이 필드를 사용할 수 없습니다.
c) **pxGrid** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.
d) **pxGrid Cloud(pxGrid** 클라우드**)** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI를 통해서만 활성화할 수 있습니다. 따라서 이 필드를 사용할 수 없습니다.

사용자 세부 정보 추가

사용자 세부 사항을 추가하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Next(**다음**)** 를 클릭하여 **User Details(**사용자 세부 정보**)** 탭으로 이동합니다.

단계 **2** **User Details(**사용자 세부 정보**)** 탭에서 **Enter Password for iseadmin(iseadmin**용 비밀번호 입력**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 비밀번호를 입력합니다.

비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 하며 길이는 최대 25자 이내여야 합니다.

User data 매개변수

필드	형식	**Cisco ISE** 릴리스 **3.1**	**Cisco ISE** 릴리스 **3.2**	**Cisco ISE** 릴리스 **3.3**	**Cisco ISE** 릴리스 **3.4**	**Cisco ISE** 릴리스 **3.5**
hostname	호스트 이름 =<hostname of Cisco ISE>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
primarynameserver	primarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primarynameserver=<IPv6 주소> 지원)	지원됨.	지원됨.	지원됨.	지원됨.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
secondarynameserver	secondarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiarynameserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiarynameserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
tertiarynameserver	tertiarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
dnsdomain	dnsdomain=<example.com>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ntpserver	ntpserver=<NTP FQDN IPv4 또는 서버의 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 ntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원됨.	지원됨.	지원됨.	지원되지 않음. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전부터 primaryntpserver로 대체됩니다. ntpserver를 사용하면 Cisco ISE 서비스가 시작되지 않을 수 있습니다.	지원되지 않음. 대신 primaryntpserver를 사용하십시오.
Primaryntpserver	primaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전에서 ntpserver를 대체합니다.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
secondaryntpserver	secondaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiaryntpserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiaryntpserver 필드를사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
tertiaryntpserver	tertiaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
timezone	timezone=<표준 시간대>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
username	username=<admin>	지원됨 (예: <admin>) Cisco ISE 릴리스 3.1 패치 1부터 지원됨.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.
username	username=iseadmin	필수 아님	필수	필수	필수	필수
비밀번호	password=<비밀번호>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ersapi	ersapi=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
openapi	openapi=<yes/no>	지원됨.	지원됨.	지원됨.	OpenAPI는 기본적으로 활성화되어 있습니다.	OpenAPI는 기본적으로 활성화되어 있습니다.
pxGrid	pxGrid=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
pxgrid_cloud	pxgrid_cloud=<yes/no>	지원되지 않음	지원되지 않음	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원되지 않음. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI를 통해서만 활성화할 수 있습니다.

파라미터 구문 요구 사항

Cisco ISE on Cloud의 User data 파라미터를 지정할 때 속성이나 값을 작은따옴표나 큰따옴표로 묶지 마십시오. 모든 값은 따옴표 없이 평문(Plain text)으로 입력해야 합니다.

잘못된 입력	올바른 입력
hostname="i34a"	hostname=i34a
primarynameserver="9.9.9.9"	primarynameserver="9.9.9.9"
dnsdomain="example.com"	dnsdomain=example.com
primaryntpserver="north-america.pool.ntp.org"	primaryntpserver="north-america.pool.ntp.org"

Cisco ISE 릴리스 3.3부터 시리얼 콘솔에 유효성 검사 결과 메시지가 표시됩니다. 이러한 메시지는 결과가 생성되는 시점에 시리얼 콘솔이 열려 있는 경우에만 볼 수 있습니다.

검토 및 생성

설정을 검토하고 Cisco ISE 인스턴스를 생성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** **Review + create(**검토 + 생성**)** 탭에서 인스턴스 세부 정보를 검토합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

Overview(개요**)** 창에 인스턴스 생성 진행률이 표시됩니다.

단계 **3** 검색 표시줄을 사용하여 **Virtual Machines(**가상 머신**)** 창으로 이동합니다.

Virtual Machines(가상 머신**)** 창에 Cisco ISE 인스턴스가 표시됩니다. Cisco ISE 인스턴스를 생성하는 데 약 30분이 소요됩니다.

설치 후 작업

Cisco ISE 인스턴스를 생성한 후 수행해야 하는 설치 후 작업에 대한 정보는 사용 중인 릴리스의 *Cisco ISE Installation Guide* 내 "Installation Verification and Postinstallation Tasks(설치 확인 및 설치 후 작업)" 장을 참조하십시오.

Azure 클라우드 기반 Cisco ISE의 호환성 정보

이 섹션에서는 Azure 클라우드 플랫폼의 Cisco ISE에 고유한 호환성 정보를 제공합니다. Cisco ISE의 일반적인 호환성 세부 정보는 사용 중인 릴리스의 Cisco Identity Services Engine Network Component Compatibility 가이드를 참조하십시오.

로드 밸런서 연동 지원

RADIUS 트래픽의 로드 밸런싱을 위해 Azure Load Balancer를 Cisco ISE와 연동할 수 있습니다. 하지만 다음과 같은 주의사항이 적용됩니다.

- Change of Authorization(CoA) 기능은 Azure 포털의 로드 밸런싱 규칙에서 Session Persistence 속성을 구성할 때 클라이언트 IP 보존을 활성화한 경우에만 지원됩니다.
- Azure Load Balancer는 Source IP Affinity만 지원하고 Calling Station ID 기반 Sticky Session은 지원하지 않으므로 불균등한 로드 밸런싱이 발생할 수 있습니다.
- Azure Load Balancer는 RADIUS 기반 Health Check를 지원하지 않으므로 노드에서 RADIUS 서비스가 비활성 상태이더라도 트래픽이 PSN으로 전송될 수 있습니다.

Azure Load Balancer에 대한 자세한 내용은 What is Azure Load Balancer?를 참조하십시오.

TACACS 트래픽의 로드 밸런싱을 위해 Azure Load Balancer를 Cisco ISE와 연동할 수 있습니다. 그러나 Azure Load Balancer는 TACACS+ 서비스 기반 Health Check를 지원하지 않으므로, 노드에서 TACACS 서비스가 비활성 상태이더라도 트래픽이 Cisco ISE PSN으로 전송될 수 있습니다.

Azure 클라우드 에서 비밀번호 복구 및 재설정

이러한 작업을 사용하여 Cisco ISE VM 비밀번호 재설정하거나 복구할 수 있습니다. 필요한 작업을 선택하고 자세한 단계를 수행합니다.

Azure 포털의 **Help(**도움말**) > Reset Password(**비밀번호 재설정**)** 옵션은 Cisco ISE Azure VM에서 지원되지 않습니다.

시리얼 콘솔을 통한 Cisco ISE GUI 비밀번호 재설정

프로시저

단계 **1** Azure Cloud에 로그인하고 Cisco ISE Virtual Machine이 포함된 리소스 그룹을 선택합니다.

단계 **2** 리소스 목록에서 비밀번호를 재설정할 Cisco ISE 인스턴스를 클릭합니다.

단계 **3** 왼쪽 메뉴의 **Help(**도움말**)** 섹션에서 **Serial console(**시리얼 콘솔**)**을클릭합니다.

새 창에 Azure Cloud Shell이 나타납니다.

화면이 검은색인 경우 **Enter**를 눌러 로그인 프롬프트를 표시합니다.

만약 오류 메시지가 나타난다면 다음 단계에 따라 Boot diagnostics를 활성화해야 할 수도 있습니다:

1. 왼쪽 메뉴에서 **Boot diagnostics(**부팅 진단**)**을 클릭합니다.
2. **EEnable with custom storage account(**사용자 지정 스토리지 계정으로 활성화**)**를 클릭합니다.
3. 스토리지 계정을 선택하고 **Save(**저장**)**를클릭합니다.

단계 **4** 시리얼 콘솔에 로그인합니다.

시리얼 콘솔에 로그인하려면 인스턴스를 처음 설치할 때 구성했던 초기 비밀번호를 사용해야 합니다.

application reset-passwd iseadmin 명령을 사용하여 iseadmin 계정에 사용할 새 GUI 비밀번호를 구성합니다.

SSH 액세스를 위한 새 퍼블릭 키 쌍 생성

다음 단계에 따라 리포지토리에 추가 키 쌍을 등록하십시오.

Cisco ISE 인스턴스 구성 시점에 생성했던 기존 키 쌍은 사용자가 새로 생성하는 퍼블릭 키로 교체되지 않습니다.

프로시저

단계 **1** Azure Cloud에서 새 퍼블릭 키를 생성합니다. Generate and store SSH keys in the Azure portal을 참조하십시오.

단계 **2** Azure Cloud 시리얼 콘솔에 로그인합니다.

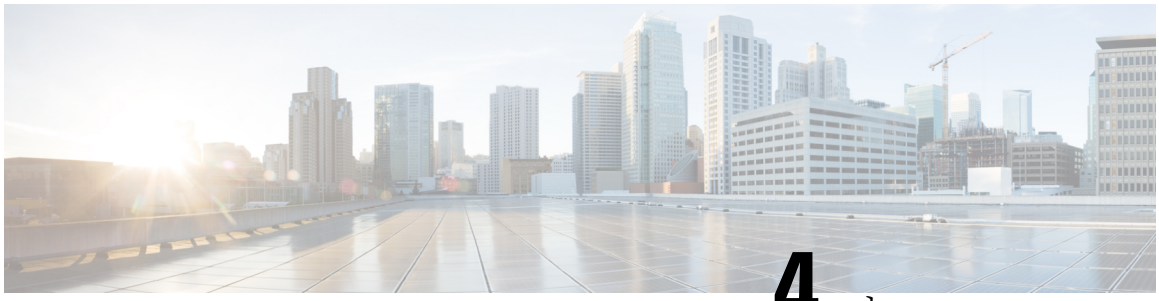
단계 **3** 퍼블릭 키를 저장할 새 리포지토리를 생성하려면 Azure Repos documentation을 참조하십시오.

CLI를 통해 접근할 수 있는 리포지토리가 이미 있는 경우 4단계로 건너뛰십시오.

단계 **4** 새 퍼블릭 키를 가져오려면 다음 명령을 사용합니다:

crypto key import <public key filename> repository <repository name>

가져오기가 완료되면 새 퍼블릭 키를 활용하여 SSH를 통해 Cisco ISE에 로그인할 수 있습니다.



4 장

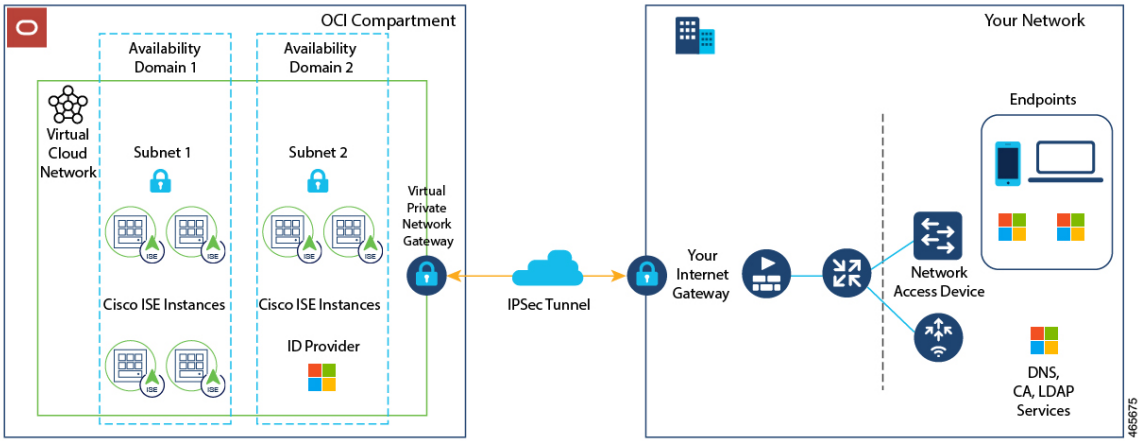
Oracle Cloud Infrastructure의 Cisco ISE

- Oracle Cloud Infrastructure의 Cisco ISE , 57 페이지
- Cisco ISE가 지원하는 OCI 인스턴스, 58 페이지
- OCI에서 Cisco ISE 사용 시 알려진 제한 사항 , 59 페이지
- OCI에서 Cisco ISE 인스턴스 생성, 59 페이지
- Terraform Stack 파일을 사용하여 OCI에서 Cisco ISE 인스턴스 생성 , 68 페이지
- 설치 후 작업, 71 페이지
- OCI의 Cisco ISE 에 대한 호환성 정보, 71 페이지
- OCI 환경의 비밀번호 복구 및 재설정, 72 페이지

Oracle Cloud Infrastructure의 Cisco ISE

Cisco ISE는 OCI(Oracle Cloud Infrastructure)에서 Image(이미지)와 Stack(스택) 두 가지 형태로 제공됩니다. Stack 유형은 Cisco ISE 사용자가 더 쉽게 사용할 수 있도록 맞춤화된 리소스 유형이므로, 이를 사용하여 Cisco ISE를 설치하는 것을 권장합니다.

이 그림은 Oracle Cloud에 연결된 구축 환경의 예를 보여줍니다.



OCI에 Cisco ISE를 구성하고 설치하려면 특정 OCI 기능 및 솔루션을 숙지해야 합니다. 시작하기 전에 구획(Compartments), 가용성 도메인(Availability domains), 이미지, 셰이프 및 부팅 볼륨을 이해하십시오.

OCI는 컴퓨팅 리소스 단위로 Oracle CPU(OCPU)를 사용합니다. 1개의 OCPU는 2개의 vCPU와 동일합니다. 자세한 내용은 Oracle Cloud Infrastructure Documentation을 참조하십시오.

중요 기존 OCI 이미지를 복제하여 Cisco ISE 인스턴스를 생성하지 마십시오.

Cisco ISE가 지원하는 OCI 인스턴스

Cisco ISE에서 사용할 수 있는 OCI 인스턴스는 다음과 같습니다.

OCI 인스턴스 유형	OCPU	OCI 인스턴스 메모리(GB)
Standard3.Flex 이 인스턴스는 Cisco ISE 평가 사용 사례를 지원합니다. 100개의 동시 활성 엔드포인트를 지원합니다.	2	16
Optimized3.Flex	8	32
	16	64
Standard3.Flex	4	32
	8	64
	16	128
	32	256

Optimized3.Flex 셰이프는 컴퓨팅에 최적화된 인스턴스입니다. 이 셰이프는 컴퓨팅 집약적 작업 및 애플리케이션용 PSN으로 사용하는 것이 가장 적합합니다.

Standard3.Flex 셰이프는 PAN, MnT 노드, 또는 이 둘 모두의 역할로 사용하기에 가장 적합한 범용 셰이프입니다. 이 셰이프는 데이터 처리 및 데이터베이스 작업을 위해 설계되었습니다.

범용 인스턴스를 PSN으로 사용할 경우, 컴퓨팅 최적화 인스턴스를 PSN으로 사용할 때보다 성능 수치가 낮아집니다.

Standard3.Flex (4 OCPU, 32 GB) 셰이프는 Extra-small PSN으로만 사용해야 합니다.

Standard3.Flex (4 OCPU, 32 GB) 셰이프는 Extra-small PSN으로만 사용해야 합니다.

- 2 OCPU 및 16 GB 메모리
- 8 OCPU 및 64 GB 메모리

OCI 인스턴스 유형에 따른 확장성 및 성능 데이터 정보는 *Performance and Scalability Guide for Cisco Identity Services Engine*참조하십시오.

OCI에서 Cisco ISE 사용 시 알려진 제한 사항

- OCI에서는 Cisco ISE 업그레이드 워크플로가 지원되지 않습니다. 신규 설치만 지원됩니다. 그러나 구성 데이터의 백업 및 복원은 수행할 수 있습니다. 하이브리드 Cisco ISE 구축 환경 업그레이드에 대한 자세한 내용은 Upgrade Guidelines for Hybrid Deployments를 참조하십시오.
- 퍼블릭 클라우드는 Layer 3 기능만 지원합니다. OCI의 Cisco ISE 노드는 Layer 2 기능에 의존하는 기능을 지원하지 않습니다. 예를 들어, Cisco ISE CLI를 통해 액세스하는 DHCP SPAN 프로파일러 프로브 및 CDP 프로토콜 기능은 지원되지 않습니다.
- Cisco ISE에서 IPv6 주소를 활성화하려면 OCI 포털에서 Cisco ISE용 IPv6 주소를 구성하고 인터페이스 Gigabit Ethernet 0을 재시작하십시오. Cisco ISE 시리얼 콘솔에 administrator(관리자)로 로그인하여 다음 명령을 실행합니다.

```
#configure terminal
Entering configuration mode terminal
(config)#interface GigabitEthernet 0
(config-GigabitEthernet-0)#shutdown
(config-GigabitEthernet-0)#no shutdown
(config-GigabitEthernet-0)#exit
(config)#exit
```

- 구성 데이터의 백업 및 복원 작업을 수행할 때 백업 작업이 완료되면 먼저 CLI를 통해 Cisco ISE를 재시작하십시오. 그런 다음 Cisco ISE GUI에서 복원 작업을 시작하십시오. Cisco ISE 백업 및 복원 프로세스에 대한 자세한 내용은 사용 중인 릴리스의 *Cisco ISE Administrator Guide* 내 "Maintain and Monitor" 장을 참조하십시오.
- OCI에서는 비밀번호 기반 인증을 사용하는 Cisco ISE CLI에 대한 SSH 액세스가 지원되지 않습니다. 키 쌍을 통해서만 Cisco ISE CLI에 액세스할 수 있습니다. 이 키 쌍을 안전하게 보관하십시오.

  프라이빗 키(또는 PEM) 파일을 분실하면 Cisco ISE CLI에 액세스할 수 없습니다.

  비밀번호 기반 인증 방식을 사용하여 Cisco ISE CLI에 액세스하는 연동은 지원되지 않습니다(예: Cisco Catalyst Center 2.1.2 및 이전 버전).

OCI에서 Cisco ISE 인스턴스 생성

OCI에서 Cisco ISE 인스턴스를 생성하려면 다음 단계를 따르십시오.

시작하기 전에

- 이 작업을 시작하기 전에 구획(Compartments), 사용자 지정 이미지, 셰이프, 가상 클라우드 네트워크, 서브넷 및 사이트 간 VPN을 생성합니다.

  Cisco ISE 인스턴스와 동일한 구획에 가상 클라우드 네트워크 및 서브넷을 생성합니다.

- Cisco ISE 용 가상 클라우드 네트워크를 생성할 때는 **Create VCN with Internet Connectivity(**인터넷 연결이 포함된 **VCN** 생성**)** VCN 유형을 선택하는 것을 권장합니다.

프로시저

단계 **1** OCI 콘솔에서 Cisco ISE 옵션으로 이동, 60 페이지.
단계 **2** 인스턴스 세부 정보 구성, 60 페이지.
단계 **3** Cisco ISE 인스턴스 고급 옵션 구성, 61 페이지.

OCI 콘솔에서 Cisco ISE 옵션으로 이동

다음 단계에 따라 OCI 콘솔에서 Cisco Identity Services Engine (ISE) 옵션으로 이동하십시오.

프로시저

단계 **1** OCI 계정에 로그인합니다.
단계 **2** 검색 필드에 **Marketplace**를 입력합니다.
단계 **3** **Search for licensing(**목록 검색**)** 검색 필드에 **Cisco Identity Services Engine (ISE)**을 입력합니다.

인스턴스 세부 정보 구성

OCI 콘솔에서 Cisco ISE 인스턴스 세부 정보를 추가하고 구성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** **Image** 유형의 Cisco ISE 옵션을 클릭합니다.
단계 **2** **Launch Instance(**인스턴스 실행**)**를 클릭합니다.
단계 **3** **List Scope(**목록 범위**)** 영역에 있는 **Compartment(**구획**)** 드롭다운 목록에서 구획을 선택합니다.
단계 **4** **Create instance(**인스턴스 생성**)**를 클릭합니다.
단계 **5** **Create Compute Instance(**컴퓨팅 인스턴스 생성**)** 창에서 Cisco ISE 인스턴스의 이름을 입력합니다.
단계 **6** **Create in compartment(**구획에 생성**)** 드롭다운 목록에서 Cisco ISE 인스턴스의 구획을 선택합니다.

Cisco ISE용 Virtual Cloud Networks 및 서브넷 등 다른 리소스를 생성해 둔 구획을 선택하십시오.

단계 **7** **Placement(**배치**)** 영역에서 가용성 도메인 클릭합니다.

선택한 도메인에 따라 사용할 수 있는 컴퓨팅 셰이프가 결정됩니다.

단계 **8** **Image and Shape(**이미지 및 셰이프**)** 영역에서 다음을 수행합니다.

a) **Image and Shape(**이미지 및 셰이프**)** 영역에서 **Change Shape(**셰이프 변경**)**를 클릭합니다.

b) **Shape Series(**셰이프 시리즈**)** 영역에서 **Intel**을 클릭합니다.

사용 가능한 셰이프 목록이 표시됩니다.

c) 필요한 모양 이름 옆의 확인란을 선택하고 **Select** 모양**(**셰이프 선택**)**을 클릭합니다.

단계 **9** **Networking(**네트워킹**)** 영역에서 다음을 수행합니다:

a) **Primary Network(**기본 네트워크**)** 영역에서 **Select existing virtual cloud network(**기존 가상 클라우드 네트워크 선택**)** 라디오 버튼을 클릭합니다.

b) 드롭다운 목록에서 네트워크 유형 ID를 선택합니다.

c) **Subnet(**서브넷**)** 영역에서 **Select existing subnet(**기존 서브넷 선택**)**을 클릭합니다.

d) 드롭다운 목록에서 서브넷을 선택합니다.

시스템은 동일한 구획에서 생성된 서브넷들을 표시합니다.

단계 **10** **Add SSH Keys(SSH** 키 추가**)** 영역에서 해당 라디오 버튼을 클릭하여 새 키 쌍을 생성하거나 기존 퍼블릭 키를 사용할 수 있습니다.

단계 **11** **Boot Volume(**부팅 볼륨**)** 영역에서 **Specify a custom boot volume size(**사용자 지정 부팅 볼륨 크기 지정**)** 확인란을 선택하고 필요한 부팅 볼륨 크기를 GB 단위로 입력합니다.

Cisco ISE 프로덕션 환경에 필요한 최소 볼륨 크기는 600GB입니다. 이 단계에서 부팅 볼륨을 지정하지 않으면 인스턴스에 기본적으로 250GB의 볼륨이 할당됩니다.

참고
Encrypt this volume with a key that you manage(사용자가 관리하는 키로 이 볼륨 암호화**)** 필드에서 암호화용으로 Customer-managed key(고객 관리 키)를 사용하는 것을 권장합니다. 기본적으로 Oracle-managed key가 사용됩니다. 키 생성에 대한 자세한 내용은 Key Management를참조하십시오.

Cisco ISE 인스턴스 고급 옵션 구성

고급 옵션을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** **Show advanced options(**고급 옵션 표시**)**를 클릭합니다.

단계 **2** **Management(**관리**)** 탭의 **Instance metadata service(**인스턴스 메타데이터 서비스**)** 섹션에서 **Require an authorization header(**권한 부여 헤더 필요**)** 토글을 비활성화합니다.

참고
OCI의 Cisco ISE는 IMDSv2를 지원하지 않습니다.

단계 **3** **Initialization script(**초기화 스크립트**)** 탭에서 **Paste cloud-init script(cloud-init** 스크립트 붙여넣기) 옵션을 선택합니다.

단계 **4** **Cloud-init script(Cloud-init** 스크립트**)** 텍스트 상자에 필요한 사용자 데이터를 입력합니다.

단계 **5** **User data(**사용자 데이터**)** 필드에 파라미터를 올바른 형식으로 입력합니다.

User data(사용자 데이터) 입력을 통해 구성하는 각 필드에는 올바른 구문을 사용해야 합니다. **User data(**사용자 데이터**)** 필드에 입력하는 정보는 별도의 유효성 검사를 거치지 않습니다. 잘못된 구문을 사용하면 이미지를 실행할 때 Cisco ISE 서비스가 시작되지 않을 수 있습니다.

User data(사용자 데이터**)** 필드를 통해 제출하는 구성에 대해 다음의 지침을 따르십시오:

표 ***9: User data(***사용자 데이터***)*** 필드 구성 지침

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
hostname	알파벳과 숫자, 하이픈(-)만 포함된 호스트 이름을 입력합니다. 호스트 이름의 길이는 19자 미만이어야 하며 밑줄(_)을 포함해서는 안 됩니다.	구문은 권장 사항을 충족해야 합니다.
primarynameserver	기본 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	Cisco ISE 릴리스 3.4부터: • Cisco ISE 릴리스 3.4부터: 설치 중 **secondarynameserver(**보조 네임 서버**)** 및 **tertiarynameserver(3**차 네임 서버) 필드를 사용하여 보조 및 3차 네임 서버를 구성할 수 있습니다.
secondarynameserver (Cisco ISE 릴리스 3.4부터)	보조 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	• **secondarynameserver** 필드를 비워 두고 **tertiarynameserver** 필드만 사용하는 경우 Cisco ISE 서비스가 시작되지 않습니다.
tertiarynameserver (Cisco ISE 릴리스 3.4부터)	3차 네임 서버의 IP 주소를 입력합니다. IPv4 주소만 지원됩니다.	secondarynameserver 값이 설정된 후에만 사용하십시오.
dnsdomain	DNS 도메인 의 FQDN을 입력합니다. 이 항목에는 ASCII 문자, 숫자, 하이픈(-), 마침표(.)를 포함할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.
ntpserver (Cisco ISE 릴리스 3.4부터 **primaryntpserver**로 이름이 변경됨)	동기화에 사용할 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다(예: time.nist.gov).	Cisco ISE 릴리스 3.4부터: • **ntpserver** 필드 이름이 **primaryntpserver**로 변경되었습니다. **ntpserver**를 사용하면 Cisco ISE 서비스가 시작되지 않습니다.

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
secondaryntpserver (Cisco ISE 릴리스 3.4부터)	보조 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다.	• **secondaryntpserver** 필드를 비워두고 **tertiaryntpserver** 필드만 사용하는 경우 Cisco ISE 서비스가 시작되지 않습니다.
tertiaryntpserver (Cisco ISE 릴리스 3.4부터)	3차 NTP 서버의 IPv4 주소 또는 FQDN을 입력합니다.	secondaryntpserver 값이 설정된 후에만 사용하십시오.
timezone	시간대를 입력합니다(예: Etc/UTC). 특히 Cisco ISE 노드가 분산 구축 환경에 설치된 경우, 모든 Cisco ISE 노드를 협정 세계시(UTC) 표준 시간대로 설정하는 것을 권장합니다. 이를 통해 구축 환경 내 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프를 항상 동기화할 수 있습니다.	구문은 권장 사항을 충족해야 합니다.
비밀번호	Cisco ISE의 GUI 기반 로그인에 사용할 비밀번호를 구성합니다. 입력하는 비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 합니다. 비밀번호는 6~25자 사이여야 하며 숫자, 대문자, 소문자를 각각 하나 이상 포함해야 합니다. 비밀번호 는 사용자 이름 또는 사용자 이름의 역순(iseadmin 또는 nimdaesi), cisco 또는 ocsic과 같거나 이를 포함할 수 없습니다. 허용되는 특수 문자는 @~*!,+=_- 입니다. .	사용 중인 릴리스의 Cisco ISE Administrator Guide 내 "Basic Setup" 장의 "User Password Policy" 섹션을 참조하십시오.
ersapi	ERS를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.
openapi	OpenAPI를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	Cisco ISE 릴리스 3.4부터 OpenAPI 서비스는 기본적으로 활성화됩니다. 인스턴스를 시작할 때 OpenAPI 관련 옵션을 지정할 필요가 없습니다.
pxGrid	pxGrid를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	구문은 권장 사항을 충족해야 합니다.

필드 이름	필드 설명	규정 준수 및 동작 변경 사항
pxgrid_cloud	pxGrid Cloud를 활성화하려면 **yes**를, 비활성화하려면 **no**를 입력합니다.	pxGrid Cloud를 활성화하려면 반드시 pxGrid를 먼저 활성화해야 합니다. pxGrid를 비활성화한 상태에서 pxGrid Cloud를 활성화하면, 실행 시 pxGrid Cloud 서비스가 활성화되지 않습니다. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI에서만 활성화할 수 있습니다. 따라서 이 필드는 User data에 포함되지 않습니다.

단계 **6** **Create(**생성**)**를 클릭합니다.

인스턴스가 생성되어 사용 가능해지기까지 약 30분이 소요됩니다. Cisco ISE 인스턴스가 **Instances(**인스턴스**)** 페이지에 표시됩니다.

User data 매개변수

필드	형식	**Cisco ISE** 릴리스 **3.1**	**Cisco ISE** 릴리스 **3.2**	**Cisco ISE** 릴리스 **3.3**	**Cisco ISE** 릴리스 **3.4**	**Cisco ISE** 릴리스 **3.5**
hostname	호스트 이름 =<hostname of Cisco ISE>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
primarynameserver	primarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primarynameserver=<IPv6 주소> 지원)	지원됨.	지원됨.	지원됨.	지원됨.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
secondarynameserver	secondarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiarynameserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiarynameserver 필드를사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
tertiarynameserver	tertiarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiarynameserver=<IPv6 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondarynameserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를지원합니다.
dnsdomain	dnsdomain=<example.com>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ntpserver	ntpserver=<NTP FQDN IPv4 또는 서버의 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 ntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원됨.	지원됨.	지원됨.	지원되지 않음. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전부터 primaryntpserver로 대체됩니다. ntpserver를사용하면 Cisco ISE 서비스가 시작되지 않을 수 있습니다.	지원되지 않음. 대신 primaryntpserver를 사용하십시오.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
Primaryntpserver	primaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 primaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드는 Cisco ISE 릴리스 3.4 및 이후 버전에서 ntpserver를 대체합니다.	지원됨. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
secondaryntpserver	secondaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 secondaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiaryntpserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiaryntpserver 필드를사용하려면 이 필드에 반드시 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
tertiaryntpserver	tertiaryntpserver=<IPv4 FQDN 또는 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiaryntpserver=<NTP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다.	지원됨. 이 필드를 사용하려면 먼저 secondaryntpserver 필드에 값을 입력해야 합니다. Cisco ISE 릴리스 3.5 및 이후 버전은 AWS 구축 환경에서 IPv6 주소를 지원합니다.
timezone	timezone=<표준 시간대>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.

필드	형식	Cisco ISE 릴리스 3.1	Cisco ISE 릴리스 3.2	Cisco ISE 릴리스 3.3	Cisco ISE 릴리스 3.4	Cisco ISE 릴리스 3.5
username	username=<admin>	지원됨 (예: <admin>) Cisco ISE 릴리스 3.1 패치 1부터 지원됨.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.	지원되지 않음. iseadmin이 기본 사용자입니다.
username	username=iseadmin	필수 아님	필수	필수	필수	필수
비밀번호	password=<비밀번호>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
ersapi	ersapi=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
openapi	openapi=<yes/no>	지원됨.	지원됨.	지원됨.	OpenAPI는 기본적으로 활성화되어 있습니다.	OpenAPI는 기본적으로 활성화되어 있습니다.
pxGrid	pxGrid=<yes/no>	지원됨.	지원됨.	지원됨.	지원됨.	지원됨.
pxgrid_cloud	pxgrid_cloud=<yes/no>	지원되지 않음	지원되지 않음	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원됨. Cisco ISE 릴리스 3.3 및 3.4에서만 지원됩니다.	지원되지 않음. Cisco ISE 릴리스 3.5부터 pxGrid Cloud는 Cisco ISE GUI를 통해서만 활성화할 수 있습니다.

파라미터 구문 요구 사항

Cisco ISE on Cloud의 User data 파라미터를 지정할 때 속성이나 값을 작은따옴표나 큰따옴표로 묶지 마십시오. 모든 값은 따옴표 없이 평문(Plain text)으로 입력해야 합니다.

잘못된 입력	올바른 입력
hostname="i34a"	hostname=i34a
primarynameserver="9.9.9.9"	primarynameserver="9.9.9.9"
dnsdomain="example.com"	dnsdomain=example.com
primaryntpserver="north-america.pool.ntp.org"	primaryntpserver="north-america.pool.ntp.org"

Cisco ISE 릴리스 3.3부터 시리얼 콘솔에 유효성 검사 결과 메시지가 표시됩니다. 이러한 메시지는 결과가 생성되는 시점에 시리얼 콘솔이 열려 있는 경우에만 볼 수 있습니다.

Terraform Stack 파일을 사용하여 OCI에서 Cisco ISE 인스턴스 생성

Terraform Stack 파일을 사용하여 OCI에서 Cisco ISE 인스턴스를 생성하려면 다음 단계를 따르십시오.

시작하기 전에

OCI에서 Cisco ISE 인스턴스에 필요한 리소스(예: SSH 키, Virtual Cloud Network(VCN), 서브넷, 네트워크 보안 그룹 및 기타 필수 구성 요소)를 생성합니다. OCI에서 Terraform을 사용하는 방법에 대한 자세한 내용은 Oracle 설명서를 참조하십시오.

프로시저

단계 **1** OCI에서 Cisco ISE 스택 생성, 68 페이지.
단계 **2** Cisco ISE 인스턴스에 대한 변수 구성, 69 페이지.
단계 **3** 구성을 검토하고 OCI에서 Cisco ISE 인스턴스 생성, 70 페이지.

OCI에서 Cisco ISE 스택 생성

OCI에서 Cisco ISE 스택을 생성하려면 다음 단계를 따르십시오.

프로시저

단계 **1** OCI 계정에 로그인합니다.
단계 **2** 검색 필드를 사용하여 **Marketplace**를 검색합니다.
단계 **3** **Search for licensing(**목록 검색**)** 필드에 **Cisco Identity Services Engine (ISE)**을 입력합니다.
단계 **4** **Cisco Identity Services Engine (ISE) Stack**을 클릭합니다.
단계 **5** 새 창이 표시되면 **Create Stack(**스택 생성**)**을 클릭합니다.
단계 **6** **Stack Information(**스택 정보**)** 창에서 다음을 수행합니다.
a) **My Configuration(**나의 구성**)**을 클릭합니다.
b) **Create in Compartment(**구획에 생성**)** 드롭다운 목록에서 Cisco ISE 인스턴스를 생성할 구획(Compartment)을 선택합니다.

Cisco ISE 인스턴스에 대한 변수 구성

다음 단계에 따라 Cisco ISE 인스턴스의 변수를 구성하십시오.

프로시저

단계 **1** **Configure Variables(**변수 구성**)** 페이지에서 다음을 수행합니다.

a) **Hostname(**호스트 이름**)** 필드에 호스트 이름을 입력합니다.

b) **Shape(**셰이프**)** 드롭다운 목록에서 사용할 OCI 셰이프를 선택합니다.

VM.Optimized3.Flex 를선택하는 경우 **Flex OCPU** 드롭다운 목록에서 필요한 값을 선택합니다. **Flex Memory in GB(**플렉스 메모리**(GB))** 필드에 해당 값이 표시됩니다. 다른 셰이프의 경우 이러한 값들이 사전 구성되어 있으므로 스택 양식에 표시되지 않습니다.

c) **Boot Volume Size(**부팅 볼륨 크기**)** 필드에는 이전 단계에서 선택한 셰이프에 따라 필요한 값이 자동으로 표시됩니다.

1. **Vault(**저장소**)** 필드에서 부팅 볼륨 암호화 키에 대한 저장소를 선택합니다.
2. **Volume Encryption Key(**볼륨 암호화 키**)** 필드에서 부팅 볼륨을 암호화할 키를 선택합니다.

Cisco ISE 릴리스 3.3부터는 **Volume Encryption Key(**볼륨 암호화 키**)** 및 **Vault(**저장소**)** 필드에서 암호화 에 고객 관리 키를 사용하는 것을 권장합니다. 기본적으로 **Oracle Managed Key(**오라클 관리 키**)**가 사용됩니다. 키 생성에 대한 자세한 내용은 Key Management를참조하십시오.

d) **SSH Key(SSH** 키**)** 영역에서 SSH 키 파일을 업로드하거나 SSH 키 코드를 붙여넣습니다.

e) **Time Zone(**표준 시간대**)** 드롭다운 목록에서 표준 시간대를 선택합니다.

f) **Availability Domain(**가용성 도메인**)** 드롭다운 목록에서 해당 지역의 도메인 중 하나를 선택합니다.

g) **Virtual Cloud Network(**가상 클라우드 네트워크**)** 드롭다운 목록에서 이전에 선택한 구역의 VCN 목록에서 옵션을 선택합니다.

h) **Subnet(**서브넷**)** 드롭다운 목록에서 선택한 VCN과 연결된 서브넷 목록의 옵션을 선택합니다.

i) (선택 사항) **Network Security Group(**네트워크 보안 그룹**)** 드롭다운 목록에서 이전에 선택한 구성 요소와 연결된 보안 그룹을 선택합니다.

Assign Public IP Address(공용 **IP** 주소 할당**)** 확인란은 기본적으로 선택되어 있습니다. Cisco ISE 인스턴스에 프라이빗 IP 주소만 할당하려면 이 확인란을 선택 해제하십시오.

j) 선택한 서브넷 에 대해 정의된 범위 내의 IP 주소를 **Private IP Address(**프라이빗 **IP** 주소**)** 필드에 입력합니다.

이 필드를 비워 두면 OCI DHCP 서버가 Cisco ISE에 IP 주소를 할당합니다.

k) **DNS Server(DHCP** 서버**)** 필드에 도메인 이름을 입력합니다.

l) **Name Server(**네임 서버**)** 필드에 네임 서버의 IP 주소를 입력합니다.

Cisco ISE 릴리스 3.4부터:

- **Name Server(**네임 서버**)** 필드 이름이 **Primary Name Server(**기본 네임 서버**)**로 변경됩니다.
- 보조 네임 서버의 IP 주소는 **Secondary Name Server(**보조 네임 서버**)** 필드에 입력할 수 있습니다.

- 3차 네임 서버의 IP 주소는 **Tertiary Name Server(3**차 네임 서버**)** 필드에 입력할 수 있습니다. 이 필드를 사용하고 애플리케이션을 성공적으로 실행하려면 **Secondary Name Server(**보조 네임 서버**)** 필드를 비워 두지 않아야 합니다.

m) **NTP Server(NTP** 서버**)** 필드에 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다.

Cisco ISE 릴리스 3.4부터:

- **NTP Server(NTP** 서버**)** 필드 이름이 **Primary NTP Server(**기본 **NTP** 서버**)**로 변경됩니다.
- 보조 NTP 서버의 IP 주소 또는 호스트 이름을 **Secondary NTP Server(**보조 **NTP** 서버**)** 필드에 입력할 수 있습니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다.
- 3차 NTP 서버의 IP 주소 또는 호스트 이름을 **Tertiary NTP Server(3**차 **NTP** 서버**)** 필드에 입력할 수 있습니다. 입력한 정보는 별도로 유효성 검사를 거치지 않습니다. 이 필드를 사용하고 애플리케이션을 성공적으로 실행하려면 **Secondary NTP Server(**보조 **NTP** 서버**)** 필드를 비워 두면 안 됩니다.

n) **ERS** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.
o) **Open API** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.
p) **pxGrid** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.
q) **pxGrid Cloud(pxGrid** 클라우드**)** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다. Cisco ISE 릴리스 3.5부터는 pxGrid Cloud UI에서만 활성화할 수 있습니다. 따라서 이 필드를 사용할 수 없습니다.
r) **Password(**비밀번호**)** 및 **Re-Enter the Password(**비밀번호 다시 입력**)** 필드에 Cisco ISE 의 비밀번호 입력합니다. 비밀번호는 Cisco ISE 비밀번호 정책을 준수해야 하며 길이는 최대 25자 이내여야 합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

Review(검토**)** 창에 스택에 정의된 모든 구성 요약이 표시됩니다.

구성을 검토하고 **OCI**에서 **Cisco ISE** 인스턴스 생성

다음 단계에 따라 지금까지 수행한 구성을 검토하고 Cisco ISE 인스턴스를 생성합니다.

프로시저

단계 **1** 정보를 검토하고 변경할 사항이 있면 **Previous(**이전**)**를 클릭합니다.

단계 **2** **'Run Apply on the created stack?(**생성된 스택에 적용을 실행하시겠습니까**?)'**영역에서 **Run Apply(**적용 실행**)** 확인란을 선택하면 **Create(**생성**)**를 클릭할 때 스택이 빌드됩니다.

Run Apply(적용 실행**)**를 선택하지 않으면 **Create(**생성**)**를 클릭할 때 스택 정보만 저장됩니다. 나중에 **Stacks(**스택**)** 창에서 스택을 선택하고 **Apply(**적용**)**를 클릭하여 빌드를 실행할 수 있습니다.

단계 **3** **Create(**생성**)**를 클릭합니다.

단계 **4** OCI에서 **Instances(**인스턴스**)** 창으로 이동합니다.

스택 양식에 입력한 호스트 이름으로 인스턴스가 표시됩니다. 호스트 이름을 클릭하여 구성 세부 정보를 확인합니다.

OCI의 Cisco ISE 인스턴스는 약 30분 후에 실행 준비가 완료됩니다.

설치 후 작업

Cisco ISE 인스턴스를 생성한 후 수행해야 하는 설치 후 작업에 대한 정보는 사용 중인 릴리스의 *Cisco ISE Installation Guide* 내 "Installation Verification and Postinstallation Tasks(설치 확인 및 설치 후 작업)" 장을 참조하십시오.

OCI의 Cisco ISE 에 대한 호환성 정보

이 섹션에서는 OCI의 Cisco ISE 에 고유한 호환성 정보를 제공합니다. Cisco ISE 의 일반 호환성 세부 정보는 해당 릴리스의 Cisco Identity Services Engine Network Component Compatibility 가이드를 참조하십시오.

로드 밸런서 연동 지원

RADIUS 트래픽의 로드 밸런싱을 위해 OCI 네이티브 네트워크 로드 밸런서를 Cisco ISE와 연동할 수 있습니다. 하지만 다음과 같은 주의사항이 적용됩니다.

- Change of Authorization(CoA) 기능은 네트워크 로드 밸런서를 생성할 때 Source or Destination Header (IP,Port) Preservation(소스 또는 대상 헤더(IP,포트) 보존) 섹션에서 클라이언트 IP 보존을 활성화한 경우에만 지원됩니다.
- 네트워크 로드 밸런서가 Source IP Affinity(소스 IP 선호도)만 지원하고 Calling Station ID 기반의 Sticky Session(고정 세션)을 지원하지 않으므로 불균등한 로드 밸런싱이 발생할 수 있습니다.
- 네트워크 로드 밸런서는 RADIUS 기반의 Health Check(상태 확인)를 지원하지 않으므로, 노드에서 RADIUS 서비스가 비활성 상태이더라도 트래픽을 PSN으로 전송할 수 있습니다.

OCI 기본 네트워크 로드 밸런서 에 대한 자세한 내용은 Introduction to Network Load Balancer를 참조하십시오.

TACACS+ 트래픽의 로드 밸런싱을 위해 OCI 네이티브 네트워크 로드 밸런서를 Cisco ISE와 연동할 수 있습니다. 그러나 네트워크 로드 밸런서가 TACACS+ 서비스 기반의 Health Check를 지원하지 않으므로, 노드에서 TACACS+ 서비스가 비활성 상태이더라도 트래픽이 PSN으로 전송될 수 있습니다.

NIC 점보 프레임 지원

Cisco ISE는 점보 프레임(Jumbo frames)을 지원합니다. Cisco ISE의 최대 전송 단위(MTU)는 9,001바이트인 반면, 네트워크 액세스 디바이스(NAD)의 MTU는 일반적으로 1,500바이트입니다. Cisco ISE

는 문제없이 표준 프레임과 점보 프레임을 모두 지원합니다. 구성 모드(Configuration mode)에서 CLI를 통해 필요에 따라 Cisco ISE용 MTU를 재설정할 수 있습니다.

OCI 환경의 비밀번호 복구 및 재설정

Cisco ISE 가상 머신 비밀번호를 재설정하려면 다음 작업들을 활용하십시오. 필요한 작업을 선택하고 단계를 수행하십시오.

시리얼 콘솔을 통한 Cisco ISE GUI 비밀번호 재설정

OCI 시리얼 콘솔을 통해 Cisco ISE GUI 비밀번호를 재설정하려면 다음 단계를 따르십시오.

프로시저

단계 1 OCI에 로그인하고 **Compute(**컴퓨팅**) > Instances(**인스턴스**)**를 선택합니다.

단계 2 인스턴스 목록에서 비밀번호를 변경할 인스턴스를 선택합니다.

단계 3 **Resources(**리소스**) > Console connection(**콘솔 연결**)**을 선택합니다.

단계 4 **Launch Cloud Shell connection (Cloud Shell** 연결 시작**)**을 클릭합니다.

새 화면에 Oracle Cloud Shell이 표시됩니다. 화면이 검은색인 경우 **Enter**를 눌러 로그인 프롬프트를 표시합니다.

단계 5 시리얼 콘솔에 로그인합니다.

시리얼 콘솔에 로그인하려면 인스턴스 설치 시 설정된 원래 비밀번호 사용해야 합니다. OCI는 이 비밀번호 값을 마스킹합니다. 비밀번호가 기억나지 않는 경우 Password Recovery 섹션을 참조하십시오.

단계 6 **application reset-passwd ise iseadmin** 명령을 사용하여 iseadmin 계정에 사용할 새 Cisco ISE GUI 비밀번호를 구성합니다.

OCI에서 새 퍼블릭 키 쌍 생성

이 작업은 리포지토리에 추가 키 쌍을 저장하는 데 도움이 됩니다. 새 퍼블릭 키는 Cisco ISE 인스턴스 구성 시 생성한 기존 키 쌍을 대체하지 않습니다.

프로시저

단계 1 OCI에서 새 퍼블릭 키를 생성합니다. Creating a Key Pair를 참조하십시오.

단계 2 OCI 콘솔에 로그인합니다.

단계 3 퍼블릭 키를 저장할 새 리포지토리를 생성합니다. Creating a Repository를 참조하십시오.

CLI를 통해 접근할 수 있는 리포지토리가 이미 있는 경우 이 단계를 건너뜁니다.

단계 **4** 다음 명령을 사용하여 새 퍼블릭 키를 가져옵니다:

crypto key import <public key filename> repository <repository name>

가져오기가 완료되면 SSH와 새로 생성한 퍼블릭 키를 사용하여 Cisco ISE에 로그인할 수 있습니다.

비밀번호 복구

OCI 환경의 Cisco ISE에는 비밀번호 복구 메커니즘이 없습니다. 새로운 Cisco ISE 인스턴스를 생성하고 구성 데이터의 백업 및 복원을 수행해야 할 수 있습니다.

OCI 스택 변수를 편집하면 기존 Cisco ISE 인스턴스가 제거되고 새 인스턴스가 생성됩니다. 시스템은 기존의 설정이나 구성값을 유지하지 않습니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.