



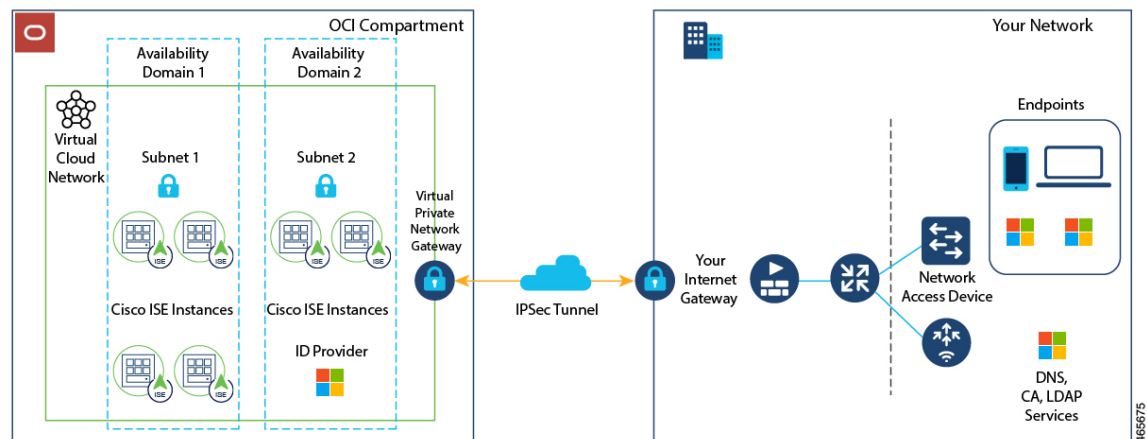
Oracle Cloud Infrastructure의 Cisco ISE

- Oracle Cloud Infrastructure의 Cisco ISE , 1 페이지
- Cisco ISE가 지원하는 OCI 인스턴스, 2 페이지
- OCI에서 Cisco ISE 사용 시 알려진 제한 사항, 3 페이지
- OCI에서 Cisco ISE 인스턴스 생성, 3 페이지
- Terraform Stack 파일을 사용하여 OCI에서 Cisco ISE 인스턴스 생성 , 12 페이지
- 설치 후 작업, 15 페이지
- OCI의 Cisco ISE 에 대한 호환성 정보, 15 페이지
- OCI 환경의 비밀번호 복구 및 재설정, 16 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 Documentation](#)을 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, 서버넷 및 사이트 간 VPN을 생성합니다.

Cisco ISE 인스턴스와 동일한 구획에 가상 클라우드 네트워크 및 서버넷을 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, 4 페이지.

단계 2 인스턴스 세부 정보 구성, 4 페이지.

단계 3 Cisco ISE 인스턴스 고급 옵션 구성, 5 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)**를 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 Management](#)를 참조하십시오.

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 **파라미터**를 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 1: **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(3차 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 비워두고 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 primaryntpserver로 변경되었습니다. ntpserver를 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. 비밀번호는 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.

User data 매개변수

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=<IPv4 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.
tertiarynameserver	tertiarynameserver=<IPv4 주소> (Cisco ISE 릴리스 3.5부터 AWS 환경에서는 tertiarynameserver=<IPv4 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	admin=<admin>	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.

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 =<NIP 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 =<NIP FQDN IPv6 또는 서버의 주소> 지원)	지원되지 않음	지원되지 않음	지원되지 않음	지원됨. tertiaryntpserver 필드를 사용하려면 이 필드에 반드시 값을 입력해야 합니다.	지원됨. tertiaryntpserver 필드를 사용하려면 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 =<NIP 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, 12 페이지.
 - 단계 2 Cisco ISE 인스턴스에 대한 변수 구성, 13 페이지.
 - 단계 3 구성을 검토하고 OCI에서 Cisco ISE 인스턴스 생성, 14 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.Flex를 선택하는 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 암호화에 고객 관리 키를 사용하는 것을 권장합니다. 기본적으로 **Oracle Managed Key**(오라클 관리 키)가 사용됩니다. 키 생성에 대한 자세한 내용은 [Key Management](#)를 참조하십시오.
- 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 서브넷에 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**(3차 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**(3차 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 ISE의 비밀번호를 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 OCI에서 Cisco ISE 인스턴스 생성

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

프로시저

단계 1 정보를 검토하고 변경할 사항이 있으면 **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 Balancer](#)를 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 마스크합니다. 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 Pair](#)를 참조하십시오.

단계 2 OCI 콘솔에 로그인합니다.

단계 3 퍼블릭 키를 저장할 새 리포지토리를 생성합니다. [Creating a Repository](#)를 참조하십시오.

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

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.

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.