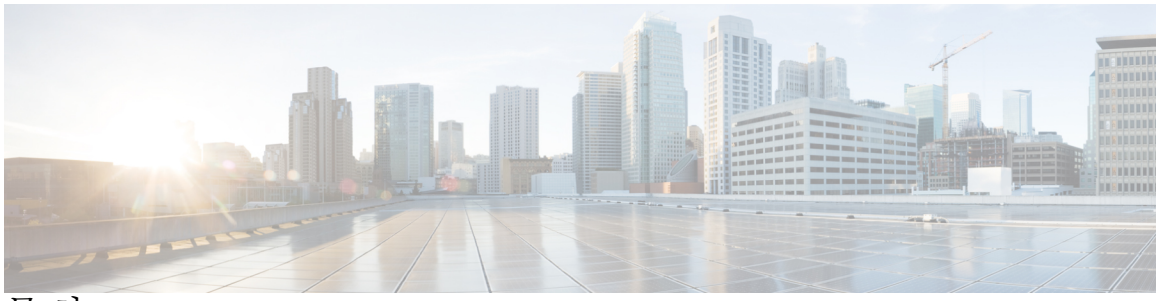
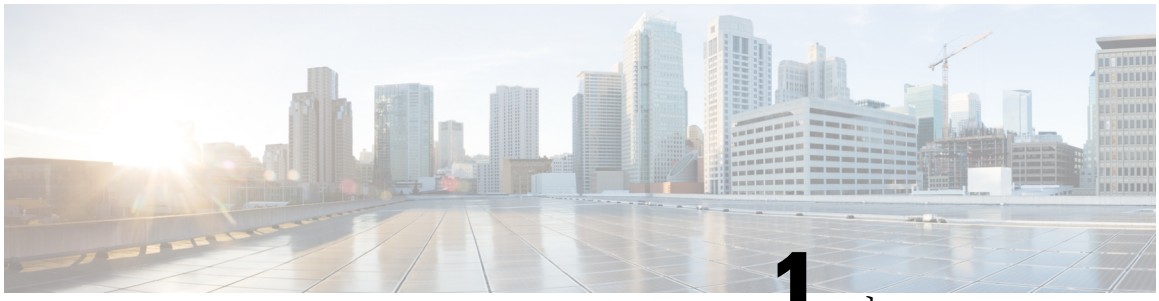
Cisco Identity Services Engine 설치 설명서, 릴리스 3.0

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



목 차



1 장

Cisco ISE 네트워크 구축

참고 이 제품에 대한 문서 세트는 편견 없는 언어를 사용하기 위해 노력합니다. 이 설명서 세트의 목적상, 편향이 없는 언어는 나이, 장애, 성별, 인종 정체성, 민족 정체성, 성적 지향성, 사회 경제적 지위 및 교차성에 기초한 차별을 의미하지 않는 언어로 정의됩니다. 제품 소프트웨어의 사용자 인터페이스에서 하드코딩된 언어, RFP 설명서에 기초한 언어 또는 참조된 타사 제품에서 사용하는 언어로 인해 설명서에 예외가 있을 수 있습니다.

Cisco ISE 네트워크 아키텍처

Cisco ISE 아키텍처는 다음 구성 요소를 포함합니다.

- 노드 및 페르소나 유형
  - Cisco ISE 노드—Cisco ISE 노드는 관리, 정책 서비스, 모니터링, pxGrid 페르소나 중 하나 또는 전부를 맡을 수 있습니다.
- 네트워크 리소스
- 엔드포인트

정책 정보 지점은 외부 정보가 정책 서비스 페르소나에 전달되는 지점을 나타냅니다. 예를 들어 외부 정보는 LDAP(Lightweight Directory Access Protocol (LDAP) 특성일 수 있습니다.

Cisco ISE 구축 용어

이 설명서에서는 Cisco ISE 구축 시나리오를 다룰 때 다음 용어를 사용합니다.

용어	정의
서비스	페르소나에서 제공하는 구체적인 기능이며 네트워크 액세스, 프로파일링, 포스처, 보안 그룹 액세스, 모니터링, 문제 해결 등이 있습니다.
노드	개별 물리적 또는 가상 Cisco ISE 어플라이언스.
노드 유형	Cisco ISE 노드는 관리, 정책 서비스, 모니터링의 페르소나 중 무엇이든 맡을 수 있습니다.
페르소나	노드에서 제공하는 서비스를 결정합니다. Cisco ISE 노드는 페르소나 중 하나를 취할 수 있습니다. 관리자 사용자 인터페이스에서 제공하는 메뉴 옵션은 노드의 역할 및 페르소나에 따라 달라집니다.
역할	노드가 독립형, 기본 또는 보조 노드인가를 결정하며 관리 및 모니터링 노드에만 적용됩니다.

분산 구축의 노드 유형 및 페르소나

Cisco ISE 노드는 그 페르소나에 따라 다양한 서비스를 제공할 수 있습니다. 구축의 각 노드는 관리, 정책 서비스, pxGrid 및 모니터링 페르소나를 취할 수 있습니다. 분산형 구축에서는 다음과 같은 노드 조합으로 네트워크를 구성할 수 있습니다.

- 고가용성을 위한 기본 및 보조 관리 노드
- 자동 장애 조치를 위한 한 쌍의 모니터링 노드
- 세션 장애 조치를 위한 하나 이상의 정책 서비스 노드
- pxGrid 서비스를 위한 하나 이상의 pxGrid 노드

관리 노드

관리 페르소나의 Cisco ISE 노드에서는 Cisco ISE에 대한 모든 관리 작업을 수행할 수 있습니다. 인증, 권한 부여, 계정 관리 등의 기능과 관련된 모든 시스템 관련 컨피그레이션을 다룹니다. 분산 구축에

서는 최대 2개의 노드에서 관리 페르소나를 실행할 수 있습니다. 관리 페르소나는 독립형, 기본 또는 보조의 역할을 맡을 수 있습니다.

정책 서비스 노드

정책 서비스 페르소나의 Cisco ISE 노드에서는 네트워크 액세스, 포스처, 게스트 액세스, 클라이언트 프로비저닝, 프로파일링 서비스를 제공할 수 있습니다. 이 페르소나는 정책을 평가하고 모든 결정을 내립니다. 여러 노드에서 이 페르소나를 맡게 할 수 있습니다. 일반적으로 분산형 구축에는 두 개 이상의 정책 서비스 노드가 있습니다. 같은 고속 LAN(Local Area Network)이나 로드 밸런서 뒤에 있는 모든 정책 서비스 노드는 함께 그룹화하여 하나의 노드 그룹을 만들 수 있습니다. 노드 그룹의 노드 중 하나에 장애가 발생하면 다른 노드가 장애를 탐지하고 URL로 리디렉션된 세션을 재설정합니다.

분산 설정에서 하나 이상의 노드가 정책 서비스 페르소나를 맡아야 합니다.

모니터링 노드

모니터링 페르소나의 Cisco ISE 노드는 로그 컬렉터의 기능을 하며, 네트워크의 모든 관리 및 정책 서비스 노드로부터 생성된 로그 메시지를 저장합니다. 이 페르소나는 고급 모니터링 및 문제 해결 툴을 제공하며, 이는 네트워크 및 리소스를 효과적으로 관리하는 데 사용할 수 있습니다. 이 페르소나의 노드는 수집하는 데이터를 취합하여 상관성을 파악하고 유의미한 보고서를 제공합니다. Cisco ISE에서는 이 페르소나의 노드를 2개까지 둘 수 있으며, 이 노드는 고가용성을 위해 기본 또는 보조 역할을 맡을 수 있습니다. 기본 및 보조 모니터링 노드 모두 로그 메시지를 수집합니다. 기본 모니터링 노드의 작동이 중단될 경우 보조 모니터링 노드가 자동으로 기본 모니터링 노드가 됩니다.

분산 설정에서 하나 이상의 노드가 모니터링 페르소나를 맡아야 합니다. 모니터링 페르소나와 정책 서비스 페르소나를 동일한 Cisco ISE 노드에서 활성화하지 않는 것이 좋습니다. 최적의 성능을 위해 모니터링 노드는 모니터링 전용으로 두는 것이 좋습니다.

pxGrid 노드

Cisco pxGrid는 Cisco ISE 세션 디렉토리에서 다른 정책 네트워크 시스템(예: ISE Eco 시스템 파트너 시스템 및 기타 Cisco 플랫폼)과 상황 민감 정보를 공유하는 데 사용됩니다. 또한 pxGrid 프레임워크를 사용하여 노드 간에 정책 및 컨피그레이션 데이터를 교환하고(예: ISE와 서드파티 벤더 간에 태그 및 정책 객체 공유) 다른 정보도 교환할 수 있습니다. 또한 Cisco pxGrid에서는 타사 시스템이 네트워크 또는 보안 이벤트에 대한 응답으로 사용자/장치를 격리하기 위해 EPS(적응형 네트워크 제어 작업)를 호출할 수 있습니다. 태그 정의, 값 및 설명과 같은 TrustSec 정보는 TrustSec 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. FQN(Fully Qualified Names)을 사용하는 엔드포인트 프로파일은 엔드포인트 프로파일 메타 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. Cisco pxGrid는 태그 및 엔드포인트 프로파일의 대량 다운로드도 지원합니다.

pxGrid를 통해 SXP 바인딩(IP-SGT 매핑)을 게시하고 구독할 수 있습니다. SXP 바인딩에 대 한 자세한 내용은 *Cisco Identity Services Engine* 관리자 설명서의 소스 그룹 태그 프로토콜 섹션을 참조 하십시오.

고가용성 컨피그레이션에서 Cisco pxGrid 서버는 PAN을 통해 노드 간에 정보를 복제합니다. PAN이 다운되면 pxGrid 서버는 클라이언트 등록 및 서브스크립션 처리를 중단합니다. pxGrid 서버가 활성화되도록 PAN을 수동으로 승격해야 합니다.

독립형 및 분산 ISE 구축

단일 Cisco ISE 노드가 있는 구축을 독립형 구축이라고 합니다. 이 노드에서 관리, 정책 서비스, 모니터링 페르소나를 담당합니다.

둘 이상의 Cisco ISE 노드가 있는 구축을 분산 구축이라고 합니다. 장애 조치를 지원하고 성능을 높이기 위해 여러 Cisco ISE 노드로 구성된 분산형 구축을 설정할 수 있습니다. Cisco ISE 분산 구축에서는 관리 및 모니터링 활동이 중앙 집중식으로 이루어지며 처리 작업은 정책 서비스 노드에 분산됩니다. 성능 요구 사항에 따라 구축을 확장할 수 있습니다. Cisco ISE 노드는 관리, 정책 서비스, 모니터링의 페르소나 중 무엇이든 맡을 수 있습니다.

분산 구축 시나리오

- 소형 네트워크 구축
- 중형 네트워크 구축
- 대형 네트워크 구축

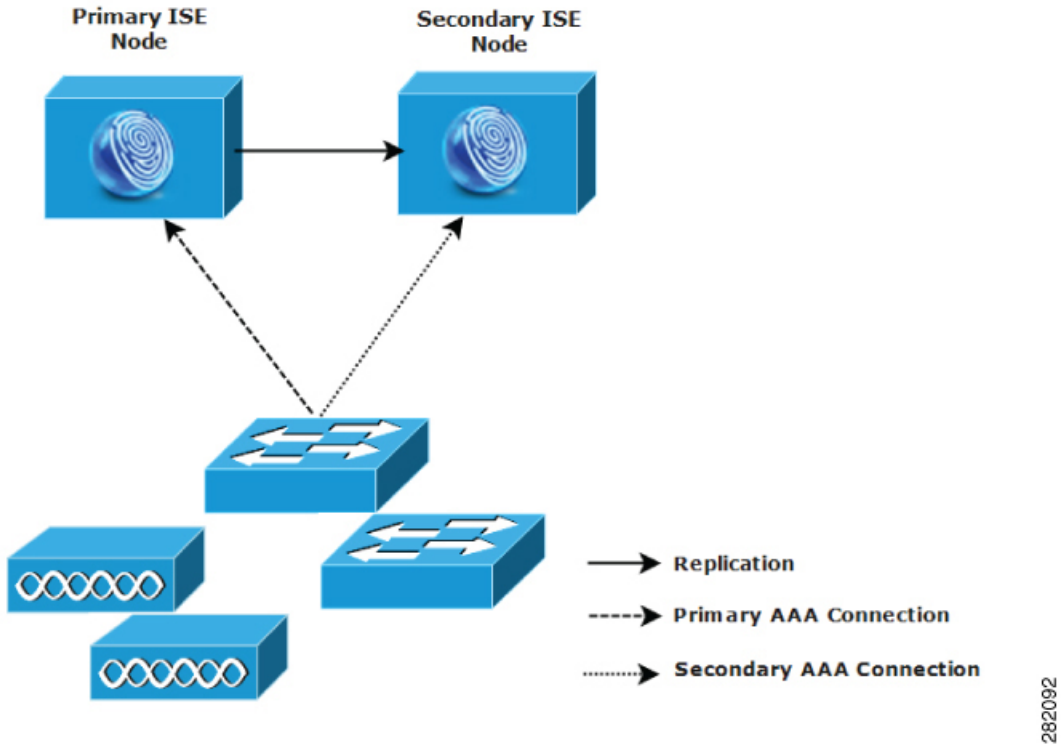
소형 네트워크 구축

Cisco ISE 구축의 가장 작은 형태는 Cisco ISE 노드 2개로 구성되며, 그중 한 Cisco ISE 노드가 소형 네트워크의 기본 어플라이언스로 작동합니다.

기본 노드가 이 네트워크 모델에 필요한 모든 컨피그레이션, 인증, 정책 기능을 제공합니다. 보조 Cisco ISE 노드는 백업의 역할을 합니다. 보조 노드는 기본 노드를 지원하면서 기본 노드와 네트워크 어플라이언스, 네트워크 리소스 또는 RADIUS 간의 연결이 끊길 때마다 네트워크를 정상 작동 상태로 유지합니다.

클라이언트와 기본 Cisco ISE 노드 간의 중앙 집중식 AAA(인증, 권한 부여 및 계정 관리) 작업은 RADIUS 프로토콜을 사용하여 수행합니다. Cisco ISE는 기본 Cisco ISE 노드에 상주하는 모든 콘텐츠를 보조 Cisco ISE 노드와 동기화하거나 복제합니다. 이런 방법으로 보조 노드가 기본 노드와 동일한 상태로 유지됩니다. 소형 네트워크 구축에서 이러한 유형의 컨피그레이션 모델은 이 구축 유형 또는 비슷한 방식으로 모든 RADIUS 클라이언트에 기본 노드와 보조 노드 둘 다 구성할 수 있게 합니다.

그림 *1:* 소형 네트워크 구축



네트워크 환경에서 디바이스, 네트워크 리소스, 사용자, AAA 클라이언트의 수가 증가하면 구축 컨피그레이션을 기본적인 소형 모델에서 벗어나 분할 또는 분산 구축 모델을 더 많이 사용하게끔 바꿔야 합니다.

분할 구축

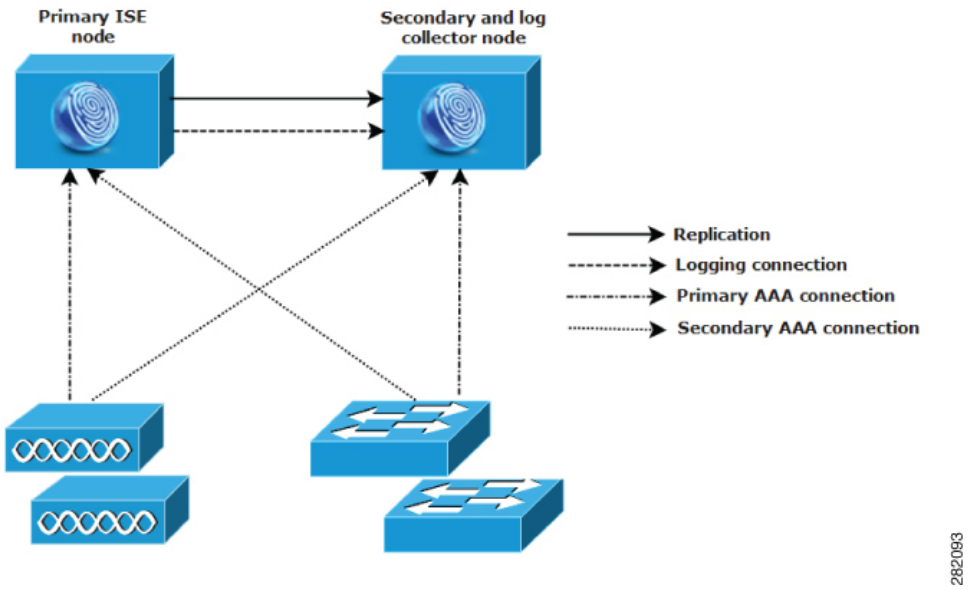
분할 Cisco ISE 구축에서는 소형 Cisco ISE 구축에서 설명한 기본 노드와 보조 노드를 계속 유지합니다. 그러나 AAA 워크플로 최적화를 위해 두 Cisco ISE 노드 간에 AAA 로드가 분할됩니다. 각 Cisco ISE 어플라이언스(기본 또는 보조)는 AAA 연결에 문제가 생길 경우 전체 워크로드를 처리할 수 있어야 합니다. 정상적인 네트워크 운영 상태에서는 기본 노드와 보조 노드 모두 모든 AAA 요청을 처리하지는 않습니다. 이 워크로드가 두 노드에 분산되어 있기 때문입니다.

이와 같이 로드를 분할할 수 있으면 시스템의 각 Cisco ISE 노드가 받는 스트레스가 곧바로 줄어듭니다. 또한 로드를 분할하면 정상적인 네트워크 운영 중에 보조 노드의 기능 상태가 유지되면서 더 효과적인 로딩이 이루어집니다.

분할 Cisco ISE 구축에서 각 노드는 네트워크 접근, 디바이스 관리와 같은 각자의 작업을 수행하면서 장애 발생 시 모든 AAA 기능도 수행할 수 있습니다. 2개의 Cisco ISE 노드에서 인증 요청을 처리하고 AAA 클라이언트로부터 계정 관리 데이터를 수집할 경우 Cisco ISE 노드 중 하나를 로그 컬렉터로 설정하는 것이 좋습니다.

또한 분할 Cisco ISE 구축 설계는 확장을 허용하기 때문에 유리합니다.

그림 2: 분할 네트워크 구축



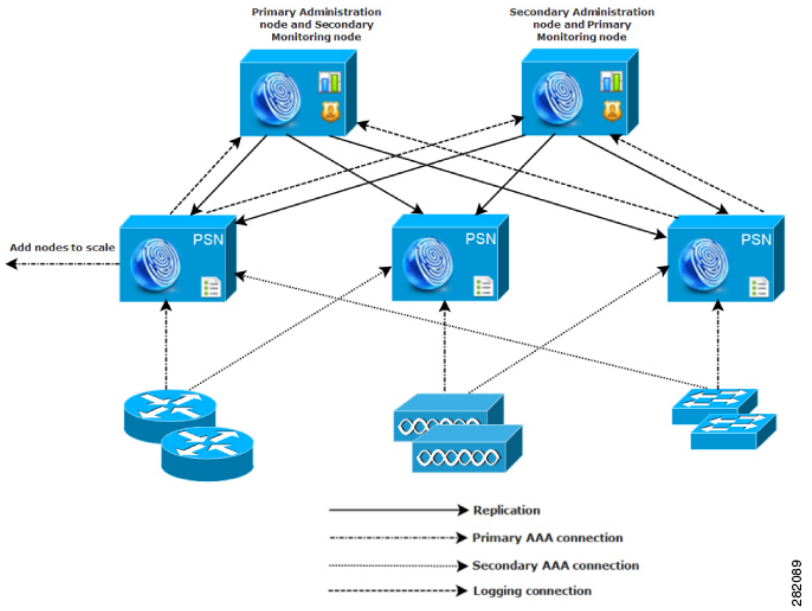
중형 네트워크 구축

소형 네트워크가 커지면 Cisco ISE 노드를 추가하여 중형 네트워크를 생성하는 방법으로 네트워크 확장에 대처하고 관리할 수 있습니다. 중형 네트워크 구축에서는 신규 노드에서 모든 AAA 기능을 전담하게 하고 원래의 노드는 컨피그레이션 및 로깅 기능에 사용할 수 있습니다.

참고 중간 규모의 네트워크 구축의 경우 관리 페르소나, 모니터링 페르소나 혹은 두 페르소나 모두를 실행하는 노드에서는 정책 서비스 페르소나를 활성화할 수 없습니다. 전용 정책 서비스 노드가 필요합니다.

네트워크에서 로그 트래픽의 양이 증가함에 따라 보조 Cisco ISE 노드 중 한두 개를 네트워크의 로그 수집 전용으로 두는 방법도 있습니다.

그림 3: 중형 네트워크 구축



대형 네트워크 구축

중앙 집중식 로깅

대형 Cisco ISE 네트워크에서는 중앙 집중식 로깅을 사용하는 것이 좋습니다. 중앙 집중식 로깅을 사용하려면 먼저 사용량이 많은 대형 네트워크에서 생성될 만한 방대한 syslog 트래픽을 처리할 수 있도록 (모니터링 및 로깅을 위해) 모니터링 페르소나가 될 전용 로깅 서버를 설정해야 합니다.

syslog 메시지는 아웃바운드 로그 트래픽에 대해 생성되므로 RFC 3164 표준에 부합하는 어떤 syslog 어플라이언스도 아웃바운드 로깅 트래픽의 컬렉터가 될 수 있습니다. 전용 로깅 서버가 있으면 Cisco ISE에서 제공하는 보고서 및 알림 기능을 사용하여 모든 Cisco ISE 노드를 지원할 수 있습니다.

또한 어플라이언스에서 Cisco ISE 노드의 모니터링 페르소나와 일반 syslog 서버 모두에 로그를 보내는 것도 고려할 수 있습니다. 일반 syslog 서버를 추가하면 Cisco ISE 노드에서 모니터링 페르소나가 작동 중단될 경우 이중 백업의 역할을 합니다.

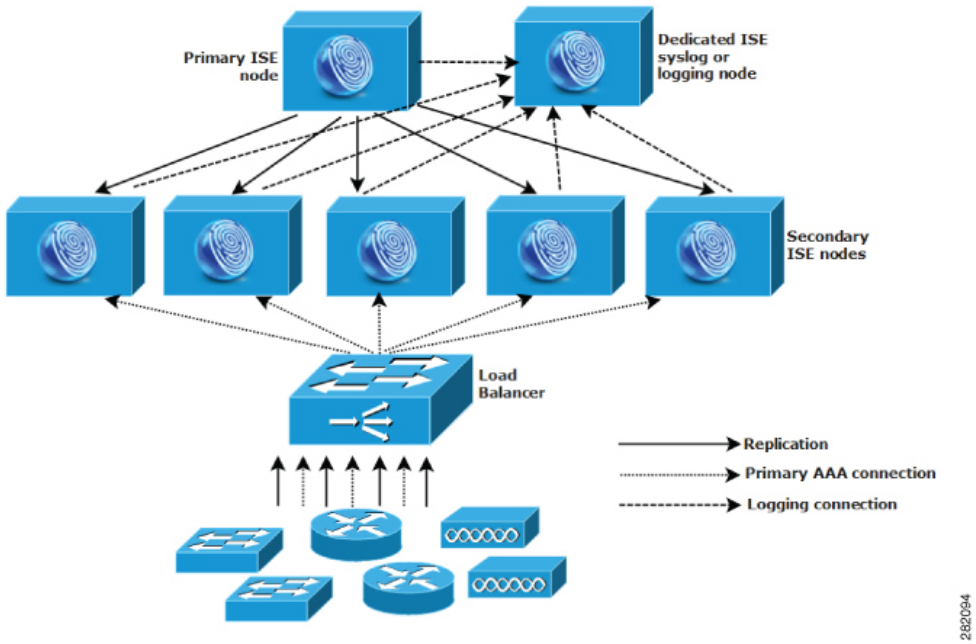
로드 밸런서

대형 중앙 집중식 네트워크에서는 AAA 클라이언트 구축을 간소화하는 로드 밸런서를 사용해야 합니다. 로드 밸런서 사용 시 AAA 서버에 대해서는 단일 엔트리만 있으면 됩니다. 그리고 로드 밸런서가 사용 가능한 서버에 대한 AAA 요청의 라우팅을 최적화합니다.

그러나 단일 로드 밸런서만 있으므로 단일 장애 지점이 발생할 가능성이 있습니다. 이러한 잠재적 문제를 방지하기 위해 이중화 및 장애 조치 차원에서 2개의 로드 밸런서를 구축합니다. 이 컨피그레이

션에서는 각 AAA 클라이언트에 AAA 서버 엔트리를 2개씩 설정해야 하며, 이 컨피그레이션은 네트워크 전 범위에서 일관됩니다.

그림 *4:* 대규모 네트워크 구축

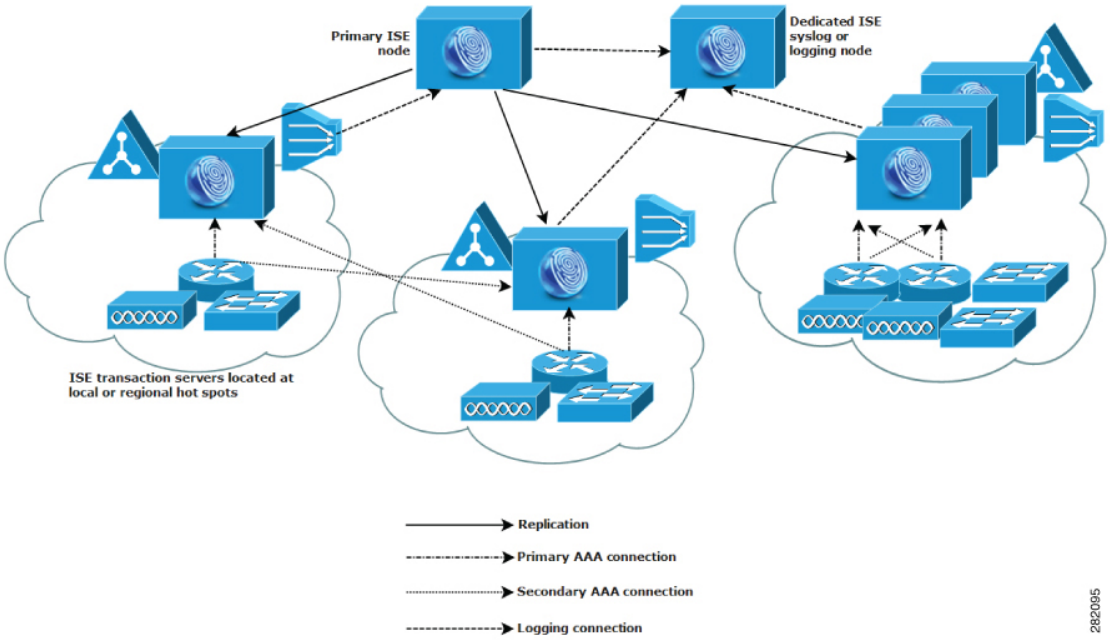


분산 네트워크 구축

분산 Cisco ISE 네트워크 구축은 메인 캠퍼스가 있고 다른 곳에 지역별, 국가별 또는 위성 사업장이 있는 기업에서 가장 효과적입니다. 메인 캠퍼스는 기본 네트워크가 상주하는 곳이며 다른 LAN과 연결됩니다. 크고 작은 다양한 규모이며 여러 지역과 위치의 어플라이언스 및 사용자를 지원합니다.

대형 원격 사이트는 최적의 AAA 성능을 위해 자체적으로 AAA 인프라를 구축하기도 합니다. 중앙 집중식 관리 모델을 통해 일관성 있고 동기화된 AAA 정책을 유지할 수 있습니다. 중앙 집중식 컨피그레이션 모델에서는 기본 Cisco ISE 노드와 보조 Cisco ISE 노드를 사용합니다. 물론 Cisco ISE 노드에서 별도의 모니터링 페르소나를 사용하는 것이 좋지만, 각 원격 위치는 저마다의 고유한 네트워크 요구 사항을 가져야 합니다.

그림 5: 분산 구축



여러 원격 사이트가 있는 네트워크 계획 시 고려 사항

- Microsoft Active Directory, LDAP(Lightweight Directory Access Protocol) 등과 같은 중앙 또는 외부 데이터베이스가 사용되는지 확인합니다. 각 원격 사이트는 외부 데이터베이스의 동기화된 인스턴스를 가져야 합니다. 이는 Cisco ISE에서 AAA 성능 최적화를 위한 액세스에 사용할 수 있습니다.
- AAA 클라이언트의 위치가 중요합니다. Cisco ISE 노드를 AAA 클라이언트와 최대한 가깝게 배치해야 WAN 장애로 인한 액세스 상실 위험 및 네트워크 레이턴시 현상을 줄일 수 있습니다.
- Cisco ISE는 백업과 같은 일부 기능을 위해 콘솔 액세스를 제공합니다. 모든 노드에 네트워크 액세스할 필요 없이 직접적이고 안전한 콘솔 액세스를 지원하도록 각 사이트에서 터미널을 사용하는 것을 고려해보십시오.
- 소규모의 원격 사이트들이 서로 가까이에 있고 안정적인 WAN 연결을 통해 다른 사이트와 연결되는 경우, 이중화를 위해 Cisco ISE 노드 하나를 로컬 사이트용 백업으로 사용하는 것을 고려해보십시오.
- 외부 데이터베이스에 대한 액세스를 보장하기 위해 모든 Cisco ISE 노드에서 DNS(Domain Name System)를 알맞게 구성해야 합니다.

각 구축 모델에 지원되는 최대 세션 수

다음 표에는 각 구축 모델에서 지원되는 최대 세션 수가 나와 있습니다.

표 *1:* 구축 모델별로 지원되는 최대 세션 수

구축 모델	**Platform**(플랫폼)	최대 세션 수
독립형(단일 노드의 모든 페르소나)	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
기본 2 노드 구축(이중화)	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
하이브리드 분산형 구축(동일한 어플라이언스 상의 관리자 및 MnT, 전용 어플라이언스에서의 정책 서비스)	PAN 및 MnT로 3615	10,000
	PAN 및 MnT로 3655	25,000
	PAN 및 MnT로 3695	50,000
	PAN 및 MnT로 3515	7,500
	PAN 및 MnT로 3595	20,000
전용(PAN, MnT, PXG 및 PSN 노드)	PAN 및 MnT로 3595	500,000
	PAN 및 MnT로 3655	500,000
	PAN/MnT로 3695	2,000,000

표 *2: PSN*당 최대 활성 세션 수

PSN[1]	최대 활성 세션 수
SNS 3615	10,000
SNS 3655	50,000

PSN[1]	최대 활성 세션 수
SNS 3695	100,000
SNS 3515	7,500
SNS 3595	40,000

[1] 전용 정책 노드별 확장(총 구축 크기로 제어하는 최대 세션)

SNS 3500/3600 시리즈 어플라이언스의 구축 크기 및 확장 권장 사항

표 *3: SNS 3500/3600* 시리즈 어플라이언스의 최대 *RADIUS* 확장

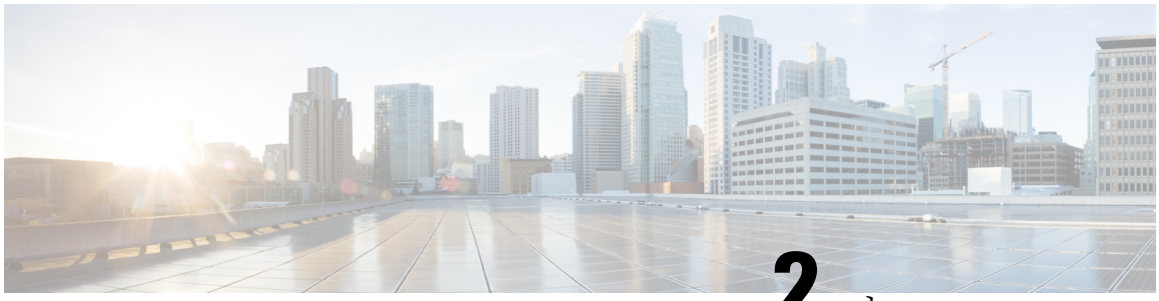
구축 모델	Platform(플랫폼)	최대 전용 PSN 수	구축당 최대 RADIUS 세션 수
독립형	3515	0	7500
	3595	0	20,000
	3615	0	10,000
	3655	0	25,000
	3695	0	50,000
동일한 노드 및 전용 PSN의 PAN 및 MnT	PAN 및 MnT로 3515	6	7,500
	PAN 및 MnT로 3595	6	20,000
	PAN 및 MnT로 3615	6	10,000
	PAN 및 MnT로 3655	6	25,000
	PAN 및 MnT로 3695	6	50,000
전용(PAN, MnT, PXG 및 PSN 노드)	PAN 및 MnT로 3595	50	500,000
	PAN 및 MnT로 3655	50	500,000
	PAN 및 MnT로 3695	50	2,000,000

Cisco ISE 기능을 지원하는 데 필요한 스위치 및 무선 LAN 컨트롤러 컨피그레이션

Cisco ISE와 네트워크 스위치의 상호 운용성을 보장하고 Cisco ISE 기능이 네트워크 세그먼트 전 범위에서 제대로 작동하게 하려면 특정 필수 NTP(Network Time Protocol), RADIUS/AAA, IEEE 802.1X, MAB(MAC Authentication Bypass), 기타 설정으로 네트워크 스위치를 구성해야 합니다.

ISE 커뮤니티 리소스

WLC를 이용한 Cisco ISE 설정 관련 정보는 Cisco ISE with WLC Setup Video(WLC를 이용한 Cisco ISE 설정 비디오)를 참조하십시오.



2 장

SNS 3500/3600 시리즈 어플라이언스 및 가상 머신 요구 사항

하드웨어 및 가상 어플라이언스 요구 사항

Cisco SNS 하드웨어 또는 가상 어플라이언스에 Cisco Identity Services Engine(ISE)를 설치할 수 있습니다. 가상 머신이 Cisco ISE 하드웨어 어플라이언스에 준하는 성능 및 확장성을 제공하려면 Cisco SNS 3500 또는 3600 시리즈 어플라이언스에서와 같은 시스템 리소스가 할당되어야 합니다. 이 섹션에는 Cisco ISE를 설치하는 데 필요한 하드웨어, 소프트웨어 및 가상 머신 요구 사항이 나와 있습니다.

참고 가상 환경을 강화하고 모든 보안 업데이트가 최신 버전인지 확인합니다. Cisco는 하이퍼바이저에서 발견된 보안 문제는 책임지지 않습니다.

Cisco SNS-3500 및 SNS-3600 시리즈 어플라이언스

SNS 하드웨어 어플라이언스 사양은 Cisco Secure Network Server 데이터 시트에 있는 '표 1, 제품 사양'을 참조하십시오.

SNS-3500 시리즈 어플라이언스 관련 정보는 Cisco SNS-3500 시리즈 어플라이언스 하드웨어 설치 설명서를 참조하십시오.

SNS-3600 시리즈 어플라이언스 관련 정보는 Cisco SNS-3600 시리즈 어플라이언스 하드웨어 설치 설명서를 참조하십시오.

VMware 가상 머신 요구 사항

Cisco ISE는 다음 VMware 서버 및 클라이언트를 지원합니다.

- ESXi 5.*x*의 경우 VMware 버전 8(기본값) (최소 5.1 U2)
- ESXi 6.*x*의 경우 VMware 버전 11(기본값)
- ESXi 7.*x*의 경우 VMware 버전 13(기본값)

Cisco ISE는 콜드 VMware vMotion 기능을 지원하므로, (임의의 페르소나를 실행하는) 가상 머신 인스턴스를 호스트 간에 마이그레이션할 수 있습니다. VMware vMotion 기능이 작동하려면 다음 조건을 충족해야 합니다.

- Cisco ISE를 종료하고 전원을 꺼야 합니다. Cisco ISE는 vMotion 중에 데이터베이스 작업을 중지하거나 일시 정지할 수 없습니다. 이 경우 데이터 손상 문제가 발생할 수 있습니다. 따라서 마이그레이션 중에 Cisco ISE가 실행되거나 활성 상태면 안 됩니다.

참고 Cisco ISE VM은 Hot vMotion을 지원하지 않습니다.

VMotion 요구 사항에 관한 자세한 내용은 VMware 설명서를 참조하십시오.

주의 VM에서 스냅샷 기능을 활성화하면 VM 구성이 손상될 수 있습니다. 이 문제가 발생한다면 VM을 다시 설치하고 VM 스냅샷을 비활성화해야 할 수 있습니다.

참고 VMware 스냅샷은 지정된 시점에 VM의 상태를 저장하므로, Cisco ISE는 VMware 스냅샷으로 ISE 데이터를 백업하는 기능은 지원하지 않습니다. 멀티 노드 Cisco ISE 구축에서는 모든 노드의 데이터가 현재의 데이터베이스 정보와 지속적으로 동기화됩니다. 스냅샷을 복원하면, 데이터베이스 복제 및 동기화 문제가 발생할 수 있습니다. 데이터 보관 및 복원을 위해서는 Cisco ISE에 포함된 백업 기능을 사용하는 것이 좋습니다. VMware 스냅샷으로 ISE 데이터를 백업하면, Cisco ISE 서비스가 중지됩니다. ISE 노드를 가져오려면, 재부팅해야 합니다.

Cisco ISE는 VM(가상 머신)에 Cisco ISE를 설치하고 구축할 수 있는 다음과 같은 OVA 템플릿을 제공합니다.

참고 전용 정책 서비스 또는 pxGrid 노드 역할을 하는 Cisco ISE 노드에는 300GB OVA 템플릿으로도 충분합니다.

600GB 및 1.2TB OVA 템플릿은 관리 또는 모니터링 페르소나를 실행하는 ISE 노드의 최소 요구 사항을 충족하는 데 권장됩니다. 디스크 공간 요구 사항 관련 추가 정보는 디스크 공간 요구 사항, 23 페이지 항목을 참조하십시오.

디스크 크기, CPU 또는 메모리 할당을 사용자 지정해야 한다면, 표준 .iso 이미지로 Cisco ISE를 수동으로 구축할 수 있습니다. 하지만 이 문서에 지정된 최소 요구 사항 및 리소스 예약을 반드시 충족해야 합니다. OVA 템플릿은 각 플랫폼에 필요한 최소 리소스를 자동으로 적용하여 ISE 가상 어플라이언스 구축을 간소화 합니다.

- ISE-3.0.0.*xxx*-virtual-SNS3615-SNS3655-300.ova
- ISE-3.0.0.*xxx*-virtual-SNS3615-SNS3655-600.ova
- ISE-3.0.0.*xxx*-virtual-SNS3655-SNS3695-1200.ova
- ISE-3.0.0.*xxx*-virtual-SNS3695-2400.ova

표 ***4: OVA*** 템플릿 예약

OVA 템플릿 유형	**CPU** 수	**CPU** 예약 **(MHz)**	메모리 **(GB)**	메모리 예약 **(GB)**
평가	4	예약 없음	16	예약 없음
소형	16	16,000	32	32
중간	24	24,000	96	96
대규모	24	24,000	256	256

다음 표에는 VMware 가상 머신 요구 사항이 나와 있습니다.

표 *5: VMware* 가상 머신 요구 사항

요구 사항 유형	사양
CPU	• 평가 • 클럭 속도: 2.0 GHz 이상 • CPU 코어 수: CPU 코어 4개 • 프로덕션 • 클럭 속도: 2.0 GHz 이상 • 코어 수: • **SNS 3600** 시리즈 어플라이언스**:** • 소형: 16 • 중형: 24 • 대형: 24 참고 코어 수는 하이퍼 스레딩으로 인해 Cisco Secure Network Server 3600 시리즈에 해당하는 것의 두 배입니다. 예를 들어 소규모 네트워크 구축의 경우 CPU 사양이 8개이거나 스레드가 16개인 SNS 3615의 CPU 사양을 충족하도록 16개의 vCPU 코어를 할당해야 합니다.
메모리	• 평가: 16GB • 프로덕션 • 소형: SNS 3615의 경우 32GB • 중형: SNS 3655의 경우 96GB • 대형: 256GB

요구 사항 유형	사양
하드 디스크	• 평가: 300GB • 프로덕션 300GB~2.4TB 디스크 스토리지(크기는 구축 및 작업에 따라 달라짐) 디스크 공간 요구 사항 링크를 이용해 VM에 권장되는 디스크 공간을 확인하십시오. VM 호스트 서버에서 속도가 10,000RPM 이상인 하드 디스크를 사용하는 것이 좋습니다. 참고 Cisco ISE용 가상 머신을 생성할 때는 스토리지 요구 사항에 부합하는 단일 가상 디스크를 사용해야 합니다. 둘 이상의 가상 디스크를 사용하여 디스크 공간 요구 사항을 충족할 경우 설치 프로그램에서 일부 디스크 공간을 인식하지 못할 수 있습니다.
스토리지 및 파일 시스템	Cisco ISE 가상 어플라이언스용 스토리지 시스템은 초당 50MB의 최소 쓰기 성능과 초당 300MB의 읽기 성능을 요구합니다. 이러한 성능 기준을 충족 하고 VMware 서버에서 지원되는 스토리지 시스템을 구축해야 합니다. Cisco ISE는 Cisco ISE 설치 전후 및 설치 과정에서 스토리지 시스템이 이러한 최소 요구 사항을 충족 하는지 확인하는 다양한 방법을 제공합니다. 자세한 내용은 가상 머신 리소스 및 성능 확인, 37 페이지를 참조하십시오. VMFS 파일 시스템은 철저한 테스트를 거치므로 사용을 권장하지만, 위의 요구 사항을 충족한다면 다른 파일 시스템, 전송 및 미디어를 구축해도 됩니다.
디스크 컨트롤러	Paravirtual 또는 LSI Logic Parallel 최상의 성능과 이중화를 위해 캐싱 RAID 컨트롤러를 권장합니다. 예를 들어 RAID 10(1+0라고도 함) 같은 컨트롤러 옵션은 RAID 5 보다 전체적인 쓰기 성능 및 이중화 수준이 우수합니다. 배터리 전원 컨트롤러 캐시도 쓰기 작업을 크게 개선할 수 있습니다. 참고 ISE VM의 디스크 SCSI 컨트롤러를 다른 유형에서 VMware Paravirtual로 업데이트하면 부팅되지 않을 수 있습니다.
NIC	NIC 인터페이스 1개가 필요합니다(권장 사항은 NIC 2개 이상이며, NIC는 6개까지 지원됩니다). Cisco ISE는 E1000 및 VMXNET3 어댑터를 지원합니다. 참고 기본적으로 올바른 어댑터 순서를 보장하기 위해 E1000을 선택하는 것이 좋습니다. VMXNET3를 선택할 경우 ESXi 어댑터를 다시 매핑하여 ISE 어댑터 순서와 동기화하는 작업이 필요할 수 있습니다.

요구 사항 유형	사양
VMware 가상 하드웨어 버전/하이퍼바이저	ESXi 5.*x*(5.1 U2 최소) 및 6.*x*의 경우 VMware 가상 머신 하드웨어 버전 8 이상.

Linux KVM 요구 사항

표 ***6: Linux KVM*** 가상 머신 요구 사항

요구 사항 유형	최소 요구 사항
CPU	• 평가 • 클럭 속도: 2.0 GHz 이상 • 코어 수: CPU 코어 4개 • 프로덕션 • 클럭 속도: 2.0 GHz 이상 • 코어 수: • **SNS 3600** 시리즈 어플라이언스: • 소형: 16 • 중형: 24 • 대형: 24 참고 코어 수는 하이퍼 스레딩으로 인해 Cisco Secure Network Server 3600 시리즈에 해당하는 것의 두 배입니다. 예를 들어 소규모 네트워크 구축의 경우 CPU 사양이 8개이거나 스레드가 16개인 SNS 3615의 CPU 사양을 충족하도록 16개의 vCPU 코어를 할당해야 합니다.

요구 사항 유형	최소 요구 사항

메모리	• 평가: 16GB
	• 프로덕션
	  • 소형: SNS 3615의 경우 32GB
	  • 중형: SNS 3655의 경우 96GB
	  • 대형: 256GB

하드 디스크	• 평가: 300GB • 프로덕션 300GB~2.4TB 디스크 스토리지(크기는 구축 및 작업에 따라 달라짐) 디스크 공간 요구 사항 링크를 이용해 VM에 권장되는 디스크 공간을 확인하십시오. VM 호스트 서버에서 속도가 10,000RPM 이상인 하드 디스크를 사용하는 것이 좋습니다. 참고 Cisco ISE용 가상 머신을 생성할 때는 스토리지 요구 사항에 부합하는 단일 가상 디스크를 사용해야 합니다. 둘 이상의 가상 디스크를 사용하여 디스크 공간 요구 사항을 충족할 경우 설치 프로그램에서 일부 디스크 공간을 인식하지 못할 수 있습니다.
KVM 디스크 장치	디스크 버스 - virtio, 캐시 모드 - 없음, I/O 모드 - 기본 Preallocated RAW 스토리지 형식을 사용합니다.
NIC	NIC 인터페이스 1개가 필요합니다(권장 사항은 NIC 2개 이상이며, NIC는 6개까지 지원됩니다). Cisco ISE는 VirtIO 드라이버를 지원합니다. 더 나은 성능을 위해 VirtIO 드라이버를 권장합니다.
하이퍼바이저	QEMU 1.5.3-160상의 KVM

Microsoft Hyper-V 요구 사항

표 *7: Microsoft Hyper-V* 가상 머신 요구 사항

요구 사항 유형	최소 요구 사항
CPU	• 평가 • 클럭 속도: 2.0 GHz 이상 • 코어 수: CPU 코어 4개 • 프로덕션 • 클럭 속도: 2.0 GHz 이상 • 코어 수: • **SNS 3600** 시리즈 어플라이언스: • 소형: 16 • 중형: 24 • 대형: 24 참고 코어 수는 하이퍼 스레딩으로 인해 Cisco Secure Network Server 3600 시리즈에 해당하는 것의 두 배입니다. 예를 들어 소규모 네트워크 구축의 경우 CPU 사양이 8개이거나 스레드가 16개인 SNS 3615의 CPU 사양을 충족하도록 16개의 vCPU 코어를 할당해야 합니다.
메모리	• 평가: 16GB • 프로덕션 • 소형: SNS 3615의 경우 32GB • 중형: SNS 3655의 경우 96GB • 대형: 256GB

요구 사항 유형	최소 요구 사항
하드 디스크	• 평가: 300GB • 프로덕션 300GB~2.4TB 디스크 스토리지(크기는 구축 및 작업에 따라 달라짐) 디스크 공간 요구 사항 링크를 이용해 VM에 권장되는 디스크 공간을 확인하십시오. VM 호스트 서버에서 속도가 10,000RPM 이상인 하드 디스크를 사용하는 것이 좋습니다. 참고 Cisco ISE용 가상 머신을 생성할 때는 스토리지 요구 사항에 부합하는 단일 가상 디스크를 사용해야 합니다. 둘 이상의 가상 디스크를 사용하여 디스크 공간 요구 사항을 충족할 경우 설치 프로그램에서 일부 디스크 공간을 인식하지 못할 수 있습니다.
NIC	NIC 인터페이스 1개가 필요합니다(권장 사항은 NIC 2개 이상이며, NIC는 6개까지 지원됩니다).
하이퍼바이저	Hyper-V(Microsoft)

VMware Cloud on AWS(Amazon Web Services) 및 AVS(Azure VMware Solution)의 VMware 클라우드에서 Cisco ISE 지원

VMware 클라우드에 Cisco ISE를 설치하는 프로세스는 VMware 가상 컴퓨터에 Cisco ISE를 설치하는 프로세스와 정확히 동일합니다.

- AWS(Amazon Web Services)의 VMware Cloud에 구축되니 Cisco ISE 가상 컴퓨터: Cisco Cloud가 AWS에서 제공하는 SDDC(Software Defined Data Center)에서 Cisco ISE를 호스팅할 수 있습니다. 온프레미스 구축, 필수 디바이스 및 서비스에 연결할 수 있도록, VMware Cloud(**Networking and Security(**네트워킹 및 보안**) > Security(**보안**) > Gateway Firewall Settings(**게이트웨이 방화벽 설정**))**에 적절한 보안 그룹 정책을 구성해야 합니다.
- Azure VMware 솔루션(AVS)에 구축된 Cisco ISE 가상 컴퓨터: AVS는 기본적으로 Cisco ISE를 VMware 가상 컴퓨터로 호스팅할 수 있는 Microsoft Azure에서 VMware 워크로드를 실행합니다.

가상 머신 어플라이언스 크기 권장 사항

모니터링 노드용 대형 VM은 Cisco ISE 2.4에서 도입되었습니다. 대형 VM에 모니터링 페르소나를 구축하면 실시간 로그 쿼리 및 보고 완료에 대한 응답이 빨라져 성능이 개선됩니다.

참고 이 폼 팩터는 릴리스 2.4 이상에서 VM으로만 사용할 수 있으며, 대형 VM 라이센스가 필요합니다.

가상 머신(VM) 어플라이언스 사양은 프로덕션 환경에서 실행되는 물리적 어플라이언스에 필적해야 합니다. 다음 표에서는 SNS 3500 또는 SNS 3600 물리적 어플라이언스와 비슷하도록 가상 어플라이언스의 크기를 조정하는 데 필요한 최소 리소스를 확인할 수 있습니다.

어플라이언스를 위한 리소스를 할당할 때 다음 지침을 기억하십시오.

- 지정된 리소스를 할당하지 못하면 성능이 저하되거나 서비스 장애가 발생할 수 있습니다. 전용 VM 리소스를 구축하고, 여러 게스트 VM 간에 리소스를 공유하거나 초과 구독하지는 않는 것이 좋습니다. OVF 템플릿을 사용하여 Cisco ISE 가상 어플라이언스를 구축하면 각 VM에 적절한 리소스가 할당됩니다. OVF 템플릿을 사용하지 않는다면, ISO 이미지를 사용하여 Cisco ISE를 수동으로 설치할 때 상승하는 리소스 예약을 할당하는지 확인하십시오.

  참고 권장 예약 없이 Cisco ISE를 수동으로 구축하기로 했다면, 본인이 직접 어플라이언스의 리소스 사용을 면밀하게 모니터링하고 필요하다면 리소스를 늘려야 Cisco ISE 구축의 적절한 상태와 작동을 보장할 수 있습니다.

  참고 OVF 템플릿은 Linux KVM에는 적용되지 않습니다. 시스템 템플릿 템플릿은 VMware 가상 머신에만 사용할 수 있습니다.

- 설치에 OVA 템플릿을 사용한다면, 설치 완료 후 다음 설정을 확인합니다.
  - Cisco ISE 구축이 적절한 상태를 유지하고 올바르게 작동하도록 하려면 CPU/메모리 **Reservation(**예약**)** 필드 (**Edit Settings(**설정 수정**)** 창의 **Virtual Hardware(**가상 하드웨어**)** 탭 아래) VMware 가상 머신 요구 사항, 14 페이지 섹션에 지정된 리소스 예약을 할당해야 합니다.
  - (**Edit Settings(**설정 수정**)** 창의 **Virtual Hardware(**가상 하드웨어**)** 탭에 있는) **CPU Limit(CPU** 제한**)** 필드에 있는 CPU 사용량이 **Unlimited(**무제한**)**으로 설정되어 있는지 확인합니다. CPU 사용량 제한 설정(예: CPU 사용량 제한을 12000MHz로 설정)은 시스템 성능에 영향을 미칩니다. 제한을 설정했다면 VM 클라이언트를 종료하고, 제한을 제거한 다음 VM 클라이언트를 다시 시작해야 합니다.
  - (**Edit Settings(**설정 수정**)** 창의 **Virtual Hardware(**가상 하드웨어**)** 탭에 있는) **Memory Limit(**메모리 제한**)** 필드에 있는 메모리 사용량이 **Unlimited(**무제한**)**으로 설정되어 있는지 확인합니다. 메모리 사용량 제한 설정(예: 제한을 12000MB로 설정)은 시스템 성능에 영향을 미칩니다.
  - (**Edit Settings(**설정 수정**)** 창의 **Virtual Hardware(**가상 하드웨어**)** 탭에 있는) **Shares(**공유**)** 옵션이 **Hard Disk(**하드 디스크**)** 영역에서 **High(**높음**)**으로 설정되어 있는지 확인합니다.

관리자 및 MnT 노드는 디스크 사용량에 크게 의존합니다. 공유 디스크 스토리지 VMware 환경을 사용하면 디스크 성능에 영향을 줄 수 있습니다. 노드의 성능을 높이려면 노드에 할당된 디스크 공유의 수를 늘려야 합니다.

- VM의 정책 서비스 노드는 관리 또는 모니터링 노드보다 적은 디스크 공간으로 구축할 수 있습니다. 프로덕션 Cisco ISE 노드의 최소 디스크 공간은 300GB입니다. 다양한 Cisco ISE 노드 및 페르소나에 필요한 디스크 공간에 관한 자세한 내용은 디스크 공간 요구 사항, 23 페이지 항목을 참조하십시오.
- VM은 NIC 1~6개로 구성할 수 있습니다. 2개 이상의 NIC를 허용하는 것이 좋습니다. 추가 인터페이스를 사용하여 프로파일링, 게스트 서비스나 RADIUS 같은 여러 서비스를 지원할 수 있습니다.

참고 VM의 RAM 및 CPU 조정에는 이미지를 다시 설치할 필요가 없습니다.

디스크 공간 요구 사항

다음 표에서는 프로덕션 구축에서 가상 머신을 실행할 때 권장되는 Cisco ISE 디스크 공간을 알려줍니다.

참고 2TB 이상의 GPT 파티션으로 부팅하려면 VM 설정의 부팅 모드에서 펌웨어를 **BIOS**에서 **EFI**로 변경해야 합니다.

표 ***8:*** 가상 머신에 권장되는 디스크 공간

Cisco ISE 페르소나	평가용 최소 디스크 공간	프로덕션용 최소 디스크 공간	프로덕션을 위한 권장 디스크 공간	최대 디스크 공간
독립형 Cisco ISE	300GB	600GB	600GB~2.4TB	2.4TB
분산형 Cisco ISE, 관리 전용	300GB	600GB	600GB	2.4TB
분산형 Cisco ISE, 모니터링 전용	300GB	600GB	600GB~2.4TB	2.4TB
분산형 Cisco ISE, 정책 서비스 전용	300GB	300 GB	300 GB	2.4TB
분산형 Cisco ISE, pxGrid 전용	300GB	300 GB	300 GB	2.4TB

Cisco ISE 페르소나	평가용 최소 디스크 공간	프로덕션용 최소 디스크 공간	프로덕션을 위한 권장 디스크 공간	최대 디스크 공간
분산형 Cisco ISE, 관리 및 모니터링(선택 사항으로 pxGrid도 가능)	300GB	600GB	600GB~2.4TB	2.4TB
분산형 Cisco ISE, 관리, 모니터링 및 정책 서비스(선택 사항으로 pxGrid도 가능)	300GB	600GB	600GB~2.4TB	2.4TB

참고 기본 관리 노드가 일시적으로 모니터링 노드가 된다면, 추가 디스크 공간이 있어야 업그레이드 중에 로컬 디버그 로그와 준비 파일을 저장하고 로그 데이터를 처리할 수 있습니다.

디스크 공간 지침

Cisco ISE를 위한 디스크 공간을 결정할 때 다음 지침을 기억하십시오.

- Cisco ISE는 가상 머신에서 단일 디스크에 설치해야 합니다.
- 디스크 할당량은 로깅 보존 요구 사항에 따라 달라집니다. 모니터링 페르소나가 활성화된 노드에서 VM 디스크 공간의 60%는 로그 저장 용도로 할당됩니다. 25,000개 엔드포인트로 구성된 구축에서 1일 약 1GB의 로그가 생성됩니다.

  예를 들어 모니터링 노드가 600GB VM 디스크 공간을 사용할 경우 로그 저장용으로 360GB가 할당됩니다. 엔드포인트 100,000개가 이 네트워크에 매일 연결되는 경우 매일 약 4GB의 로그가 생성됩니다. 이러한 경우 모니터링 노드에서 76일분의 로그를 저장할 수 있습니다. 38일이 경과하면 오래된 데이터를 리포지토리로 전송하고 모니터링 데이터베이스에서는 삭제해야 합니다.

추가 로그 저장소를 확보하기 위해 VM 디스크 공간을 늘릴 수 있습니다. 100GB 디스크 공간을 추가할 때마다 로그 저장용으로 60GB가 추가되는 셈입니다.

최초 설치 후 가상 머신의 디스크 크기를 늘리는 경우에는 가상 머신에 Cisco ISE를 새로 설치해야 전체 디스크 할당을 올바르게 탐지하고 활용할 수 있습니다.

아래 표에는 할당된 디스크 공간 및 네트워크에 연결된 엔드포인트 수를 기준으로 모니터링 노드에서 며칠 분의 RADIUS 로그를 보존할 수 있는지가 나와 있습니다. 이 숫자는 로깅 억제가 활성화된 엔드포인트별로 하루에 10개 이상의 인증을 사용한다는 가정에 따른 결과입니다.

표 ***9:*** 모니터링 노드 로그 저장소—***RADIUS*** 보관 기간***(***일***)***

엔드포인트 수	**300GB**	**600GB**	**1024GB**	**2048GB**
5,000	504	1510	2577	5154
10,000	252	755	1289	2577

엔드포인트 수	300GB	600GB	1024GB	2048GB
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

아래 표에는 할당된 디스크 공간 및 네트워크에 연결된 엔드포인트 수를 기준으로 모니터링 노드에서 며칠 분의 TACACS+ 로그를 보존할 수 있는지가 나와 있습니다. 이 숫자는 스크립트가 모든 NAD, 매일 세션 4개, 세션별 명령 5개를 기준으로 실행된다는 가정에 따른 결과입니다.

표 ***10:*** 모니터링 노드 로그 저장소—***TACACS+*** 보관 기간***(***일***)***

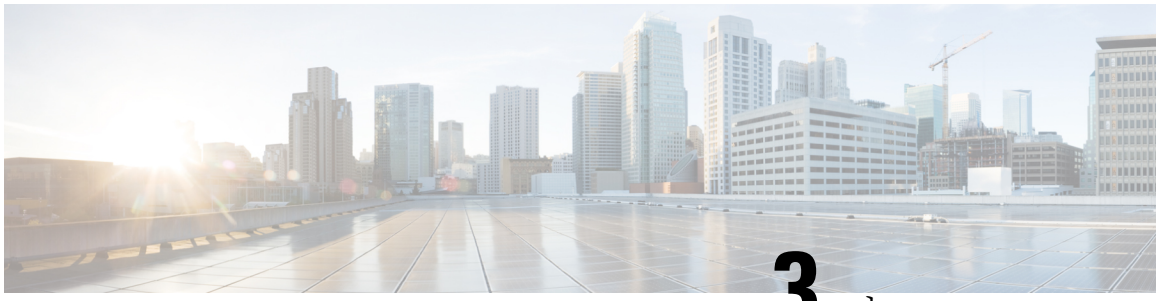
엔드포인트 수	300GB	600GB	1024GB	2048GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3775	6443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

디스크 크기 증가

상황 및 가시성 속도가 느리거나 로그용 공간이 부족하다면 추가 디스크 공간을 할당해야 합니다.

추가 로그 저장소 계획을 위해 100GB 디스크 공간을 추가할 때마다 60GB 로그 저장소를 사용할 수 있습니다.

ISE가 새 디스크 할당을 탐지하고 활용하려면 노드를 등록 취소하고, VM 설정을 업데이트하고, ISE를 다시 설치해야 합니다. 이 작업을 수행하는 한 가지 방법은 새 대형 노드에 ISE를 설치하고 해당 노드를 구축에 고가용성으로 추가하는 것입니다. 노드가 동기화되면 새 VM을 기본으로 설정하고 원래 VM을 등록 취소합니다.



3 장

Cisco ISE 설치

CIMC를 사용하여 Cisco ISE 설치

이 섹션에는 Cisco ISE를 신속하게 설치할 수 있는 고수준 설치 단계가 나와 있습니다.

시작하기 전에

- 이 가이드에 지정된 하드웨어 및 가상 어플라이언스 요구 사항을 충족했는지 확인합니다.
- (선택 사항: 가상 머신에 Cisco ISE를 설치하는 경우에만 필요) 가상 머신을 올바르게 생성했는지 확인합니다. 자세한 내용은 다음 항목을 참고하십시오.
  - VMware 서버 구성, 39 페이지
  - KVM에 Cisco ISE 설치, 50 페이지
  - Hyper-v에서 Cisco ISE 가상 머신 생성, 52 페이지
- (선택 사항: SNS 하드웨어에 Cisco ISE를 설치하는 경우에만 필요) 어플라이언스 관리및 BIOS 구성을 위해 CIMC(Cisco Integrated Management Interface) 구성 유틸리티를 설정합니다. 자세한 내용은 다음 문서를 참조하십시오.
  - SNS 3500 시리즈 어플라이언스 관련 정보는 Cisco SNS-3500 시리즈 어플라이언스 하드웨어 설치 설명서를 참조하십시오.
  - SNS-3600 시리즈 어플라이언스 관련 정보는 Cisco SNS-3600 시리즈 어플라이언스 하드웨어 설치 설명서를 참조하십시오.

단계 **1** Cisco ISE를 다음에 설치한다면,

- Cisco SNS 어플라이언스: 하드웨어 어플라이언스를 설치합니다. 서버 관리를 위해 CIMC에 연결합니다.

- 가상 머신: VM이 올바르게 구성되었는지 확인합니다.

단계 **2** Cisco ISE ISO 이미지를 다운로드합니다.

a) http://www.cisco.com/go/ise로 이동합니다. 이 링크에 액세스하려면 유효한 Cisco.com 로그인 인증서가 있어야 합니다.

b) **Download Software for this Product**를 클릭합니다.

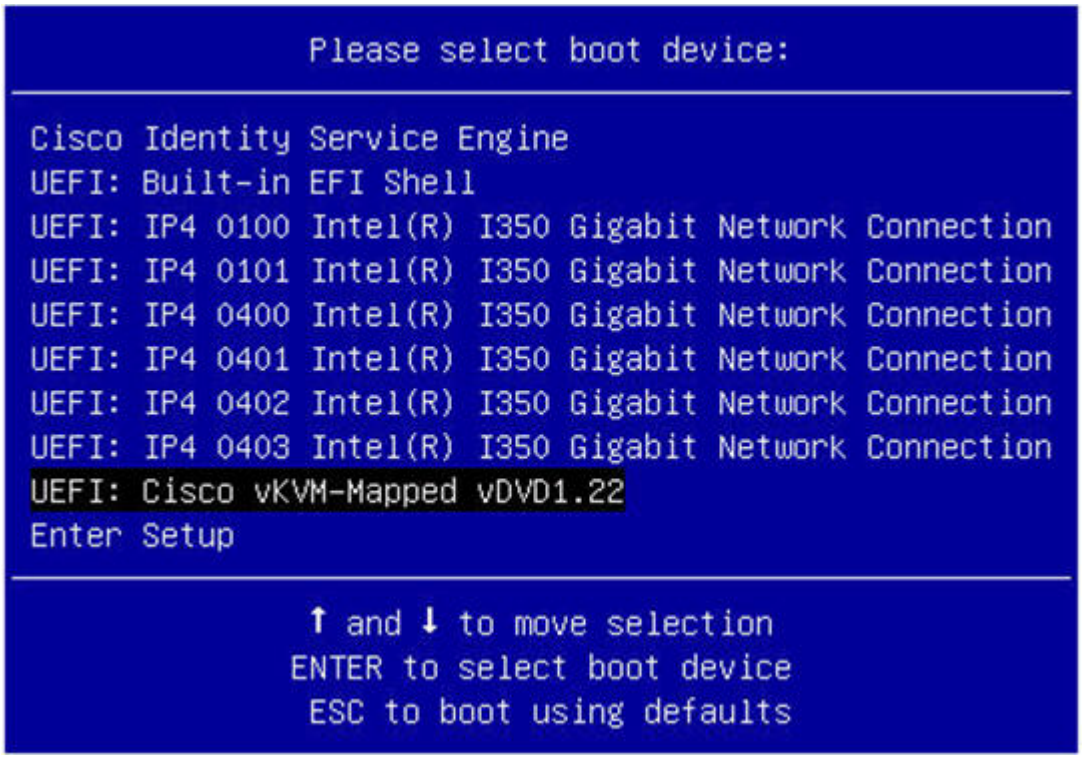
Cisco ISE 이미지는 90일 평가판 라이센스가 설치된 상태로 제공되므로 설치 및 초기 컨피그레이션이 완료되면 즉시 모든 Cisco ISE 서비스를 테스트해볼 수 있습니다.

단계 **3** 어플라이언스 또는 가상 머신을 부팅합니다.

- Cisco SNS 어플라이언스:

1. CIMC에 연결하고 CIMC 자격 증명을 사용하여 로그인합니다.
2. KVM 콘솔을 실행합니다.
3. Virtual Media(가상 미디어) > Activate Virtual Devices(가상 장치 활성화)를 선택합니다.
4. Virtual Media(가상 미디어) > Map CD/DVD(CD/DVD 매핑)를 선택하고 ISE ISO 이미지를 선택한 다음 Map Device(장치 매핑)를 클릭합니다.
5. ISE ISO 이미지로 어플라이언스를 부팅하도록 Macros(매크로) > Static Macros(정적 매크로) > Ctrl-Alt-Del을 선택합니다.
6. F6을 눌러 부팅 메뉴를 시작합니다. 다음과 비슷한 화면이 나타납니다.

그림 *6:* 부팅 디바이스 선택



참고 물리적 액세스 권한이 없고 원격 서버에서 CIMC 설치를 수행해야 하는 원격 위치(예: 데이터 센터)에 SNS 어플라이언스를 배치해야 한다면, 설치 시간이 오래 걸릴 수 있습니다. USB 드라이브에 ISO 파일을 복사하고 원격 위치에서 사용하여 설치 프로세스 속도를 높이는 방법을 권장합니다.

- 가상 머신:

1. CD/DVD를 ISO 이미지에 매핑합니다. 다음과 비슷한 화면이 나타납니다. 다음 메시지 및 설치 메뉴가 표시됩니다.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 3.0.0.xxx


Available boot options:

Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

단계 **4** 부팅 프롬프트에서 **1**을 누르고 **Enter**를 눌러 직렬 콘솔로 Cisco ISE를 설치합니다.

키보드 및 모니터를 사용하고 싶다면 화살표 키를 사용하여 **Cisco ISE** 설치**(**키보드/모니터**)** 옵션을 선택합니다. 다음 메시지가 나타납니다.

```
*******************************************
Please type 'setup' to configure the appliance
*******************************************
```

단계 **5** 프롬프트에서 **setup**을 입력하여 Setup(설정) 프로그램을 시작합니다. Setup(설정) 프로그램 매개 변수에 관한 자세한 내용은 설정 프로그램 실행, 30 페이지 항목을 참조하십시오.

단계 **6** Setup(설정) 모드에서 네트워크 구성 매개 변수를 입력하면, 어플라이언스는 자동으로 재부팅된 후 셸 프롬프트 모드로 돌아갑니다.

단계 **7** 셸 프롬프트 모드를 종료합니다. 어플라이언스가 작동합니다.

단계 **8** 설치 프로세스 확인, 33 페이지를 계속 진행합니다.

설정 프로그램 실행

이 섹션에서는 ISE 서버를 구성하는 설정 프로세스를 설명합니다.

설정 프로그램은 필수 매개 변수를 입력하라는 메시지를 표시하는 대화형 CLI(command-line interface)를 시작합니다. 관리자는 콘솔이나 단순 단말기를 사용하여 초기 네트워크 설정을 구성하고, 설정 프로그램을 사용하는 ISE 서버에 초기 관리자 자격 증명을 제공합니다. 이 설정 프로세스는 일회성 구성 작업입니다.

참고 Active Directory(AD)와 통합하는 경우에는 ISE용으로 특별히 생성한 전용 사이트의 IP 및 서브넷 주소를 사용하는 것이 가장 좋습니다. 설치 및 구성 전에 AD를 담당하는 조직 내 직원에게 문의하여 ISE 노드용 관련 IP 및 서브넷 주소를 검색하십시오.

참고 시스템이 불안정해질 수 있으므로 Cisco ISE의 오프라인 설치 시도는 권장하지 않습니다. Cisco ISE 설치 스크립트를 오프라인으로 실행하면 다음 오류가 표시됩니다.

'NTP 서버와의 동기화 실패**'** 잘못된 시간을 사용하면 다시 설치할 때까지 시스템을 사용하지 못하게 될 수도 있습니다**. Retry?(**다시 시도하시겠습니까**?) Y/N [Y]:**

설치를 계속 진행하려면 **Yes(**예**)**를 선택합니다. NTP 서버와의 동기화를 다시 시도하려면 **No(**아니요**)**를 선택합니다.

설치 스크립트를 실행하는 동안 NTP 서버 및 DNS 서버 모두에 네트워크 연결을 설정하는 것이 좋습니다.

설정 프로그램 실행 방법

단계 **1** 설치용으로 지정된 어플라이언스를 켭니다.

설정 프롬프트가 나타납니다.

```
Please type 'setup' to configure the appliance
localhost login:
```

단계 **2** 로그인 프롬프트에서 **setup**를 입력하고 **Enter**를 누릅니다.

콘솔에 매개 변수 집합이 표시됩니다. 다음 표에 설명된 대로 매개 변수 값을 입력해야 합니다.

참고 IPv6 주소를 사용하여 도메인 이름 서버 또는 NTP 서버를 추가하려면 ISE의 eth0 인터페이스를 IPv6 주소를 이용해 정적으로 구성해야 합니다.

표 ***11: Cisco ISE*** 설정 프로그램 매개변수

프롬프트	설명	예
Hostname	19자를 초과하면 안 됩니다. 영숫자(A–Z, a–z, 0–9)와 하이픈(-)을 사용할 수 있습니다. 문자로 시작해야 합니다. 참고 인증서 기반 검증의 사소한 차이 때문에 Cisco ISE의 인증서 인증이 영향을 받지 않도록 소문자를 사용하는 것이 좋습니다. 노드의 호스트 이름으로 "localhost"를 사용할 수 없습니다.	isebeta1
(eth0) Ethernet interface address	기가비트 이더넷 0(eth0) 인터페이스를 위한 유효 IPv4 또는 Global IPv6 주소여야 합니다.	10.12.13.14/2001:420:54ff: 4:: 458:121:119
Netmask	유효한 IPv4또는 IPv6 넷마스크여야 합니다.	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
기본 게이트웨이	기본 게이트웨이를 위한 유효한 IPv4 또는 Global IPv6 주소여야 합니다.	10.12.13.1/ 2001:420:54ff:4::458:1
DNS domain name	IP 주소가 되어서는 안 됩니다. ASCII 문자, 임의의 숫자, 하이픈(-), 마침표(.) 등을 사용할 수 있습니다.	example.com
Primary name server	기본 이름 서버를 위한 유효 IPv4 또는 Global IPv6 주소여야 합니다.	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	기본 이름 서버를 위한 유효 IPv4 또는 Global IPv6 주소여야 합니다.	(선택 사항) 여러 이름 서버를 구성할 수 있습니다. 그러기 위해서는 **y**를 입력하여 계속합니다.

프롬프트	설명	예
Primary NTP server	NTP(Network Time Protocol) 서버의 유효한 IPv4 또는 Global IPv6 주소나 호스트 이름이어야 합니다. 참고 기본 NTP 서버에 연결할 수 있는지 확인합니다.	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
다른 **NTP** 서버 추가/수정	유효한 NTP 도메인이어야 합니다.	(선택 사항) 여러 NTP 서버를 구성할 수 있습니다. 그러기 위해서는 **y**를 입력하여 계속합니다.
System Time Zone	유효한 표준 시간대여야 합니다. 예를 들어 태평양 표준시(PST)의 경우 System Time Zone은 PST8PDT 또는 Coordinated Universal Time (UTC) minus 8 hours입니다. 참고 시스템 시간과 표준 시간대가 CIMC 또는 하이퍼바이저 호스트 OS 시간 및 시간대와 일치하는지 확인합니다. 표준 시간대가 일치하지 않는다면 시스템 성능이 영향받을 수 있습니다. Cisco ISE CLI에서 **show timezones** 명령을 실행하면 지원되는 표준 시간대의 전체 목록을 볼 수 있습니다. 참고 모든 Cisco ISE 노드를 UTC 표준 시간대로 설정하는 것이 좋습니다. 이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서, 로그, 포스처 에이전트 로그 파일의 타임스탬프가 항상 동기화됩니다.	UTC(기본값)
Username(사용자 이름**)**	Cisco ISE 시스템에 대한 CLI 액세스에 사용되는 관리자 사용자 이름입니다. 기본값(admin)을 사용하지 않으려면 새 사용자 이름을 만들어야 합니다. 사용자 이름은 3~8자이고 유효한 영숫자(A~Z, a~z, 0~9)로 구성되어야 합니다.	admin(기본값)

프롬프트	설명	예
비밀번호	Cisco ISE 시스템에 대한 CLI 액세스에 사용되는 관리자 비밀번호입니다. 기본 암호가 없으므로 계속 진행하려면 암호를 만들어야 합니다. 비밀번호는 6자 이상이고 소문자(a–z), 대문자(A–Z), 숫자(0–9)를 각각 하나 이상 포함해야 합니다.	MyIseYPass2

참고 CLI에서의 설치 중 또는 설치 후에 관리자용 암호를 만들 때는 암호에 $ 문자는 사용하면 안 됩니다. 단, 암호의 마지막 문자로는 사용할 수 있습니다. 이 문자가 첫 번째 또는 중간 위치에 온다면 암호는 수락되지만 CLI에 로그인하는 데 사용할 수는 없습니다.

실수로 이러한 암호를 생성했다면, 콘솔에 로그인하여 CLI 명령을 사용하거나 ISE CD 또는 ISO 파일을 가져와 암호를 재설정하면 됩니다. ISO 파일을 사용하여 암호를 재설정하는 방법은 다음 문서에서 설명합니다. https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

설정 프로그램이 실행되면 시스템이 자동으로 재부팅됩니다.

이제 설정 프로세스 중에 구성한 사용자 이름과 암호를 사용하여 Cisco ISE에 로그인할 수 있습니다.

설치 프로세스 확인

설치 프로세스를 올바르게 완료했는지 확인하려면 다음을 수행합니다.

단계 **1** 시스템이 재부팅되면 설정 중에 구성한 사용자 이름을 로그인 프롬프트에 입력하고 **Enter**를 누릅니다.

단계 **2** 새 비밀번호를 입력합니다.

단계 **3** **show application** 명령을 입력하여 애플리케이션을 제대로 설치했는지 확인하고 **Enter**를 누릅니다.
콘솔에 다음과 같이 표시됩니다.

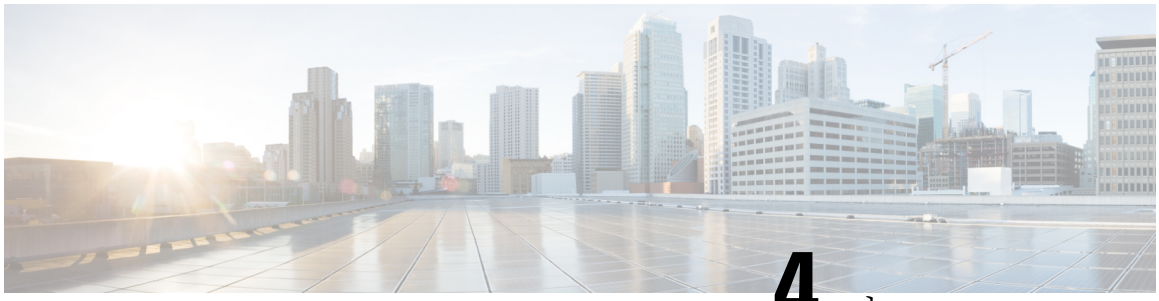
```
ise/admin# show application
<name>          <Description>
ise             Cisco Identity Services Engine
```

참고 버전 및 날짜는 이 릴리스의 버전에 따라 다를 수 있습니다.

단계 **4** **show application status ise** 명령을 입력하여 ISE 프로세스의 상태를 확인한 후 **Enter**를 누릅니다.
콘솔에 다음과 같이 표시됩니다.

```
ise/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          14890
Database Server                        running          70 PROCESSES
```

```
Application Server                      running          19158
Profiler Database                       running          16293
ISE Indexing Engine                     running          20773
AD Connector                            running          22466
M&T Session Database                    running          16195
M&T Log Collector                       running          19294
M&T Log Processor                       running          19207
Certificate Authority Service           running          22237
EST Service                             running          29847
SXP Engine Service                      disabled
Docker Daemon                           running          21197
TC-NAC Service                          disabled
Wifi Setup Helper Container             not running
pxGrid Infrastructure Service           disabled
pxGrid Publisher Subscriber Service     disabled
pxGrid Connection Manager               disabled
pxGrid Controller                       disabled
PassiveID WMI Service                   disabled
PassiveID Syslog Service                disabled
PassiveID API Service                   disabled
PassiveID Agent Service                 disabled
PassiveID Endpoint Service              disabled
PassiveID SPAN Service                  disabled
DHCP Server (dhcpd)                     disabled
DNS Server (named)                      disabled

ise/admin#
```



4 장

추가 설치 정보

SNS 어플라이언스 참조

Cisco ISE 설치용 부팅 가능 USB 장치 생성

LiveUSB-creator 도구를 사용하여 Cisco ISE 설치 ISO 파일에서 부팅 가능한 USB 장치를 만듭니다.

시작하기 전에

- 다음 위치에서 LiveUSB-creator를 로컬 시스템 https://github.com/lmacken/liveusb-creator/releases/tag/3.12.0에 다운로드합니다.
- Cisco ISE 설치 ISO 파일을 로컬 시스템에 다운로드합니다.
- 16GB 또는 32GB USB 디바이스를 사용합니다.

단계 **1** FAT16 또는 FAT32로 USB 장치를 다시 포맷하면 전체 공간을 비웁니다.

단계 **2** USB 장치를 로컬 시스템에 연결하고 **LiveUSB-creator**를 실행합니다.

단계 **3** **Use existing Live CD(**기존 라이브 **CD** 사용**)** 영역에서 **Browse(**찾아보기**)**를 클릭하고 Cisco ISE ISO 파일을 선택합니다.

단계 **4** **Target Device(**대상 디바이스**)** 드롭다운 목록에서 USB 디바이스를 선택합니다.

로컬 시스템에 연결된 USB 장치가 하나뿐인 경우 자동으로 선택됩니다.

단계 **5** **Create Live USB(**라이브 **USB** 생성**)**를 클릭합니다.

진행률 표시줄에 부팅 가능 USB 생성 진행률이 표시됩니다. 이 프로세스가 끝나면 USB 드라이브의 콘텐츠를 USB 도구를 실행하는 데 사용한 로컬 시스템에서 사용할 수 있습니다. Cisco ISE를 설치하려면 텍스트 파일 2개를 수동으로 업데이트해야 합니다.

단계 **6** USB 장치에서 텍스트 편집기에 다음 텍스트 파일을 엽니다.

- isolinux/*isolinux.cfg* 또는 syslinux/*syslinux.cfg*
- EFI/BOOT/*grub.cfg*

단계 **7** 두 파일 모두에서 '**cdrom**'이라는 단어를 교체합니다.

- SNS 3515, 3595, 3615, 3655 또는 3695 어플라이언스를 사용하는 경우 두 파일 모두에서 "**cdrom**" 이라는 단어를 '**hd:sdb1**'로 교체합니다.

특히 '**cdrom**' 문자열의 모든 인스턴스를 교체해야 합니다. 예를 들어

ks=*cdrom*/ks.cfg

를

ks=*hd:sdb1:*/ks.cfg로 교체합니다.

단계 **8** 파일을 저장하고 종료합니다.

단계 **9** 로컬 시스템에서 USB 장치를 안전하게 제거합니다.

단계 **10** 부팅 가능 USB 장치를 Cisco ISE 어플라이언스에 연결하고, 어플라이언스를 재시작한 다음 USB 장치에서 부팅하여 Cisco ISE를 설치합니다.

Cisco SNS 3500/3600 시리즈 어플라이언스 재설치

Cisco SNS 3500/3600 시리즈 어플라이언스에는 내장된 DVD 드라이브가 없습니다. 따라서 Cisco ISE 하드웨어 어플라이언스를 Cisco ISE 소프트웨어로 재설치하려면 다음 중 하나를 수행해야 합니다.

참고 SNS 3500 및 3600 시리즈 어플라이언스는 UEFI(Unified Extensible Firmware Interface) 보안 부팅 기능을 지원합니다. 이 기능을 사용하면 Cisco에서 서명한 ISE 이미지만 SNS 3500 및 3600 시리즈 어플라이언스에 설치할 수 있으며, 서명하지 않은 운영 체제는 장치에 물리적으로 연결하더라도 설치할 수 없게 됩니다. 예를 들어 Red Hat Enterprise Linux나 Microsoft Windows 같은 일반 운영 체제는 이 어플라이언스에서 부팅할 수 없습니다.

SNS 3515 및 SNS 3595 어플라이언스는 Cisco ISE 2.0.1 이상 릴리스만 지원합니다. SNS 3515 또는 SNS 3595 어플라이언스에는 2.0.1 이전 릴리스를 설치할 수 없습니다.

- Cisco Integrated Management Controller(CIMC) 인터페이스로 설치 .iso 파일을 가상 DVD 장치에 매핑합니다. 자세한 내용은 CIMC를 사용하여 Cisco ISE 설치, 27 페이지를 참조하십시오.
- 설치 .iso 파일을 사용하여 설치 DVD를 생성하고 USB 외장 DVD 드라이브를 꽂은 다음 DVD 드라이브를 이용해 어플라이언스를 부팅합니다.

- 설치 .iso 파일을 사용하여 부팅 가능 USB 장치를 생성하고 USB 드라이브를 이용해 어플라이언스를 부팅합니다. 자세한 내용은 Cisco ISE 설치용 부팅 가능 USB 장치 생성, 35 페이지 및 CIMC를 사용하여 Cisco ISE 설치, 27 페이지를 참고하십시오.

VMware 가상 머신

참고 이 문서에서 제공하는 VMware 폼 팩터 지침은 Cisco HyperFlex에 설치된 ISE에도 적용됩니다.

가상 머신 리소스 및 성능 확인

가상 머신에 Cisco ISE를 설치하기 전에 설치 프로그램은 가상 머신의 가용 하드웨어 리소스를 권장 사양과 비교하여 하드웨어 무결성 검사를 수행합니다.

VM 리소스 검사 과정에서 설치 프로그램은 하드 디스크 공간, VM에 할당된 CPU 코어 수, CPU 클록 속도, VM에 할당된 RAM을 확인합니다. VM 리소스가 기본 평가 사양에 미치지 못할 경우 설치가 중단됩니다. 이러한 리소스 검사는 ISO 기반 설치에만 적용됩니다.

설정 프로그램을 실행할 경우 VM 성능 검사가 수행되는데, 여기서 설치 프로그램이 디스크 I/O 성능을 확인합니다. 디스크 I/O 성능이 권장 사양에 미치지 못할 경우 화면에 경고가 나타나지만 설치는 계속할 수 있습니다.

VM 성능 검사는 정기적으로 (매시간) 실시되며 그 결과는 1일 평균값으로 나타납니다. 디스크 I/O 성능이 권장 사양에 미치지 못할 경우 경보가 생성됩니다.

VM 성능 검사는 Cisco ISE CLI에서 **show tech-support** 명령을 사용하면 온디맨드 방식으로 수행할 수 있습니다.

VM 리소스 및 성능 검사는 Cisco ISE 설치와 별개로 실행할 수 있습니다. Cisco ISE 부팅 메뉴에서 이 테스트를 수행할 수 있습니다.

ISO 파일을 사용하여 VMware 가상 머신에 Cisco ISE 설치

이 섹션에서는 ISO 파일을 사용하여 VMware 가상 머신에 Cisco ISE를 설치하는 방법을 설명합니다.

VMware ESXi 서버 구성 시 전제 조건

VMWare ESXi 서버를 구성하기 전에 이 섹션의 다음 컨피그레이션 전제 조건을 참조하십시오.

- 관리자 권한이 있는 사용자(루트 사용자)로 ESXi 서버에 로그인해야 합니다.
- Cisco ISE는 64비트 시스템입니다. 64비트 시스템을 설치하기 전에 ESXi 서버에서 VT(Virtualization Technology)가 활성화되었는지 확인합니다.
- VMware 가상 머신에 권장량의 디스크 공간을 할당해야 합니다. 자세한 내용은 디스크 공간 요구 사항, 23 페이지 섹션을 참조하십시오.

- VMware VMFS(virtual machine file system)를 생성하지 않은 경우 Cisco ISE 가상 어플라이언스 지원을 위해 하나를 생성해야 합니다. VMFS는 VMware 호스트에 구성된 스토리지 볼륨 각각에 대해 설정됩니다. VMFS5의 경우 1MB의 블록 크기가 최대 1.999TB의 가상 디스크 크기를 지원합니다.

가상화 기술 확인

ESXi 서버가 이미 설치된 경우 재부팅하지 않고도 VT가 활성화되었는지 확인할 수 있습니다. 이를 수행하려면 **esxcfg-info** 명령을 사용합니다. 예를 들면 다음과 같습니다.

```
~ # esxcfg-info |grep "HV Support"
|----HV Support.......................................3
|----World Command Line..............................grep HV Support
```

HV Support의 값이 3일 경우 VT는 ESXi 서버에서 활성화되었으며 설치를 계속할 수 있습니다.

HV Support의 값이 2일 경우 VT가 지원되지만 ESXi 서버에서 활성화되지는 않았습니다. BIOS 설정을 수정하여 ESXi 서버에서 VT를 활성화해야 합니다.

ESXi 서버에 가상화 기술 활성화

이전 버전의 Cisco ISE 가상 머신을 호스팅하는 데 사용했던 하드웨어를 재사용할 수 있습니다. 그러나 최신 릴리스를 설치하기 전에 ESXi 서버에서 VT(Virtualization Technology)를 활성화해야 합니다.

단계 **1** 어플라이언스를 재부팅합니다.

단계 **2** **F2**를 눌러 설정을 입력합니다.

단계 **3** **Advanced(**고급**)** > **Processor Configuration(**프로세서 구성**)**을 선택합니다.

단계 **4** **Intel(R) VT**를 선택하고 활성화합니다.

단계 **5** **F10**을 눌러 변경 사항을 저장하고 종료합니다.

Cisco ISE 프로파일러 서비스를 위한 **VMware** 서버 인터페이스 구성

Cisco ISE 프로파일러 서비스를 위해 전용 프로브 인터페이스에 SPAN(Switch Port Analyzer) 또는 미러링 트래픽을 수집하는 것을 지원하도록 VMware 서버 인터페이스를 구성합니다.

단계 **1** **Configuration** > **Networking** > **Properties** > **VMNetwork**(VMware 서버 인스턴스의 이름)**VMswitch0**(VMware ESXi 서버 인터페이스 중 하나) **Properties** **Security**를 선택합니다.

단계 **2** **Security** 탭의 Policy Exceptions 창에서 **Promiscuous Mode** 확인란을 선택합니다.

단계 **3** Promiscuous Mode 드롭다운 목록에서 **Accept**를 선택하고 **OK**를 클릭합니다.

SPAN 또는 미러링된 트래픽에 대한 프로파일러 데이터 수집에 사용되는 다른 VMware ESXi 서버 인터페이스에서 동일한 단계를 반복합니다.

직렬 콘솔을 사용하여 **VMware** 서버에 연결

단계 **1** 해당 VMware 서버(예: ISE-120)를 끕니다.

단계 **2** VMware 서버를 마우스 오른쪽 단추로 클릭하고 **Edit**를 선택합니다.

단계 **3** Hardware(하드웨어) 탭에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Serial Port(**직렬 포트**)**를 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **5** Serial Port Output(직렬 포트 출력) 영역에서 **Use physical serial port on the host(**호스트에서 물리적 직렬 포트 사용**)** 또는 **Connect via Network(**네트워크를 통해 연결**)** 라디오 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.

- Connect via Network 옵션을 선택할 경우 ESXi 서버를 통해 방화벽 포트를 열어야 합니다.
- Use physical serial port on the host를 선택할 경우 포트를 선택합니다. 다음 2가지 옵션 중 하나를 선택할 수 있습니다.
  - **/dev/ttyS0** (DOS 또는 Windows 운영 체제에서는 COM1으로 표시됨)
  - **/dev/ttyS1** (DOS 또는 Windows 운영 체제에서는 COM2로 표시됨)

단계 **6** **Next**를 클릭합니다.

단계 **7** Device Status 영역에서 알맞은 확인란을 선택합니다. 기본값은 Connected입니다.

단계 **8** **OK**를 클릭하여 VMware 서버에 연결합니다.

VMware 서버 구성

시작하기 전에

VMware ESXi 서버 구성 시 전제 조건, 37 페이지 섹션의 세부 사항을 확인합니다.

단계 **1** ESXi 서버에 로그인합니다.

단계 **2** VMware vSphere Client의 왼쪽 창에서 호스트 컨테이너를 마우스 오른쪽 버튼으로 클릭하고 **New Virtual Machine**을 선택합니다.

단계 **3** Configuration 대화 상자에서 VMware 컨피그레이션에 대해 **Custom**을 선택하고 **Next**를 클릭합니다.

단계 **4** VMware 시스템의 이름을 입력하고 **Next**를 클릭합니다.

팁 팁: VMware 호스트에 사용하려는 호스트 이름을 사용합니다.

단계 **5** 권장량의 사용 가능 공간이 있는 데이터 저장소를 선택하고 **Next**를 클릭합니다.

단계 **6** (선택 사항) VM 호스트 또는 클러스터가 둘 이상의 VMware 가상 머신 버전을 지원할 경우 Virtual Machine Version 7과 같은 가상 머신 버전을 선택하고 **Next**를 클릭합니다.

단계 **7** **Linux**를 선택하고 **Version(**버전**)** 드롭다운 목록에서 지원되는 Red Hat Enterprise Linux 버전을 선택합니다.

단계 **8** Number of virtual sockets 및 Number of cores per virtual socket 드롭다운 목록에서 값을 선택합니다. 총 코어 수는 다음과 같아야 합니다.

SNS 3600 시리즈 어플라이언스**:**

- 소형-16
- 중형—24
- 대형—24

코어 수는 하이퍼 스레딩으로 인해 Cisco Secure Network Server 3600 시리즈에 해당하는 것의 두 배입니다. 예를 들어 소규모 네트워크 구축의 경우 CPU 사양이 8개이거나 스레드가 16개인 SNS 3615의 CPU 사양을 충족하도록 16개의 vCPU 코어를 할당해야 합니다.

참고 리소스 할당과 일치하도록 CPU 및 메모리 리소스를 예약하는 것이 좋습니다. 이렇게 하지 않으면 ISE 성능 및 안정성이 크게 떨어질 수 있습니다.

단계 **9** 메모리의 양을 선택하고 **Next**를 클릭합니다.

단계 **10** Adapter 드롭다운 목록에서 **E1000** NIC 드라이버를 선택하고 **Next**를 클릭합니다.

참고 기본적으로 올바른 어댑터 순서를 보장하기 위해 E1000을 선택하는 것이 좋습니다. VMXNET3를 선택할 경우 ESXi 어댑터를 다시 매핑하여 ISE 어댑터 순서와 동기화하는 작업이 필요할 수 있습니다.

단계 **11** **Paravirtual**을 SCSI 컨트롤러로 선택하고 **Next**를 클릭합니다.

단계 **12** **Create a new virtual disk**를 선택하고 **Next**를 클릭합니다.

단계 **13** Disk Provisioning 대화 상자에서 **Thick Provision** 라디오 버튼과 **Next**를 클릭하고 계속합니다.

Cisco ISE 는 씩 프로비저닝과 씬 프로비저닝을 모두 지원합니다. 그러나 더 우수한 성능을 위해, 특히 모니터링 노드에서는 씩 프로비저닝을 선택하는 것이 좋습니다. 씬 프로비저닝을 선택할 경우, 초기 디스크 확장 과정에서 업그레이드, 백업, 복원과 같은 작업 및 더 많은 디스크 공간을 필요로 하는 디버그 로깅이 영향을 받을 수 있습니다.

단계 **14** **Support clustering features such as Fault Tolerance** 확인란을 선택 취소합니다.

단계 **15** 고급 옵션을 선택하고 **Next**를 클릭합니다.

단계 **16** 새로 생성되는 VMware 시스템의 구성 세부 사항, 즉 Name, Guest OS, CPUs, Memory, Disk Size 등을 확인합니다.

단계 **17** **Finish**를 클릭합니다.

VMware 시스템이 설치되었습니다.

다음에 수행할 작업

새로 생성된 VMware 시스템을 활성화하려면 VMware 클라이언트 사용자 인터페이스의 왼쪽 창에서 VM을 마우스 오른쪽 버튼으로 클릭하고 **Power > Power On**을 선택합니다.

가상 머신 가동 시 부팅 지연 구성

VMware 가상 머신에서는 기본적으로 부팅 지연이 0으로 설정됩니다. 이 부팅 지연을 변경하면 부팅 옵션을 쉽게 선택할 수 있습니다(예: 관리자 암호 재설정).

단계 **1** VSphere 클라이언트에서 VM을 오른쪽 마우스 버튼으로 클릭하고 **Edit Settings(**설정 편집**)**를 선택합니다.

단계 **2** **Options(**옵션**)** 탭을 클릭합니다.

단계 **3** **Advanced(**고급**) > Boot Options(**부팅 옵션**)**를 선택합니다.

단계 **4** **Power on Boot Delay(**가동 시 부팅 지연**)** 영역에서 부팅 작업을 지연할 시간을 밀리초 단위로 선택합니다.

단계 **5** 다음 VM 부팅 때 BIOS 설정 화면에 들어가려면 **Force BIOS Setup(**강제 **BIOS** 설정**)** 영역의 확인란을 선택합니다.

단계 **6** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

VMware 시스템에 Cisco ISE 소프트웨어 설치

시작하기 전에

- 설치 후 영구 라이센스를 설치하지 않을 경우 Cisco ISE에서는 최대 100개의 엔드포인트를 지원하는 90일 평가 라이센스를 자동으로 설치합니다.
- Cisco 소프트웨어 다운로드 사이트(http://www.cisco.com/en/US/products/ps11640/index.html)에서 Cisco ISE 소프트웨어를 다운로드하고 DVD에 굽습니다. Cisco.com 인증서를 제공해야 합니다.
- (선택 사항, VMware Cloud에 Cisco ISE를 설치하는 경우에만 적용 가능) VMware 클라우드에 Cisco ISE를 설치하는 프로세스는 VMware 가상 컴퓨터에 Cisco ISE를 설치하는 프로세스와 정확히 동일합니다.
  - AWS(Amazon Web Services)의 VMware Cloud에 구축되니 Cisco ISE 가상 컴퓨터: Cisco Cloud가 AWS에서 제공하는 SDDC(Software Defined Data Center)에서 Cisco ISE를 호스팅할 수 있습니다. 온프레미스 구축, 필수 디바이스 및 서비스에 연결할 수 있도록, VMware Cloud(**Networking and Security(**네트워킹 및 보안**) > Security(**보안**) > Gateway Firewall Settings(**게이트웨이 방화벽 설정**)**)에 적절한 보안 그룹 정책을 구성해야 합니다.
  - Azure VMware 솔루션(AVS)에 구축된 Cisco ISE 가상 컴퓨터: AVS는 기본적으로 Cisco ISE를 VMware 가상 컴퓨터로 호스팅할 수 있는 Microsoft Azure에서 VMware 워크로드를 실행합니다.

단계 **1** VMware 클라이언트에 로그인합니다.

단계 **2** 가상 머신이 BIOS 설정 모드로 들어가도록 VM을 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** **Options(**옵션**)** 탭을 클릭합니다.

단계 **4** **Boot Options(**부팅 옵션**)**를 선택하고 다음 옵션을 구성합니다.

a) **Force BIOS Setup(**강제 **BIOS** 설정**)** 영역에서 확인란을 선택하여 가상 머신 부팅 시 BIOS 설정 화면에 들어가게 합니다.

참고 2TB 이상의 GPT 파티션으로 부팅하려면 VM 설정의 부팅 모드에서 펌웨어를 **BIOS**에서 **EFI**로 변경해야 합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** BIOS에서 Coordinated Universal Time(UTC)과 올바른 부팅 순서가 설정되었는지 확인합니다.

a) 가상 머신이 켜진 상태라면 시스템을 끕니다.

b) 가상 머신을 켭니다.

시스템이 BIOS 설정 모드에 들어갑니다.

c) 메인 BIOS 메뉴에서 화살표 키를 사용하여 Date and Time(날짜 및 시간) 필드로 이동하고 **Enter**를 누릅니다.

d) UTC/Greenwich Mean Time (GMT) 표준 시간대를 입력합니다.

이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서, 로그, 포스처 에이전트 로그 파일의 타임스탬프가 항상 동기화됩니다.

e) 화살표 키를 사용하여 Boot(부팅) 메뉴로 이동하고 **Enter**를 누릅니다.

f) 화살표 키를 사용하여 CD-ROM Drive(CD-ROM 드라이브)를 선택하고 + 를 눌러 CD-ROM 드라이브를 순서를 위로 올립니다.

g) 화살표 키를 사용하여 Exit(종료) 메뉴로 이동하고 **Exit Saving Changes(**변경 사항 저장 및 종료**)**를 선택합니다.

h) **Yes(**예**)**를 선택하여 변경 사항을 저장하고 종료합니다.

단계 **7** VMware ESXi 호스트 CD/DVD 드라이브에 Cisco ISE 소프트웨어 DVD를 삽입하고 가상 머신을 켭니다.

DVD가 부팅되면 콘솔에 다음과 같이 표시됩니다.

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

단계 **8** 화살표 키를 사용하여 **Cisco ISE Installation (Serial Console)** 또는 **Cisco ISE Installation (Keyboard/Monitor)**을 선택하고 **Enter**를 누릅니다. 직렬 콘솔 옵션을 선택하는 경우, 가상 머신에 직렬 콘솔이 설정되어 있어야 합니다. 콘솔을 생성하는 방법에 관한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.
설치 관리자에서 VMware 시스템에 Cisco ISE 소프트웨어를 설치하기 시작합니다. 설치 프로세스가 완료되는 데 20분가량 걸립니다. 설치 프로세스가 끝나면 가상 머신이 자동으로 재부팅됩니다. VM이 재부팅되면 콘솔에 다음과 같이 표시됩니다.

```
Type 'setup' to configure your appliance
localhost:
```

단계 **9** 시스템 프롬프트에서 **setup**을 입력하고 **Enter**를 누릅니다.

참고 Cisco ISE 릴리스 3.0부터는 ISE 가상 머신을 호스팅하는 가상화 플랫폼의 CPU가 (스트리밍 SIMD 확장) SSE 4.2 명령 집합을 지원해야 합니다. 그렇지 않으면 특정 ISE 서비스(예: ISE API 게이트웨이)가 작동하지 않으며 Cisco ISE GUI를 시작할 수 없습니다. Intel 및 AMD 프로세서 모두 2011년부터 SSE 4.2 버전을 지원하고 있습니다.

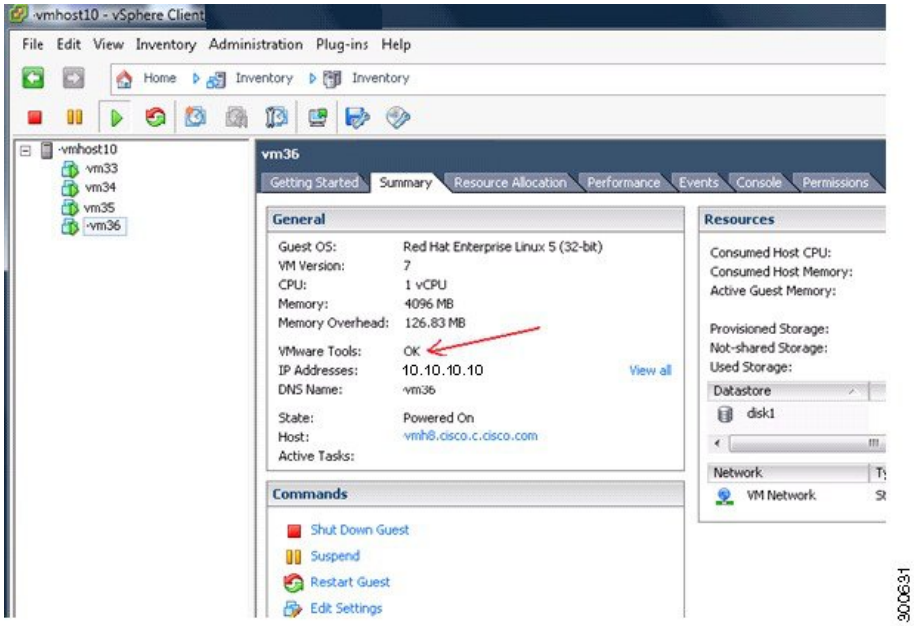
Setup Wizard가 나타나 초기 컨피그레이션을 차례로 안내합니다.

VMware Tools 설치 확인

vSphere Client의 Summary 탭을 사용하여 VMWare Tools 설치 확인

vShpere Client에서 해당 VMware 호스트의 Summary 탭으로 이동합니다. VMware Tools 필드의 값이 OK가 되어야 합니다.

그림 *7: vSphere Client*에서 *VMware Tools* 확인



CLI를 사용하여 VMWare Tools 설치 확인

show inventory 명령을 사용하여 VMware 도구 설치 여부를 확인할 수 있습니다. 이 명령은 NIC 드라이버 정보를 나열합니다. VMware Tools가 설치된 가상 머신에서 VMware Virtual Ethernet 드라이버가 Driver Descr 필드에 나열됩니다.

```
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9       , VID: A0  , SN: FCH184X9XXX
Total RAM Memory: 65700380 kB
CPU Core Count: 16
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 4: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 5: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 6: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 7: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 8: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 9: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 10: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 11: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 12: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 13: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 14: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 15: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
```

```
Hard Disk Count(*): 1
Disk 0: Device Name: /xxx/abc
Disk 0: Capacity: 1198.00 GB
NIC Count: 6
NIC 0: Device Name: eth0:
NIC 0: HW Address: xx:xx:xx:xx:xx:xx
NIC 0: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 1: Device Name: eth1:
NIC 1: HW Address: xx:xx:xx:xx:xx:xx
NIC 1: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: HW Address: xx:xx:xx:xx:xx:xx
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: HW Address: xx:xx:xx:xx:xx:xx
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: HW Address: xx:xx:xx:xx:xx:xx
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
NIC 5: HW Address: xx:xx:xx:xx:xx:xx
NIC 5: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical.
```

VMware Tools 업그레이드 지원

Cisco ISE ISO 이미지(일반, 업그레이드, 패치)에는 지원되는 VMware Tools가 포함되어 있습니다. VMware Client 사용자 인터페이스를 통해 VMware Tools를 업그레이드하는 것은 Cisco ISE에서 지원되지 않습니다. VMware Tools를 더 높은 버전으로 업그레이드하려는 경우 새 버전의 Cisco ISE(일반, 업그레이드, 패치 릴리스)를 통해 업그레이드하면 됩니다.

Cisco ISE 가상 머신 복제

Cisco ISE VMware 가상 머신을 복제하여 Cisco ISE 노드의 정확한 복제본을 만들 수 있습니다. 예를 들어 여러 PSN(Policy Service node)으로 구성된 분산 구축에서는 VM 복제를 통해 빠르고 효과적으로 PSN을 구축할 수 있습니다. PSN을 개별적으로 설치하고 구성할 필요 없습니다.

템플릿을 사용하여 Cisco ISE VM을 복제할 수도 있습니다.

참고 복제하려면 VMware vCenter 필요합니다. 설치 프로그램을 실행하기 전에 복제를 수행해야 합니다.

시작하기 전에

- 복제할 Cisco ISE VM을 종료했는지 확인합니다. vSphere 클라이언트에서 복제할 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Power** > **Shut Down Guest**를 선택합니다.
- 복제한 가상 머신을 켜고 네트워크에 연결하기 전에 그 IP 주소 및 호스트 이름을 변경해야 합니다.

단계 **1** 관리자 권한이 있는 사용자(루트 사용자)로 ESXi 서버에 로그인합니다.

이 단계를 수행하려면 VMware vCenter가 필요합니다.

단계 **2** 복제할 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Clone**을 클릭합니다.

단계 **3** 생성할 새 가상 머신의 이름을 Name and Location 대화 상자에 입력하고 **Next**를 클릭합니다.

이는 생성할 새 Cisco ISE VM의 호스트 이름이 아니라 참조를 위한 설명 차원의 이름입니다.

단계 **4** 새 Cisco ISE VM을 실행할 호스트 또는 클러스터를 선택하고 **Next**를 클릭합니다.

단계 **5** 생성할 새 Cisco ISE VM의 데이터 저장소를 선택하고 **Next**를 클릭합니다.

이 데이터 저장소는 ESXi 서버의 로컬 데이터 저장소이거나 원격 스토리지일 수 있습니다. 데이터 저장소에 충분한 디스크 공간이 있는지 확인합니다.

단계 **6** Disk Format 대화 상자에서 **Same format as source** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.

이 옵션은 복제의 원본인 Cisco ISE VM에서 사용하는 형식을 그대로 복사합니다.

단계 **7** Guest Customization 대화 상자에서 **Do not customize** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.

단계 **8** **Finish**를 클릭합니다.

다음에 수행할 작업

- 복제된 가상 머신의 IP 주소 및 호스트 이름 변경
- 네트워크에 복제된 Cisco 가상 머신 연결

템플릿을 사용하여 **Cisco ISE** 가상 머신 복제

vCenter를 사용하는 경우 VMware 템플릿을 사용하여 Cisco ISE VM을 복제할 수 있습니다. Cisco ISE 노드를 템플릿에 복제하고 그 템플릿을 사용하여 여러 개의 새 Cisco ISE 노드를 생성할 수 있습니다. 템플릿을 사용하여 가상 머신을 복제하는 프로세스는 2단계로 구성됩니다.

시작하기 전에

참고 복제하려면 VMware vCenter 필요합니다. 설치 프로그램을 실행하기 전에 복제를 수행해야 합니다.

단계 **1** 가상 머신 템플릿 생성, 46 페이지

단계 **2** 가상 머신 템플릿 구축, 46 페이지

가상 머신 템플릿 생성

시작하기 전에

- 복제할 Cisco ISE VM을 종료했는지 확인합니다. vSphere 클라이언트에서 복제할 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Power > Shut Down Guest**를 선택합니다.
- 방금 설치했고 설정 프로그램을 실행하지 않은 Cisco ISE VM에서 템플릿을 만드는 것이 좋습니다. 그런 다음 생성한 Cisco ISE 노드 각각에서 설정 프로그램을 실행하고 개별적으로 IP 주소 및 호스트 이름을 구성할 수 있습니다.

단계 **1** 관리자 권한이 있는 사용자(루트 사용자)로 ESXi 서버에 로그인합니다.

이 단계를 수행하려면 VMware vCenter가 필요합니다.

단계 **2** 복제할 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Clone** > **Clone to Template**을 선택합니다.

단계 **3** Name and Location 대화 상자에서 템플릿의 이름을 입력하고 템플릿을 저장할 위치를 선택한 다음 **Next**를 클릭합니다.

단계 **4** 템플릿을 저장할 ESXi 호스트를 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **5** 템플릿 저장에 사용할 데이터 저장소를 선택하고 **Next**를 클릭합니다.

이 데이터 저장소에 필요한 양의 디스크 공간이 있는지 확인합니다.

단계 **6** Disk Format 대화 상자에서 **Same format as source** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.

Ready to Complete 대화 상자가 나타납니다.

단계 **7** **Finish(**종료**)**를 클릭합니다.

가상 머신 템플릿 구축

가상 머신 템플릿을 생성하고 이를 다른 VM에 구축할 수 있습니다.

단계 **1** 생성한 Cisco ISE VM 템플릿을 마우스 오른쪽 버튼으로 클릭하고 **Deploy Virtual Machine from this template**을 선택합니다.

단계 **2** Name and Location 대화 상자에서 새 Cisco ISE 노드의 이름을 입력하고 노드의 위치를 선택한 다음 **Next**를 클릭합니다.

단계 **3** 새 Cisco ISE 노드를 저장할 ESXi 호스트를 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **4** 새 Cisco ISE 노드에 사용할 데이터 저장소를 선택하고 **Next**를 클릭합니다.

이 데이터 저장소에 필요한 양의 디스크 공간이 있는지 확인합니다.

단계 **5** Disk Format 대화 상자에서 **Same format as source** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.

단계 **6** Guest Customization 대화 상자에서 **Do not customize** 라디오 버튼을 클릭합니다.

Ready to Complete 대화 상자가 나타납니다.

단계 **7** **Edit Virtual Hardware** 확인란을 선택하고 **Continue**를 클릭합니다.

Virtual Machine Properties 페이지가 나타납니다.

단계 **8** **Network adapter**를 선택하고 **Connected** 및 **Connect at power on** 확인란을 선택 취소한 다음 **OK**를 클릭합니다.

단계 **9** **Finish**를 클릭합니다.

이제 이 Cisco ISE 노드를 켜고 IP 주소 및 호스트 이름을 구성하고 네트워크에 연결할 수 있습니다.

다음에 수행할 작업

- 복제된 가상 머신의 IP 주소 및 호스트 이름 변경
- 네트워크에 복제된 Cisco 가상 머신 연결

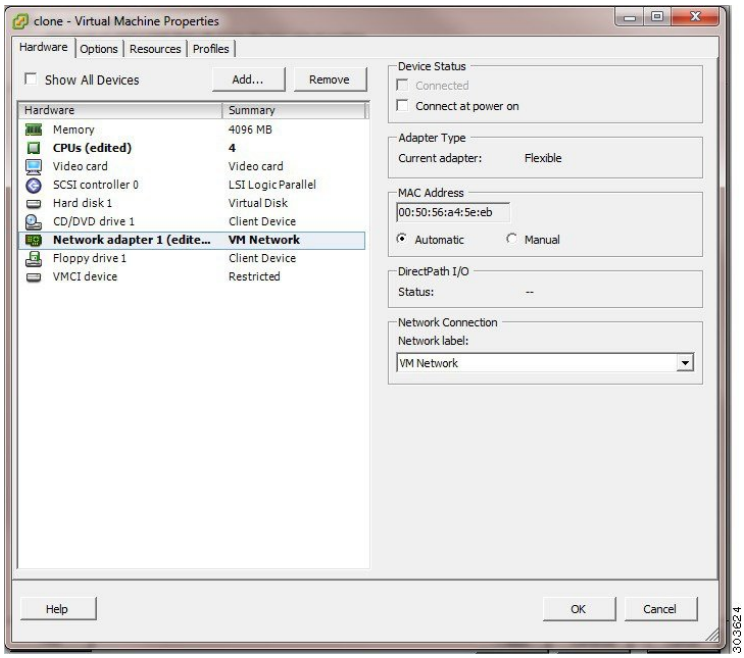
복제된 가상 머신의 IP 주소 및 호스트 이름 변경

Cisco ISE VM을 복제한 다음 이를 켜고 IP 주소 및 호스트 이름을 변경해야 합니다.

시작하기 전에

- Cisco ISE 노드가 독립형 상태인지 확인합니다.
- 새로 복제한 Cisco ISE VM을 켤 때 그 네트워크 어댑터가 연결되어 있지 않음을 확인합니다. **Connected** 및 **Connect at power on** 확인란을 선택 취소합니다. 그렇지 않으면 이 노드가 시작할 때 복제 원본 머신과 동일한 IP 주소를 갖게 됩니다.

그림 *8:* 네트워크 어댑터 연결 끊기



- 새로 복제한 VM을 켜는 즉시 이 VM에 대해 구성할 IP 주소 및 호스트 이름이 있어야 합니다. 이 IP 주소 및 호스트 이름 항목이 DNS 서버에 있어야 합니다. 노드의 호스트 이름으로 "localhost"를 사용할 수 없습니다.
- 새 IP 주소 또는 호스트 이름을 기반으로 하는 Cisco ISE 노드를 위한 인증서가 있는지 확인합니다.

절차

단계 **1** 새로 복제한 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Power** > **Power On**을 선택합니다.

단계 **2** 새로 복제한 Cisco ISE VM을 선택하고 **Console** 탭을 클릭합니다.

단계 **3** Cisco ISE CLI에서 다음 명령을 입력합니다.

```
configure terminal
hostname hostname
```

hostname은 구성하려는 새 호스트 이름입니다. Cisco ISE 서비스가 다시 시작합니다.

단계 **4** 다음 명령을 입력합니다.

```
interface gigabit 0
ip address ip_address netmask
```

ip_address는 3단계에서 입력한 호스트 이름의 주소이고, netmask는 ip_address의 서브넷 마스크입니다. Cisco ISE 서비스를 다시 시작하라는 메시지가 표시됩니다. ip address 및 hostname 명령에 대해서는 *Cisco Identity Services Engine CLI* 참조 설명서를 참조하십시오.

단계 **5** **Y**를 입력하여 Cisco ISE 서비스를 다시 시작합니다.

네트워크에 복제된 **Cisco** 가상 머신 연결

전원을 켜고 IP 주소 및 호스트 이름을 변경한 다음 Cisco ISE 노드를 네트워크에 연결해야 합니다.

단계 **1** 새로 복제된 Cisco ISE VM을 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings**를 클릭합니다.

단계 **2** Virtual Machine Properties 대화 상자에서 **Network adapter**를 클릭합니다.

단계 **3** Device Status 영역에서 **Connected** 및 **Connect at power on** 확인란을 선택합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

평가 환경에서 프로덕션 환경으로 **Cisco ISE VM** 마이그레이션

Cisco ISE 릴리스에 대한 평가를 마치고 평가 시스템에서 정식 라이센스를 취득한 프로덕션 시스템으로 마이그레이션할 수 있습니다.

시작하기 전에

- 더 많은 수의 사용자를 지원하는 프로덕션 환경으로 VMware 서버를 이전할 경우 Cisco ISE 설치를 권장 최소 디스크 크기 또는 그 이상으로 (최대 한도인 2.4TB는 넘지 않게) 다시 구성해야 합니다.
- 300GB보다 작은 디스크 공간으로 생성한 VM에서 프로덕션 VM으로 데이터를 마이그레이션할 수 없습니다. 300GB 이상인 디스크 공간으로 생성한 VM의 데이터만 프로덕션 환경으로 마이그레이션할 수 있습니다.

단계 **1** 평가 버전의 컨피그레이션을 백업합니다.

단계 **2** 프로덕션 VM에 필요한 양의 디스크 공간이 있는지 확인합니다.

단계 **3** 프로덕션 구축 라이센스를 설치합니다.

단계 **4** 프로덕션 시스템에 컨피그레이션을 복원합니다.

show tech-support 명령을 이용한 온디맨드 가상 머신 성능 확인

언제든 CLI에서 **show tech-support** 명령을 실행하여 VM 성능을 확인할 수 있습니다. 이 명령을 실행하면 다음과 비슷한 출력이 표시됩니다.

```
ise-vm123/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
****************************************
Average I/O bandwidth writing to disk device: 48 MB/second
Average I/O bandwidth reading from disk device: 193 MB/second
WARNING: VM I/O PERFORMANCE TESTS FAILED!
WARNING: The bandwidth writing to disk must be at least 50 MB/second,
WARNING: and bandwidth reading from disk must be at least 300 MB/second.
WARNING: This VM should not be used for production use until disk
WARNING: performance issue is addressed.
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 7.81502 s, 40.3 MB/s
Disk I/O bandwidth filesystem read test, reading 300 MB from /opt:
314572800 bytes (315 MB) copied, 0.416897 s, 755 MB/s
```

Cisco ISE 부트 메뉴에서 가상 머신 리소스 확인

Cisco ISE 설치와 별개로 부팅 메뉴에서 가상 머신 리소스를 확인할 수 있습니다.

CLI 기록은 다음과 같이 나타납니다.

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

화살표 키를 사용하여 시스템 유틸리티**(**직렬콘솔**)** 또는 시스템 유틸리티**(**키보드/모니터**)**를 선택하고 **Enter**를 누릅니다. 다음 화면이 나타납니다.

```
Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload

Enter option [1 - 3] q to Quit
```

2를 입력하여 VM 리소스를 확인합니다. 다음과 같이 출력됩니다.

```
*****
***** Virtual Machine host detected…
***** Hard disk(s) total size detected: 600 Gigabyte
***** Physical RAM size detected: 16267516 Kbytes
***** Number of network interfaces detected: 6
***** Number of CPU cores: 12
***** CPU Mhz: 2300.00
***** Verifying CPU requirement…
***** Verifying RAM requirement…
***** Writing disk partition table…
```

Linux KVM

KVM 가상화 확인

KVM 가상화는 호스트 프로세서에 제공하는 가상화 지원을 요구합니다. Intel 프로세서에는 Intel VT-x, AMD 프로세서에는 AMD-V가 필요합니다. 호스트에서 터미널 창을 열고 **cat /proc/cpuinfo** 명령을 입력합니다. vmx 또는 svm 플래그 중 하나가 표시되어야 합니다.

- Intel VT-x의 경우:

```
# cat /proc/cpuinfo
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
 dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc
 aperfmperf eagerfpu pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer aes xsave avx lahf_lm arat epb xsaveopt
pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
```

- AMD-V의 경우:

```
# cat /proc/cpuinfo
flags: fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush mmx fxsr sse sse2
ht syscall nx mmxext fxsr_opt rdtscp lm 3dnowext 3dnow
 pni cx16 lahf_lm cmp_legacy svm cr8_legacy
```

KVM에 Cisco ISE 설치

이 절차에서는 RHEL에서 KVM을 생성하고 Virtual Machine Manager(virt manager)를 사용하여 KVM에 Cisco ISE를 설치하는 방법을 설명합니다.

CLI를 통해 Cisco ISE를 설치하기로 했다면 다음과 유사한 명령을 입력합니다.

```
#virt-install --name=kvm-ise1 --arch=x86_64 --cpu=host --vcpus=2 --ram=4096

--os-type=linux --os-variant=rhel6 --hvm --virt-type=kvm
--cdrom=/home/admin/Desktop/ise-3.0.0.x.SPA.x86_64.iso
--disk=/home/libvirt-images/kvm-ise1.img,size=100
--network type=direct,model=virtio,source=eth2,source_mode=bridge
```

여기서 *ise-3.0.0.x.SPA.x86_64.iso*는 Cisco ISE ISO 이미지의 이름입니다.

시작하기 전에

Cisco ISE ISO 이미지를 로컬 시스템에 다운로드합니다.

단계 **1** virt-manager에서 **New(**새로 만들기**)**를 클릭합니다.

Create a new virtual machine(새 가상 머신 생성) 창이 열립니다.

단계 **2** 로컬 설치 미디어**(ISO** 이미지 또는 **CDROM)**를 선택하고 **Forward(**전달**)**를 클릭합니다.

단계 **3** **Use ISO image(ISO** 이미지 사용**)** 라디오 버튼을 클릭하고 **Browse(**찾아보기**)**를 클린한 다음 로컬 시스템에서 ISO 이미지를 선택합니다.

a) **Automatically detect operating system based on install media(**설치 미디어를 바탕으로 운영 체제 자동 탐지**)** 확인란을 선택 해제하고, OS 유형으로 Linux를 선택하고, 지원되는 Red Hat Enterprise Linux 버전을 선택한 다음 **Forward(**전달**)**를 클릭합니다.

QEMU 1.5.3-160에서 지원되는 KVM

단계 **4** RAM 및 CPU 설정을 선택하고 **Forward (**전달**)**를 클릭합니다.

단계 **5** **Enable storage for this virtual machine(**이 가상 머신에 스토리지 활성화**)** 확인란을 선택하고 스토리지 설정을 선택합니다.

a) **Select managed or other existing storage(**관리형 또는 다른 기존 스토리지 선택**)** 라디오 버튼을 클릭합니다.
b) **Browse(**찾아보기**)**를 클릭합니다.
c) 왼쪽의 Storage Pools(스토리지 풀) 탐색 창에서 **disk FileSystem Directory**를 클릭합니다.
d) **New Volume(**새 볼륨**)**을 클릭합니다.

Create storage volume(스토리지 볼륨 생성) 창이 열립니다.

e) 스토리지 볼륨의 이름을 입력합니다.
f) **Format(**형식**)** 드롭다운 목록에서 **raw**를 선택합니다.
g) Maximum Capacity(최대 용량)를 입력합니다.
h) 마침을 클릭합니다.
i) 생성한 볼륨을 선택하고 **Choose Volume(**볼륨 선택**)**을 클릭합니다.
j) **Forward(**전달**)**를 클릭합니다.

Ready to begin the installation(설치 시작 준비 완료) 화면이 나타납니다.

단계 **6** **Customize configuration before install(**설치 전에 구성 맞춤화**)** 확인란을 선택합니다.

단계 **7** Advanced(고급) 옵션에서 인터페이스 소스로 macvtap을 선택하고, Source mode(소스 모드) 드롭다운 목록에서 Bridge(브리지)를 선택한 다음 **Finish(**마침**)**를 클릭합니다.

a) (선택 사항) **Add Hardware(**하드웨어 추가**)**를 클릭하여 다른 NIC를 추가합니다.

Network(네트워크) 소스로 macvtap을, Device(장치) 모델로 virtio를 선택합니다.

b) 마침을 클릭합니다.

단계 **8** Virtual Machine(가상 머신) 화면에서 디스크 장치를 선택하고 Advanced and Performance Options(고급 및 성능 옵션)에서 아래 옵션을 선택한 다음 **Apply(**적용**)**를 클릭합니다.

필드	값
디스크 버스	VirtIO
캐시 모드	없음
IO 모드	native

단계 **9** **Begin Installation(**설치 시작**)**을 클릭하여 KVM에 Cisco ISE를 설치합니다.
Cisco ISE 설치 부팅 메뉴가 나타납니다.

단계 **10** 시스템 프롬프트에서 **1**을 입력하여 모니터 및 키보드 포트를 선택하거나 **2**를 입력하여 콘솔 포트를 선택하고 **Enter**를 누릅니다.

설치 관리자에서 VM에 Cisco ISE 소프트웨어를 설치하기 시작합니다. 설치 프로세스가 완료되면 콘솔에 다음이 표시됩니다.

```
Type 'setup' to configure your appliance
localhost:
```

단계 **11** 시스템 프롬프트에서 **setup**을 입력하고 **Enter**를 누릅니다.
Setup Wizard가 나타나 초기 컨피그레이션을 차례로 안내합니다.

Microsoft Hyper-V

Hyper-v에서 Cisco ISE 가상 머신 생성

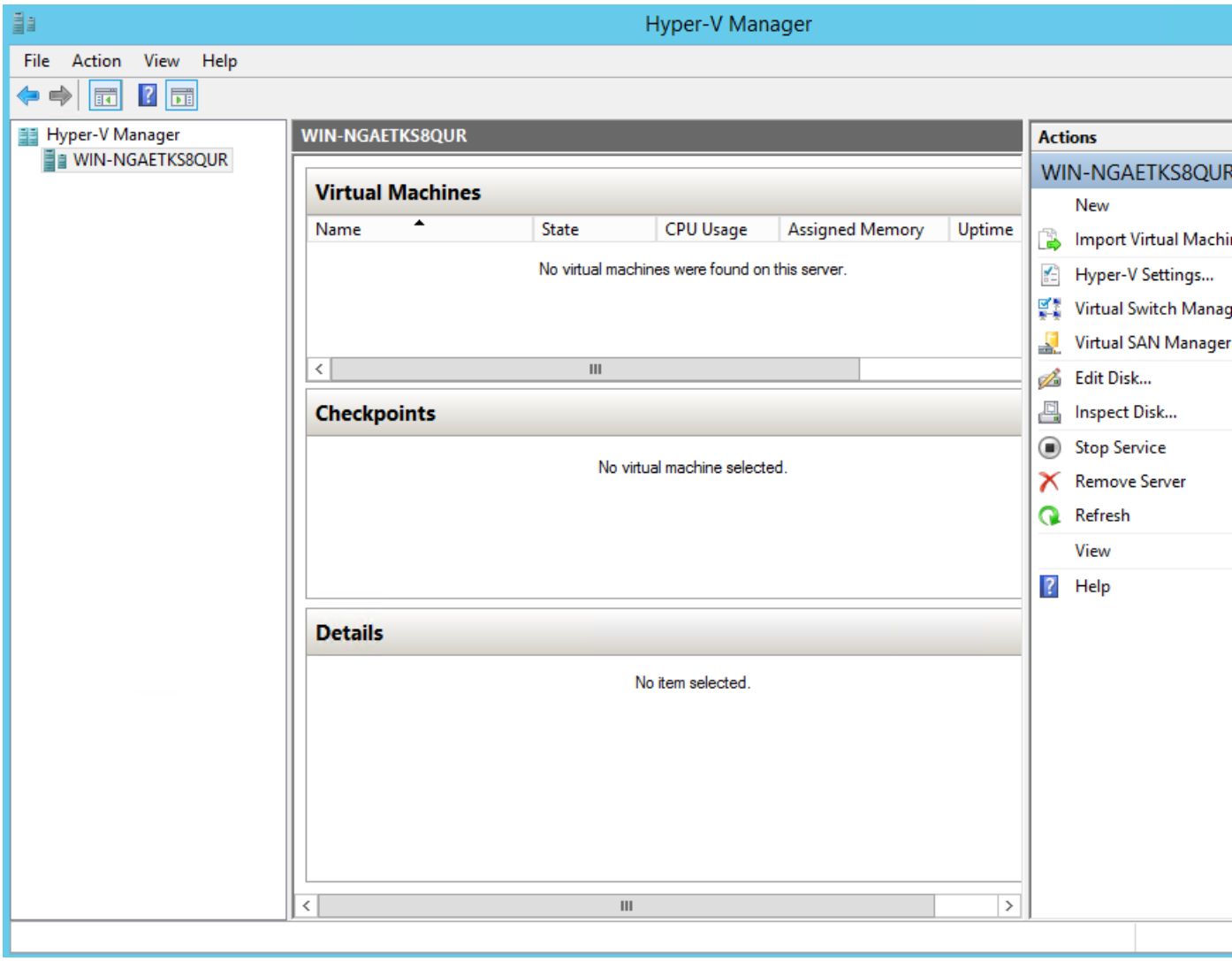
이 섹션에서는 새 가상 머신을 생성하고, 로컬 디스크에서 가상 CD/DVD 드라이브로 ISO 이미지를 매핑하고, CPU 설정을 수정하고, Hyper-v에 Cisco ISE를 설치하는 방법을 설명합니다.

시작하기 전에

Cisco.com에서 Cisco ISE ISO 이미지를 로컬 시스템으로 다운로드합니다.

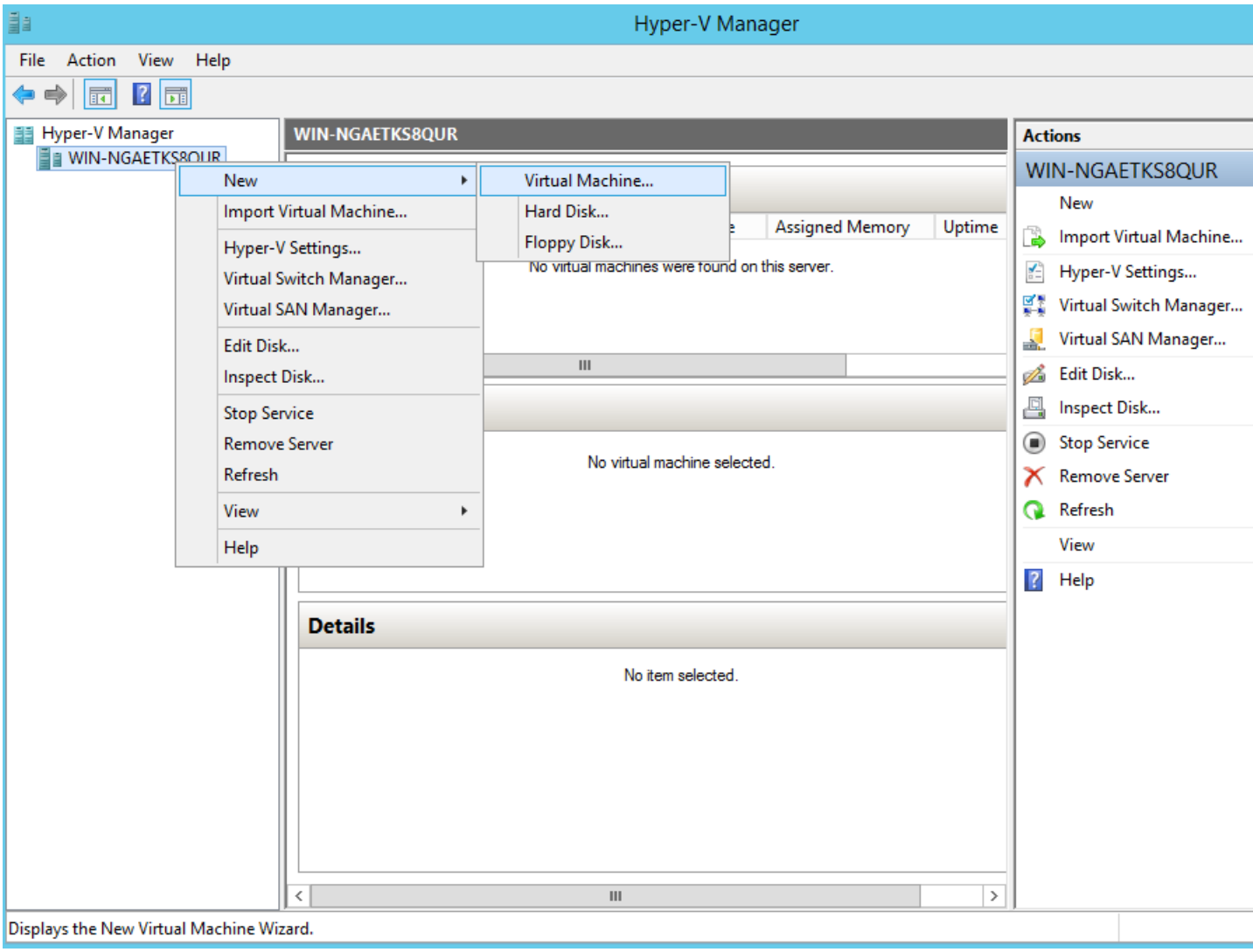
단계 **1** 지원되는 Windows 서버에서 Hyper-v Manager를 시작합니다.

그림 *9: Hyper-v Manager* 콘솔



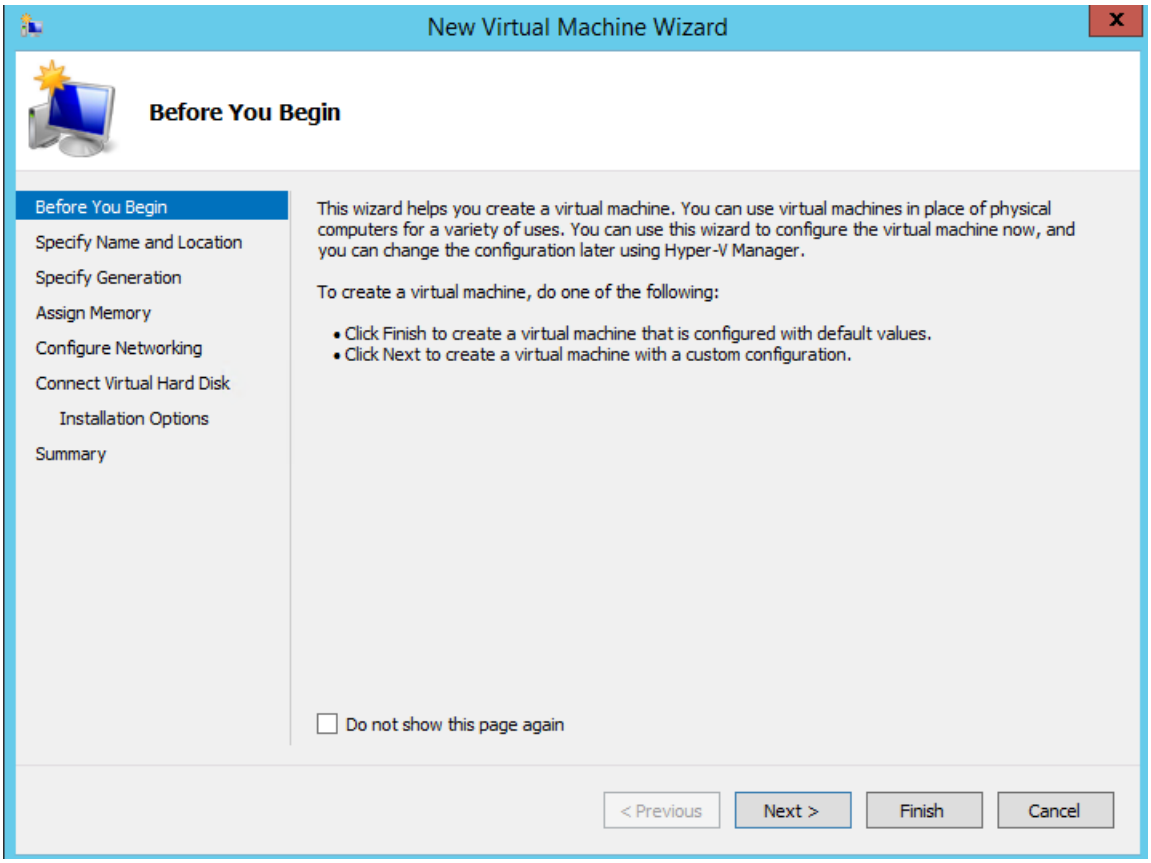
단계 **2** VM 호스트를 마우스 오른쪽 버튼으로 클릭하고 **New(**새로 만들기**)** > **Virtual Machine(**가상 머신**)**을 선택합니다.

그림 *10:* 새 가상 머신 생성



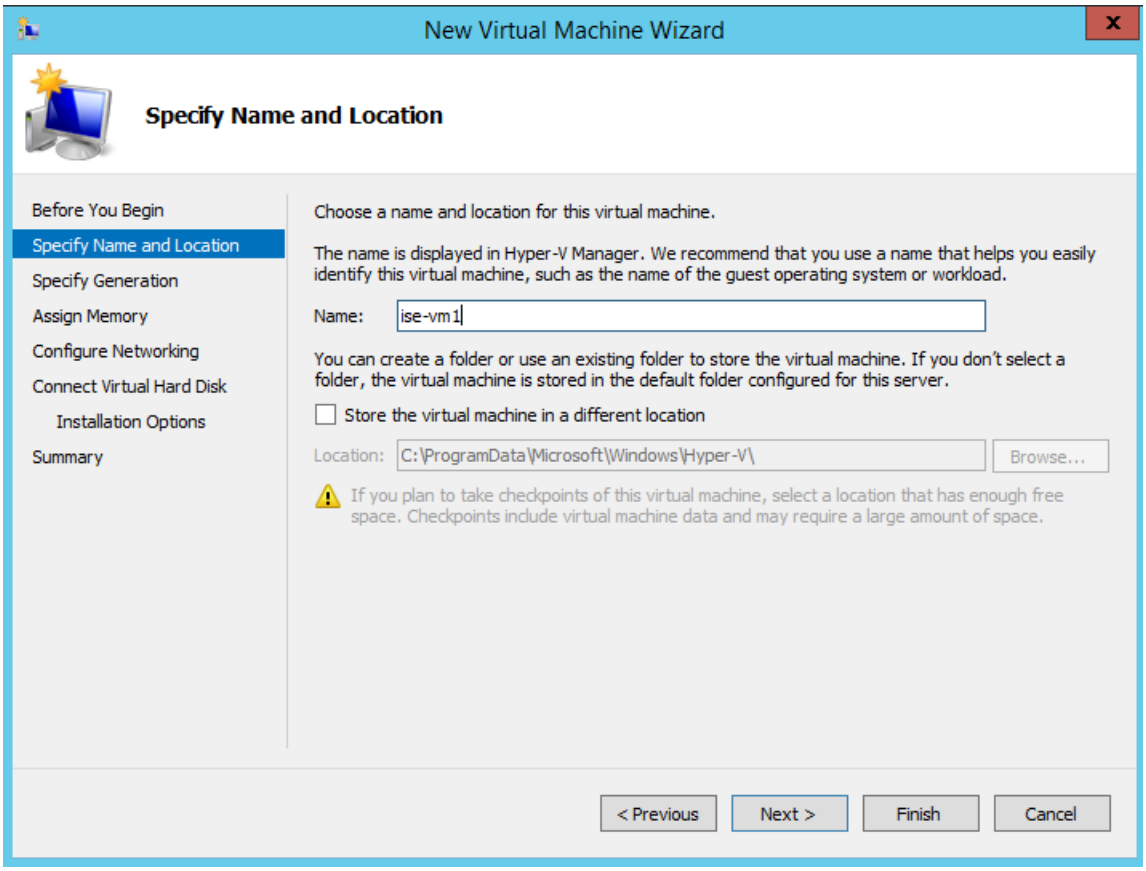
단계 **3** **Next(**다음**)**를 클릭하여 VM 구성을 사용자 정의합니다.

그림 ***11: New Virtual Machine Wizard(***새 가상 머신 마법사***)***



단계 **4** VM의 이름을 입력하고, (선택 사항) VM을 저장할 다른 경로를 선택하고, **Next(**다음**)**를 클릭합니다.

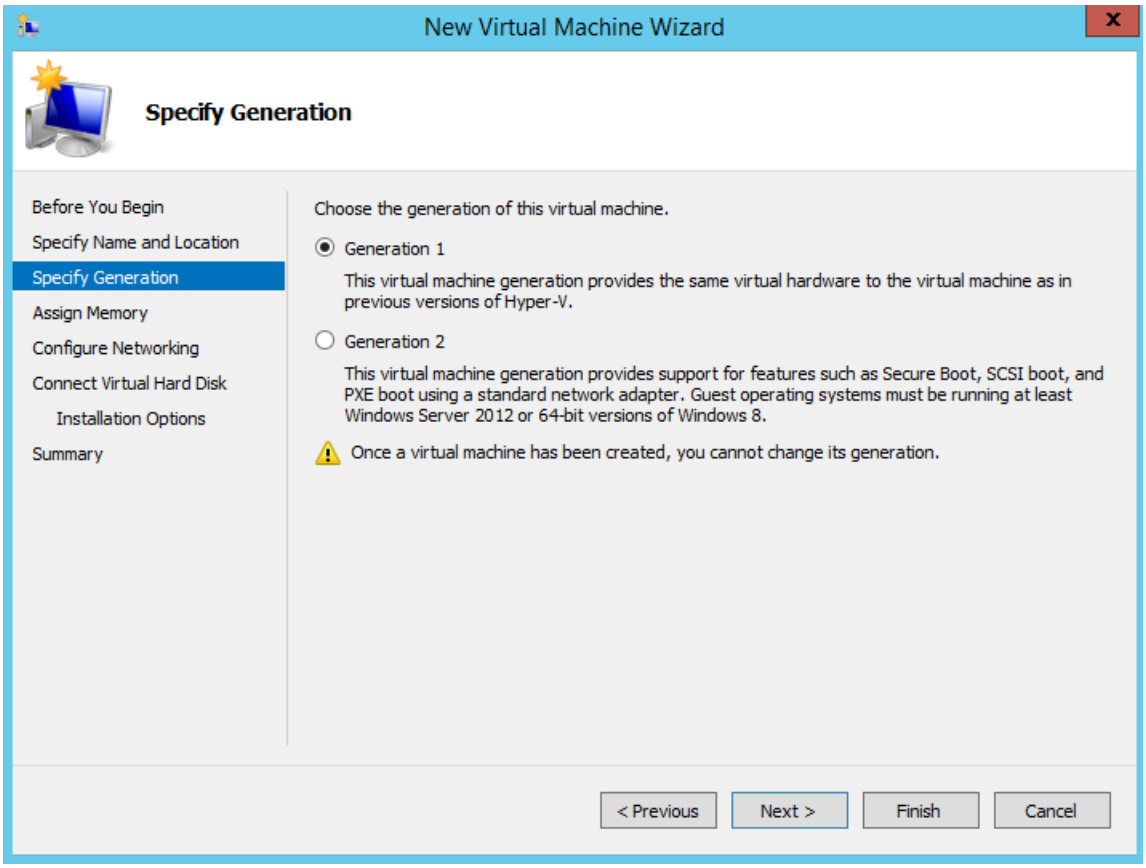
그림 *12:* 이름 및 위치 지정



단계 **5** **Generation 1(1**세대**)** 라디오 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.

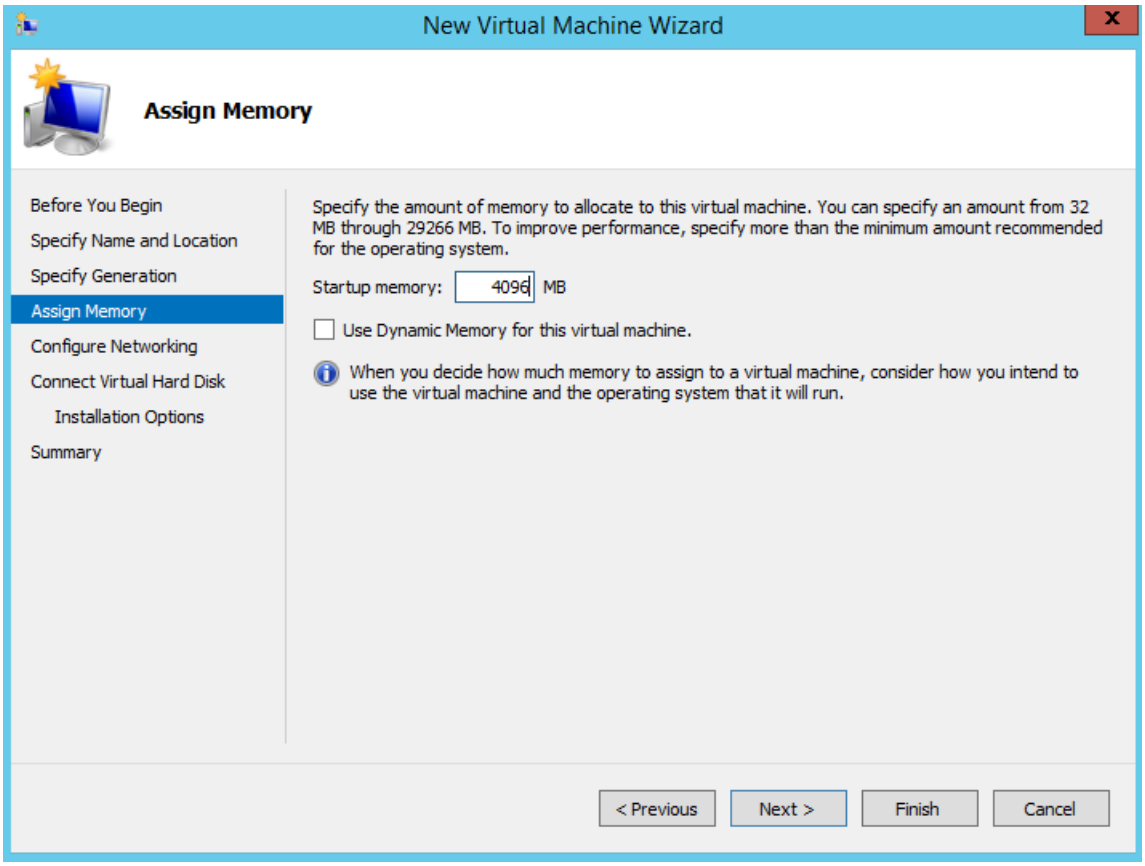
Generation 2(2세대) ISE VM을 생성한다면, VM 설정에서 **Secure Boot(**보안 부팅**)** 옵션을 비활성화해야 합니다.

그림 *13:* 세대 지정



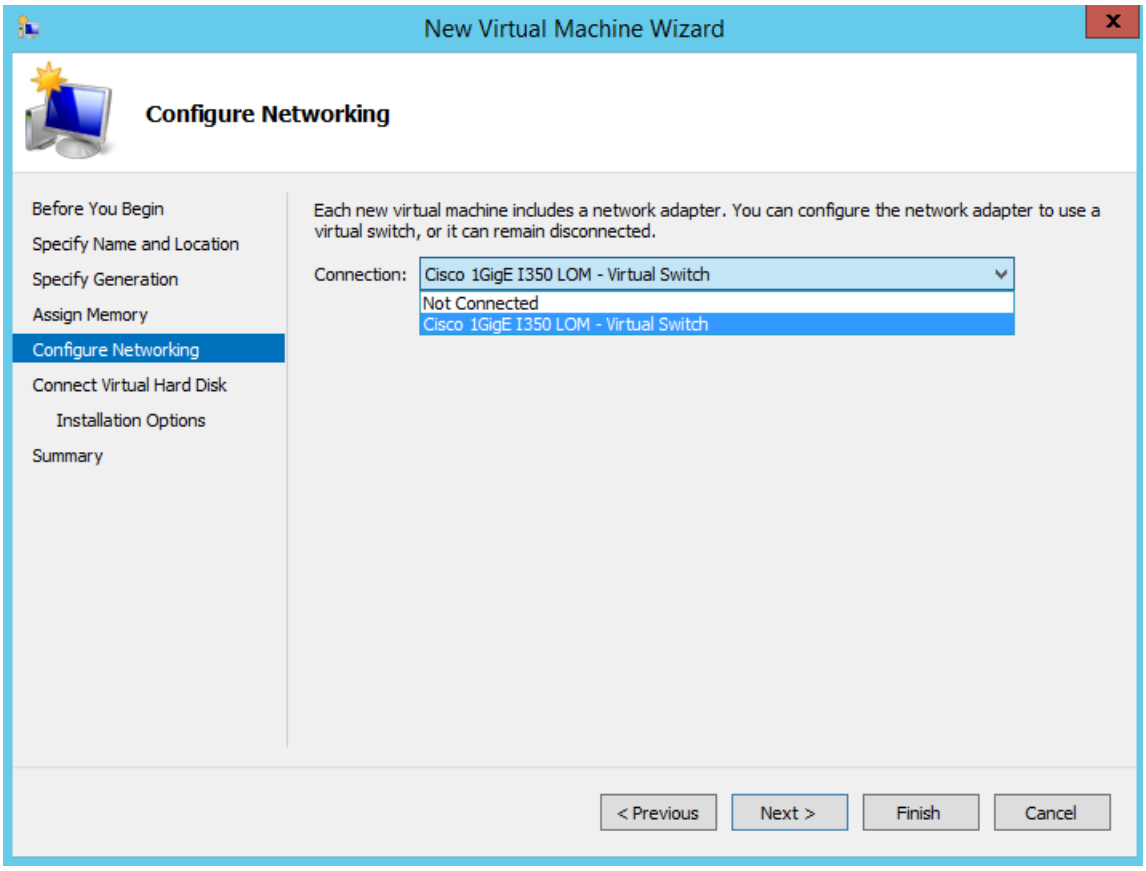
단계 **6** 이 VM에 할당할 메모리의 크기(예: 16000MB)를 지정하고 **Next(**다음**)**를 클릭합니다.

그림 *14:* 메모리 할당



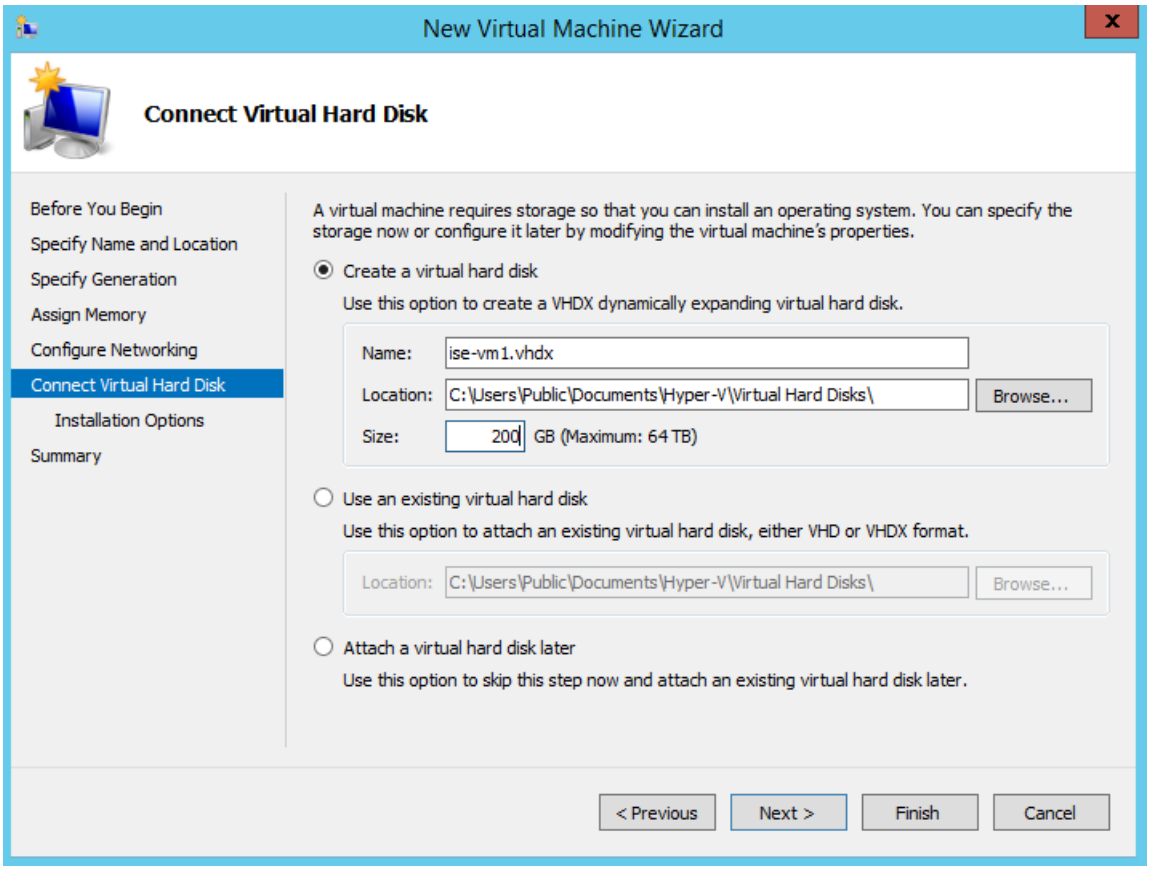
단계 **7** 네트워크 어댑터를 선택하고 **Next(**다음**)**를 클릭합니다.

그림 *15:* 네트워킹 구성



단계 **8** **Create a virtual hard disk(**가상 하드 디스크 생성**)** 라디오 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.

그림 *16:* 가상 하드 디스크 연결

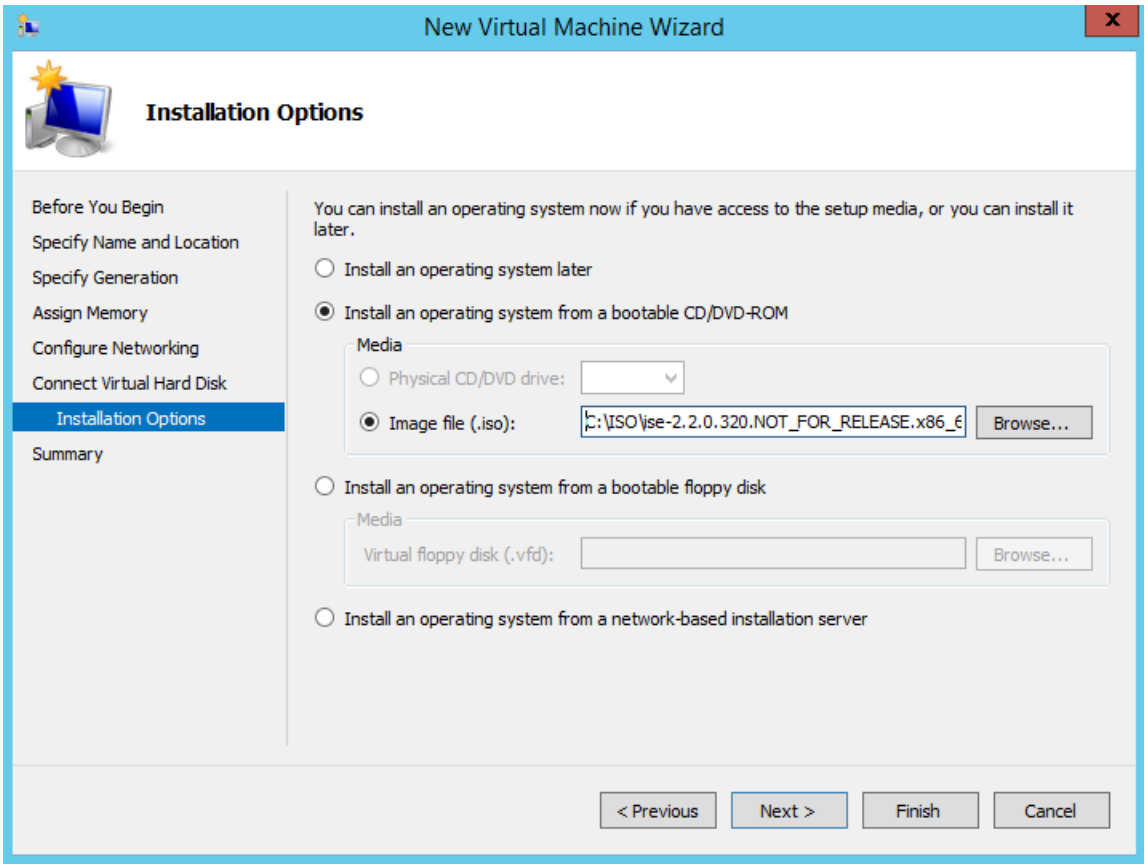


단계 **9** **Install an operating system from a bootable CD/DVD-ROM(**부팅 가능 **CD/DVD-ROM**에서 운영 체제 설치**)** 라디오 버튼을 클릭합니다.

a) Media(미디어) 영역에서 **Image file (.iso)** 라디오 버튼을 클릭합니다.

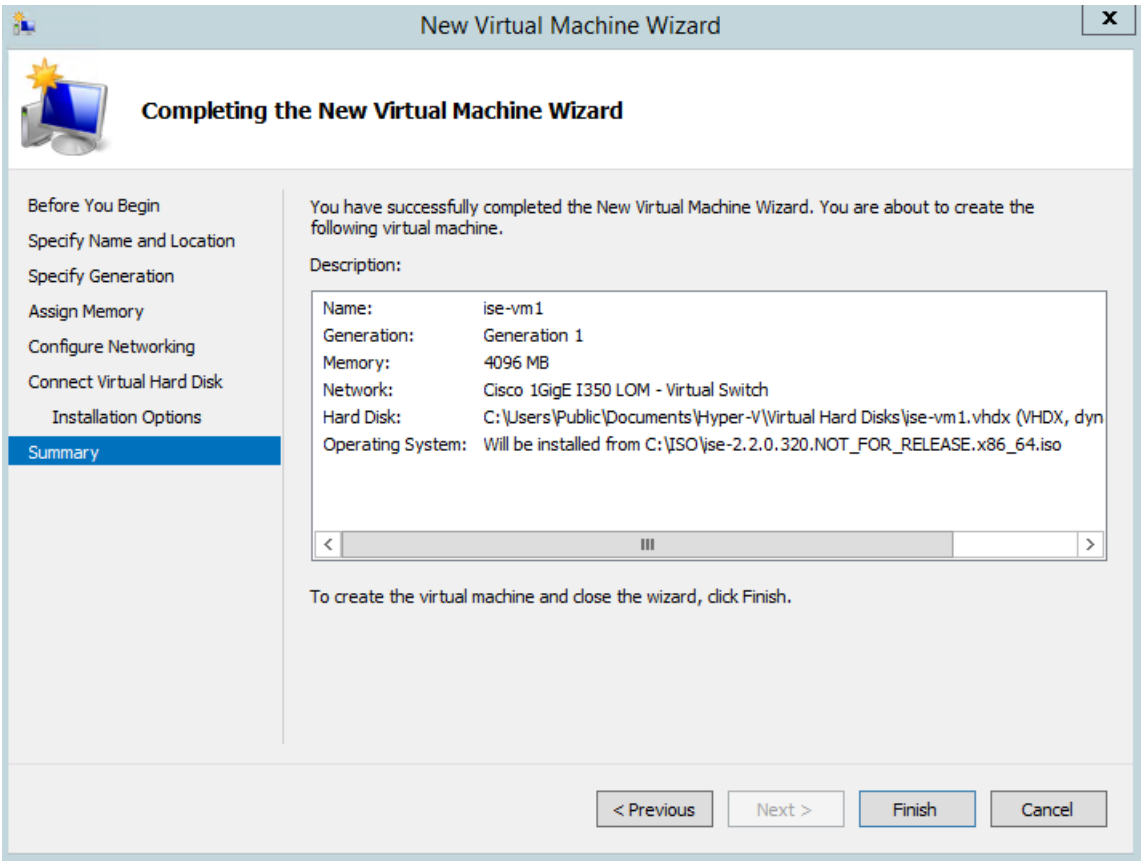
b) **Browse(**찾아보기**)**를 클릭하여 로컬 시스템에서 ISE ISO 이미지를 선택한 후 **Next(**다음**)**를 클릭합니다.

그림 *17:* 설치 옵션



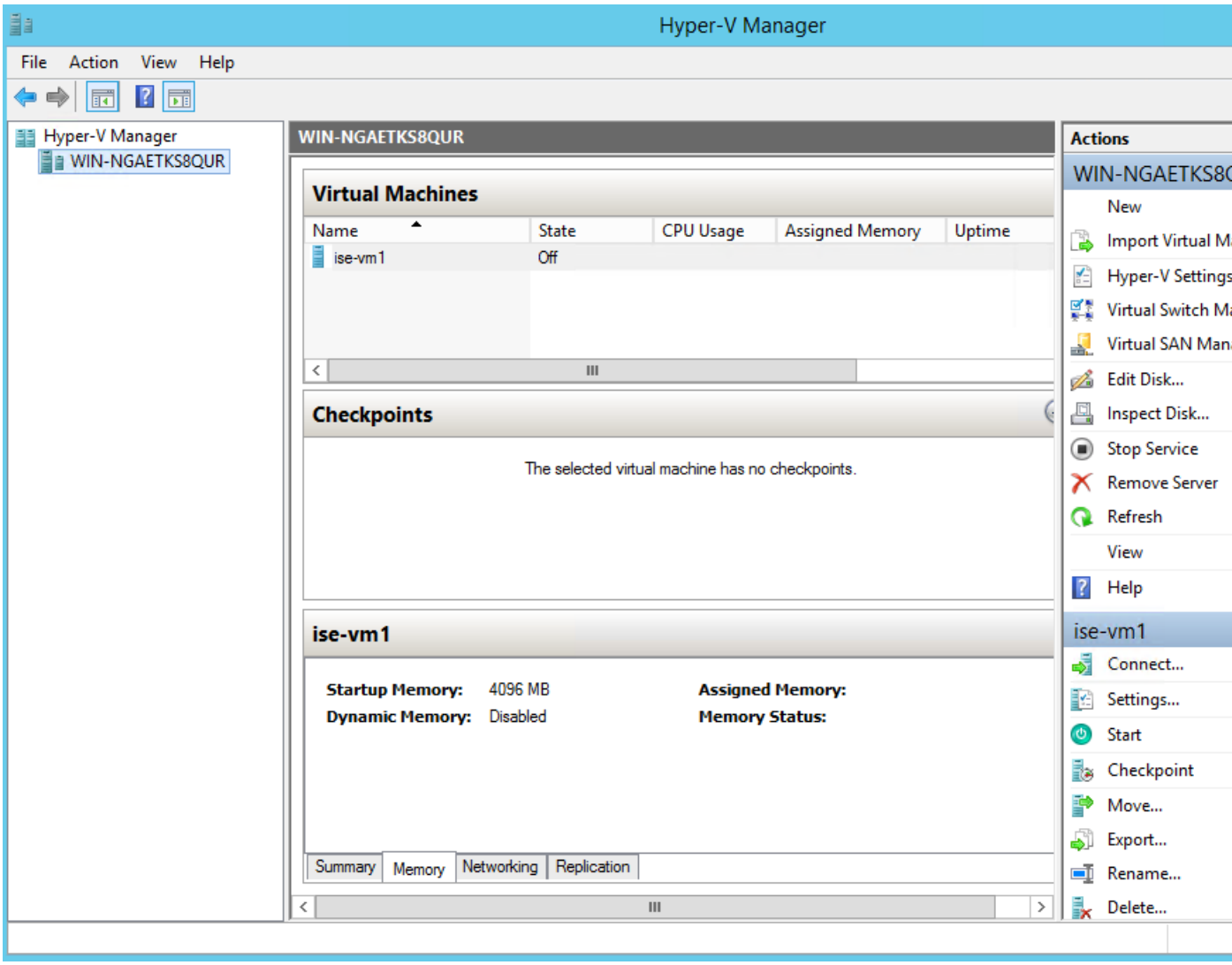
단계 **10** 마침을 클릭합니다.

그림 *18:* 새 가상 머신 마법사 완료



Cisco ISE VM은 Hyper-v에서 생성됩니다.

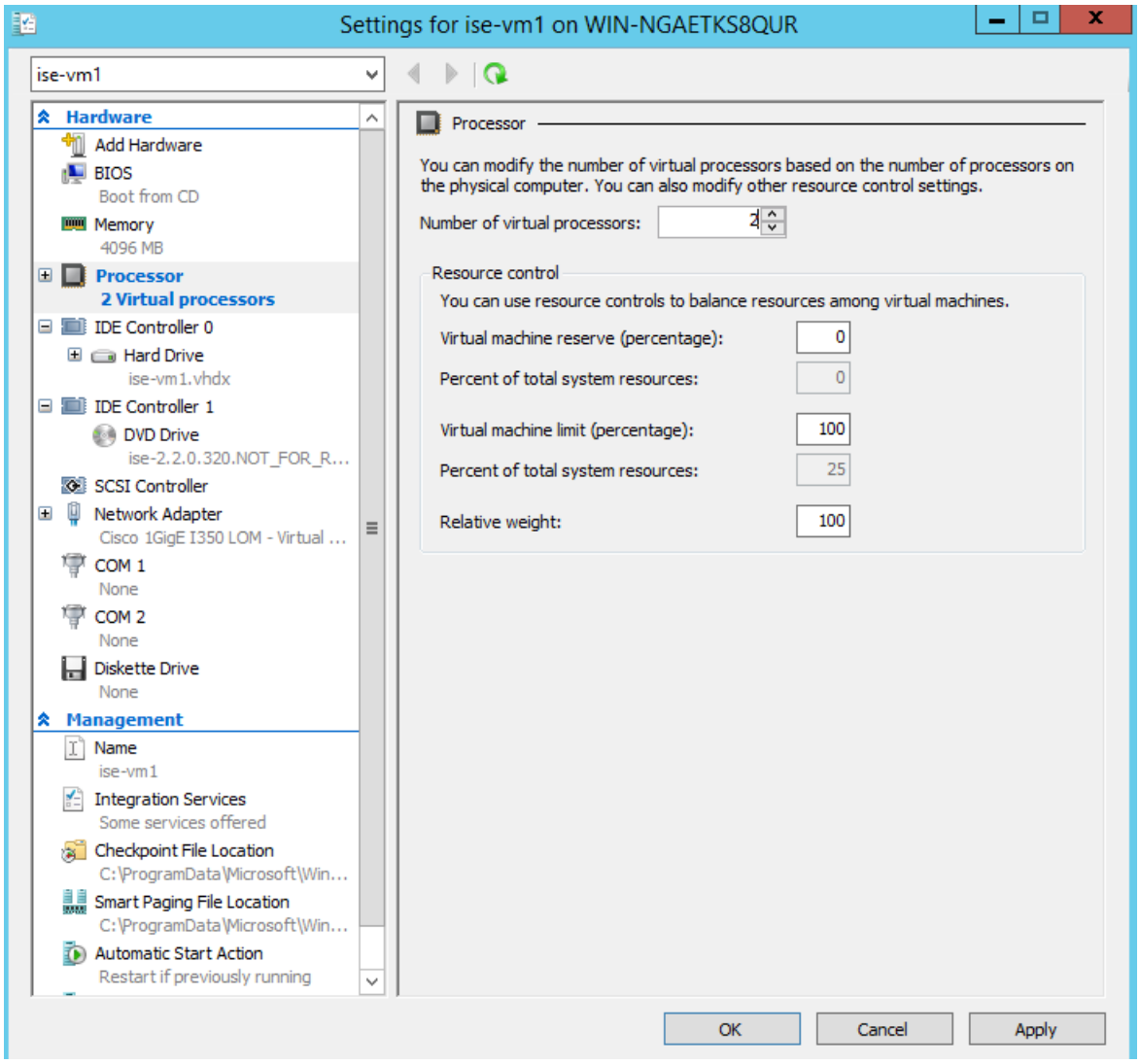
그림 *19:* 새 가상 머신 생성됨



단계 **11** VM을 선택하고 VM 설정을 수정합니다.

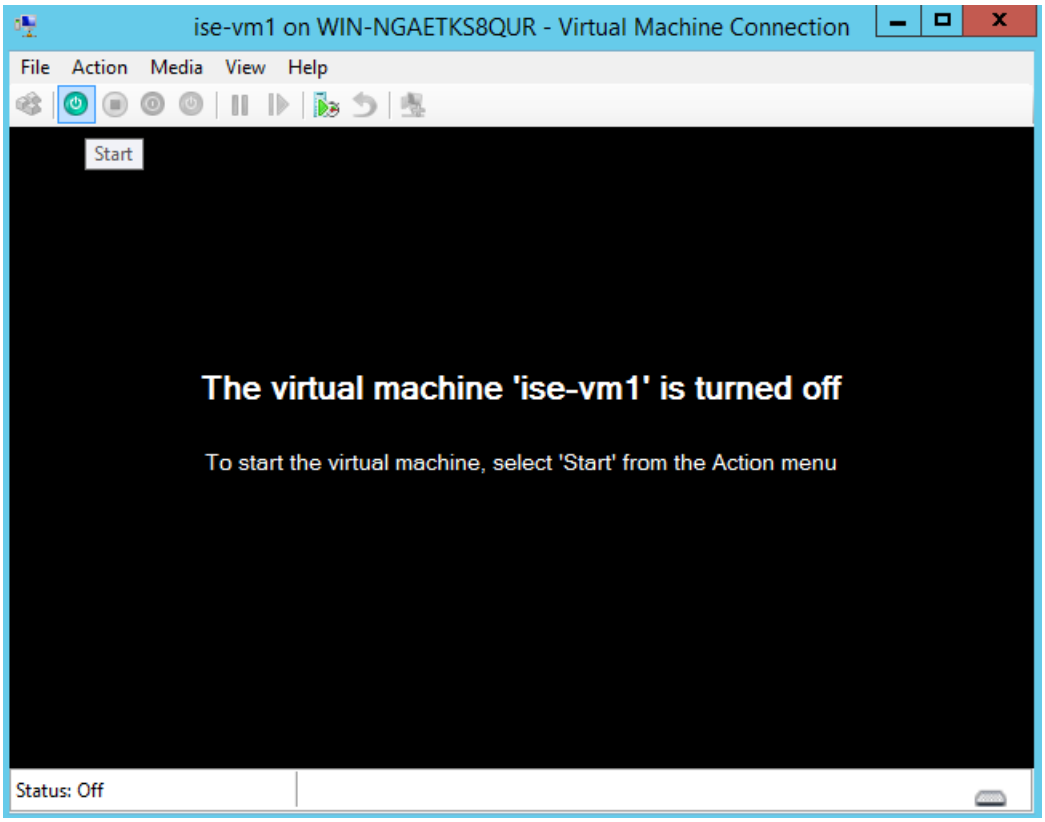
a) **Processor(**프로세서**)**를 선택합니다. 가상 프로세서 수(예: 6)를 입력하고 **OK(**확인**)**를 클릭합니다.

그림 *20: VM* 설정 수정



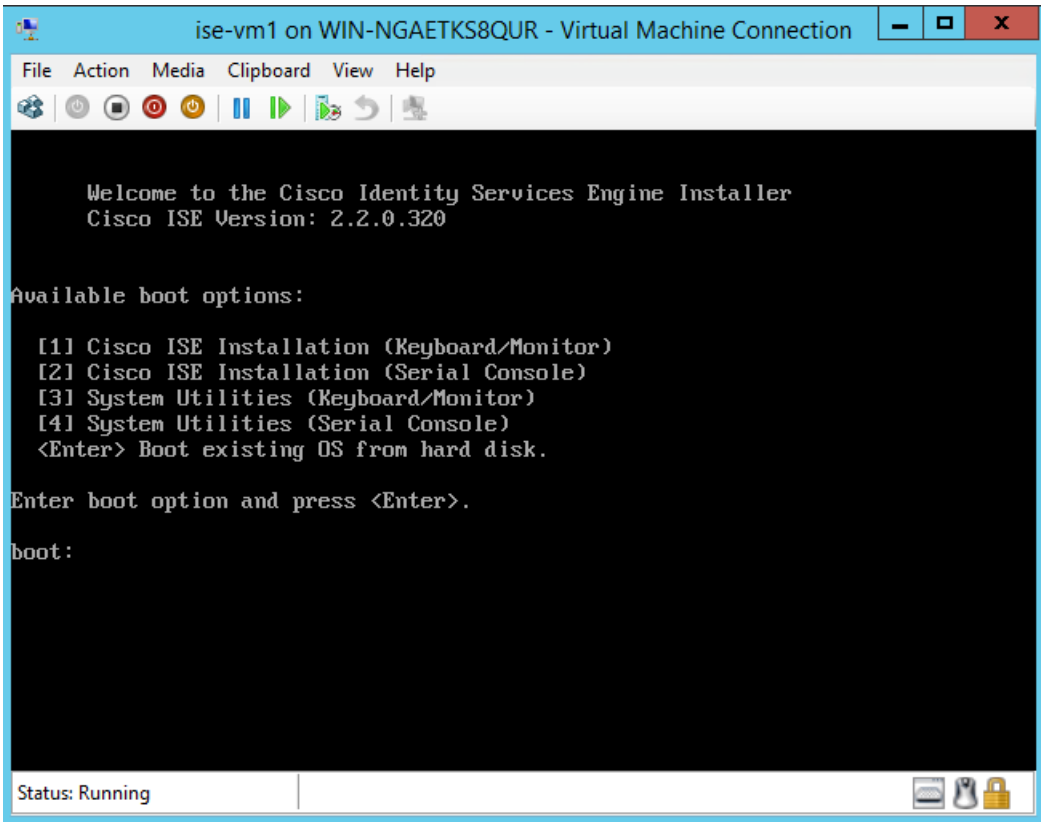
단계 **12** VM을 선택하고 **Connect(**연결**)**를 클릭하여 VM 콘솔을 시작합니다. 시작 버튼을 클릭하여 Cisco ISE VM을 켭니다.

그림 ***21: Cisco ISE VM*** 시작

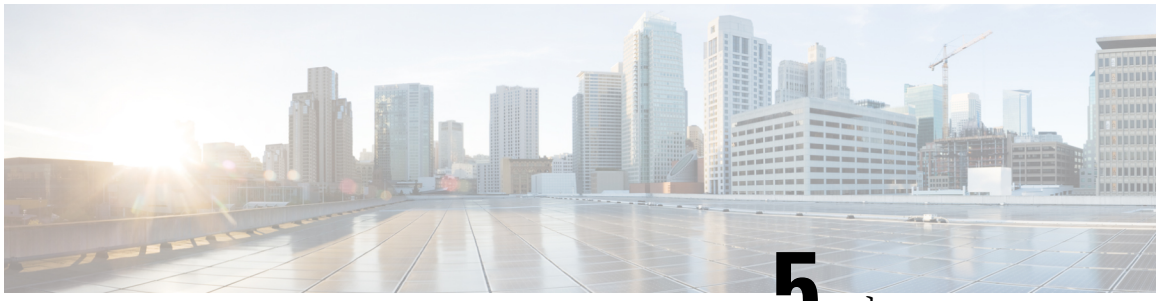


Cisco ISE 설치 메뉴가 나타납니다.

그림 *22: Cisco ISE* 설치 메뉴



단계 **13** **1**을 입력하여 키보드와 모니터로 Cisco ISE를 설치합니다.



5 장

설치 확인 및 설치 후 작업

Cisco ISE 웹 기반 인터페이스에 로그인

Cisco ISE 웹 기반 인터페이스에 처음으로 로그인할 때는 미리 설치된 평가 라이센스를 사용합니다.

참고 Cisco ISE 사용자 인터페이스를 사용하여 정기적으로 관리자 로그인 비밀번호를 재설정하는 것이 좋습니다.

주의 보안을 위해 관리 세션을 완료하면 로그아웃하는 것이 좋습니다. 사용자가 로그아웃하지 않고 30분간 활동이 없으면 Cisco ISE 웹 기반 인터페이스가 사용자를 로그아웃하며 전송되지 않은 컨피그레이션 데이터는 저장되지 않습니다.

시작하기 전에

Cisco ISE 관리 포털은 Admin Portal(관리자 포털)에 다음 브라우저를 지원합니다.

- Mozilla Firefox 61 이하 버전
- Mozilla Firefox ESR 60.9 이하 버전
- Google Chrome 80 이하 버전
- Microsoft Internet Explorer 11.x

단계 **1** Cisco ISE 어플라이언스 재부팅이 완료되면 지원되는 웹 브라우저 중 하나를 실행합니다.

단계 **2** Address 필드에서 다음 형식으로 Cisco ISE 어플라이언스의 IP 주소(또는 호스트 이름)를 입력하고 **Enter**를 누릅니다.

```
https://<IP address or host name>/admin/
```

단계 **3** 설정 과정에서 정의한 사용자 이름 및 비밀번호를 입력합니다.

단계 **4** **Login(**로그인**)**을 클릭합니다.

CLI 관리자와 웹 기반 관리자 사용자 작업의 차이점

Cisco ISE 설정 프로그램을 사용하여 구성한 사용자 이름 및 비밀번호는 Cisco ISE CLI 및 Cisco ISE 웹 인터페이스에 대한 관리 액세스에 사용합니다. Cisco ISE CLI에 액세스할 수 있는 관리자는 CLI 관리자 사용자라고 합니다. 기본적으로 CLI 관리자 사용자의 사용자 이름은 admin이며 비밀번호는 설정 프로세스에서 사용자가 정의합니다. 비밀번호는 기본값이 없습니다.

처음에는 CLI 관리자 사용자 이름 및 설정 프로세스에서 정의한 비밀번호를 사용하여 Cisco ISE 웹 인터페이스에 액세스할 수 있습니다. 웹 기반 관리자는 기본 사용자 이름과 비밀번호가 없습니다.

CLI 관리자 사용자는 Cisco ISE 웹 기반 관리자 사용자 데이터베이스에 복사됩니다. 첫 번째 CLI 관리자 사용자만 웹 기반 관리자 사용자로 복사됩니다. 두 관리자 역할에 동일한 사용자 이름과 비밀번호를 사용할 수 있도록 CLI 및 웹 기반 관리자 사용자 저장소를 동기화해야 합니다.

Cisco ISE CLI 관리자 사용자는 Cisco ISE 웹 기반 관리자 사용자와 다른 권한과 기능을 가지며, 별도의 관리 작업을 수행할 수 있습니다.

표 ***12: CLI*** 관리자 및 웹 기반 관리자 사용자가 수행할 작업

관리자 사용자 유형	작업
CLI 관리자 및 웹 기반 관리자 모두	• Cisco ISE 애플리케이션 데이터 백업 • Cisco ISE 어플라이언스의 모든 시스템, 애플리케이션, 진단 로그 표시 • Cisco ISE 소프트웨어 패치, 유지 관리 릴리스, 업그레이드 적용 • NTP 서버 컨피그레이션 설정
CLI 관리자만	• Cisco ISE 애플리케이션 소프트웨어 시작 및 중지 • Cisco ISE 어플라이언스 다시 로드 및 종료 • 잠긴 경우 웹 기반 관리자 사용자 재설정 • ISE CLI 액세스

CLI 관리자 생성

Cisco ISE에서는 설정 프로세스에서 생성한 것이 아닌 CLI 관리자 사용자 계정을 추가로 생성할 수 있습니다. CLI 관리자 사용자 인증서를 보호하기 위해 Cisco ISE CLI 액세스에 최소한 필요한 수의 CLI 관리자 사용자를 생성합니다.

구성 모드에서 다음 명령을 사용하여 CLI 관리자 사용자를 추가할 수 있습니다.

```
username <username> password [plain/hash] <password> role admin
```

웹 기반 관리자 생성

처음으로 웹에서 Cisco ISE 시스템에 액세스할 때 관리자 사용자 이름 및 비밀번호는 설정 과정에서 구성한 CLI 기반 액세스 정보와 동일합니다.

관리자를 추가하려면 다음을 수행합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) System(**시스템**) Admin Access(**관리자 액세스**) Administrators(**관리자**) > Admin Users(**관리 사용자**)**를 선택합니다.
2. **Add(**추가**) > Create an Admin User(**관리자 사용자 생성**)**를 선택합니다.
3. 이름, 암호, 관리자 그룹 및 기타 필수 세부 사항을 입력합니다.
4. **Submit(**제출**)**을 클릭합니다.

관리자 잠금 때문에 비활성화된 암호 재설정

관리자는 잘못된 비밀번호를 몇 번까지 입력하면 계정을 비활성화할 것인지 지정할 수 있습니다. 최소값이자 기본값은 5입니다.

다음 지침을 따르면 Cisco ISE CLI에서 **application reset-passwd ise** 명령으로 관리자 사용자 인터페이스 암호를 재설정할 수 있습니다. 이는 관리자의 CLI 비밀번호에는 영향을 주지 않습니다. 관리자 비밀번호를 성공적으로 재설정하면 인증서가 즉시 활성화되고 시스템 재부팅 없이 로그인할 수 있습니다. .

Cisco ISE가 **Administrator Logins(**관리자 로그인**)** 창에 로그 항목을 추가합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 운영 > 보고서 > 보고서 > 감사 > 관리자 로그인입니다. 해당 관리자 ID의 인증서는 해당 관리자 ID와 연결된 암호를 재설정할 때까지 일시 중단됩니다.

단계 **1** 직접 콘솔 CLI에 액세스하고 다음을 입력합니다.

application reset-passwd ise administrator_ID

단계 **2** 이 관리자 ID에 사용되었던 이전의 두 비밀번호와 다른 새 비밀번호를 지정하고 확인합니다.

```
Enter new password:
Confirm new password:
```

```
Password reset successfully
```

Cisco ISE 컨피그레이션 확인

웹 브라우저와 CLI에서 각기 다른 사용자 이름 및 비밀번호 인증서를 사용하여 Cisco ISE 컨피그레이션을 확인할 수 있습니다.

참고 Cisco ISE에서는 CLI 관리자 사용자의 인증서와 웹 기반 관리자 사용자의 인증서가 서로 다릅니다.

웹 브라우저에서 컨피그레이션 확인

단계 **1** Cisco ISE 어플라이언스 재부팅이 완료되면 지원되는 웹 브라우저 중 하나를 실행합니다.

단계 **2** 주소 필드에 Cisco ISE 어플라이언스의 IP 주소(또는 호스트 이름)를 다음 형식으로 입력하고 **Enter**를 누릅니다.

단계 **3** Cisco ISE Login 페이지에서 설정 과정에 정의한 사용자 이름 및 비밀번호를 입력하고 **Login**을 클릭합니다.

예를 들어 https://10.10.10.10/admin/을 입력하면 Cisco ISE Login 페이지가 표시됩니다.

```
https://<IP address or host name>/admin/
```

참고 처음으로 웹에서 Cisco ISE 시스템에 액세스할 때 관리자 사용자 이름 및 비밀번호는 설정 과정에서 구성한 CLI 기반 액세스 정보와 동일합니다.

단계 **4** Cisco ISE 대시보드를 사용하여 어플라이언스가 제대로 작동하는지 확인합니다.

다음에 수행할 작업

Cisco ISE 웹 기반 사용자 인터페이스 메뉴 및 옵션을 사용하여 필요에 맞게 Cisco ISE 시스템을 구성할 수 있습니다. Cisco ISE 구성에 대한 자세한 내용은 *Cisco Identity Services Engine* 관리자 설명서를 참조하십시오.

CLI로 컨피그레이션 확인

시작하기 전에

최신 Cisco ISE 패치를 가져오고 Cisco ISE를 최신 버전으로 유지하려면 https://software.cisco.com/download/home/283801620/type를 방문하십시오.

단계 **1** Cisco ISE 어플라이언스 재부팅이 완료되면 Cisco ISE 어플라이언스와의 SSH(Secure Shell) 연결을 설정하기 위해 PuTTY와 같이 지원되는 제품을 실행합니다.

단계 **2** Host Name(또는 IP Address) 필드에 호스트 이름(또는 점으로 구분된 10진수 형식인 Cisco ISE 어플라이언스의 IP 주소)을 입력하고 **Open**을 클릭합니다.

단계 **3** 로그인 프롬프트에 설정 과정에서 구성한 CLI 관리자 사용자 이름(admin이 기본값)을 입력하고 **Enter**를 누릅니다.

단계 **4** 비밀번호 프롬프트에 설정 과정에서 구성한 CLI 관리자 비밀번호를 입력하고(사용자가 정의한 값이며 기본값은 없음) **Enter**를 누릅니다.

단계 **5** 시스템 프롬프트에서 **show application version ise**을 입력하고 **Enter**를 누릅니다.

단계 **6** Cisco ISE 프로세스의 상태를 확인하려면 **show application status ise**를 입력하고 **Enter**를 누릅니다.

콘솔에 아래와 같이 출력됩니다.

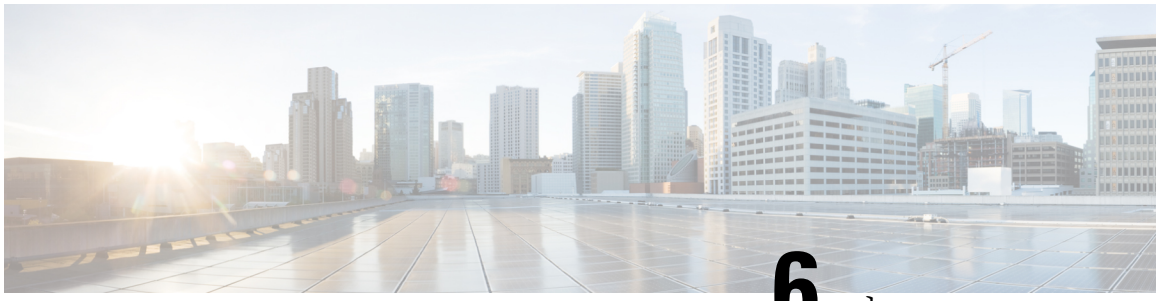
```
ise-server/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4930
Database Server                        running          66 PROCESSES
Application Server                     running          8231
Profiler Database                      running          6022
ISE Indexing Engine                    running          8634
AD Connector                           running          9485
M&T Session Database                   running          3059
M&T Log Collector                      running          9271
M&T Log Processor                      running          9129
Certificate Authority Service          running          8968
EST Service                            running          18887
SXP Engine Service                     disabled
TC-NAC Docker Service                  disabled
TC-NAC MongoDB Container               disabled
TC-NAC RabbitMQ Container              disabled
TC-NAC Core Engine Container           disabled
VA Database                            disabled
VA Service                             disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID Service                      disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
```

설치 후 작업 목록

Cisco ISE 설치가 끝나면 다음 필수 작업을 수행해야 합니다.

표 **13:** 필수 설치 후 작업

작업	관리 지침서 내 링크
(존재하는 경우) 최신 패치 적용	해당 릴리스의 *Cisco ISE* 관리자 가이드에서 "유지 보수 및 모니터링" 장의 "소프트웨어 패치 설치 지침"섹션을 참조하십시오.
라이센스 설치	자세한 내용은 Cisco ISE Ordering Guide(Cisco ISE 주문 가이드)를 참조하십시오. 해당 릴리스의 *Cisco ISE* 관리자 가이드에서 "라이선싱" 장을 참조하십시오.
인증서 설치	릴리스에 대한 *Cisco ISE* 관리자 설명서의 "기본 설정" 장에서 "Cisco ISE의 인증서 관리" 섹션을 참조하십시오.
백업용 저장소 생성	릴리스에 대한 *Cisco ISE* 관리자 가이드의 "유지 관리 및 모니터링" 장에서 "리포지토리 생성" 섹션을 참조하십시오.
백업 예약 구성	해당 릴리스의 *Cisco ISE* 관리자 가이드에서 "유지 관리 및 모니터링" 장의 "백업 예약" 섹션을 참조하십시오.
Cisco ISE 페르소나 구축	릴리스에 대한 *Cisco ISE* 관리자 가이드의 "구축" 장에서 "Cisco ISE 분산 구축" 섹션을 참조하십시오.



6 장

일반적인 시스템 유지 보수 작업

고가용성을 위한 이더넷 인터페이스 결합

Cisco ISE는 이더넷 인터페이스 2개를 단일 가상 인터페이스로 결합하여 물리적 인터페이스에 고가용성을 제공하는 기능을 지원합니다. 이 기능을 NIC(Network Interface Card) 결합 또는 NIC 티밍이라고 합니다. 인터페이스 2개가 결합되면 NIC 2개가 같은 장치에서 같은 MAC 주소를 사용하는 것처럼 보입니다.

Cisco ISE의 NIC 결합 기능은 로드 밸런싱이나 링크 어그리게이션 기능은 지원하지 않습니다. Cisco ISE는 NIC 결합의 고가용성 기능만 지원합니다.

인터페이스를 결합하면 다음과 같은 경우에도 Cisco ISE 서비스가 영향을 받지 않게 됩니다.

- 물리적 인터페이스 장애
- 스위치 포트 연결 끊김(종료 또는 장애)
- 스위치 라인 카드 장애

인터페이스 2개가 결합되면 인터페이스 하나가 기본 인터페이스가 되고 다른 인터페이스는 백업 인터페이스가 됩니다. 인터페이스 2개가 결합되면 모든 트래픽은 일반적으로 기본 인터페이스를 통해 흐릅니다. 어떤 이유로 기본 인터페이스에서 장애가 발생하면, 백업 인터페이스가 대신 모든 트래픽을 처리합니다. 결합한 인터페이스는 기본 인터페이스의 IP 주소와 MAC 주소를 가져옵니다.

NIC 결합 기능을 구성할 때 Cisco ISE는 고정된 물리적 NIC를 페어링하여 NIC 결합체를 형성합니다. 다음 표에는 함께 결합하여 결합된 인터페이스를 형성할 수 있는 NIC가 요약되어 있습니다.

표 ***14:*** 물리적 ***NIC***가 결합되어 인터페이스 형성

Cisco ISE 물리적 **NIC** 이름	**Linux** 물리적 **NIC** 이름	결합한 **NIC**에서의 역할	결합한 **NIC** 이름
기가비트 이더넷 0	Eth0	기본	결합 0
기가비트 이더넷 1	Eth1	백업	
기가비트 이더넷 2	Eth2	기본	결합 1
기가비트 이더넷 3	Eth3	백업	
기가비트 이더넷 4	Eth4	기본	결합 2
기가비트 이더넷 5	Eth5	백업	

지원되는 플랫폼

NIC 결합 기능은 지원되는 모든 플랫폼과 노드 페르소나에서 지원됩니다. 지원되는 플랫폼은 다음과 같습니다.

- SNS 3500 및 3600 시리즈 어플라이언스 - 결합 0, 1, 2
- VMware 가상 머신 - 결합 0, 1, 2(가상 머신에 NIC 6개를 사용할 수 있는 경우)
- Linux KVM 노드 - 결합 0, 1, 2(가상 머신에 NIC 6개를 사용할 수 있는 경우)

이더넷 인터페이스 결합 지침

- Cisco ISE는 이더넷 인터페이스를 6개까지 지원하므로 결합 3개, 즉 결합 0, 결합 1, 결합 2만 가질 수 있습니다.
- 결합에 속하는 인터페이스를 변경하거나 결합 내 인터페이스의 역할을 변경할 수는 없습니다. 결합할 수 있는 NIC와 결합에서 NIC가 하는 역할에 관한 정보는 위의 표를 참조하십시오.
- Eth0 인터페이스는 관리 인터페이스와 런타임 인터페이스 역할을 모두 수행합니다. 다른 인터페이스는 런타임 인터페이스 역할을 합니다.
- 결합을 생성하기 전에 기본 인터페이스(기본 NIC)에 IP 주소를 할당해야 합니다. 결합 0을 생성하기 전에 Eth0 인터페이스에 IPv4 주소를 할당해야 합니다. 마찬가지로 결합 1과 2를 생성하기 전에 Eth2 및 Eth4 인터페이스에 각각 IPv4 또는 IPv6 주소를 할당해야 합니다.
- 결합을 생성하기 전에 백업 인터페이스(Eth1, Eth3 및 Eth5)에 IP 주소가 할당되어 있다면, 백업 인터페이스에서 IP 주소를 제거해야 합니다. 백업 인터페이스에는 IP 주소를 할당하면 안 됩니다.

- 결합을 하나만(결합 0) 생성하고 인터페이스의 나머지 부분은 그대로 유지되게 할 수도 있습니다. 이 경우 결합 0은 관리 인터페이스와 런타임 인터페이스 역할을 하며, 인터페이스의 나머지 부분은 런타임 인터페이스 역할을 합니다.
- 결합 내 기본 인터페이스의 IP 주소를 변경할 수 있습니다. 새 IP 주소는 기본 인터페이스의 IP 주소를 가정하기 때문에 결합된 인터페이스에 할당됩니다.
- 두 인터페이스 간의 결합을 제거하면, 결합된 인터페이스에 할당된 IP 주소가 기본 인터페이스에 다시 할당됩니다.
- 구축의 일부인 Cisco ISE 노드에서 NIC 결합 기능을 구성하고 싶다면 구축에서 노드를 등록 취소하고, NIC 결합을 구성한 다음 노드를 구축에 다시 등록해야 합니다.
- 결합(Eth0, Eth2 또는 Eth4 인터페이스)에서 기본 인터페이스 역할을 하는 물리적 인터페이스에 정적 경로가 구성되었다면, 정적 경로는 물리적 인터페이스가 아닌 결합된 인터페이스에서 작동하도록 자동으로 업데이트됩니다.

NIC 결합 구성

Cisco ISE CLI에서 NIC 결합을 구성할 수 있습니다. 다음 절차에서는 Eth0 및 Eth1 인터페이스 간에 결합 0을 구성하는 방법을 설명합니다.

시작하기 전에

백업 인터페이스 역할을 하는 물리적 인터페이스(예: Eth1, Eth3, Eth5 인터페이스)가 IP 주소를 사용하여 구성되었다면, 백업 인터페이스에서 IP 주소를 제거해야 합니다. 백업 인터페이스에는 IP 주소를 할당하면 안 됩니다.

단계 **1** 관리자 계정으로 Cisco ISE CLI에 로그인합니다.

단계 **2** **configure terminal**을 입력하여 구성 모드에 들어갑니다.

단계 **3** **interface GigabitEthernet 0** 명령을 입력합니다.

단계 **4** **backup interface GigabitEthernet 1** 명령을 입력합니다.
콘솔에 다음과 같이 표시됩니다.

```
 % Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure you
want to proceed? Y/N [N]:
```

단계 **5** **Y**를 입력하고 **Enter**를 누릅니다.

이제 결합 0이 구성되었습니다. Cisco ISE가 자동으로 재시작됩니다. 모든 서비스가 정상적으로 작동할 수 있도록 잠시 기다립니다. CLI에서 **show application status ise** 명령을 입력하여 모든 서비스가 실행 중인지 확인합니다.

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
```

```
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

NIC 결합 구성 확인

NIC 결합 기능이 구성되었는지 확인하려면 Cisco ISE CLI에서 **show running-config** 명령을 실행합니다. 다음과 비슷한 출력이 표시됩니다.

```
!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
```

위의 출력에서 'backup interface GigabitEthernet 1'은 NIC 결합이 기가비트 이더넷 0에 구성되었음을 보여줍니다. 기가비트 이더넷 0은 기본 인터페이스이고 기가비트 이더넷 1은 백업 인터페이스입니다. 또한 기본 및 백업 인터페이스가 사실상 동일한 IP 주소를 이용하더라도, ADE-OS 구성은 실행 중인 컨피그레이션의 백업 인터페이스에 IP 주소를 표시하지 않습니다.

show interface 명령을 실행하여 결합된 인터페이스를 확인하는 방법도 있습니다.

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::8a5a:92ff:fe88:4aea  prefixlen 64  scopeid 0x20<link>
        ether 88:5a:92:88:4a:ea  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
```

```
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfab00000-fabfffff

GigabitEthernet 1
        flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfaa00000-faafffff
```

NIC 결합 제거

backup interface 명령의 **no** 양식을 이용해 NIC 결합을 제거합니다.

시작하기 전에

단계 **1** 관리자 계정으로 Cisco ISE CLI에 로그인합니다.

단계 **2** **configure terminal**을 입력하여 구성 모드에 들어갑니다.

단계 **3** **interface GigabitEthernet 0** 명령을 입력합니다.

단계 **4** **no backup interface GigabitEthernet 1** 명령을 입력합니다.

```
% Notice: Bonded Interface bond 0 has been removed.
```

단계 **5** **Y**를 입력하고 Enter를 누릅니다.

결합 0이 제거되었습니다. Cisco ISE가 자동으로 재시작됩니다. 모든 서비스가 정상적으로 작동할 수 있도록 잠시 기다립니다. CLI에서 **show application status ise** 명령을 입력하여 모든 서비스가 실행 중인지 확인합니다.

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
```

```
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

DVD를 사용하여 잊었거나 손상된 암호 재설정

시작하기 전에

Cisco ISE 소프트웨어 DVD를 사용하여 Cisco ISE 어플라이언스를 시작할 때 문제를 일으킬 수 있는 다음과 같은 연결 관련 조건을 알아두십시오.

- 터미널 서버가 exec으로 설정된 Cisco ISE 어플라이언스에 직렬 콘솔을 통해 연결되어 있습니다. 이를 *no exec*으로 설정하면 키보드 및 비디오 모니터 연결과 직렬 콘솔 연결을 사용할 수 있습니다.
- Cisco ISE 어플라이언스와 키보드 및 비디오 모니터 연결이 설정되어 있습니다(원격 키보드 및 비디오 모니터 연결 또는 VMware vSphere 클라이언트 콘솔 연결).
- Cisco ISE 어플라이언스와의 직렬 콘솔 연결이 설정되어 있습니다.

단계 **1** Cisco ISE 어플라이언스의 전원이 켜져 있어야 합니다.

단계 **2** Cisco ISE 소프트웨어 DVD를 삽입합니다.

예를 들어 Cisco ISE 3515 콘솔에 다음과 같은 메시지가 표시됩니다.

```
Cisco ISE Installation (Serial Console)
  Cisco ISE Installation (Keyboard/Monitor)
  System Utilities (Serial Console)
  System Utilities (Keyboard/Monitor)
```

단계 **3** 로컬 직렬 콘솔 포트 연결을 사용한다면 화살표 키를 사용하여 시스템 유틸리티**(**직렬 콘솔**)**를 선택하고, 어플라이언스에 키보드 및 비디오 모니터 연결을 사용한다면 시스템 유틸리티**(**키보드/모니터를 선택한 다음, **Enter**를 누릅니다.

ISO 유틸리티 메뉴가 아래와 같이 표시됩니다.

```
Available System Utilities:
  [1] Recover Administrator Password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload
Enter option [1 - 3] q to Quit:
```

단계 **4** 관리자 비밀번호를 복구하려면 **1**을 입력합니다.

콘솔에 다음과 같이 표시됩니다.

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.

[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4

Enter choice between [1 - 4] or q to Quit: 2

Password:
Verify password:

Save change and reboot? [Y/N]:
```

단계 **5** 비밀번호를 재설정하려는 관리자 사용자에 해당하는 번호를 입력합니다.

단계 **6** 새 비밀번호를 입력하고 확인합니다.

단계 **7** **Y**를 입력하여 변경 사항을 저장합니다.

관리자 잠금 때문에 비활성화된 암호 재설정

관리자는 잘못된 비밀번호를 몇 번까지 입력하면 계정을 비활성화할 것인지 지정할 수 있습니다. 최소값이자 기본값은 5입니다.

다음 지침을 따르면 Cisco ISE CLI에서 **application reset-passwd ise** 명령으로 관리자 사용자 인터페이스 암호를 재설정할 수 있습니다. 이는 관리자의 CLI 비밀번호에는 영향을 주지 않습니다. 관리자 비밀번호를 성공적으로 재설정하면 인증서가 즉시 활성화되고 시스템 재부팅 없이 로그인할 수 있습니다. .

Cisco ISE가 **Administrator Logins(**관리자 로그인**)** 창에 로그 항목을 추가합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 운영 > 보고서 > 보고서 > 감사 > 관리자 로그인입니다. 해당 관리자 ID의 인증서는 해당 관리자 ID와 연결된 암호를 재설정할 때까지 일시 중단됩니다.

단계 **1** 직접 콘솔 CLI에 액세스하고 다음을 입력합니다.

application reset-passwd ise administrator_ID

단계 **2** 이 관리자 ID에 사용되었던 이전의 두 비밀번호와 다른 새 비밀번호를 지정하고 확인합니다.

```
Enter new password:
Confirm new password:

Password reset successfully
```

RMA(Return Material Authorization)

RMA(Return Material Authorization)의 경우 SNS 서버에서 개별 구성 요소를 교체한다면, Cisco ISE를 설치 하기 전에 어플라이언스를 다시 설치해야 합니다. Cisco TAC에 지원을 요청하십시오.

Cisco ISE Appliance의 IP 주소 변경

시작하기 전에

- IP 주소를 변경하기에 앞서 Cisco ISE 노드가 독립형 상태인지 확인합니다. 노드가 분산 구축에 포함된 경우 그 구축에서 노드를 등록 취소하고 독립형 노드로 만듭니다.
- Cisco ISE Appliance IP 주소를 변경할 때는 **no ip address** 명령은 사용하지 마십시오.

단계 **1** Cisco ISE CLI에 로그인합니다.

단계 **2** 다음 명령을 입력합니다.

a) **configure terminal**
b) **interface GigabitEthernet 0**
c) **ip address new_ip_address new_subnet_mask**

IP 주소 변경에 대한 메시지가 표시됩니다. **Y**을 입력합니다. 다음과 비슷한 화면이 나타납니다.

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0

% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
```

```
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
```

Cisco ISE에서 시스템을 다시 시작하라는 메시지를 표시합니다.

단계 **3** **Y**를 입력하여 시스템을 다시 시작합니다.

설치 및 업그레이드 기록 보기

Cisco ISE에서는 Cisco ISE 릴리스 및 패치의 설치, 업그레이드, 제거 세부 사항을 볼 수 있도록 CLI(Command Line Interface) 명령을 제공합니다. **show version history** 명령은 다음 세부 사항을 제공합니다.

- Date—설치 또는 제거가 수행된 날짜와 시간
- Application—Cisco ISE 애플리케이션
- Version—설치되었거나 제거된 버전
- Action—설치, 제거, 패치 설치 또는 패치 제거
- Bundle Filename—설치되었거나 제거된 번들의 이름
- Repository—설치된 Cisco ISE 애플리케이션 번들이 있던 리포지토리 제거에는 해당되지 않습니다.

단계 **1** Cisco ISE CLI에 로그인합니다.

단계 **2** **show version history** 명령을 입력합니다.

다음과 같이 출력됩니다.

```
ise/admin# show version history
--------------------------------------------
Install Date: Fri Nov 30 21:48:58 UTC 2018
Application: ise
Version: 3.0.0.xxx
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

시스템 지우기 수행

시스템 지우기를 수행하여 Cisco ISE 어플라이언스 또는 VM의 모든 정보를 안전하게 지울 수 있습니다. 이 시스템 지우기 옵션을 통해 Cisco ISE에서 NIST Special Publication 800-88 데이터 삭제 표준을 준수할 수 있습니다.

시작하기 전에

Cisco ISE 소프트웨어 DVD를 사용하여 Cisco ISE 어플라이언스를 시작할 때 문제를 일으킬 수 있는 다음과 같은 연결 관련 조건을 알아두십시오.

- 터미널 서버가 exec으로 설정된 Cisco ISE 어플라이언스에 직렬 콘솔을 통해 연결되어 있습니다. 이를 *no exec*으로 설정하면 KVM 연결 및 직렬 콘솔 연결을 사용할 수 있습니다.
- Cisco ISE 어플라이언스와 KVM(keyboard and video monitor) 연결이 설정되어 있습니다(원격 KVM 또는 VMware vSphere 클라이언트 콘솔 연결).
- Cisco ISE 어플라이언스와의 직렬 콘솔 연결이 설정되어 있습니다.

단계 **1** Cisco ISE 어플라이언스의 전원이 켜져 있어야 합니다.

단계 **2** Cisco ISE 소프트웨어 DVD를 삽입합니다.

예를 들어 Cisco ISE 3515 콘솔에 다음과 같은 메시지가 표시됩니다.

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

단계 **3** 화살표 키를 사용하여시스템 유틸리티**(**직렬 콘솔**)**를 선택하고 Enter를 누릅니다.

ISO 유틸리티 메뉴가 아래와 같이 표시됩니다.

```
Available System Utilities:

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reload

Enter option [1 - 3] q to Quit:
```

단계 **4** **3**을 입력하여 시스템 지우기를 수행합니다.

콘솔에 다음과 같이 표시됩니다.

```
 **********   W A R N I N G   **********
THIS UTILITY WILL PERFORM A SYSTEM ERASE ON THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS TO
COMPLETE. THE RESULT WILL BE COMPLETE
```

```
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL MEDIA
 TO RESTORE TO FACTORY DEFAULT STATE.

ARE YOU SURE YOU WANT TO CONTINUE? [Y/N] Y
```

단계 **5** **Y**를 입력합니다.

콘솔에서 또 다른 경고를 표시합니다.

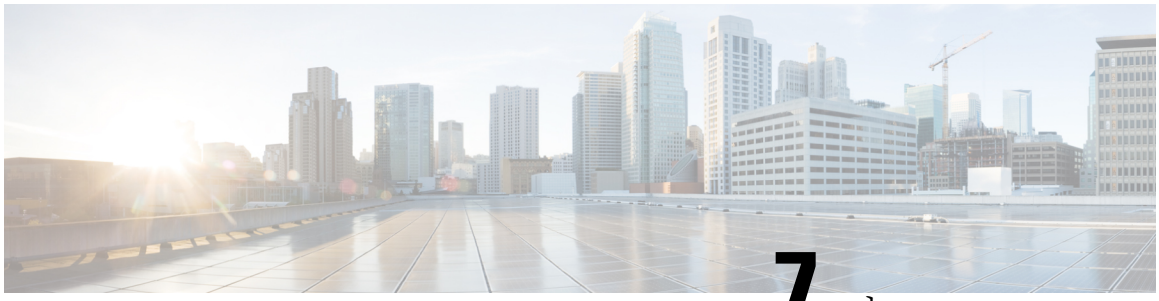
```
THIS IS YOUR LAST CHANGE TO CANCEL. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

단계 **6** **Y**를 입력하여 시스템 지우기를 수행합니다.

콘솔에 다음과 같이 표시됩니다.

```
Deleting system disk, please wait…
Writing random data to all sectors of disk device (/dev/sda)…
Writing zeros to all sectors of disk device (/dev/sda)…
Completed!  System is now erased.
Press <Enter> to reboot.
```

시스템 지우기를 수행한 다음 어플라이언스를 재사용하려면 Cisco ISE DVD를 사용하여 시스템을 부팅하고 부트 메뉴에서 설치 옵션을 선택해야 합니다.



7 장

Cisco ISE 포트 참조

Cisco ISE 모든 페르소나 노드 포트

표 ***15:*** 모든 노드에서 사용하는 포트

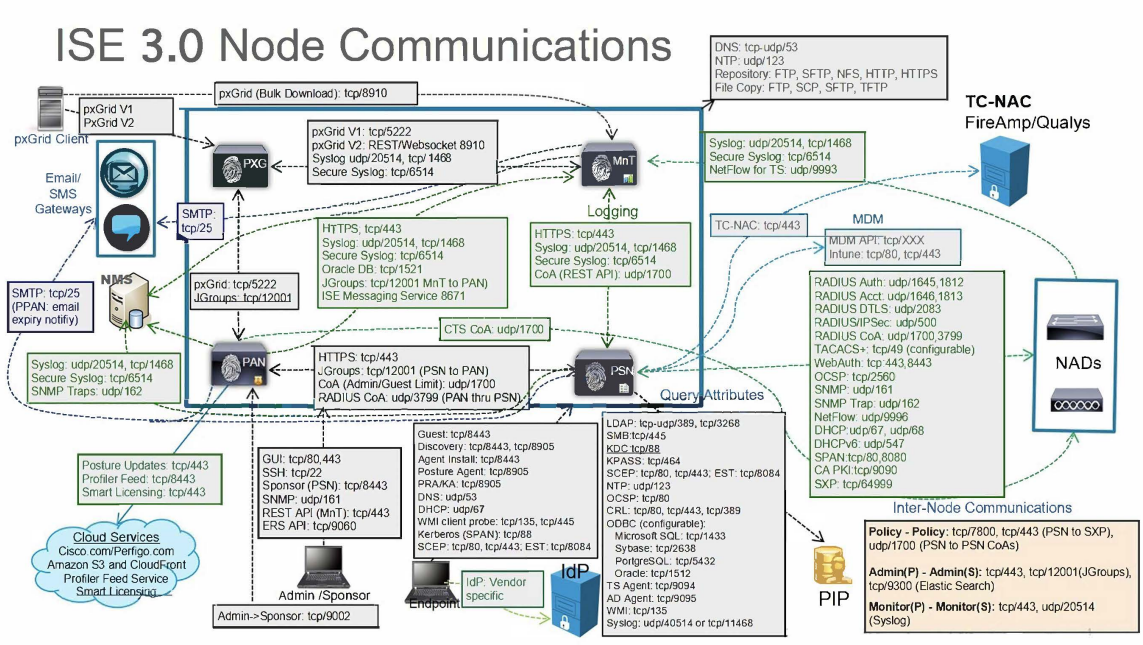
Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스(기가비트 이더넷 **1~5**, 결합 **1** 및 **2**)의 포트
복제 및 동기화	• HTTPS(SOAP): TCP/443 • 데이터 동기화/복제(JGroups): TCP/12001(글로벌) • ISE 메시징 서비스: SSL: TCP/8671 • 프로파일러 엔드포인트 소유권 동기화/복제: TCP/6379	—

Cisco ISE 인프라

이 부록에서는 Cisco ISE에서 외부 애플리케이션 및 디바이스와의 인트라네트워크 통신에 사용하는 TCP 및 User Datagram Protocol UDP 포트를 나열합니다. 이 부록에 나열된 Cisco ISE 포트는 해당 방화벽에서 열린 상태여야 합니다.

Cisco ISE 네트워크에서 서비스를 구성할 때 다음 사항을 기억하십시오.

- 포트는 구축에서 활성화된 서비스에 따라 활성화됩니다. Cisco ISE는 ISE에서 실행 중인 서비스가 여는 포트 외의 다른 모든 포트에 대한 액세스를 거부합니다.
- Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다.
- RADIUS는 모든 NIC(Network Interface Card)에서 수신합니다.
- Cisco ISE 서버 인터페이스는 VLAN 태깅을 지원하지 않습니다. 하드웨어 어플라이언스에 설치하는 경우, Cisco ISE 노드에 연결하는 데 사용하는 스위치 포트에서 VLAN 트렁킹를 비활성화하고 이러한 포트를 액세스 레이어 포트로 구성해야 합니다.
- 임시 포트 범위는 10000 ~ 65500입니다. 이는 Cisco ISE 릴리스 2.1 이상에서도 동일하게 유지됩니다.
- 클라우드의 VMware는 사이트 대 사이트 VPN 네트워크 구성에서 지원됩니다. 따라서 NAT 또는 포트 필터링 없이 네트워크 액세스 디바이스 및 클라이언트에서 Cisco ISE 로의 IP 주소 또는 포트 연결성을 설정해야 합니다.
- 모든 NIC는 IP 주소로 구성할 수 있습니다.



참고 ISE에서 TCP 연결 유지 시간은 60분입니다. ISE 노드간에 TCP 시간 초과 값이 있으면 방화벽에서 적절하게 조정합니다.

Cisco ISE 관리 노드 포트

다음 표에는 관리 노드에서 사용하는 포트가 나와 있습니다.

표 *16:* 관리 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443(TCP/80이 TCP/443으로 리디렉션, 구성 불가) • SSH 서버: TCP/22 • 외부 RESTful 서비스(ERS) REST API: TCP/9060 • 관리자 GUI에서의 게스트 계정 관리: TCP/9002 • ElasticSearch(상황 가시성, 기본 관리자 노드의 데이터를 보조 관리자 노드로 복제): TCP/9300 참고 포트 80 및 443은 관리 웹 애플리케이션을 지원하며 기본적으로 활성화되어 있습니다. Cisco ISE에 대한 HTTPS 및 SSH 액세스는 기가비트 이더넷 0으로 제한됩니다. TCP/9300는 수신 트래픽용 기본 및 보조 관리 노드 모두에서 열려 있어야 합니다.	—

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트
모니터링	• SNMP 쿼리: UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • ICMP	
로깅(아웃바운드)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SNMP 트랩: UDP/162	
외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증 • LDAP: TCP/389, 3268, UDP/389 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • WMI: TCP/135 • ODBC: 참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다. • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PortgreSQL: TCP/5432 • Oracle: TCP/1521 • NTP: UDP/123 • DNS: UDP/53, TCP/53 참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트
Email(이메일)	게스트 계정 및 사용자 암호 만료 이메일 알림: SMTP: TCP/25	
스마트 라이선싱	TCP/443을 통한 Cisco 클라우드 연결	

Cisco ISE 모니터링 노드 포트

다음 표에는 모니터링 노드에서 사용하는 포트가 나와 있습니다.

표 *17:* 모니터링 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443 • SSH 서버: TCP/22	—
모니터링	SNMP(Simple Network Management Protocol): UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • ICMP	
로깅	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SMTP: 알림 이메일용 TCP/25 • SNMP 트랩: UDP/162	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스(기가비트 이더넷 1~5, 결합 1 및 2)의 포트

외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88, UDP/88
	  • KPASS: TCP/464
	• WMI: TCP/135
	• ODBC:
	참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521, 15723, 16820
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

pxGrid용 일괄 다운로드	SSL: TCP/8910	

Cisco ISE 정책 서비스 노드 포트

보안 강화를 위해 Cisco ISE는 HSTS(HTTP Strict Transport Security)를 지원합니다. Cisco ISE는 HTTPS 응답을 보내 HTTPS를 이용해야 ISE에만 액세스할 수 있음을 브라우저에 알립니다. 사용자가 HTTPS가 아닌 HTTP를 이용해 ISE에 액세스하려고 하면, 브라우저는 HTTPS 연결로 변경한 다음 네트워크 트래픽 생성을 시작합니다. 이 기능을 사용하면 서버가 리디렉션하기 전에 브라우저가 암호화되지 않은 HTTP를 사용하여 Cisco ISE에 요청을 전송하는 일을 방지할 수 있습니다.

다음 표에는 정책 서비스 노드에서 사용하는 포트가 나와 있습니다.

표 *18:* 정책 서비스 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트
관리	• HTTP: TCP/80, HTTPS: TCP/443 • SSH 서버: TCP/22 • OCSP: TCP/2560	Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다.
클러스터링(노드 그룹)	노드 그룹/JGroups: TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
디바이스 관리	TACACS+: TCP/49 참고 이 포트는 릴리스 2.1 이상에서 구성할 수 있습니다.	
SXP	• PSN(SXP 노드)에서 NAD: TCP/64999 • PSN에서 SXP(노드 간 통신): TCP/443	
TC-NAC	TCP/443	
모니터링	SNMP(Simple Network Management Protocol): UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다.	
로깅(아웃바운드)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. • SNMP 트랩: UDP/162	
세션	• RADIUS 인증: UDP/1645, 1812 • RADIUS 계정 관리: UDP/1646, 1813 • RADIUS DTLS 인증/계정 관리: UDP/2083. • RADIUS CoA(Change of Authorization) Send: UDP/1700 • RADIUS CoA(Change of Authorization) Listen/Relay: UDP/1700, 3799 참고 UDP 포트 3799는 구성 불가합니다.	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트

외부 ID 소스 및 리소스(아웃바운드)	• 관리자 사용자 인터페이스 및 엔드포인트 인증
	  • LDAP: TCP/389, 3268
	  • SMB: TCP/445
	  • KDC: TCP/88
	  • KPASS: TCP/464
	• WMI: TCP/135
	• ODBC:
	참고 ODBC 포트는 타사 데이터베이스 서버에서 구성할 수 있습니다.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.	

패시브 ID(인바운드)	• TS Agent: tcp/9094 • AD Agent: tcp/9095 • Syslog: UDP/40514, TCP/11468	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트
웹 포털서비스 - 게스트/웹 인증 - 게스트 스폰서 포털 - 내 디바이스 포털 - 클라이언트 프로비저닝 - 인증서 프로비저닝 - 차단 목록 포털	HTTPS(Cisco ISE 서비스를 위해 인터페이스가 활성화되어야 함) • 차단 목록 포털: TCP/8000-8999(기본 포트는 TCP/8444.) • 게스트 포털 및 클라이언트 프로비저닝: TCP/8000-8999(기본 포트는 TCP/8443) • 인증서 프로비저닝 포털: TCP/8000~8999(기본 포트는 TCP/8443입니다.) • 내 디바이스 포털: TCP/8000-8999(기본 포트는 TCP/8443) • 스폰서 포털: TCP/8000-8999(기본 포트는 TCP/8443) • 게스트 및 스폰서 포털의 SMTP 게스트 알림: TCP/25	
포스처 - 검색 - 프로비저닝 - 평가/하트비트	• 검색(클라이언트): TCP/80(HTTP), TCP/8905(HTTPS) 참고 기본적으로 TCP/80은 TCP/8443으로 리디렉션됩니다. 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 Cisco ISE는 TCP 포트 8905에서 포스처 및 클라이언트 프로비저닝용 관리자 인증서를 제공합니다. Cisco ISE는 TCP 포트 8443(또는 포털 사용을 위해 구성한 포트)에서 포털 인증서를 제공합니다. • 검색(정책 서비스 노드): TCP/8443, 8905(HTTPS) AnyConnect를 지원하는 Cisco ISE, 릴리스 2.2 이상 또는 릴리스 4.4 이상에서 이 포트를 구성할 수 있습니다. • 평가 - 포스처 협상 및 에이전트 보고서: TCP/8905(HTTPS)	

Cisco ISE Service	기가비트 이더넷 0 또는 결합 0의 포트	다른 이더넷 인터페이스 또는 결합 1 및 2의 포트
BYOD(Bring Your Own Device)/NSP(Network Service Protocol) - 리디렉션 - 프로비저닝 - SCEP	• 프로비저닝 - URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • EST 인증이 포함된 Android 장치의 경우: TCP/8084. 포트 8084은 Android 장치용 Redirect ACL에 추가해야 합니다. • 프로비저닝 - Active-X 및 Java Applet 설치(마법사 설치 시작 포함): 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • 프로비저닝 - Cisco ISE에서 마법사 설치(Windows, Mac OS): TCP/8443 • 프로비저닝 - Google Play에서 마법사 설치(Android): TCP/443 • 프로비저닝 - 신청자 프로비저닝 프로세스: TCP/8905 • SCEP 프록시-CA: TCP/80 또는 TCP/443(SCEP RA URL 컨피그레이션 기반)	
MDM(Mobile Device Management) API 통합	• URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조 • API: 벤더별 • 에이전트 설치 및 디바이스 등록: 벤더별	
프로파일링	• NetFlow: UDP/9996 참고 이 포트는 구성 가능합니다. • DHCP: UDP/67 참고 이 포트는 구성 가능합니다. • DHCP SPAN Probe: UDP/68 • HTTP: TCP/80, 8080 • DNS: UDP/53(lookup) 참고 이 포트는 라우트 테이블에 따라 달라집니다. • SNMP 쿼리: UDP/161 참고 이 포트는 라우트 테이블에 따라 달라집니다. • SNMP 트랩: UDP/162 참고 이 포트는 구성 가능합니다.	

Cisco ISE pxGrid Service 포트

다음 표에는 pxGrid 서비스 노드에서 사용하는 포트가 나와 있습니다.

표 ***19: pxGrid*** 서비스 노드에서 사용하는 포트

Cisco ISE Service	기가비트 이더넷 **0** 또는 결합 **0**의 포트	다른 이더넷 인터페이스**(**기가비트 이더넷 **1~5,** 결합 **1** 및 **2)**의 포트
관리	• SSL: TCP/5222(노드 간 통신) • SSL: TCP/7400(노드 그룹 통신)	—
pxGrid 가입자	TCP/8910	

OCSP 및 CRL 서비스 포트

OCSP(Online Certificate Status Protocol) 서비스 및 CRL(Certificate Revocation List)에서는 OCSP/CRL을 호스팅하는 서비스 또는 CA 서버에 따라 포트가 달라집니다. 다만 Cisco ISE 서비스 및 포트에 대한 참조에서는 Cisco ISE 관리 노드, 정책 서비스 노드모니터링 노드에서 각각 사용하는 기본 포트가 나열됩니다.

OCSP의 경우 사용 가능한 기본 포트는 TCP 80/TCP 443입니다. Cisco ISE 관리 포털에서는 OCSP 서비스에 대해 http 기반 URL을 기대하므로 TCP 80이 기본값입니다. 비기본 포트를 사용할 수도 있습니다.

CRL에서는 기본 프로토콜에 HTTP, HTTPS, LDAP가 포함되며 기본 포트는 각각 80, 443, 389입니다. 실제 포트는 CRL 서버에 따라 달라집니다.

Cisco ISE 프로세스

다음 표에는 Cisco ISE 프로세스 및 프로세스 서비스 영향이 나와 있습니다.

프로세스 이름	Description(설명)	서비스 영향
데이터베이스 리스너	Oracle 엔터프라이즈 데이터베이스 리스너	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
데이터베이스 서버	Oracle 엔터프라이즈 데이터베이스 서버입니다. 구성 및 운영 데이터를 모두 저장합니다.	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.

Application Server(애플리케이션 서버)	ISE용 메인 Tomcat 서버	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
프로파일러 데이터베이스	ISE 프로파일링 서비스용 Redis 데이터베이스	ISE 프로파일링 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
AD 커넥터	Active Directory Runtime	Active Directory 인증을 수행하려면 ISE에 대해 Running(실행 중) 상태여야 합니다.
MnT 세션 데이터베이스	MnT 서비스용 Oracle TimesTen 데이터베이스	모든 서비스가 제대로 작동하려면 Running(실행 중) 상태여야 합니다.
MnT 로그 수집기	MnT 서비스용 로그 수집기	MnT 운영 데이터에 대해 Running(실행 중) 상태여야 합니다.
MnT 로그 프로세서	MnT 서비스용 로그 프로세서	MnT 운영 데이터에 대해 Running(실행 중) 상태여야 합니다.
Certificate Authority 서비스	ISE 내부 CA 서비스	ISE 내부 CA가 활성화되었다면 Running(실행 중) 상태여야 합니다.

필수 인터넷 URL

다음 표에는 특정 URL을 사용하는 기능이 나와 있습니다. IP 트래픽이 Cisco ISE 및 이러한 리소스 간에 이동할 수 있도록 네트워크 방화벽 또는 프록시 서버 중 하나를 구성해야 합니다. 나열된 URL에 대해 이 액세스를 제공할 수 없는 경우에는 관련된 기능이 손상되거나 작동하지 않습니다.

표 ***20:*** 필수 ***URL*** 액세스

기능	**URL**
포스처 업데이트	https://www.cisco.com/ https://iseservice.cisco.com
프로파일링 피드 서비스	https://ise.cisco.com
스마트 라이선싱	https://tools.cisco.com
대화형 도움말	https://cdn.walkme.com https://playerserver.walkme.com https://ec.walkme.com https://rapi.walkme.com https://papi.walkme.com https://s3.amazonaws.com https://s3.walkmeusercontent.com