



Cisco Identify Services Engine Release 1.4 하드웨어 설치 설명서

초판: 2015년 02월 15일

최종 변경: 2015년 03월 30일

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

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패키지에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. 모든 권리는 저작권자의 소유입니다. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에서 언급한 공급자는 상품성, 특정 목적에의 적합성 및 비침해에 대한 보증을 포함하되 이에 제한되지 않으며 거래 과정, 사용 또는 거래 관행으로부터 발생하는 모든 명시적이거나 묵시적인 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco 및/또는 해당 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL을 방문하십시오. <http://www.cisco.com/go/trademarks> 여기에 언급된 타사 상표는 해당 소유권자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



목 차

Cisco ISE 네트워크 구축 1

Cisco ISE 네트워크 아키텍처 1

Cisco ISE 구축 용어 2

분산 구축의 노드 유형 및 페르소나 3

관리 노드 3

정책 서비스 노드 4

모니터링 노드 4

인라인 포스처 노드 4

인라인 포스처 노드 설치 5

인라인 포스처 노드 재사용 5

독립형 및 분산 ISE 구축 5

분산 구축 시나리오 5

소형 네트워크 구축 6

분할 구축 7

중형 네트워크 구축 7

대형 네트워크 구축 8

중앙 집중식 로깅 8

로드 밸런서 9

분산 네트워크 구축 9

여러 원격 사이트가 있는 네트워크 계획 시 고려 사항 10

구축 크기 및 확장 권장 사항 11

인라인 포스처 계획 고려 사항 12

Cisco ISE 기능을 지원하는 데 필요한 스위치 및 무선 LAN 컨트롤러 컨피그레이션 13

Cisco SNS-3400 Series Appliance 15

Cisco ISE를 위한 Cisco SNS 지원 15

Cisco SNS-3400 Series Appliance 하드웨어 사양 15

Cisco SNS-3400 Series 전면 패널 16

- Cisco SNS-3400 Series 후면 패널 17
- Cisco SNS-3400 Series Appliance 설치 및 구성 19**
 - SNS-3400 Series Appliance 설치 전제 조건 19
 - Cisco.com에서 Cisco ISE ISO 이미지 다운로드 20
 - SNS-3400 Series Appliance에 Cisco ISE 소프트웨어를 설치하는 방법 20
 - Cisco Integrated Management Controller 구성 21
 - 부팅 가능 USB 드라이브 만들기 22
 - Cisco ISE 설정 프로그램 매개변수 23
 - CIMC를 사용하여 Cisco SNS-3400 Series Appliance에서 ISE 구성 25
 - 지원되는 표준 시간대 27
 - 설정 프로세스 확인 29
- VMware 가상 머신에 ISE 설치 31**
 - 가상 머신에서 지원되지 않는 ISE 기능 31
 - 지원되는 VMware 버전 31
 - VMware vMotion 지원 32
 - Open Virtualization Format 지원 32
 - 가상 머신 요구 사항 33
 - VMware 어플라이언스 크기 권장 사항 34
 - 디스크 공간 요구 사항 35
 - 디스크 공간 지침 35
 - 가상 머신 리소스 및 성능 확인 36
 - Show Tech Support 명령을 사용하는 온디맨드 가상 머신 성능 확인 37
 - Cisco ISE 부트 메뉴에서 가상 머신 리소스 확인 37
 - Cisco ISE 릴리스 평가 38
 - 가상 머신에 Cisco ISE 설치 38
 - OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 구축 39
 - ISO 파일을 사용하여 가상 머신에 Cisco ISE 설치 39
 - VMware ESX 또는 ESXi Server 구성 시 전제 조건 40
 - 가상화 기술 확인 41
 - ESX 또는 ESXi 서버에 가상화 기술 활성화 41
 - Cisco ISE 프로파일러 서비스를 위한 VMware 서버 인터페이스 구성 42
 - 직렬 콘솔을 사용하여 VMware 서버에 연결 42

- VMware 서버 구성 43
- Cisco ISE 소프트웨어 DVD에서 부팅하도록 VMware 시스템 구성 44
- VMware 시스템에 Cisco ISE 소프트웨어 설치 45
- 가상 머신에 대한 Cisco ISE ISO 설치 실패 46
- Cisco ISE 가상 머신 복제 46
 - 템플릿을 사용하여 Cisco ISE 가상 머신 복제 47
 - 가상 머신 템플릿 생성 47
 - 가상 머신 템플릿 구축 48
 - 복제된 가상 머신의 IP 주소 및 호스트 이름 변경 49
 - 네트워크에 복제된 Cisco 가상 머신 연결 50
- 평가 환경에서 프로덕션 환경으로 Cisco ISE VM 마이그레이션 50
- Cisco ISE 3300 Series, Cisco NAC, Cisco Secure ACS Appliance에 Cisco ISE 소프트웨어 설치 53**
 - 지원되는 Cisco ISE, Secure ACS, NAC Appliance 53
 - DVD에서 Cisco ISE 소프트웨어 설치 54
 - 리이미징된 Cisco ISE-3300 Series Appliance에 Cisco ISE 소프트웨어 설치 54
 - 리이미징된 Cisco Secure ACS Appliance에 Cisco ISE 소프트웨어 설치 55
 - 리이미징된 Cisco NAC Appliance에 Cisco ISE 소프트웨어 설치 56
 - Cisco NAC Appliance의 기존 RAID 컨피그레이션 재설정 57
- 관리자 계정 관리 59
 - CLI 관리자와 웹 기반 관리자의 사용자 권한 차이점 59
 - CLI 관리자 사용자 생성 60
 - 웹 기반 관리자 사용자 생성 60
- 설치 후 작업 61
 - Cisco ISE 웹 기반 인터페이스 로그인 61
 - Cisco ISE 컨피그레이션 확인 62
 - 웹 브라우저에서 컨피그레이션 확인 62
 - CLI에서 컨피그레이션 확인 63
 - VMware Tools 설치 확인 64
 - vSphere Client의 Summary 탭을 사용하여 VMWare Tools 설치 확인 64
 - CLI를 사용하여 VMWare Tools 설치 확인 65
 - VMware Tools 업그레이드 지원 65

관리자 비밀번호 재설정 65

 DVD를 사용하여 잊었거나 손상된 비밀번호 재설정 65

 관리자 잠금에 따른 비밀번호 재설정 67

Cisco ISE Appliance의 IP 주소 변경 67

설치 및 업그레이드 기록 보기 68

SNS-3415 Appliance에 RAID 구성 69

CIMC를 사용하여 SNS-3495 Appliance에 RAID 구성 70

시스템 지우기 수행 71

Cisco SNS-3400 Series 서버 사양 75

 제품 외장 사양 75

 환경 사양 75

 전원 사양 76

 450와트 전원 공급 장치 76

 650와트 전원 공급 장치 77

Cisco SNS-3400 Series Appliance 포트 참조 79

 Cisco ISE 인프라 79

 Cisco ISE 관리 노드 포트 81

 Cisco ISE 모니터링 노드 포트 82

 Cisco ISE 정책 서비스 노드 포트 84

 인라인 포스처 노드 포트 87

 Cisco ISE pxGrid Service 포트 89

 OCSP 및 CRL 서비스 포트 89



Cisco ISE 네트워크 구축

- Cisco ISE 네트워크 아키텍처, 1 페이지
- Cisco ISE 구축 용어, 2 페이지
- 분산 구축의 노드 유형 및 페르소나, 3 페이지
- 독립형 및 분산 ISE 구축, 5 페이지
- 분산 구축 시나리오, 5 페이지
- 소형 네트워크 구축, 6 페이지
- 중형 네트워크 구축, 7 페이지
- 대형 네트워크 구축, 8 페이지
- 구축 크기 및 확장 권장 사항, 11 페이지
- 인라인 포스처 계획 고려 사항, 12 페이지
- Cisco ISE 기능을 지원하는 데 필요한 스위치 및 무선 LAN 컨트롤러 컨피그레이션, 13 페이지

Cisco ISE 네트워크 아키텍처

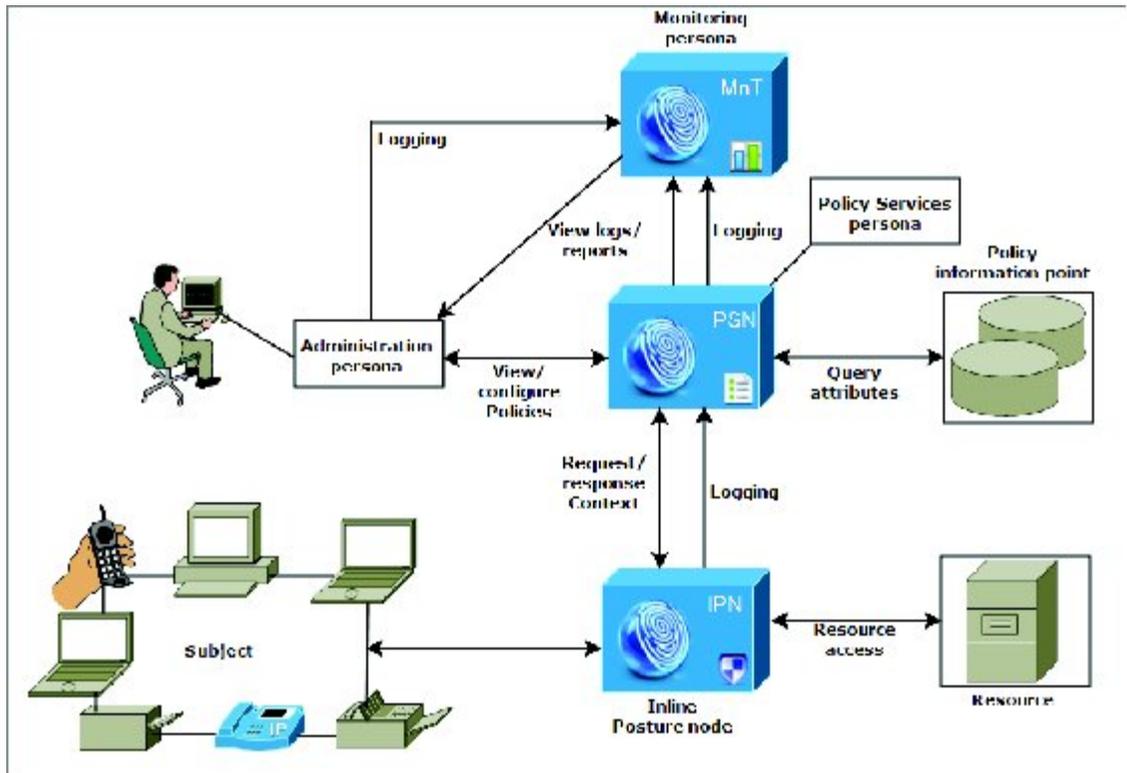
Cisco ISE 아키텍처는 다음 구성 요소를 포함합니다.

- 노드 및 페르소나 유형
 - Cisco ISE 노드—Cisco ISE 노드는 관리, 정책 서비스, 모니터링, pxGrid 페르소나 중 하나 또는 전부를 맡을 수 있습니다.
 - 인라인 포스처 노드—액세스 정책의 시행을 다루는 게이트키퍼 노드입니다.
- 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.

다음 그림은 Cisco ISE 노드 및 페르소나(관리, 정책 서비스, 모니터링), 인라인 포스처 노드, 정책 정보 지점을 보여줍니다.

그림 1: Cisco ISE 아키텍처



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	Cisco ISE 소프트웨어를 실행하는 개별 인스턴스. Cisco ISE는 어플라이언스의 형태로 또는 VMware에서 실행 가능한 소프트웨어의 형태로 사용할 수 있습니다.

용어	정의
노드 유형	노드는 2가지 유형, 즉 Cisco ISE 노드 또는 인라인 포스처 노드 중 하나일 수 있습니다. 노드 유형 및 페르소나에 의해 노드에서 제공하는 기능의 유형이 결정됩니다.
페르소나	노드에서 제공하는 서비스를 결정합니다. Cisco ISE 노드는 관리, 정책 서비스, 모니터링의 페르소나 중 무엇이든 또는 전부를 맡을 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 분산 구축에서는 2가지 유형의 노드가 있습니다.

- Cisco ISE 노드(관리, 정책 서비스, 모니터링)
- 인라인 포스처 노드

Cisco ISE 노드는 그 페르소나에 따라 다양한 서비스를 제공할 수 있습니다. 인라인 포스처 노드를 제외하고 구축의 각 노드는 관리, 정책 서비스, 모니터링 페르소나를 맡을 수 있습니다. 분산 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
- 고가용성을 위한 한 쌍의 인라인 포스처 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 구축에서는 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 정책 평가의 결과에 따라 엔드포인트에 네트워크 액세스를 제공합니다. 일반적으로 분산 구축에서는 둘 이상의 정책 서비스 노드가 있습니다. 로드 밸런서의 뒤에 있는 모든 정책 서비스 노드는 공통 멀티캐스트 주소를 공유하며 이를 그룹화하여 노드 그룹을 만들 수 있습니다. 노드 그룹에 속한 노드 중 하나의 작동이 중단되면 나머지 노드가 장애를 감지하고 보류 중인 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.

인라인 포스처 노드

인라인 포스처 노드는 게이트키퍼 노드이며 네트워크에서 WLC(wireless LAN controller), VPN 집중기 등과 같은 네트워크 액세스 디바이스의 뒤에 위치합니다. 인라인 포스처는 사용자가 인증되고 액세스 권한을 부여받은 후에 액세스 정책을 적용하며, WLC 또는 VPN에서 수용하지 못하는 COA(change of authorization) 요청을 처리합니다. Cisco ISE에서는 2개의 인라인 포스처 노드를 둘 수 있으며, 이 노드는 고가용성을 위해 기본 역할 또는 보조 역할을 맡을 수 있습니다.

인라인 포스처 노드는 전용 노드여야 합니다. 인라인 포스처 서비스 전용이어야 하며, 다른 Cisco ISE 서비스와 동시에 작동할 수 없습니다. 또한 인라인 포스처 노드는 그 서비스의 전문성 때문에 어떤 페르소나도 맡을 수 없습니다. 즉 관리 노드(관리 서비스 제공), 정책 서비스 노드(네트워크 액세스, 포스처, 프로파일, 게스트 서비스 제공) 또는 모니터링 노드(모니터링 및 문제 해결 서비스 제공)가 될 수 없습니다.

인라인 포스처는 Cisco SNS 3495 플랫폼에서 지원되지 않습니다. 인라인 포스처는 다음 지원되는 플랫폼 중 하나에 설치해야 합니다.

- Cisco ISE 3315
- Cisco ISE 3355
- Cisco ISE 3395

- Cisco SNS 3415

인라인 포스처 노드 설치

시작하기 전에

- Cisco.com에서 인라인 상태 ISO 이미지를 다운로드 합니다
- 해당 인증서를 구성하고 기본 관리 노드에 등록합니다.

절차

-
- 단계 1 지원되는 플랫폼 중 하나에 인라인 포스처 ISO 이미지를 설치합니다.
 - 단계 2 CLI에 로그인합니다.
 - 단계 3 노드에 대한 인증서를 구성합니다.
 - 단계 4 기본 관리 노드의 사용자 인터페이스에 로그인합니다.
 - 단계 5 인라인 포스처 노드를 등록합니다.
-

인라인 포스처 노드 재사용

더 이상 인라인 포스처 노드가 필요하지 않을 경우, 여기에 서비스나 역할을 추가할 수는 없지만 Cisco ISE 노드로 변경한 다음 여기에 페르소나를 지정할 수 있습니다. 인라인 포스처 노드를 재사용하려는 경우 먼저 등록 취소한 다음 어플라이언스를 리이미징하고 여기에 Cisco ISE를 설치해야 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. 인라인 포스처 노드는 그 특수성 때문에 다른 페르소나를 맡을 수 없으며 전용 노드가 되어야 합니다.

분산 구축 시나리오

- 소형 네트워크 구축

- 중형 네트워크 구축
- 대형 네트워크 구축

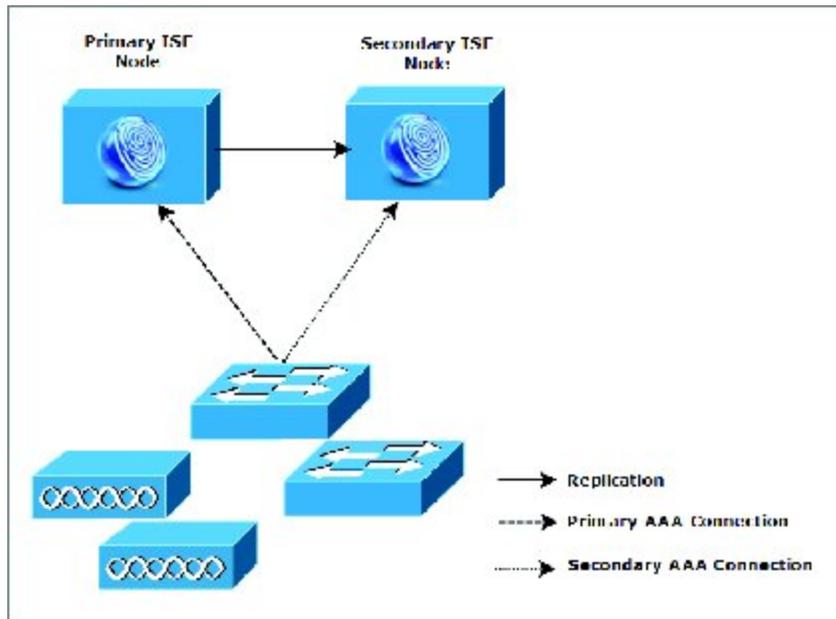
소형 네트워크 구축

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 인증, 권한 부여, 계정 관리(AAA) 작업은 RADIUS 프로토콜을 사용하여 수행됩니다. 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 2: 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 바뀌어 합니다.

분할 구축

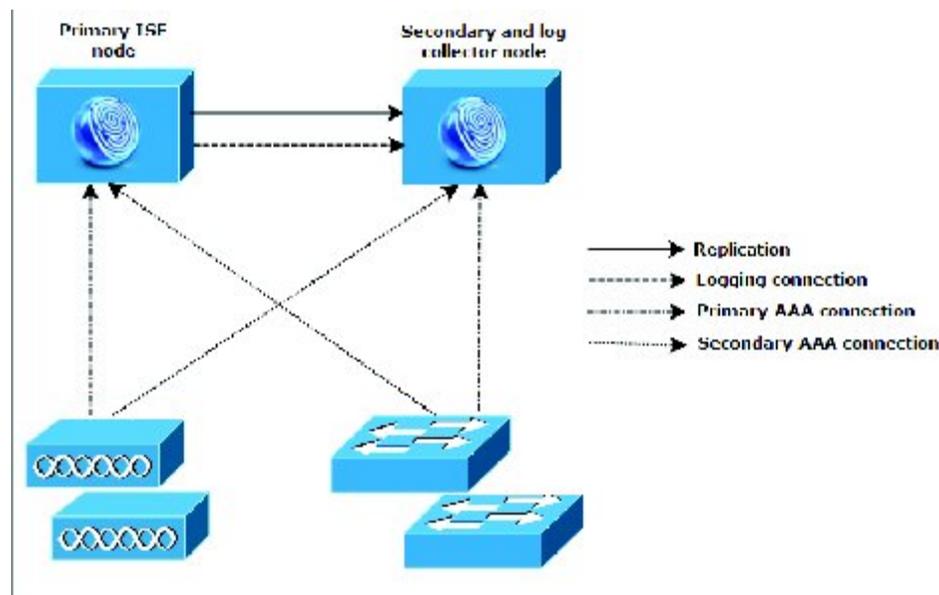
분할 Cisco ISE 구축에서는 소형 Cisco ISE 구축에서 설명한 기본 노드와 보조 노드를 계속 유지합니다. 그러나 AAA 워크플로 최적화를 위해 두 Cisco ISE 노드 간에 AAA 로드가 분할됩니다. 각 Cisco ISE 어플라이언스(기본 또는 보조)는 AAA 연결에 문제가 생길 경우 전체 워크로드를 처리할 수 있어야 합니다. 정상적인 네트워크 운영 상태에서는 기본 노드와 보조 노드 모두 모든 AAA 요청을 처리하지는 않습니다. 이 워크로드가 두 노드에 분산되어 있기 때문입니다.

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 3: 분할 네트워크 구축

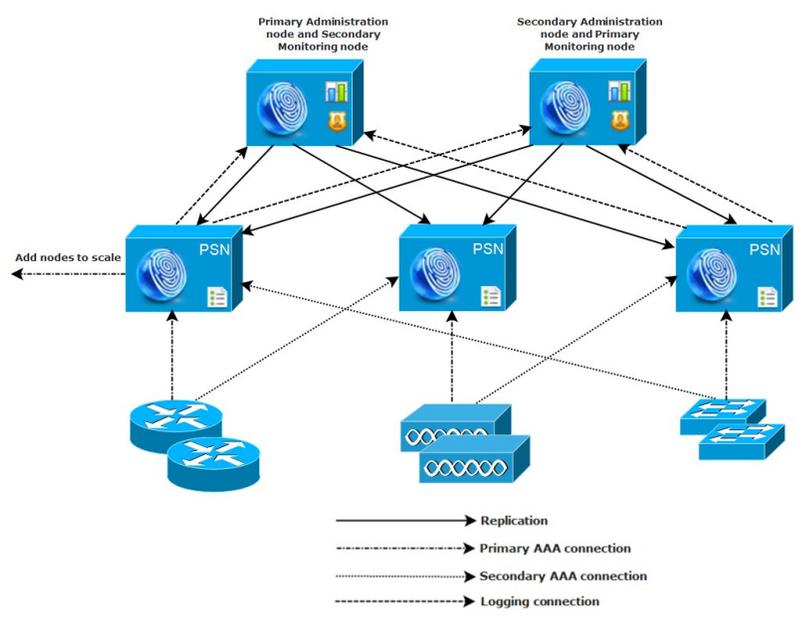


중형 네트워크 구축

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.

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

그림 4: 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.

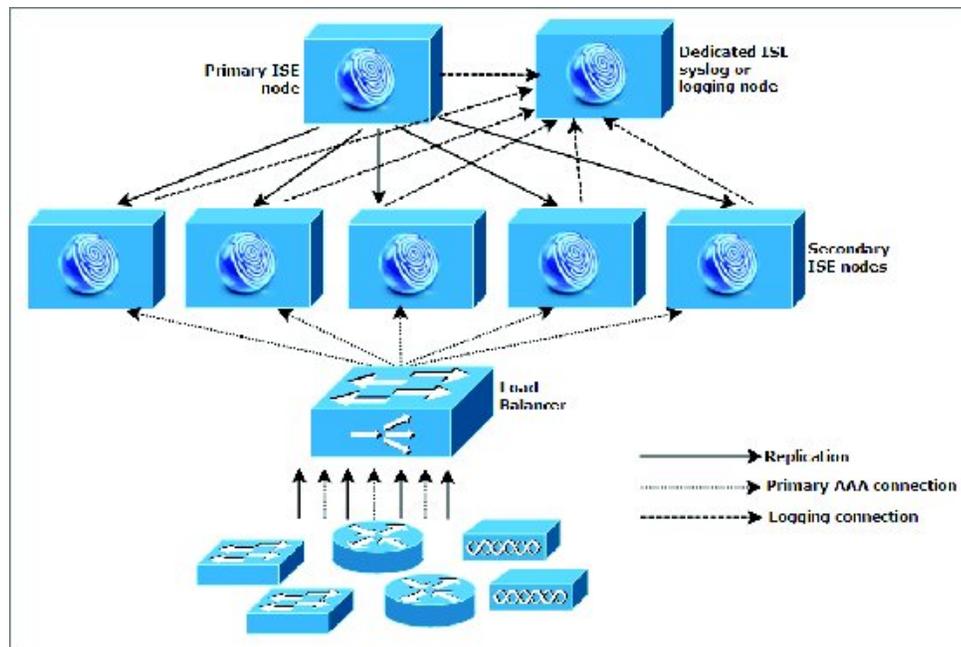
또한 어플라이언스에서 Cisco ISE 노드의 모니터링 페르소나와 일반 syslog 서버 모두에 로그를 보내는 것도 고려할 수 있습니다. 일반 syslog 서버를 추가하면 Cisco ISE 노드에서 모니터링 페르소나가 작동 중단될 경우 이중 백업의 역할을 합니다.

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

그림 5: 대규모 네트워크 구축



28120194

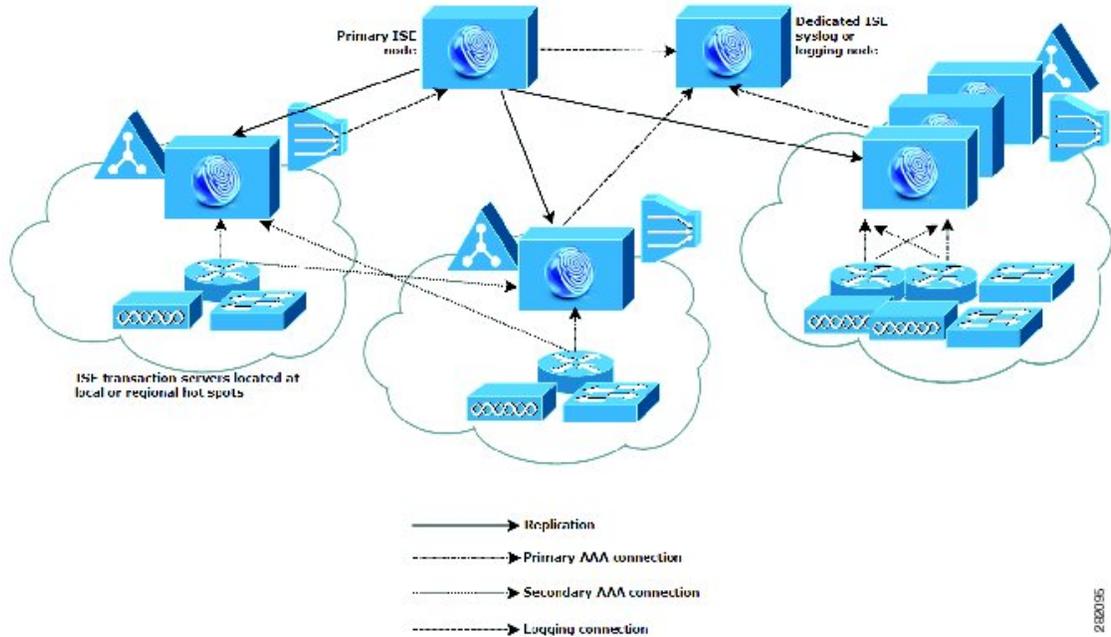
분산 네트워크 구축

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 노드

에서 별도의 모니터링 페르소나를 사용하는 것이 좋지만, 각 원격 위치는 저마다의 고유한 네트워크 요구 사항을 가져야 합니다.

그림 6: 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 고려해 보십시오.
- 외부 데이터베이스에 대한 액세스를 보장하기 위해 모든 Cisco ISE 노드에서 DNS(Domain Name System)를 알맞게 구성해야 합니다.

구축 크기 및 확장 권장 사항

다음 표에서는 네트워크에 연결할 엔드포인트 수에 따라 필요한 구축 수, Cisco ISE 노드 수, 어플라이언스 유형(소형, 중형, 대형)에 대한 지침을 제공합니다.

표 1: Cisco ISE 구축 - 크기 및 확장 권장 사항

구축 유형	노드/페르소나 수	어플라이언스 플랫폼	전용 정책 서비스 노드의 최대 개수	활성 엔드포인트 수
소형	독립형 또는 이중 (2) 노드 - 관리, 정책 서비스, 모니터링 페르소나 활성화	Cisco ISE 3300 Series(3315, 3355, 3395)	0	최대 2,000개의 엔드포인트
		Cisco ISE 3415	0	최대 5,000개의 엔드포인트
		Cisco ISE 3495	0	최대 10,000개의 엔드포인트
중형	단일 또는 이중 노드에서 관리 및 모니터링 페르소나. 최대 2개의 관리 및 모니터링 노드.	Cisco ISE-3355 또는 Cisco SNS 3415 어플라이언스 - 관리 및 모니터링 페르소나	5	최대 5,000개의 엔드포인트
		Cisco ISE-3395 또는 Cisco SNS 3495 어플라이언스 - 관리 및 모니터링 페르소나	5	최대 10,000개의 엔드포인트
대형	전용 관리 노드. 최대 2개의 관리 노드. 전용 모니터링 노드. 최대 2개의 모니터링 노드. 전용 정책 서비스 노드. 최대 40개의 정책 서비스 노드.	Cisco ISE 3395 어플라이언스 - 관리 및 모니터링 페르소나	40	최대 100,000개의 엔드포인트
		Cisco SNS 3495 어플라이언스 - 관리 및 모니터링 페르소나	40	최대 250,000개의 엔드포인트

다음 표에서는 노드가 서비스할 활성 엔드포인트 수에 따라 전용 정책 서비스 노드에 필요할 어플라이언스 유형을 알려줍니다.

표 2: 정책 서비스 노드 크기 권장 사항

폼 팩터	플랫폼 크기	어플라이언스	최대 엔드포인트
물리적	소형	Cisco ISE-3315	3,000
		Cisco SNS-3415	5,000
	중형	Cisco ISE-3355	6,000
	대형	Cisco ISE-3395	10,000
		Cisco SNS-3495	20,000
가상 머신	소형/중형/대형	물리적 어플라이언스와 동급	3,000 ~ 20,000

다음 표에서는 단일 인라인 포스처 노드에서 지원할 수 있는 최대 처리량 및 최대 엔드포인트 수를 알려줍니다.

표 3: 인라인 포스처 노드 사이징 권장 사항

특성	성능
물리적 어플라이언스당 최대 엔드포인트 수	5,000에서 20,000(정책 서비스 노드에서 제어)
물리적 어플라이언스당 최대 처리량	936Mbps

인라인 포스처 계획 고려 사항

네트워크 또는 시스템 설계자는 인라인 포스처 노드의 구축을 계획할 때 다음과 같은 기본적인 질문에 대한 답을 찾아야 합니다.

- 구축 계획에 인라인 포스처 기본-보조 쌍 컨피그레이션이 포함됩니까? Cisco ISE 네트워크는 임의의 시점에 하나의 네트워크에서 최대 2개의 인라인 포스처 노드를 구성할 수 있습니다.
- 어떤 유형의 인라인 포스처 운영 모드를 선택할 것입니까?



주의

인라인 포스처 노드가 구성되는 동안 인라인 포스처 노드에서 인증되지 않은 인터페이스는 연결을 끊어야 합니다. 초기 컨피그레이션 과정에서 인증된 인터페이스와 인증되지 않은 인터페이스가 동일한 VLAN에 연결된 경우, 페르소나 변경 후 인라인 포스처 노드가 부팅되면 인증되지 않은 인터페이스 때문에 멀티캐스트 패킷 트래픽이 폭증합니다. 이러한 멀티캐스트 이벤트로 인해 동일한 서브넷 또는 VLAN에 연결된 디바이스의 작동이 중단될 수 있습니다. 현 시점에 인라인 포스처 노드는 유지 관리 모드입니다.



주의

구축에 추가된 후에는 인라인 포스처 노드의 CLI 비밀번호를 변경하지 마십시오. 비밀번호가 변경된 경우, 관리 노드를 통해 인라인 포스처 노드에 액세스하면 Java 예외 오류가 표시되고 CLI가 잠깁니다. 설치 DVD를 사용하고 인라인 포스처 노드를 재부팅하여 비밀번호를 복구해야 합니다. 또는 비밀번호를 최초의 값으로 설정할 수 있습니다.

비밀번호를 변경해야 하는 경우 구축에서 인라인 포스처 노드를 등록 취소하고 비밀번호를 변경한 다음 새 인증서를 사용하여 구축에 노드를 추가합니다.

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.



Cisco SNS-3400 Series Appliance

- [Cisco ISE를 위한 Cisco SNS 지원, 15 페이지](#)
- [Cisco SNS-3400 Series Appliance 하드웨어 사양, 15 페이지](#)
- [Cisco SNS-3400 Series 전면 패널, 16 페이지](#)
- [Cisco SNS-3400 Series 후면 패널, 17 페이지](#)

Cisco ISE를 위한 Cisco SNS 지원

Cisco ISE 소프트웨어는 전용 Cisco SNS-3400 Series Appliance에서 또는 VMware 서버에서 실행됩니다. Cisco ISE 소프트웨어는 이러한 전용 플랫폼에 다른 패키지나 애플리케이션을 설치하는 것을 지원하지 않습니다.

이 Cisco ISE 소프트웨어는 Cisco ISE 3300 Series, Cisco NAC 3300 Series, Cisco Secure ACS 1121 Appliance에서도 지원됩니다. 기존 Cisco ISE 3300 Series Appliance를 최신 릴리스로 업그레이드할 수 있습니다.

Cisco SNS-3400 Series Appliance 하드웨어 사양

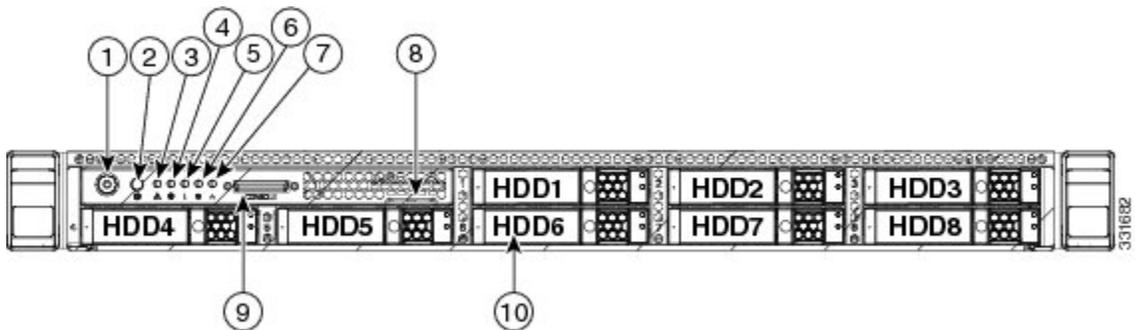
Cisco SNS-3400 Series Appliance 하드웨어는 Cisco SNS 3415 및 3495 Appliance로 구성됩니다.

표 4: Cisco ISE SNS 3415/3495 Appliance 하드웨어 개요

Cisco ISE Appliance	하드웨어 사양
Cisco SNS- 3415-K9	<ul style="list-style-type: none"> • Cisco UCS C220 M3 • 단일 소켓 Intel E5-2609 2.4Ghz CPU 총 4코어, 4스레드 • 16GB RAM • 600GB 디스크 1개 • 임베디드 소프트웨어 RAID 0 • GE 네트워크 인터페이스 4개
Cisco SNS- 3495-K9	<ul style="list-style-type: none"> • Cisco UCS C220 M3 • 듀얼 소켓 Intel E5-2609 2.4Ghz CPU 총 8코어, 8스레드 • 32GB RAM • 600GB 디스크 2개 • RAID 0+1 • GE 네트워크 인터페이스 4개

Cisco SNS-3400 Series 전면 패널

그림 7: Cisco SNS 3415/3495 전면 패널

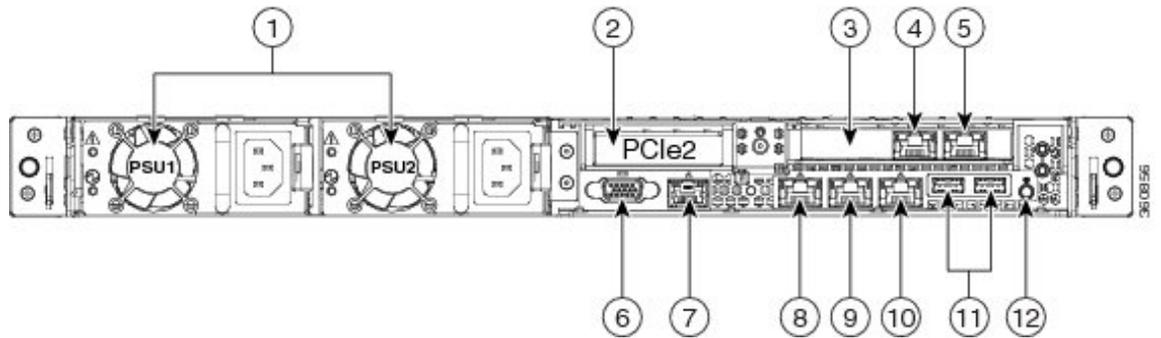


1	전원 버튼/전원 상태 LED	6	전원 공급 장치 상태 LED
2	식별 버튼 LED	7	네트워크 링크 활동 LED

3	시스템 상태 LED	8	자산 태그(일련 번호)
4	팬 상태 LED	9	KVM(keyboard, video, mouse) 커넥터(USB 2개, VGA(Video Graphics Adapter) 1개, 시리얼 커넥터 1개를 제공하는 KVM 케이블과 함께 사용)
5	온도 상태 LED	10	드라이브(운영 중 교체 가능한 2인치에서 5인치 드라이브 최대 8개)

Cisco SNS-3400 Series 후면 패널

그림 8: SNS 3415/3495 후면 패널



1	전원 공급 장치(최대 2개)	7	시리얼 포트(RJ-45 커넥터)
2	슬롯 2: 라이저의 low-profile PCIe(Peripheral Component Interconnect Express) 슬롯(절반 높이, 절반 길이 x16 커넥터, x16 레인 너비)	8	CIMC 액세스에 사용되는 1GB 이더넷 전용 관리 포트(레이블 M)
3	슬롯 1: PCIe1 카드, 1GB 이더넷 포트 포함(GigE2, GigE3)	9	Cisco ISE 관리 통신용 1GB 이더넷 포트 1(GigE0)
4	1GB 이더넷 포트 3(GigE2)	10	1GB 이더넷 포트 2(GigE1)
5	1GB 이더넷 포트 4(GigE3)	11	USB 포트
6	VGA 비디오 커넥터	12	후면 식별 버튼

일련 번호 위치

서버의 일련 번호는 서버 맨 위, 전면 근처의 레이블에 인쇄되어 있습니다.



Cisco SNS-3400 Series Appliance 설치 및 구성

- SNS-3400 Series Appliance 설치 전제 조건, 19 페이지
- Cisco.com에서 Cisco ISE ISO 이미지 다운로드, 20 페이지
- SNS-3400 Series Appliance에 Cisco ISE 소프트웨어를 설치하는 방법, 20 페이지
- Cisco Integrated Management Controller 구성, 21 페이지
- 부팅 가능 USB 드라이브 만들기, 22 페이지
- Cisco ISE 설정 프로그램 매개변수, 23 페이지
- CIMC를 사용하여 Cisco SNS-3400 Series Appliance에서 ISE 구성, 25 페이지
- 설정 프로세스 확인, 29 페이지

SNS-3400 Series Appliance 설치 전제 조건

Cisco SNS-3400 Series Appliance에 Cisco ISE 소프트웨어를 구성하기 전에 이 장의 컨피그레이션 전제 조건을 검토하고 본 설명서에서 다룬 물리적 환경 및 전원 사양도 참조하십시오. 규정 준수 및 안전에 대해서는 [RCSI for Cisco SNS-3415 and Cisco SNS-3495 Appliances](#)를 참조하십시오.

Cisco SNS-3400 Series Appliance에는 Cisco Application Deployment Engine operating system(ADE-OS) 및 Cisco ISE 소프트웨어가 미리 설치되어 있습니다.

구축의 각 노드에 대해 다음 컨피그레이션 설정을 모두 확인한 다음 진행해야 합니다.

- 호스트 이름
- 기가비트 이더넷 0(eth0) 인터페이스의 IP 주소
- 넷마스크
- 기본 게이트웨이
- DNS(Domain Name System) 도메인
- 기본 이름 서버

- 기본 NTP(Network Time Protocol) 서버
- 시스템 표준 시간대
- 사용자 이름(CLI 관리자 사용자)
- 비밀번호(CLI 관리자 사용자)

Cisco ISE 설정 프로그램 매개변수, 23 페이지에서 이 매개변수에 대한 설명 및 값의 예를 확인하십시오.



참고

Cisco SNS-3400 Series Appliance에 RAID가 구성되어야 Cisco ISE를 설치할 수 있습니다. Cisco SNS-3400 Series Appliance에서 RAID 컨피그레이션을 삭제한 경우 다시 구성해야 합니다. 자세한 내용은 SNS-3415 Appliance에 RAID 구성, 69 페이지 및 CIMC를 사용하여 SNS-3495 Appliance에 RAID 구성, 70 페이지(를) 참조하십시오.

Cisco.com에서 Cisco ISE ISO 이미지 다운로드

Cisco SNS-3400 Series Appliance에 Cisco ISE를 설치하기 위해 ISO 이미지를 다운로드합니다.

시작하기 전에

인라인 포스터 노드를 위해 인라인 포스터 노드 ISO를 다운로드하고 설치 프로세스를 진행해야 합니다.

단계 1 <http://www.cisco.com/go/ise>로 이동합니다. 이 링크에 액세스하려면 유효한 Cisco.com 로그인 인증서가 있어야 합니다.

단계 2 **Download Software for this Product**를 클릭합니다.
Cisco ISE 소프트웨어 이미지는 90일 평가판 라이선스가 설치된 상태로 제공되므로 설치 및 초기 컨피그레이션이 완료되면 즉시 모든 Cisco ISE 서비스를 테스트해볼 수 있습니다.

SNS-3400 Series Appliance에 Cisco ISE 소프트웨어를 설치하는 방법

SNS-3400 Series Appliance에서 이전 버전의 Cisco ISE를 실행하는 경우 애플리케이션 업그레이드 명령을 사용하여 업그레이드할 수 있습니다. 또는 기존 SNS-3400 Series Appliance를 리이미징하여 Cisco ISE를 새로 설치하고 기존 구축에 등록하는 방법도 있습니다.

ISO 이미지를 다운로드하고 다음 방법 중 하나로 SNS-3400 Series Appliance에 설치할 수 있습니다.

- CIMC 원격 관리 유틸리티를 사용하여 ISO 이미지를 설치합니다. CIMC에서 이 원격 설치를 수행하도록 구성해야 합니다.
 - 1 CIMC를 구성합니다.
 - 2 원격으로 Cisco ISE 소프트웨어를 설치합니다.
- USB 플래시 드라이브를 사용하여 ISO 이미지를 설치합니다.
 - 1 iso-to-usb.sh 스크립트를 사용하여 부팅 가능 USB 플래시 드라이브를 만듭니다.
 - 2 SNS-3400 Series Appliance에 USB 플래시 디바이스를 연결합니다.
 - 3 로컬 KVM을 사용하여 또는 원격으로 CIMC KVM을 사용하여 Cisco ISE 소프트웨어를 설치합니다.
- USB 포트와 외부 DVD 드라이브를 사용하여 ISO를 설치합니다.
 - 1 DVD에 ISO 이미지를 굽습니다.
 - 2 SNS-3400 Series Appliance에 외부 USB DVD를 연결합니다.
 - 3 로컬 KVM을 사용하여 또는 원격으로 CIMC KVM을 사용하여 Cisco ISE 소프트웨어를 설치합니다.



참고 USB 플래시 디바이스를 사용하여 또는 USB 포트와 외부 DVD를 사용하여 Cisco ISE 소프트웨어를 설치할 경우 CIMC 컨피그레이션은 선택 사항입니다.

Cisco Integrated Management Controller 구성

서버 및 서버 이벤트 로그 모니터링을 비롯하여 Cisco SNS-3400 Series Appliance에 대한 모든 작업을 CIMC를 통해 수행할 수 있습니다. 이를 위해서는 먼저 웹 기반 브라우저에서 CIMC에 액세스하기 위한 IP 주소 및 IP 게이트웨이를 구성해야 합니다.

- 단계 1 전원 코드를 연결합니다.
- 단계 2 전원 버튼을 눌러 서버를 부팅합니다.
- 단계 3 부팅 과정에서 BIOS CIMC Configuration Utility를 열라는 메시지가 나타나면 **F8**을 누릅니다.
- 단계 4 서버 관리를 위해 어떤 포트에서 CIMC에 액세스하는가를 지정하기 위해 NIC 모드를 설정합니다. Cisco ISE는 최대 4개의 기가비트 이더넷 포트를 사용할 수 있습니다.
 - Dedicated—1Gb 이더넷 관리 포트를 사용하여 CIMC에 액세스합니다. NIC redundancy *None*을 선택하고 IP 설정을 선택해야 합니다.

- **Shared LOM (default)**—2개의 1Gb 이더넷 포트를 사용하여 CIMC에 액세스합니다. 이는 액티브-액티브 NIC 이중화 및 DHCP 활성화와 함께 공장 기본 설정입니다.
- **Cisco Card**—설치된 Cisco UCS P81E VIC의 포트를 사용하여 CIMC에 액세스합니다. NIC 이중화 및 IP 설정을 선택해야 합니다.
참고 Cisco Card NIC 모드는 현재 PCIe 슬롯 1에 설치된 Cisco UCS P81E VIC(N2XX-ACPCI01)에서만 지원됩니다.

단계 5 NIC 이중화 설정을 지정합니다.

- **None**—이더넷 포트가 독자적으로 작동하며 문제가 생기더라도 장애 조치하지 않습니다.
- **Active-standby**—액티브 이더넷 포트에 장애가 생길 경우 트래픽이 스탠바이 포트에 장애 조치됩니다.
- **Active-active**—모든 이더넷 포트가 동시에 사용됩니다.

단계 6 동적 네트워크 설정에 DHCP를 활성화할 것인지 아니면 고정 네트워크 설정을 입력할 것인지 선택합니다.

참고 DHCP를 활성화하기 전에 이 DHCP 서버에서 서버의 MAC 주소 범위가 미리 구성되어 있어야 합니다. MAC 주소는 서버 후면의 레이블에 인쇄되어 있습니다. 이 서버는 MAC 주소 6개로 이루어진 범위가 CIMC에 지정되어 있습니다. 레이블에 인쇄된 MAC 주소는 연속적인 MAC 주소 6개로 된 범위의 시작입니다.

단계 7 (선택 사항) VLAN 설정을 지정하고 기본 CIMC 사용자 비밀번호를 설정합니다.

참고 설정 변경 사항은 약 45초 후에 적용됩니다. **F5**를 눌러 새로 고치고 새 설정이 나타날 때까지 기다린 다음 서버를 재부팅합니다.

단계 8 **F10**을 눌러 설정을 저장하고 서버를 재부팅합니다.

참고 DHCP를 활성화하도록 선택한 경우 동적으로 지정된 IP 및 MAC 주소가 부팅 과정에서 콘솔 화면에 표시됩니다.

다음에 할 작업

CIMC를 사용하여 Cisco SNS-3400 Series Appliance에서 ISE 구성

부팅 가능 USB 드라이브 만들기

Cisco ISE ISO 이미지의 “images” 디렉토리에는 Readme 파일과 Cisco ISE 설치용 부팅 가능 USB 드라이브를 만드는 스크립트가 있습니다.

시작하기 전에

- 먼저 “images” 디렉토리의 Readme 파일을 읽습니다.
- 다음 항목이 필요합니다.
 - Linux 시스템(RHEL-6.4, CentOS 6.4). PC 또는 MAC을 사용할 경우 Linux VM이 설치되어 있어야 합니다.

- 8GB USB 드라이브
- iso-to-usb.sh 스크립트

- 단계 1 USB 포트에 USB 드라이브를 꽂습니다.
- 단계 2 iso-to-usb.sh 스크립트 및 Cisco ISE ISO 이미지를 Linux 시스템의 디렉토리에 복사합니다.
- 단계 3 다음의 명령을 입력합니다.
iso-to-usb.sh *source_iso usb_device*
- 예: # **.iso-to-usb.sh** *ise-1.4.0.253-x86_64.iso /dev/sdb* 여기서 **iso-to-usb.sh**는 스크립트의 이름이고 *ise-1.4.0.253-x86_64.iso /dev/sdb*는 ISO 이미지의 이름이며 */dev/sdb*는 USB 디바이스입니다.
- 단계 4 이미지를 설치할 어플라이언스에 대한 값을 입력합니다.
- 단계 5 계속하려면 **Y**를 입력합니다.
- 단계 6 성공 메시지가 나타납니다.
- 단계 7 USB 드라이브를 분리합니다.

다음에 할 작업

CIMC를 사용하여 Cisco SNS-3400 Series Appliance에서 ISE 구성

Cisco ISE 설정 프로그램 매개변수

Cisco ISE 소프트웨어 컨피그레이션이 시작할 때 대화형 CLI 프롬프트에서 시스템을 구성하는 데 필요한 매개변수를 입력합니다.



참고 VMware 서버에 Cisco ISE 소프트웨어를 설치하는 경우 Cisco ISE는 초기 설정 과정에서 VMware Tools, Version 8.3.2도 설치하고 구성합니다.

표 5: Cisco ISE 설정 프로그램 매개변수

프롬프트	설명	예
Hostname	15자를 초과할 수 없습니다. 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

프롬프트	설명	예
(eth0) Ethernet interface address	기가비트 이더넷 0(eth0) 인터페이스를 위한 유효한 IPv4 주소여야 합니다.	10.12.13.14
Netmask	유효한 IPv4 넷마스크여야 합니다.	255.255.255.0
Default gateway	기본 게이트웨이를 위한 유효한 IPv4 주소여야 합니다.	10.12.13.1
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 유효한 IPv4 주소여야 합니다.	10.15.20.25
Add/Edit another name server	추가 이름 서버를 위한 유효한 IPv4 주소여야 합니다.	(선택 사항) 여러 이름 서버를 구성할 수 있습니다. 그러기 위해서는 y를 입력하여 계속합니다.
Primary NTP server	NTP(Network Time Protocol) 서버의 유효한 IPv4 주소 또는 호스트 이름이어야 합니다.	clock.nist.gov
Add/Edit another NTP server	유효한 NTP 도메인이어야 합니다.	(선택 사항) 여러 NTP 서버를 구성할 수 있습니다. 그러기 위해서는 y를 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. Cisco ISE CLI에서 show timezones 명령을 실행하여 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	Cisco ISE 시스템에 대한 CLI 액세스에 사용되는 관리자 사용자 이름입니다. 기본값(admin)을 사용하지 않으려면 새 사용자 이름을 만들어야 합니다. 사용자 이름은 3자에서 8자이고 유효한 영숫자(A-Z, a-z, 0-9)로 구성되어야 합니다.	admin(기본값)

프롬프트	설명	예
Password	Cisco ISE 시스템에 대한 CLI 액세스에 사용되는 관리자 비밀번호입니다. 이 비밀번호는 기본값이 없으므로 만들어야 합니다. 비밀번호는 6자 이상이고 소문자(a-z), 대문자(A-Z), 숫자(0-9)를 각각 하나 이상 포함해야 합니다.	MyIseYPass2

CIMC를 사용하여 Cisco SNS-3400 Series Appliance에서 ISE 구성

어플라이언스를 위한 CIMC를 구성하고 이를 사용하여 Cisco SNS-3400 Series Appliance를 관리할 수 있습니다. BIOS 컨피그레이션을 포함한 모든 작업을 CIMC에서 수행할 수 있습니다.



주의

설치 후에 Cisco ISE 어플라이언스에서 표준 시간대를 변경하면 해당 노드의 Cisco ISE 애플리케이션을 사용할 수 없게 됩니다.

시작하기 전에

- CIMC가 어플라이언스에 구성되어 있어야 합니다.
- 지원되는 어플라이언스를 권장 절차에 따라 제대로 설치, 연결, 시작했는지 확인합니다.
- CIMC에 액세스하는 클라이언트 시스템에 Cisco ISE ISO 이미지가 있거나 설치용 이미지가 저장된 부팅 가능 USB가 있어야 합니다.
- Cisco ISE 어플라이언스는 내부적으로 UTC 표준 시간대를 사용하여 시간을 추적합니다. 표준 시간대를 모를 경우 Cisco ISE 어플라이언스가 위치한 도시, 지역 또는 국가를 기준으로 하여 입력할 수 있습니다. 설치할 때 설정 프로그램에서 설정 컨피그레이션 프롬프트가 나타나면 기본 표준 시간대(기본값은 UTC)를 구성하는 것이 좋습니다.
- 인라인 포스처 노드에서 인증서를 구성하는 방법을 알아봅니다.

단계 1 서버 관리를 위해 CIMC에 연결합니다. NIC(Network Interface Card) 모드 설정에서 선택한 포트를 사용하여 LAN과 서버를 이더넷 케이블로 연결합니다. 액티브-액티브 및 액티브-패시브 NIC 이중화 설정에서는 두 포트를 연결해야 합니다.

단계 2 브라우저와 CIMC의 IP 주소를 사용하여 CIMC Setup Utility에 로그인합니다. IP 주소는 CIMC 컨피그레이션에 따라 달라집니다. 고정 주소이거나 DHCP(Dynamic Host Configuration Protocol) 서버에 의해 지정된 주소입니다. 참고 서버에 대한 기본 사용자 이름은 *admin*입니다. 기본 비밀번호는 *password*입니다.

- 단계 3 **Launch KVM Console**을 클릭합니다.
- 단계 4 CIMC 인증서를 사용하여 로그인합니다.
- 단계 5 **Virtual Media** 탭을 클릭합니다.
- 단계 6 **Add Image**를 클릭하여 클라이언트 브라우저를 실행하는 시스템에서 Cisco ISE ISO 이미지를 선택합니다.
- 단계 7 생성한 가상 CD/DVD 드라이브에 대해 **Mapped** 확인란을 선택합니다.
- 단계 8 **KVM** 탭을 클릭합니다.
- 단계 9 ISO 이미지를 사용하여 SNS-3400 Series Appliance를 부팅하기 위해 **Macros > Ctrl-Alt-Del**을 선택합니다.
- 단계 10 **F6**을 눌러 부팅 메뉴를 시작합니다.
- 단계 11 매핑한 CD/DVD를 선택하고 **Enter**를 누릅니다.
- 단계 12 부팅 프롬프트에서 **2**를 입력하고 **Enter**를 누릅니다.

 어플라이언스를 구성하기 위해 'setup'을 입력합니다.

- 단계 13 프롬프트에서 **setup** 을 입력하여 설정 프로그램을 시작합니다. 네트워킹 매개변수 및 인증서를 입력하라는 메시지가 표시됩니다.
 다음은 샘플 설정 프로그램 및 기본 프롬프트입니다.
 Press 'Ctrl-C' to abort setup
 Enter hostname[: ise-server-1
 Enter IP address[: 10.1.1.10
 Enter IP netmask[: 255.255.255.0
 Enter IP default gateway[: 172.10.10.10
 Enter default DNS domain[: cisco.com
 Enter primary nameserver[: 200.150.200.150
 Add secondary nameserver? Y/N [N]: n
 Enter NTP server[time.nist.gov]: 200.150.200.151
 Add another NTP server? Y/N[N]: n
 Enter system time zone[UTC]: UTC
 Enable SSH service?: Y/N [N]: Y
 Enter username [admin]: admin
 Enter password:
 Enter password again:
 Copying first CLI user to be first ISE admin GUI user...
 Bringing up the network interface...
 Pinging the gateway...
 Pinging the primary nameserver...

 Do not use `Ctrl-C' from this point on...

 Installing Applications...
 Installing ISE...
 Unbundling Application Package...
 Initiating Application Install...

 Application bundle (ISE) installed successfully

 ===Initial Setup for Application: ISE ===

 Welcome to the ISE initial setup. The purpose of this setup is to provision the internal ISE database.
 This setup is non-interactive, and will take roughly 15 minutes to complete.

 Running database cloning script...
 Running database network config assistant tool...
 Extracting ISE database contents...
 Starting ISE database processes...

 ...

Cisco ISE 노드 스위치가 구성되면 Cisco ISE 시스템이 자동으로 재부팅됩니다. 다시 CLI에 로그인하려면 설정 과정에서 구성했던 CLI 관리자 사용자 인증서를 입력해야 합니다.

- 단계 14** Cisco ISE CLI 셸에 로그인하고 다음 CLI 명령을 실행하여 Cisco ISE 애플리케이션 프로세스의 상태를 확인합니다.

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

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	3638
Database Server	running	45 PROCESSES
Application Server	running	5992
Profiler Database	running	4481
AD Connector	running	6401
M&T Session Database	running	2319
M&T Log Collector	running	6245
M&T Log Processor	running	6286
Certificate Authority Service	running	6211
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
Identity Mapping Service	disabled	

- 단계 15** Cisco ISE Application Server가 실행 중임을 확인하고 지원되는 웹 브라우저 중 하나를 사용하여 Cisco ISE 사용자 인터페이스에 로그인할 수 있습니다. 웹 브라우저를 사용하여 Cisco ISE 사용자 인터페이스에 로그인하려면 Address 필드에 **https://<your-ise-hostname or IP address>/admin/**을 입력합니다. 여기서 “your-ise-hostname or IP address”는 설정 과정에서 Cisco SNS-3400 Series Appliance에 대해 구성된 호스트 이름 또는 IP 주소입니다. Cisco ISE 사용자 인터페이스에 액세스하기 위해 웹 기반 관리자 로그인 인증서(사용자 이름 및 비밀번호)를 입력합니다. 처음에는 CLI 관리자 사용자 이름 및 설정 프로세스에서 정의한 비밀번호를 사용하여 Cisco ISE 웹 인터페이스에 액세스할 수 있습니다. Cisco ISE 사용자 인터페이스에 대한 웹 기반 액세스에 쓰이는 사용자 이름과 비밀번호는 설정 과정에서 Cisco ISE CLI 인터페이스 액세스를 위해 생성한 CLI 관리자 사용자 인증서와 다릅니다. Cisco ISE 사용자 인터페이스에 로그인한 다음 디바이스, 사용자 저장소, 정책, 기타 구성 요소를 구성할 수 있습니다.

지원되는 표준 시간대

이 절에서는 유럽, 미국/캐나다, 호주, 아시아의 협정 세계시(UTC) 표준 시간대를 3개의 표로 정리하여 설명합니다. Cisco ISE CLI의 **show timezones** 명령은 사용 가능한 모든 표준 시간대의 목록을 표시합니다.



참고 모든 Cisco ISE 노드를 UTC 표준 시간대로 설정하는 것이 좋습니다. 이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서, 로그, 포스터 에이전트 로그 파일의 타임스탬프가 항상 동기화됩니다.

표준 시간대의 형식은 POSIX 또는 System V입니다. POSIX 표준 시간대 형식은 America/Los_Angeles, System V 표준 시간대는 PST8PDT와 같은 구문을 사용합니다.

표 6: 유럽, 미국, 캐나다 표준 시간대

약어 또는 이름	표준 시간대 이름
유럽	
GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu	Greenwich Mean Time, UTC
GB	British
GB-Eire, Eire	Irish
WET	Western Europe Time, UTC
CET	Central Europe Time, UTC + 1시간
EET	Eastern Europe Time, UTC + 2시간
미국 및 캐나다	
EST, EST5EDT	Eastern Standard Time, UTC - 5시간
CST, CST6CDT	Central Standard Time, UTC- 6시간
MST, MST7MDT	Mountain Standard Time, UTC - 7시간
PST, PST8PDT	Pacific Standard Time, UTC - 8시간
HST	Hawaiian Standard Time, UTC - 10시간

표 7: 호주 표준 시간대

호주			
국가와 도시를 전방향 슬래시(/)로 구분하여 함께 입력합니다(예: Australia/Currie).			
ACT(Australian Capital Territory)	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHI(Lord Howe Island)	Melbourne

호주			
국가와 도시를 전방향 슬래시(/)로 구분하여 함께 입력합니다(예: Australia/Currie).			
North	NSW(New South Wales)	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna	—	—

표 8: 아시아 표준 시간대

아시아			
Aden	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Kolkata
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk	—	—
참고	아시아 표준 시간대는 동아시아, 동남아시아, 서아시아, 중앙아시아의 도시를 포함합니다. 지역과 도시 또는 국가를 전방향 슬래시(/)로 구분하여 함께 입력합니다(예: Asia/Aden).		

설정 프로세스 확인

초기 설정 프로세스를 올바르게 완료했는지 확인하려면 다음 두 가지 방법 중 하나로 Cisco ISE 어플라이언스에 로그인합니다.

- 웹 브라우저
- Cisco ISE CLI

Cisco ISE 사용자 인터페이스에 로그인하고 다음 작업을 수행해야 합니다.

- 라이선스를 등록합니다. 자세한 내용은 *Cisco ISE* 관리자 설명서의 [라이선스 등록](#) 절을 참조하십시오.
- Cisco ISE 시스템을 구성합니다. 컨피그레이션 작업에 대해서는 [Cisco ISE 관리자 설명서](#)를 참조하십시오.



VMware 가상 머신에 ISE 설치

- 가상 머신에서 지원되지 않는 ISE 기능, 31 페이지
- 지원되는 VMware 버전, 31 페이지
- VMware vMotion 지원, 32 페이지
- Open Virtualization Format 지원, 32 페이지
- 가상 머신 요구 사항, 33 페이지
- 가상 머신 리소스 및 성능 확인, 36 페이지
- Cisco ISE 릴리스 평가, 38 페이지
- 가상 머신에 Cisco ISE 설치, 38 페이지
- 평가 환경에서 프로덕션 환경으로 Cisco ISE VM 마이그레이션, 50 페이지

가상 머신에서 지원되지 않는 ISE 기능

인라인 포스처 노드는 Cisco SNS-3415 및 Cisco ISE 3300 Series Appliance에서만 지원됩니다. Cisco SNS-3495 Series 또는 VMware 서버 시스템에서는 지원되지 않습니다. 그 밖의 모든 지정된 역할은 VMware 가상 머신에서 지원됩니다.

지원되는 VMware 버전

Cisco ISE는 다음 VMware 서버 및 클라이언트를 지원합니다.

- VMware ESXi, 버전 5.x
- VMware vSphere Client 5.x

VMware vMotion 지원

Cisco ISE는 VMware vMotion 기능을 지원하므로, 실행 중인 가상 머신 인스턴스(임의의 페르소나)를 호스트 간에 마이그레이션할 수 있습니다. VMware vMotion 기능이 작동하려면 다음 조건을 충족해야 합니다.

- 공유 스토리지—VM용 스토리지는 SAN(Storage Area Network)에 있어야 하며, 이동 대상인 VM을 호스팅할 가능성이 있는 모든 VMware 호스트에서 이 SAN에 액세스할 수 있어야 합니다.
- VMFS 볼륨 공유—VMware 호스트는 공유 VMFS(virtual machine file system) 볼륨을 사용해야 합니다.
- 기가비트 이더넷 상호 연결—SAN과 VMware 호스트는 기가비트 이더넷 링크로 상호 연결되어야 합니다.
- 프로세서 호환성—호환되는 프로세서 세트를 사용해야 합니다. vMotion 호환성을 위해 프로세서는 동일한 벤더 및 프로세서 그룹에 속해야 합니다.

Open Virtualization Format 지원

Cisco ISE는 OVF(Open Virtualization Format)를 지원하며 VM(virtual machine)에 Cisco ISE를 설치하고 구축하는 데 사용 가능한 OVA 템플릿을 제공합니다. 다음 OVA 템플릿을 사용할 수 있습니다.

- ISE-1.4.xxx.xxx-eval.ova—Cisco ISE를 평가하는 경우 이 템플릿을 사용합니다. 평가 라이선스는 최대 100개의 엔드포인트를 지원합니다.
- ISE-1.4.xxx.xxx-virtual-SNS3415.ova—VMware 어플라이언스 사양이 SNS-3415 어플라이언스에 필적할 경우 이 템플릿을 사용합니다.
- ISE-1.4.xxx.xxx-virtual-SNS3495.ova—VMware 어플라이언스 사양이 SNS-3495 어플라이언스에 필적할 경우 이 템플릿을 사용합니다.

다음 표에서는 OVA 템플릿 예약을 보여줍니다.

OVA 템플릿	메모리	CPU
Virtual Eval OVA	4GB RAM	2300MHz(예약 없음)
Virtual SNS-3415 OVA	16GB RAM	8000MHz
Virtual SNS-3495 OVA	32GB RAM	16000MHz

가상 머신 요구 사항

VMware 가상 머신이 Cisco ISE 하드웨어 어플라이언스에 준하는 성능 및 확장성을 제공하려면 Cisco SNS 3415 및 3495 어플라이언스와 같은 시스템 리소스가 할당되어야 합니다.

표 9: VMware 최소 시스템 요구 사항

요구 사항 유형	최소 요구 사항
CPU	<p>싱글 쿼드 코어, 2.0GHz 이상.</p> <p>Cisco ISE는 하이퍼스레딩을 지원합니다. 하이퍼스레딩 옵션이 활성화되었거나 비활성화된 VMware 호스트에 ISE를 설치할 수 있습니다.</p> <p>참고 하이퍼스레딩으로 전반적인 VM 성능이 향상될 수 있지만 VM 어플라이언스당 지원되는 확장 한도가 바뀌지는 않습니다. 물론 논리적 프로세서 수가 아닌 필요한 물리적 코어 수를 기준으로 CPU 리소스를 할당해야 합니다.</p>
메모리	16GB에서 32GB RAM
하드 디스크	<p>200GB에서 2TB 디스크 스토리지(크기는 구축 및 작업에 따라 달라짐)</p> <p>VM 호스트 서버에서 속도가 10,000RPM 이상인 하드 디스크를 사용하는 것이 좋습니다. Cisco ISE VM에서는 초당 50MB 이상의 쓰기 대역폭, 초당 300MB 이상의 읽기 대역폭이 필요합니다. 호스팅 환경에서 10,000RPM 디스크를 사용하면 이 쓰기 대역폭을 쉽게 제공할 수 있습니다.</p> <p>참고 Cisco ISE를 위한 가상 머신을 생성할 때 스토리지 요구 사항에 부합하는 단일 가상 디스크를 사용해야 합니다. 둘 이상의 디스크를 사용하여 디스크 공간 요구 사항을 충족할 경우 설치 프로그램에서 일부 디스크 공간을 인식하지 못할 수 있습니다.</p>
스토리지	<ul style="list-style-type: none"> • 파일 시스템—VMFS <p>스토리지에 VMFS를 사용하는 것이 좋습니다. 다른 스토리지 프로토콜은 검증되지 않았으므로 파일 시스템 오류가 발생할 수도 있습니다.</p> <ul style="list-style-type: none"> • 내부 스토리지—SCSI/SAS • 외부 스토리지—iSCSI/SAN <p>NFS 스토리지 사용은 권장하지 않습니다.</p>
디스크 컨트롤러	Paravirtual(RHEL 64비트의 기본 설정) 또는 LSI Logic Parallel

요구 사항 유형	최소 요구 사항
NIC	1GB NIC 인터페이스 필요(NIC 2개 이상 권장) Cisco ISE는 E1000 및 VMXNET3 어댑터를 지원합니다. 참고 기본적으로 올바른 어댑터 순서를 보장하기 위해 E1000을 선택하는 것이 좋습니다. VMXNET3를 선택할 경우 ESX 어댑터를 다시 매핑하여 ISE 어댑터 순서와 동기화하는 작업이 필요할 수 있습니다.
하이퍼바이저	<ul style="list-style-type: none"> • ESXi 5는 VMware 버전 8.x • VMware vSphere Client 5.x

VMware 어플라이언스 크기 권장 사항

VMware 어플라이언스 사양은 프로덕션 환경에서 실행되는 물리적 어플라이언스에 필적해야 합니다.

어플라이언스를 위한 리소스를 할당할 때 다음 지침을 기억하십시오.

- 가상 머신 리소스는 전용이어야 합니다. VM 리소스는 여러 VM에서 공유하거나 오버서브스크립션해서는 안 됩니다.
- 가상 머신의 정책 서비스 노드는 관리 또는 모니터링 노드보다 적은 디스크 공간으로 구축할 수 있습니다. 정책 서비스 노드에 100GB에서 200GB까지의 디스크 공간을 할당하는 것이 좋습니다.
- 가상 머신은 NIC 1개에서 4개까지 구성할 수 있습니다. 2개 이상의 NIC를 허용하는 것이 좋습니다. 추가 인터페이스를 사용하여 프로파일링, RADIUS와 같은 여러 서비스를 지원할 수 있습니다.

표 10: 프로덕션 환경의 VMware 어플라이언스 사양

플랫폼	SNS-3415	SNS-3495
프로세서	싱글 소켓 Intel E5-2609 2.4Ghz CPU 총 4코어	듀얼 소켓 Intel E5-2609 2.4Ghz CPU 총 8코어
메모리	16GB	32GB
전체 디스크 공간	600GB	600GB
이더넷 NIC	4 x 통합 기가비트 NIC	4 x 통합 기가비트 NIC

디스크 공간 요구 사항

다음 표에서는 프로덕션 구축에서 VMware 서버를 실행할 때 권장되는 Cisco ISE 디스크 공간을 알려줍니다.

표 11: 권장 VMware 디스크 공간

ISE 페르소나	최소 디스크 공간	최대 디스크 공간	프로덕션을 위한 권장 디스크 공간
독립형 ISE	200GB	2TB	600GB에서 2TB
분산형 ISE - 관리만	200GB	2TB	250GB에서 300GB
분산 ISE - 모니터링만	200GB	2TB	600GB에서 2TB
분산형 - 정책 서비스만	200GB	2TB	200GB
분산형 ISE - 관리 및 모니터링	200GB	2TB	600GB에서 2TB
분산형 ISE — 관리, 모니터링, 정책 서비스	200GB	2TB	600GB에서 2TB

디스크 공간 지침

Cisco ISE를 위한 디스크 공간을 결정할 때 다음 지침을 기억하십시오.

- Cisco ISE 가상 머신 1개에 최대 2TB의 디스크 공간만 할당할 수 있습니다.
- Cisco ISE는 VMware에서 단일 디스크에 설치해야 합니다.
- 디스크 할당량은 로깅 보존 요구 사항에 따라 달라집니다. 모니터링 페르소나가 활성화된 노드에서 VM 디스크 공간의 30%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 저장 용도로 180GB가 할당됩니다. 엔드포인트 100,000개가 이 네트워크에 매일 연결되는 경우 매일 약 4GB의 로그가 생성됩니다. 이러한 경우 모니터링 노드에서 38일분의 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 30GB가 추가되는 셈입니다. 사용자의 요구 사항에 따라 VM 디스크 크기를 2TB까지, 즉 로그 저장소는 614GB까지 늘릴 수 있습니다.

가상 머신의 디스크 크기를 늘릴 경우 Cisco ISE로 업그레이드해서는 안 됩니다. 가상 머신에서 Cisco ISE를 새로 설치해야 합니다.

표 12: 모니터링 노드에 저장할 수 있는 로그의 양(일)에서는 할당된 디스크 공간 및 네트워크에 연결된 엔드포인트 수를 기준으로 모니터링 노드에서 며칠 분의 로그를 보존할 수 있는지 보여줍니다. 이 수치는 로그 압축 및 비정상적 클라이언트 탐지 기능이 활성화된 상태에서 얻은 것입니다.

표 12: 모니터링 노드에 저장할 수 있는 로그의 양(일)

엔드포인트 수	200GB	400GB	600GB	1024GB	2048GB
10,000	126	252	378	645	1,289
20,000	63	126	189	323	645
30,000	42	84	126	215	430
40,000	32	63	95	162	323
50,000	26	51	76	129	258
100,000	13	26	38	65	129
150,000	9	17	26	43	86
200,000	7	13	19	33	65
250,000	6	11	16	26	52

가상 머신 리소스 및 성능 확인

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

VMware 리소스 검사 과정에서 설치 프로그램은 하드 디스크 공간, VM에 할당된 CPU 코어 수, CPU 클럭 속도, VM에 할당된 RAM을 확인합니다. VM 리소스가 권장 사양에 미치지 못할 경우 설치가 중단됩니다. 이러한 VMware 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. 이러한 성능 검증 확인은 ISO 기반 및 OVA 설치에만 적용됩니다.

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 온디맨드 방식으로 가능하며, Cisco ISE CLI에서 **show tech-support** 명령을 사용합니다.

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

Show Tech Support 명령을 사용하는 온디맨드 가상 머신 성능 확인

CLI에서 **show tech-support** 명령을 실행하여 언제라도 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.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 1.4.0.205
```

Available boot options:

```
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk.
```

Enter boot option and press <Enter>.

CLI 부팅 메뉴에서 **3** 또는 **4**를 입력하여 System Utilities 메뉴로 이동합니다.

```
Cisco ISE System Utilities Menu
```

Available System Utilities:

```
[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[4] Install Media Check
[q] Exit and reload
```

Enter option and press <Enter>

2를 입력하여 VM 리소스를 확인합니다. 다음과 같이 출력됩니다.

```
*****
***** Virtual Machine host detected...
***** Hard disk(s) total size detected: 322 Gigabyte
***** Physical RAM size detected: 40443664 Kbytes
***** Number of network interfaces detected: 1
***** Number of CPU cores: 2
***** CPU Mhz: 2300.00
***** Verifying CPU requirement...
***** Verifying RAM requirement...
***** Writing disk partition table...
```

Cisco ISE 릴리스 평가

Cisco ISE 평가 소프트웨어(R-ISE-EVAL-K9)를 얻으려면 Cisco 어카운트 팀 또는 공인 Cisco 채널 파트너에 문의하십시오.

Cisco ISE 컨피그레이션을 평가 시스템에서 정식 라이선스를 취득한 프로덕션 시스템으로 마이그레이션하려면 다음 작업을 완료해야 합니다.

- 평가 버전의 컨피그레이션을 백업합니다.
- 프로덕션 VM에 필요한 양의 디스크 공간이 있는지 확인합니다. 자세한 내용은 구축 크기 및 확장 권장 사항을 참조하십시오.
- 프로덕션 구축 라이선스를 설치합니다.
- 프로덕션 시스템에 컨피그레이션을 복원합니다.



참고

평가를 위해서는 VMware 서버에서 최소한 200GB의 하드 디스크를 할당해야 합니다. 더 많은 수의 사용자를 지원하는 프로덕션 환경으로 VMware 서버를 이전할 경우 Cisco ISE 설치를 권장 최소 디스크 크기 또는 그 이상으로 (최대 한도인 2TB는 넘지 않게) 다시 구성해야 합니다.

시작하기 전에

평가 목적으로 VM 요구 사항에 적합한 지원되는 VMware VM에 Cisco ISE를 설치할 수 있습니다. Cisco ISE를 평가할 때 VM에 더 적은 디스크 공간을 구성할 수 있으나, 역시 200GB 이상의 디스크 공간을 할당해야 합니다.

단계 1 <http://www.cisco.com/go/ise>로 이동합니다. 이 링크에 액세스하려면 유효한 Cisco.com 로그인 인증서가 있어야 합니다.

단계 2 **Download Software for this Product**를 클릭합니다.
이 소프트웨어 이미지는 90일 평가판 라이선스가 설치된 상태로 제공되므로 설치 및 초기 컨피그레이션이 완료되면 즉시 모든 Cisco ISE 서비스를 테스트해볼 수 있습니다.

가상 머신에 Cisco ISE 설치

다음 방법 중 하나로 VM에 Cisco ISE를 설치할 수 있습니다. Cisco ISE OVA 템플릿을 다운로드하고 구축하는 것이 좋습니다.

- OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 구축, 39 페이지
- ISO 파일을 사용하여 가상 머신에 Cisco ISE 설치, 39 페이지

- Cisco ISE 가상 머신 복제, 46 페이지

OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 구축

OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 소프트웨어를 설치하고 구축할 수 있습니다. Cisco.com에서 OVA 템플릿을 다운로드합니다.

시작하기 전에

OVA 템플릿을 사용하여 가상 머신에 Cisco ISE 소프트웨어를 설치하고 구축할 수 있습니다.

-
- 단계 1 VMware vSphere 클라이언트를 엽니다.
 - 단계 2 VMware 호스트에 로그인합니다.
 - 단계 3 VMware vSphere 클라이언트에서 **File > Deploy OVF Template**을 선택합니다.
 - 단계 4 **Browse**를 클릭하여 OVA 템플릿을 선택하고 **Next**를 클릭합니다.
 - 단계 5 OVF Template Details 페이지에서 세부 사항을 확인하고 **Next**를 클릭합니다.
 - 단계 6 Name and Location 페이지에서 가상 머신을 고유하게 식별할 이름을 입력하고 **Next**를 클릭합니다.
 - 단계 7 OVA를 호스팅할 데이터 저장소를 선택합니다.
 - 단계 8 Disk Format 페이지에서 **Thick Provision** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.
Cisco ISE는 씹 프로비저닝과 썬 프로비저닝을 모두 지원합니다. 그러나 더 우수한 성능을 위해, 특히 모니터링 노드에서는 씹 프로비저닝을 선택하는 것이 좋습니다. 썬 프로비저닝을 선택할 경우, 초기 디스크 확장 과정에서 업그레드, 백업, 복원과 같은 작업 및 더 많은 디스크 공간을 필요로 하는 디버그 로깅이 영향을 받을 수 있습니다.
 - 단계 9 Ready to Complete 페이지의 정보를 확인합니다. **Power on after deployment** 확인란을 선택합니다.
 - 단계 10 **Finish**를 클릭합니다.
-

ISO 파일을 사용하여 가상 머신에 Cisco ISE 설치

ISO 파일을 사용하여 VM에 Cisco ISE를 설치하려면

시작하기 전에

- 이 장의 요구 사항을 읽고 그에 따라 VM 리소스를 지정해야 합니다.
- VMware ESX 또는 ESXi 서버 구성 시 전체 조건절을 숙독합니다.

- Cisco.com에서 Cisco ISE ISO 이미지를 다운로드합니다.

-
- 단계 1 VMware 서버를 구성합니다. [VMware 서버 구성, 43 페이지](#)을/를 참조하십시오.
- 단계 2 소프트웨어 DVD에서 부팅하도록 VMware 시스템을 구성합니다. [Cisco ISE 소프트웨어 DVD에서 부팅하도록 VMware 시스템 구성, 44 페이지](#)을/를 참조하십시오.
- 단계 3 VM에 Cisco ISE 소프트웨어를 설치합니다. [DVD에서 Cisco ISE 소프트웨어 설치](#)을/를 참조하십시오.
-

VMware ESX 또는 ESXi Server 구성 시 전제 조건

VMware ESX 또는 ESXi 서버를 구성하기 전에 이 절의 다음 컨피그레이션 전제 조건을 참조하십시오.

- 관리자 권한이 있는 사용자(루트 사용자)로 ESXi 서버에 로그인해야 합니다.
- Cisco ISE는 64비트 시스템입니다. 64비트 시스템을 설치하기 전에 ESX/ESXi 서버에서 VT(Virtualization Technology)가 활성화되었는지 확인합니다. 가상 머신의 게스트 운영 체제가 64비트로 설정되었는지도 확인합니다. 또한 게스트 운영 체제 유형이 Red Hat Enterprise Linux 6(64비트)로 설정되어야 합니다.
- Red Hat Enterprise Linux 6에서 기본 NIC 유형은 VMXNET3 Adapter입니다. Cisco ISE 가상 머신에 최대 4개의 NIC를 추가할 수 있지만, 모든 NIC에 동일한 어댑터를 선택해야 합니다. Cisco ISE는 E1000 Adapter를 지원합니다.



참고 기본 네트워크 드라이버(VMXNET3)를 네트워크 어댑터로 선택할 경우 물리적 어댑터 매핑을 확인합니다. Cisco ISE GigabitEthernet 0 인터페이스를 ESX의 4번째 인터페이스(NIC 4)에 매핑했는지 확인합니다. E1000 Adapter를 선택할 경우 기본적으로 ESX 및 Cisco ISE 어댑터가 올바르게 매핑됩니다.

- VMware 가상 머신에 권장량의 디스크 공간을 할당해야 합니다.
- 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.
 - VMFS5를 사용할 경우 1MB의 블록 크기가 최대 2TB의 가상 디스크 크기를 지원합니다.
 - VMFS3를 사용할 경우 VMware 호스트에서 호스팅하는 가장 큰 가상 디스크 크기에 따라 VMFS 블록 크기를 선택해야 합니다. VMFS 블록 크기를 구성한 후에 이를 변경하려면 VMFS 파티션을 다시 포맷해야 합니다. VMFS3의 경우 VMFS 블록 크기는 가장 큰 가상 디스크의 크기에 따라 결정해야 합니다.

표 13: VMFS 블록 크기

블록 크기	가상 디스크 크기
1MB	256GB
2MB	512GB
4MB	1TB
8MB	2TB

가상화 기술 확인

ESX 또는 ESXi 서버가 이미 설치된 경우 재부팅하지 않고도 VT가 활성화되었는지 확인할 수 있습니다. 이를 위해서는 **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 ESX 또는 ESXi 서버에서 활성화되었으며 설치를 계속할 수 있습니다.

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

ESX 또는 ESXi 서버에 가상화 기술 활성화

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

-
- 단계 1 SNS-3400 Series Appliance를 재부팅합니다.
 - 단계 2 F2를 눌러 설정을 입력합니다.
 - 단계 3 **Advanced > Processor Configuration**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 ESX 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 탭에서 **Add**를 클릭합니다.
- 단계 4 **Serial Port**를 선택하고 **Next**를 클릭합니다.
- 단계 5 Serial Port Output 영역에서 **Use physical serial port on the host** 또는 **Connect via Network** 라디오 버튼을 클릭하고 **Next**를 클릭합니다.
- Connect via Network 옵션을 선택할 경우 ESX 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

먼저 VMware ESX 또는 ESXi 서버 구성 시 전제 조건의 세부 사항을 숙독합니다.

-
- 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 사용합니
 다.
- 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 7**과 같은 가상 머신 버전을 선택하고 **Next**를 클릭합니다.
- 단계 7 Version 드롭다운 목록에서 **Linux 및 Red Hat Enterprise Linux 6 (64-bit)**를 선택합니다.
- 단계 8 Number of virtual sockets 및 Number of cores per virtual socket 드롭다운 목록에서 **2**를 선택합니다. 총 코어 수는 4가 되어야 합니다.
 (선택 사항. 일부 버전의 ESX 서버에서 나타납니다. Number of virtual processors만 나타날 경우 **4**를 선택합니다.)
- 단계 9 메모리의 양을 선택하고 **Next**를 클릭합니다.
- 단계 10 Adapter 드롭다운 목록에서 **E1000 NIC** 드라이버를 선택하고 **Next**를 클릭합니다.
 SCSI controller 대화 상자가 나타납니다.
- 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 씹 프로비저닝과 썬 프로비저닝을 모두 지원합니다. 그러나 더 우수한 성능을 위해, 특히 모니터링 노드에서는 씹 프로비저닝을 선택하는 것이 좋습니다. 썬 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. 그 값은 다음과 같아야 합니다.
- Guest OS—Red Hat Enterprise Linux 6 (64-bit)
 - CPUs—4
 - Memory—16GB 또는 16384MB

- Disk Size—VMware 디스크 공간에 대한 권장 사항에 따라 200GB에서 2TB까지

가상 머신에서 성공적으로 Cisco ISE를 설치하려면 이 문서의 권장 사항을 따르십시오.

- 단계 17 **Finish**를 클릭합니다.
VMware 시스템이 설치되었습니다.

다음에 할 작업

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

Cisco ISE 소프트웨어 DVD에서 부팅하도록 VMware 시스템 구성

VMware 시스템을 구성한 다음 Cisco ISE 소프트웨어를 설치할 수 있습니다. DVD에서 Cisco ISE 소프트웨어를 설치하려면 DVD에서 부팅하도록 VMware 시스템을 구성해야 합니다. 그러기 위해서는 VMware 시스템에 가상 DVD 드라이브가 구성되어야 합니다.

시작하기 전에

Cisco ISE ISO를 다운로드하고 ISO 이미지를 DVD에 구운 다음 가상 머신에 Cisco ISE를 설치하는 데 사용해야 합니다.

- 단계 1 VMware 클라이언트에서 새로 생성된 VMware 시스템을 강조 표시하고 **Edit Virtual Machine Settings**를 선택합니다.
- 단계 2 Virtual Machine Properties 대화 상자에서 **CD/DVD Drive 1**을 선택합니다.
- 단계 3 **Host Device** 라디오 버튼을 클릭하고 드롭다운 목록에서 DVD 호스트 디바이스를 선택합니다.
- 단계 4 **Connect at Power On** 옵션을 선택하고 **OK**를 클릭하여 설정을 저장합니다.
이제 VMware ESX 서버의 DVD 드라이브를 사용하여 Cisco ISE 소프트웨어를 설치할 수 있습니다.

다음에 할 작업

이 작업을 완료한 다음 VMware 클라이언트 사용자 인터페이스에서 **Console** 탭을 클릭하고 왼쪽 창에서 VM을 마우스 오른쪽 버튼으로 클릭한 다음 **Power**를 선택하고 **Reset**을 선택하여 VMware 시스템을 다시 시작합니다.

VMware 시스템에 Cisco ISE 소프트웨어 설치

시작하기 전에

- 설치 후 영구 라이선스를 설치하지 않을 경우 Cisco ISE에서는 최대 100개의 엔드포인트를 지원하는 90일 평가 라이선스를 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.

단계 1 VMware 클라이언트에 로그인합니다.

단계 2 BIOS에서 Coordinated Universal Time(UTC)이 설정되었는지 확인합니다.

- VMware 시스템이 켜져 있을 경우 끕니다.
- VMware 시스템을 켭니다.
- F1을 눌러 BIOS 설정 모드를 시작합니다.
- 화살표 키를 사용하여 Date and Time 필드로 이동하고 Enter를 누릅니다.
- 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.
- Esc를 눌러 주 BIOS 메뉴로 돌아갑니다.
- Esc를 눌러 BIOS 설정 모드를 종료합니다.

단계 3 VMware ESX 호스트 CD/DVD 드라이브에 Cisco ISE 소프트웨어 DVD를 삽입하고 가상 머신을 켭니다. DVD가 부팅되면 콘솔에 다음과 같이 표시됩니다.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 1.4.0.205
```

Available boot options:

```
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk.
```

Enter boot option and press <Enter>.

```
boot: 2
Loading vmlinuz.....
Loading initrd.img.....ready.
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-431.el6.x86_64 (mockbuild@x86-023.build.eng.bos.redhat.com) (gcc version 4.4.7
20120313 (Red Hat 4.4.7-4) (GCC) ) #1 SMP Sun Nov 10 22:19:54 EST 2013
모니터 및 키보드 포트를 선택하거나 콘솔 포트를 선택하여 초기 설정을 수행할 수 있습니다.
```

- 단계 4** 시스템 프롬프트에서 1을 입력하여 모니터 및 키보드 포트를 선택하거나 2를 입력하여 콘솔 포트를 선택하고 **Enter**를 누릅니다.
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 5** 시스템 프롬프트에서 **setup** 을 입력하고 **Enter**를 누릅니다.  
Setup Wizard가 나타나 초기 컨피그레이션을 차례로 안내합니다.

## 가상 머신에 대한 Cisco ISE ISO 설치 실패

가상 머신에 Cisco ISE를 새로 설치하는 데 실패한 경우, 기본 네트워크 드라이버(VMXNET3)가 네트워크 어댑터로 선택되었다면 물리적 어댑터 매핑을 확인합니다. Cisco ISE GigabitEthernet 0 인터페이스를 ESX의 4번째 인터페이스(NIC 4)에 매핑했는지 확인합니다. E1000 드라이버를 네트워크 어댑터로 사용하면 해결됩니다.

## 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.

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.
- 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 ESX 또는 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 할 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.

- 단계 1 가상 머신 템플릿 생성, 47 페이지
- 단계 2 가상 머신 템플릿 구축, 48 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.
- 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 ESX 호스트를 선택하고 **Next**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**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 ESX 호스트를 선택하고 **Next**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 할 작업

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

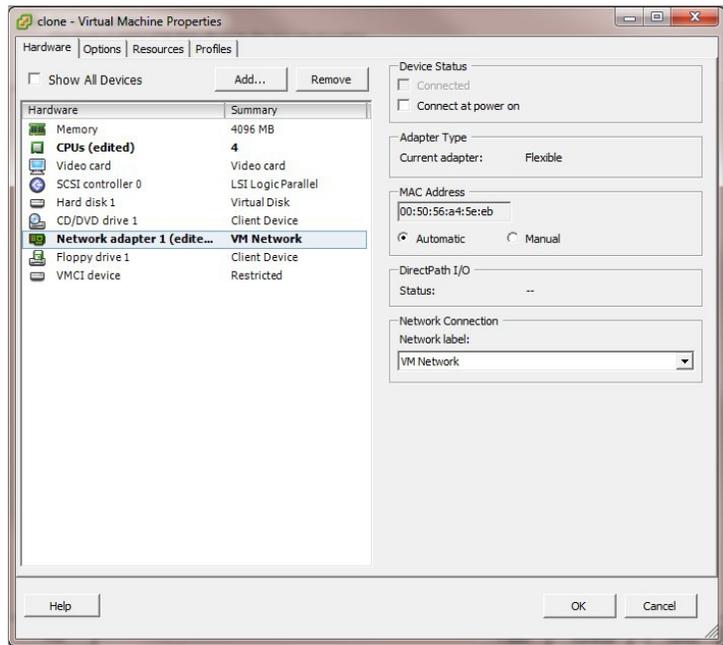
## 복제된 가상 머신의 IP 주소 및 호스트 이름 변경

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 9: 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
```

**hostname**은 구성하려는 새 호스트 이름입니다. Cisco ISE 서비스가 다시 시작합니다.
- 단계 4** 다음 명령을 입력합니다.  

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

**ip\_address**는 3단계에서 입력한 호스트 이름의 주소이고, **netmask**는 **ip\_address**의 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**를 클릭합니다.
- 

## 평가 환경에서 프로덕션 환경으로 Cisco ISE VM 마이그레이션

Cisco ISE 릴리스에 대한 평가를 마치고 평가 시스템에서 정식 라이선스를 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 2TB는 넘지 않게) 다시 구성해야 합니다.
- 200GB보다 작은 디스크 공간으로 생성한 VM에서 프로덕션 VM으로 데이터를 마이그레이션할 수 없습니다. 200GB 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 라이선스를 설치합니다.
  - 단계 4 프로덕션 시스템에 컨피그레이션을 복원합니다.
-





## Cisco ISE 3300 Series, Cisco NAC, Cisco Secure ACS Appliance에 Cisco ISE 소프트웨어 설치

- 지원되는 Cisco ISE, Secure ACS, NAC Appliance, 53 페이지
- DVD에서 Cisco ISE 소프트웨어 설치, 54 페이지
- 리이미징된 Cisco ISE-3300 Series Appliance에 Cisco ISE 소프트웨어 설치, 54 페이지
- 리이미징된 Cisco Secure ACS Appliance에 Cisco ISE 소프트웨어 설치, 55 페이지
- 리이미징된 Cisco NAC Appliance에 Cisco ISE 소프트웨어 설치, 56 페이지

### 지원되는 Cisco ISE, Secure ACS, NAC Appliance

다음 특정 Cisco 어플라이언스에서는 해당 어플라이언스가 리이미징된 경우 DVD에서 Cisco ISE 소프트웨어를 설치할 수 있습니다. 어플라이언스 유형:

- Cisco ISE-3315
- Cisco ISE-3355
- Cisco ISE-3395
- Cisco Secure ACS-1121
- Cisco NAC-3315
- Cisco NAC-3355
- Cisco NAC-3395

간소화된 프로세스를 통해 Cisco Secure ACS 또는 Cisco NAC 어플라이언스에 소프트웨어를 설치할 수 있습니다. Cisco ISE 소프트웨어가 설치될 기본 하드웨어가 동일한 물리적 디바이스 유형이기 때문입니다.

Cisco Secure ACS 또는 Cisco NAC 어플라이언스를 Cisco ISE 어플라이언스로 재사용하려면 어플라이언스를 리이미징한 다음 ISE 소프트웨어를 설치합니다.

Cisco ISE 3300 Series 하드웨어 플랫폼에 대한 자세한 내용은 *Cisco Identity Services Engine Release 1.2* 하드웨어 설치 설명서를 참조하십시오.

## DVD에서 Cisco ISE 소프트웨어 설치

### 시작하기 전에

- Cisco ISE Release 또는 인라인 포스처 노드 ISO 이미지를 다운로드하고 DVD에 ISO 이미지를 굽고 이를 사용하여 Cisco ISE-3300 Series, 레거시 Cisco NAC 및 Cisco Secure ACS Appliance에 소프트웨어를 설치합니다.
- 설정 프로그램 실행에 앞서 Cisco ISE 설정 매개변수를 검토하고 이 정보를 준비합니다.

- 
- 단계 1 키보드 및 VGA 모니터를 어플라이언스에 연결합니다.
- 단계 2 전원 코드가 어플라이언스에 연결되었는지 확인하고 어플라이언스 CD/DVD 드라이브에 DVD를 삽입하고 어플라이언스를 켭니다.  
콘솔에 부트 옵션이 표시됩니다.
- 단계 3 부트 프롬프트에서 **1**을 입력하고 **Enter**를 누릅니다.
- 단계 4 프롬프트에서 **setup** 을 입력하여 설정 프로그램을 시작합니다.
- 단계 5 설정 프로그램 매개변수에 대한 값을 입력합니다.  
Cisco ISE 또는 IPN 소프트웨어가 구성되면 시스템이 자동으로 재부팅됩니다. 다시 CLI에 로그인하려면 설정 과정에서 구성했던 CLI 관리자 사용자 인증서를 입력해야 합니다.
- 

### 다음에 할 작업

- IPN ISO를 설치한 경우 인라인 포스처 노드를 위한 인증서를 구성해야 합니다.
- Cisco ISE ISO 이미지를 설치한 경우 Cisco ISE CLI 셸에 로그인한 다음 **show application status ise** CLI 명령을 실행하여 Cisco ISE 애플리케이션 프로세스의 상태를 확인할 수 있습니다.

## 리이미징된 Cisco ISE-3300 Series Appliance에 Cisco ISE 소프트웨어 설치

### 시작하기 전에

- Cisco ISE 또는 인라인 포스처 노드 ISO 이미지를 다운로드하고 DVD에 ISO 이미지를 굽고 이를 사용하여 Cisco 어플라이언스에 소프트웨어를 설치합니다.
- Cisco SNS-3400 Appliance를 구성하기 위한 전제 조건을 검토합니다.

- 설정 프로그램 실행에 앞서 Cisco ISE 설정 프로그램 매개변수를 검토하고 이 정보를 준비합니다.
- DVD 설치 지침을 검토합니다.

- 
- 단계 1 Cisco ISE Appliance가 켜져 있을 경우 끕니다.
- 단계 2 Cisco ISE Appliance를 켭니다.
- 단계 3 **F1**을 눌러 BIOS 설정 모드를 시작합니다.
- 단계 4 화살표 키를 사용하여 Date and Time 필드로 이동하고 **Enter**를 누릅니다.
- 단계 5 시간을 UTC/GMT 표준 시간대로 설정합니다.  
참고 모든 Cisco ISE 노드를 UTC 표준 시간대로 설정하는 것이 좋습니다. 이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프가 항상 동기화됩니다.
- 단계 6 **Esc**를 눌러 주 BIOS 메뉴로 돌아갑니다.
- 단계 7 **Esc**를 눌러 BIOS 설정 모드를 종료합니다.
- 단계 8 DVD에서 소프트웨어를 설치합니다.
- 

다음에 할 작업

Cisco ISE 관리 포털에 로그인하고 라이선스를 설치합니다.

## 리이미징된 Cisco Secure ACS Appliance에 Cisco ISE 소프트웨어 설치

시작하기 전에

- Cisco ISE 또는 인라인 포스처 노드 ISO 이미지를 다운로드하고 DVD에 ISO 이미지를 굽고 이를 사용하여 레거시 Cisco Secure ACS Appliance에 Cisco ISE 또는 IPN 소프트웨어를 설치합니다.
- Cisco 어플라이언스를 구성하기 위한 전제 조건을 검토합니다.
- 설정 프로그램 실행에 앞서 Cisco ISE 설정 프로그램 매개변수를 검토하고 이 정보를 준비합니다.

- DVD 설치 지침을 검토합니다.

- 
- 단계 1 Cisco Secure ACS Appliance가 켜져 있을 경우 끕니다.
- 단계 2 Cisco Secure ACS Appliance를 켭니다.
- 단계 3 **F1**을 눌러 BIOS 설정 모드를 시작합니다.
- 단계 4 화살표 키를 사용하여 Date and Time 필드로 이동하고 **Enter**를 누릅니다.
- 단계 5 어플라이언스의 시간을 UTC/GMT 표준 시간대로 설정합니다.  
참고 모든 Cisco ISE 노드를 UTC 표준 시간대로 설정하는 것이 좋습니다. 이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프가 항상 동기화됩니다.
- 단계 6 **Esc**를 눌러 주 BIOS 메뉴로 돌아갑니다.
- 단계 7 **Esc**를 눌러 BIOS 설정 모드를 종료합니다.
- 단계 8 DVD에서 소프트웨어를 설치합니다.
- 

다음에 할 작업

Cisco ISE 관리 포털에 로그인하고 라이선스를 설치합니다.

## 리이미징된 Cisco NAC Appliance에 Cisco ISE 소프트웨어 설치

시작하기 전에

- Cisco ISE 소프트웨어 또는 인라인 포스처 노드 ISO 이미지를 다운로드하고 DVD에 ISO 이미지를 굽고 이를 사용하여 Cisco NAC Appliance에 소프트웨어를 설치합니다.
- Cisco 어플라이언스를 구성하기 위한 전제 조건을 검토합니다.
- 설정 프로그램 실행에 앞서 Cisco ISE 설정 프로그램 매개변수를 검토하고 이 정보를 준비합니다.
- DVD 설치 지침을 검토합니다.

- 
- 단계 1 Cisco NAC Appliance가 켜져 있을 경우 끕니다.
- 단계 2 Cisco NAC Appliance를 켭니다.
- 단계 3 **F1**을 눌러 BIOS 설정 모드를 시작합니다.
- 단계 4 화살표 키를 사용하여 Date and Time 필드로 이동하고 **Enter**를 누릅니다.
- 단계 5 어플라이언스의 시간을 UTC/GMT 표준 시간대로 설정합니다.

참고 모든 Cisco ISE 노드를 UTC 표준 시간대로 설정하는 것이 좋습니다. 이 표준 시간대 설정 덕분에 구축의 여러 노드에서 생성되는 보고서 및 로그의 타임스탬프가 항상 동기화됩니다.

- 단계 6 **Esc**를 눌러 주 BIOS 메뉴로 돌아갑니다.
- 단계 7 **Esc**를 눌러 BIOS 설정 모드를 종료합니다.
- 단계 8 DVD에서 소프트웨어를 설치합니다.

다음에 할 작업

Cisco ISE DVD 설치 프로세스에서 “The installer requires at least 600GB disk space for this appliance type”라는 메시지가 반환될 경우, 설치를 진행하려면 어플라이언스에서 RAID 설정의 재설정이 필요할 수 있습니다.

Cisco ISE 관리 포털에 로그인하고 라이선스를 설치합니다.

## Cisco NAC Appliance의 기존 RAID 컨피그레이션 재설정

Cisco ISE 소프트웨어 설치를 위해 NAC Appliance에서 RAID 설정을 재설정해야 하는 경우가 있습니다.

- 단계 1 Cisco ISE 소프트웨어 DVD로 Cisco NAC Appliance를 재부팅합니다.
- 단계 2 RAID 컨트롤러 버전 정보가 CLI에 나타나면 **Ctrl C**를 누릅니다. RAID 컨트롤러 버전 정보가 나타나고 LSI Corporation MPT SAS BIOS와 같은 레이블이 표시되며 LSI Corp Config Utility가 활성화됩니다.
- 단계 3 기본 컨트롤러를 지정하기 위해 **Enter**를 누릅니다. (강조 표시된 컨트롤러 이름은 SR-BR10i와 비슷한 형태여야 합니다.) Cisco NAC Appliance 어댑터 정보를 포함하는 화면이 나타납니다.
- 단계 4 화살표 키를 사용하여 “RAID properties”로 이동하고 **Enter**를 누릅니다.
- 단계 5 화살표 키를 사용하여 “Manage Array”로 이동하고 **Enter**를 누릅니다.
- 단계 6 화살표 키를 사용하여 “Delete Array”로 이동하고 **Enter**를 누릅니다.
- 단계 7 Y를 입력하여 기존 RAID 어레이를 삭제할 것임을 확인합니다.
- 단계 8 RAID 컨피그레이션 유틸리티를 종료하려면 **Esc**를 두 번 누릅니다. 시스템 프롬프트에서 Exit the Configuration Utility and Reboot?라고 묻습니다.
- 단계 9 그러면 **Enter**를 누릅니다. Cisco NAC Appliance가 재부팅됩니다. Cisco ISE 소프트웨어 DVD가 꽂혀 있는 상태에서 어플라이언스가 자동으로 부팅하여 설치 메뉴로 이동합니다.
- 단계 10 그러면 **1**을 눌러 Cisco ISE 설치를 시작합니다.





## 관리자 계정 관리

- CLI 관리자와 웹 기반 관리자의 사용자 권한 차이점, 59 페이지
- CLI 관리자 사용자 생성, 60 페이지
- 웹 기반 관리자 사용자 생성, 60 페이지

### CLI 관리자와 웹 기반 관리자의 사용자 권한 차이점

Cisco ISE 설정 프로그램을 사용하여 구성된 사용자 이름 및 비밀번호는 Cisco ISE CLI 및 Cisco ISE 웹 인터페이스에 대한 관리 액세스에 사용됩니다. Cisco ISE CLI에 액세스할 수 있는 관리자는 CLI 관리자 사용자라고 합니다. 기본적으로 CLI 관리자 사용자의 사용자 이름은 `admin`이며 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 14: CLI 관리자 및 웹 기반 관리자 사용자가 수행할 작업

| 관리자 사용자 유형            | 작업                                                                                                                                                                                                               |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLI 관리자 및 웹 기반 관리자 모두 | <ul style="list-style-type: none"> <li>• Cisco ISE 애플리케이션 데이터 백업</li> <li>• Cisco ISE 어플라이언스의 모든 시스템, 애플리케이션, 진단 로그 표시</li> <li>• Cisco ISE 소프트웨어 패치, 유지 관리 릴리스, 업그레이드 적용</li> <li>• NTP 서버 컨피그레이션 설정</li> </ul> |

| 관리자 사용자 유형 | 작업                                                                                                                                                                                 |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CLI 관리자만   | <ul style="list-style-type: none"> <li>• Cisco ISE 애플리케이션 소프트웨어 시작 및 중지</li> <li>• Cisco ISE 어플라이언스 다시 로드 및 종료</li> <li>• 잠긴 경우 웹 기반 관리자 사용자 재설정</li> <li>• ISE CLI 액세스</li> </ul> |

## CLI 관리자 사용자 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.

CLI에서 컨피그레이션 모드를 시작하고 **username** 명령을 사용하여 CLI 관리자 사용자를 추가할 수 있습니다.

## 웹 기반 관리자 사용자 생성

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

사용자 인터페이스 자체에서 웹 기반 관리자 사용자를 추가할 수 있습니다.



## 설치 후 작업

- Cisco ISE 웹 기반 인터페이스 로그인, 61 페이지
- Cisco ISE 컨피그레이션 확인, 62 페이지
- VMware Tools 설치 확인, 64 페이지
- 관리자 비밀번호 재설정, 65 페이지
- Cisco ISE Appliance의 IP 주소 변경, 67 페이지
- 설치 및 업그레이드 기록 보기, 68 페이지
- SNS-3415 Appliance에 RAID 구성, 69 페이지
- CIMC를 사용하여 SNS-3495 Appliance에 RAID 구성, 70 페이지
- 시스템 지우기 수행, 71 페이지

### Cisco ISE 웹 기반 인터페이스 로그인

Cisco ISE 웹 기반 인터페이스에 처음으로 로그인할 때는 미리 설치된 평가 라이선스를 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 30 분간 활동이 없으면 Cisco ISE 웹 기반 인터페이스가 사용자를 로그아웃하며 전송되지 않은 컨피그레이션 데이터는 저장되지 않습니다.

시작하기 전에

Cisco ISE 관리 포털은 다음 HTTPS 사용 가능 브라우저를 지원합니다.

- Mozilla Firefox 버전 31.x ESR, 36.x, 37.x
- Microsoft Internet Explorer 10.x, 11.x



참고 클라이언트 브라우저를 실행하는 시스템에 Adobe Flash Player 11.1.0.0 이상이 설치되어 있어야 합니다. Cisco ISE GUI를 보려면 화면 해상도가 1280 x 800픽셀 이상이 되어야 합니다.

- 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**을 클릭합니다.

## 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 할 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.

## CLI에서 컨피그레이션 확인

시작하기 전에

최신 Cisco ISE 패치를 가져오고 Cisco ISE를 최신 버전으로 유지하려면 <http://www.cisco.com/public/sw-center/index.shtml>를 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** 를 입력하고 **Enter**를 누릅니다.  
참고 Version 필드에는 현재 설치된 Cisco ISE 소프트웨어 버전이 나열됩니다.  
콘솔에 아래와 같이 출력됩니다.

```
ise-vm123/admin# show application version ise
```

```
Cisco Identity Services Engine
```

```

Version : 1.4.0.205
Build Date : Tue Mar 3 19:31:27 2015
Install Date : Tue Mar 3 21:06:31 2015
```

- 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 3638
Database Server running 45 PROCESSES
```

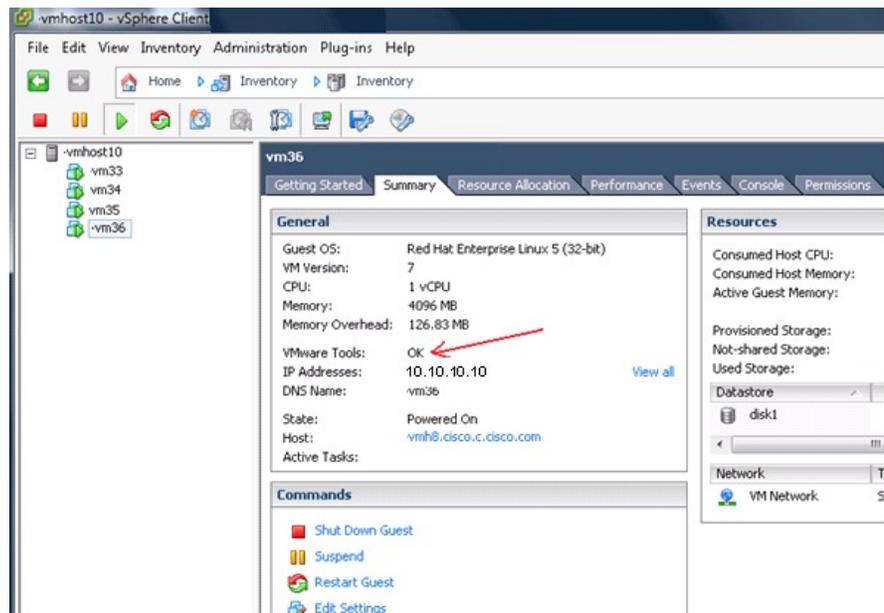
|                                     |          |      |
|-------------------------------------|----------|------|
| Application Server                  | running  | 5992 |
| Profiler Database                   | running  | 4483 |
| AD Connector                        | running  | 6401 |
| M&T Session Database                | running  | 2313 |
| M&T Log Collector                   | running  | 6247 |
| M&T Log Processor                   | running  | 6274 |
| Certificate Authority Service       | running  | 6213 |
| pxGrid Infrastructure Service       | disabled |      |
| pxGrid Publisher Subscriber Service | disabled |      |
| pxGrid Connection Manager           | disabled |      |
| pxGrid Controller                   | disabled |      |
| Identity Mapping Service            | disabled |      |

## VMware Tools 설치 확인

### vSphere Client의 Summary 탭을 사용하여 VMWare Tools 설치 확인

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

그림 10: vSphere Client에서 VMware Tools 확인



300684

## CLI를 사용하여 VMWare Tools 설치 확인

VMware Tools가 설치되었는지 확인하는 데 **show inventory** 명령을 사용할 수도 있습니다. 이 명령은 NIC 드라이버 정보를 나열합니다. VMware Tools가 설치된 가상 머신에서 VMware Virtual Ethernet 드라이버가 Driver Descr 필드에 나열됩니다.

```
vm36/admin# show inventory
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9, VID: V01 , SN: 8JDCBLIDLJA
Total RAM Memory: 4016564 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5504 @ 2.00GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:BA:C7:82
NIC 0: Driver Descr: VMware Virtual Ethernet driver
(*) Hard Disk Count may be Logical.
vm36/admin#
```

## 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.

## 관리자 비밀번호 재설정

### DVD를 사용하여 잊었거나 손상된 비밀번호 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 `exec`으로 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 3415 콘솔에 다음과 같은 메시지가 표시됩니다.  
Welcome to the Cisco Identity Services Engine Installer  
Cisco ISE Version: 1.4.0.205

Available boot options:

```
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk.
```

Enter boot option and press <Enter>.

**단계 3** 어플라이언스와의 KVM 연결을 사용하려면 시스템 프롬프트에서 3을, 로컬 직렬 콘솔 포트 연결을 사용하려면 4를 입력합니다.  
ISO 유틸리티 메뉴가 아래와 같이 표시됩니다.

Cisco ISE System Utilities Menu

Available System Utilities:

```
[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[4] Install Media Check
[q] Exit and reload
```

Enter option and press <Enter>

**단계 4** 관리자 비밀번호를 복구하려면 1을 입력합니다.  
콘솔에 다음과 같이 표시됩니다.

Admin username:

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

Enter number of admin for password recovery:2

Password:

Verify password:

Save change and reboot? [Y/N]:

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

**단계 6** 새 비밀번호를 입력하고 확인합니다.

**단계 7** Y를 입력하여 변경 사항을 저장합니다.

## 관리자 잠금에 따른 비밀번호 재설정

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

다음 지침에 따라 Cisco ISE CLI에서 **application reset-passwd ise** 명령을 사용하여 관리자 사용자 인터페이스 비밀번호를 재설정합니다. 이는 관리자의 CLI 비밀번호에는 영향을 주지 않습니다. 관리자 비밀번호를 성공적으로 재설정하면 인증서가 즉시 활성화되고 시스템 재부팅 없이 로그인할 수 있습니다.

Cisco ISE에서는 **Monitor > Reports > Catalog > Server Instance > Server Instance > Server Administrator Logins** 보고서에 로그 엔트리를 추가하고, 관리자 ID의 비밀번호를 재설정할 때까지 그 관리자 ID의 인증서를 일시 중단합니다.

단계 1 직접 콘솔 CLI에 액세스하고 다음을 입력합니다.

```
application reset-passwd iseadministrator_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 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 어플라이언스 IP 주소를 변경할 때 **no ip address** 명령을 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. 그러면 **Y**를 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 그러면 **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.

```
Positron/admin# Show version history

Install Date: Tue Mar 03 20:25:58 UTC 2015
Application: ise
Version: 1.4.0.205
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
```

## SNS-3415 Appliance에 RAID 구성

SNS-3415 어플라이언스에서 Cisco ISE를 설치하기 전에 수동으로 RAID(Redundant Array of Independent Disks)를 구성해야 합니다.

- 단계 1 Ctrl + Alt + Del를 눌러 어플라이언스를 재부팅합니다.
- 단계 2 Ctrl+M을 눌러 **LSI Software RAID Configuration** 메뉴를 시작합니다.
- 단계 3 **Management** 메뉴에서 **Configure**를 선택합니다.
- 단계 4 **Clear Configuration**을 선택하고 선택 사항을 확인합니다.
- 단계 5 **Easy Configuration**을 선택합니다.  
READY 레이블의 상자가 나타납니다.
- 단계 6 스페이스 바를 눌러 볼륨을 선택합니다.  
레이블이 ONLIN A00-xx로 바뀝니다.
- 단계 7 F10을 눌러 볼륨을 구성하고 스페이스 바를 눌러 어레이를 선택합니다.
- 단계 8 F10을 눌러 어레이를 구성합니다.  
크기(557.8GB) 및 RAID 0을 포함한 볼륨 데이터를 지정하는 상자가 나타납니다.
- 단계 9 화살표 키를 사용하여 **Accept**로 이동하고 **Enter**를 누릅니다.
- 단계 10 Escape 키를 누르고 컨피그레이션을 저장합니다.
- 단계 11 Escape 키를 세 번 눌러 모든 메뉴를 종료합니다.  
어플라이언스를 재부팅하라는 메시지가 나타납니다.

- 단계 12 어플라이언스를 재부팅합니다.
- 단계 13 Cisco ISE를 설치하고 어플라이언스를 재부팅한 다음 F6를 눌러 **Boot Order** 메뉴를 시작합니다.
- 단계 14 **Embedded SCU RAID**를 선택하여 하드 디스크에서 부팅합니다.

## CIMC를 사용하여 SNS-3495 Appliance에 RAID 구성

Cisco ISE를 설치하기 전에 CIMC를 사용하여 RAID(Redundant Array of Independent Disk)를 구성해야 합니다.

시작하기 전에

SNS-3495 Appliance에서 RAID를 구성하려면 먼저 CIMC를 구성해야 합니다. 참조: [Cisco Integrated Management Controller 구성, 21 페이지](#)

- 단계 1 CIMC 사용자 인터페이스에서 **Server > BIOS > Configure BIOS Parameter**를 선택합니다.
- 단계 2 **Advanced** 탭을 클릭합니다. **Onboard Storage** 영역에서 **Onboard SCU Storage Support** 옵션을 **Enabled**로 설정합니다.
- 단계 3 **Save Changes**를 클릭합니다. 다음 메시지가 나타납니다.  
Reboot Host Immediately option is not selected. BIOS settings will be applied only on next host reboot. Continue?
- 단계 4 **Yes**를 클릭합니다.
- 단계 5 **Server > Summary > Power Cycle Server**를 선택합니다.
- 단계 6 **OK**를 클릭합니다.
- 단계 7 **Server > Summary > Launch KVM Console**을 선택합니다.  
KVM(kernel-based virtual machine) 콘솔 화면이 나타납니다.

- 단계 8 **Server > Summary > Power Cycle Server**를 선택합니다.
- 단계 9 부팅 중에 Ctrl+H를 눌러 WebBIOS에 액세스합니다.
- 단계 10 KVM WebBIOS에서 **Start**를 클릭합니다.
- 단계 11 **BIOS Config Utility Physical Configuration** 창에서 **Configuration Wizard**를 클릭합니다.
- 단계 12 **Add Configuration**을 클릭하고 **Next**를 클릭합니다.
- 단계 13 **Automatic Configuration**을 클릭합니다.
- 단계 14 **Redundancy** 드롭다운 목록에서 **Redundancy When Possible** 옵션을 선택하고 **Next**를 클릭합니다.
- 단계 15 **Yes**를 클릭하여 컨피그레이션을 저장합니다.
- 단계 16 **Yes**를 클릭하여 새 가상 드라이브를 초기화합니다.
- 단계 17 **Set Boot Drive**를 클릭하고 **Go**를 클릭합니다.
- 단계 18 **Home**을 클릭합니다.
- 단계 19 **Exit**를 클릭합니다.
- 단계 20 **Yes**를 클릭합니다.
- 단계 21 서버를 재부팅합니다.
- 단계 22 **Inventory > Storage > Virtual Drive Info**를 선택합니다. 새로 추가된 가상 드라이브가 Virtual Drive info 탭에 나열되는지 확인합니다.

## 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 **exec**으로 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 3415 콘솔에 다음과 같은 메시지가 표시됩니다.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 1.4.0.205
```

Available boot options:

```
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk.
```

Enter boot option and press <Enter>.

**단계 3** 어플라이언스와의 KVM 연결을 사용하려면 시스템 프롬프트에서 3을, 로컬 직렬 콘솔 포트 연결을 사용하려면 4를 입력합니다.

ISO 유틸리티 메뉴가 아래와 같이 표시됩니다.

```
Cisco ISE System Utilities Menu
```

Available System Utilities:

```
[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[4] Install Media Check
[q] Exit and reload
```

Enter option and press <Enter>

**단계 4** 3을 입력하여 시스템 지우기를 수행합니다. 콘솔에 다음과 같이 표시됩니다.

```
***** W A R N I N G *****
```

```
YOU ARE ABOUT TO PERFORM A SYSTEM ERASE. THIS ACTION WILL DELETE ALL
CONTENT OF THE HARD DISK BY WRITING A SEQUENCE OF RANDOM BYTES, FOLLOWED
BY ZEROS DIRECTLY TO THE HARD DISK DEVICE.
```

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

**단계 5** Y를 입력합니다. 콘솔에서 또 다른 경고를 표시합니다.

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

**단계 6** Y를 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.







## Cisco SNS-3400 Series 서버 사양

- 제품 외장 사양, 75 페이지
- 환경 사양, 75 페이지
- 전원 사양, 76 페이지

### 제품 외장 사양

표 15: Cisco SNS-3400 Series 서버 물리적 사양

| 설명          | 사양              |
|-------------|-----------------|
| 높이          | 1.7인치(4.3cm)    |
| 너비          | 16.9인치(42.9cm)  |
| 깊이          | 28.5인치(72.4cm)  |
| 무게(풀 로드 채시) | 35.6파운드(16.1Kg) |

### 환경 사양

표 16: Cisco SNS-3400 Series 서버 환경 사양

| 설명     | 사양                                               |
|--------|--------------------------------------------------|
| 온도: 작동 | 5 - 40°C (41 - 104°F)(해발 고도 305m당 1°C씩 최대 온도 감소) |

| 설명                                                   | 사양                      |
|------------------------------------------------------|-------------------------|
| 온도: 비작동                                              | -40 ~ 149°F(-40 ~ 65°C) |
| 습도(RH): 비응축                                          | 10 to 90 percent        |
| 고도: 작동                                               | 0 - 10,000피트            |
| 고도: 비작동                                              | 0 - 40,000피트            |
| 음향 출력 A 가중 측정, ISO7779 LwAd(Bels)<br>23°C(73°F) 작동 시 | 5.4                     |
| 음향 출력 A 가중 측정, ISO7779 LpAm(dBA)<br>23°C(73°F) 작동 시  | 37                      |

## 전원 사양

### 450와트 전원 공급 장치



참고

Cisco UCS 전력 계산기를 사용하여 정확한 서버 컨피그레이션에 대한 구체적인 전력 정보를 얻을 수 있습니다.



참고

서버에서 여러 전원 공급 장치 유형을 혼합하지 마십시오. 두 전원 공급 장치 모두 450W여야 합니다.

표 17: Cisco SNS-3400 Series 서버 450와트 전원 공급 장치 사양

| 설명                 | 사양                                        |
|--------------------|-------------------------------------------|
| AC 입력 전압 범위        | 저범위: 100VAC에서 120VAC 고범위: 200VAC에서 240VAC |
| AC 입력 주파수          | 범위: 47Hz에서 63Hz(단상, 50Hz에서 60Hz 공칭)       |
| AC 라인 입력 전류(정상 상태) | 6.0A 피크(100VAC) 3.0A 피크(208VAC)           |
| 전원 공급 장치별 최대 출력    | 450와트                                     |

| 설명             | 사양                          |
|----------------|-----------------------------|
| 전원 공급 장치 출력 전압 | 주 전력: 12VDC<br>대기 전력: 12VDC |

## 650와트 전원 공급 장치



참고 [Cisco UCS 전력 계산기](#)를 사용하여 정확한 서버 컨피그레이션에 대한 구체적인 전력 정보를 얻을 수 있습니다.



참고 서버에서 여러 전원 공급 장치 유형을 혼합하지 마십시오. 두 전원 공급 장치 모두 650W여야 합니다.

표 18: Cisco SNS-3400 Series 서버 650와트 전원 공급 장치 사양

| 설명                 | 사양                                        |
|--------------------|-------------------------------------------|
| AC 입력 전압 범위        | 90VAC에서 264VAC(자체 범위, 180VAC에서 264VAC 공칭) |
| AC 입력 주파수          | 범위: 47Hz에서 63Hz(단상, 50Hz에서 60Hz 공칭)       |
| AC 라인 입력 전류(정상 상태) | 7.6 A 피크(100VAC) 3.65 A 피크(208VAC)        |
| 전원 공급 장치별 최대 출력    | 650와트                                     |
| 전원 공급 장치 출력 전압     | 주 전력: 12VDC<br>대기 전력: 12VDC               |





## Cisco SNS-3400 Series Appliance 포트 참조

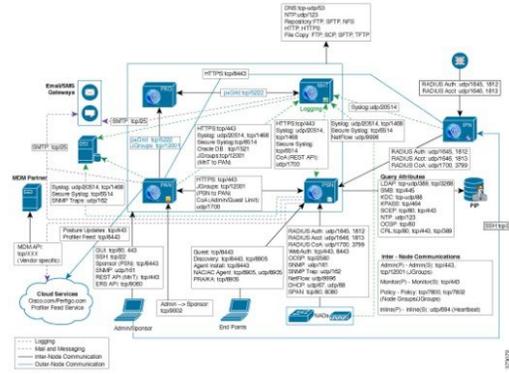
- Cisco ISE 인프라, 79 페이지
- Cisco ISE 관리 노드 포트, 81 페이지
- Cisco ISE 모니터링 노드 포트, 82 페이지
- Cisco ISE 정책 서비스 노드 포트, 84 페이지
- 인라인 포스처 노드 포트, 87 페이지
- Cisco ISE pxGrid Service 포트, 89 페이지
- OCSP 및 CRL 서비스 포트, 89 페이지

### 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.

- Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다.
- RADIUS는 모든 NIC(Network Interface Card)에서 수신합니다.
- 모든 NIC는 IP 주소로 구성할 수 있습니다.



# Cisco ISE 관리 노드 포트

| Cisco ISE Service | 기가비트 이더넷 0의 포트                                                                                                                                                                                                                                                                                                                                                          | 기가비트 이더넷 1의 포트                                                                                                                                                                                                                                                                               | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|
| 관리                | <ul style="list-style-type: none"> <li>• HTTP: TCP/80, HTTPS: TCP/443(TCP/80이 TCP/443으로 리디렉션, 구성 불가)</li> <li>• SSH 서버: TCP/22</li> <li>• 외부 RESTful 서비스 (ERS) REST API: TCP/9060</li> <li>• TCP:9002(관리 GUI에서 스폰서 포털을 표시하기 위해)</li> </ul> <p>참고 인라인 포스트처드가 관리 페르소나를 지원하지 않으므로 포트 80 및 443에 액세스할 수 없습니다.</p> <p>참고 포트 80 및 443은 관리 웹 애플리케이션을 지원하며 기본적으로 활성화되어 있습니다.</p> | <p>Cisco ISE에서 외부 인증 저장소에 보내는 아웃바운드 트래픽(관리 사용자 인터페이스 인증):</p> <ul style="list-style-type: none"> <li>• LDAP: TCP/389, 3268, UDP/389</li> <li>• SMB: TCP/445</li> <li>• KDC: TCP/88, UDP/88</li> <li>• KPASS: TCP/464</li> </ul> <p>참고 Cisco ISE에 대한 HTTPS 및 SSH 액세스는 기가비트 이더넷 0으로 제한됩니다.</p> |                |                |
| 복제 및 동기화          | <ul style="list-style-type: none"> <li>• HTTPS(SOAP): TCP/443</li> <li>• 데이터 동기화/복제 (JGroups): TCP/12001(글로벌)</li> </ul>                                                                                                                                                                                                                                                | —                                                                                                                                                                                                                                                                                            | —              | —              |
| 모니터링              | <p>SNMP 쿼리: UDP/161</p> <p>참고 이 포트는 라우트 테이블에 따라 달라집니다.</p>                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                              |                |                |

| Cisco ISE Service     | 기가비트 이더넷 0의 포트                                                                                                                                                                                                                                                                                                                                                                          | 기가비트 이더넷 1의 포트 | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|----------------|
| 로깅(아웃바운드)             | <ul style="list-style-type: none"> <li>• Syslog: UDP/20514, TCP/1468</li> <li>• Secure Syslog: TCP/6514</li> </ul> <p>참고 기본 포트는 외부 로깅을 위해 구성 가능합니다.</p> <ul style="list-style-type: none"> <li>• SNMP 트랩: UDP/162</li> </ul>                                                                                                                                                            |                |                |                |
| 외부 ID 소스 및 리소스(아웃바운드) | <ul style="list-style-type: none"> <li>• 관리자 사용자 인터페이스 및 엔드포인트 인증 <ul style="list-style-type: none"> <li>◦ LDAP: TCP/389, 3268, UDP/389</li> <li>◦ SMB: TCP/445</li> <li>◦ KDC: TCP/88, UDP/88</li> <li>◦ KPASS: TCP/464</li> </ul> </li> <li>• NTP: UDP/123</li> <li>• DNS: UDP/53, TCP/53</li> </ul> <p>참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.</p> |                |                |                |
| 게스트                   | 게스트 계정 만료 이메일 알림: SMTP: TCP/25                                                                                                                                                                                                                                                                                                                                                          |                |                |                |

## Cisco ISE 모니터링 노드 포트

| Cisco ISE Service | 기가비트 이더넷 0의 포트                                                                                             | 기가비트 이더넷 1의 포트 | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트 |
|-------------------|------------------------------------------------------------------------------------------------------------|----------------|----------------|----------------|
| 관리                | <ul style="list-style-type: none"> <li>• HTTP: TCP/80, HTTPS: TCP/443</li> <li>• SSH 서버: TCP/22</li> </ul> | —              | —              | —              |

| Cisco ISE Service     | 기가비트 이더넷 0<br>의 포트                                                                                                                                                                                                                                                                                                                                                                             | 기가비트 이더넷 1<br>의 포트           | 기가비트 이더넷 2<br>의 포트           | 기가비트 이더넷 3<br>의 포트           |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------------------|------------------------------|
| 복제 및 동기화              | <ul style="list-style-type: none"> <li>• HTTPS(SOAP): TCP/443</li> <li>• Oracle DB Listener: TCP/1521</li> <li>• 데이터 동기화/복제 (JGroups): TCP/12001(글로벌)</li> </ul>                                                                                                                                                                                                                               | Oracle DB Listener: TCP/1521 | Oracle DB Listener: TCP/1521 | Oracle DB Listener: TCP/1521 |
| 모니터링                  | SNMP(Simple Network Management Protocol): UDP/161<br>참고 이 포트는 라우트 테이블에 따라 달라집니다.                                                                                                                                                                                                                                                                                                               |                              |                              |                              |
| 로깅                    | <ul style="list-style-type: none"> <li>• Syslog: UDP/20514, TCP/1468</li> <li>• Secure Syslog: TCP/6514</li> </ul> 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. <ul style="list-style-type: none"> <li>• SMTP: TCP/25</li> <li>• SNMP 트랩: UDP/162</li> </ul>                                                                                                                                                  |                              |                              |                              |
| 외부 ID 소스 및 리소스(아웃바운드) | <ul style="list-style-type: none"> <li>• 관리자 사용자 인터페이스 및 엔드포인트 인증               <ul style="list-style-type: none"> <li>◦ LDAP: TCP/389, 3268, UDP/389</li> <li>◦ SMB: TCP/445</li> <li>◦ KDC: TCP/88, UDP/88</li> <li>◦ KPASS: TCP/464</li> </ul> </li> <li>• NTP: UDP/123</li> <li>• DNS: UDP/53, TCP/53</li> </ul> 참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다. |                              |                              |                              |

## Cisco ISE 정책 서비스 노드 포트

| Cisco ISE Service | 기가비트 이더넷 0의 포트                                                                                                                                                                                                        | 기가비트 이더넷 1의 포트                    | 기가비트 이더넷 2의 포트                    | 기가비트 이더넷 3의 포트                    |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| 관리                | <ul style="list-style-type: none"> <li>• HTTP: TCP/80, HTTPS: TCP/443</li> <li>• SSH 서버: TCP/22</li> <li>• OCSP: TCP/2560</li> </ul>                                                                                  | Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다. | Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다. | Cisco ISE 관리는 기가비트 이더넷 0으로 제한됩니다. |
| 복제 및 동기화          | <ul style="list-style-type: none"> <li>• HTTPS(SOAP): TCP/443</li> <li>• 데이터 동기화/복제(JGroups): TCP/12001(글로벌)</li> </ul>                                                                                               | —                                 | —                                 | —                                 |
| 클러스터링(노드 그룹)      | <ul style="list-style-type: none"> <li>• 노드 그룹/JGroups: TCP/7800</li> <li>• 노드 장애 감지: TCP/7802</li> </ul>                                                                                                             | —                                 | —                                 | —                                 |
| 모니터링              | SNMP(Simple Network Management Protocol): UDP/161<br>참고 이 포트는 라우트 테이블에 따라 달라집니다.                                                                                                                                      |                                   |                                   |                                   |
| 로깅(아웃바운드)         | <ul style="list-style-type: none"> <li>• Syslog: UDP/20514, TCP/1468</li> <li>• Secure Syslog: TCP/6514</li> </ul> 참고 기본 포트는 외부 로깅을 위해 구성 가능합니다. <ul style="list-style-type: none"> <li>• SNMP 트랩: UDP/162</li> </ul> |                                   |                                   |                                   |

| Cisco ISE Service                                                                                                                                                 | 기가비트 이더넷 0의 포트                                                                                                                                                                                                                                                                                                                                                         | 기가비트 이더넷 1의 포트 | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|----------------|
| 세션                                                                                                                                                                | <ul style="list-style-type: none"> <li>• RADIUS 인증: UDP/1645, 1812</li> <li>• RADIUS 계정 관리: UDP/1646, 1813</li> <li>• RADIUS CoA(Change of Authorization) Send: UDP/1700</li> <li>• RADIUS CoA(Change of Authorization) Listen/Relay: UDP/1700, 3799</li> </ul> <p>참고 UDP 포트 3799는 구성 불가능합니다.</p>                                                                      |                |                |                |
| 외부 ID 소스 및 리소스(아웃바운드)                                                                                                                                             | <ul style="list-style-type: none"> <li>• 관리자 사용자 인터페이스 및 엔드포인트 인증 <ul style="list-style-type: none"> <li>◦ LDAP: TCP/389, 3268</li> <li>◦ SMB: TCP/445</li> <li>◦ KDC: TCP/88</li> <li>◦ KPASS: TCP/464</li> </ul> </li> <li>• NTP: UDP/123</li> <li>• DNS: UDP/53, TCP/53</li> </ul> <p>참고 기가비트 이더넷 0이 아닌 인터페이스를 통해서만 접근 가능한 외부 ID 소스 및 서비스의 경우 고정 경로를 알맞게 구성합니다.</p> |                |                |                |
| <p>웹 포털서비스</p> <ul style="list-style-type: none"> <li>- 게스트/웹 인증</li> <li>- 게스트 스폰서 포털</li> <li>- 내 디바이스 포털</li> <li>- 클라이언트 프로비저닝</li> <li>- 블랙리스트 포털</li> </ul> | <p>HTTPS(Cisco ISE 서비스를 위해 인터페이스가 활성화되어야 함)</p> <ul style="list-style-type: none"> <li>• 블랙리스트 포털: TCP/8000-8999(기본 포트는 TCP/8444)</li> <li>• 게스트 포털 및 클라이언트 프로비저닝: TCP/8000-8999(기본 포트는 TCP/8443)</li> <li>• 내 디바이스 포털: TCP/8000-8999(기본 포트는 TCP/8443)</li> <li>• 스폰서 포털: TCP/8000-8999(기본 포트는 TCP/8443)</li> <li>• SMTP 알림: TCP/25</li> </ul>                         |                |                |                |

| Cisco ISE Service                                                                        | 기가비트 이더넷 0의 포트 | 기가비트 이더넷 1의 포트 | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------|----------------|----------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 포스처<br>- 검색<br>- 프로비저닝<br>- 평가/하트비트                                                      |                |                |                | <ul style="list-style-type: none"> <li>• 검색(클라이언트): TCP/80(HTTP), TCP/8905(HTTPS)<br/>참고   기본적으로 TCP/80은 TCP/8443으로 리디렉션됩니다. 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• 검색(정책 서비스 노드): TCP/8443, 8905(HTTPS)</li> <li>• 프로비저닝 - URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• 프로비저닝 - Active-X 및 Java Applet 설치(IP 새로 고침, 웹 에이전트 설치, NAC Agent 설치 시작 포함). 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• 프로비저닝 - NAC Agent 설치: TCP/8443</li> <li>• 프로비저닝 - NAC Agent 업데이트 알림: UDP/8905(SWISS)</li> <li>• 프로비저닝 - NAC Agent 및 기타 패키지/모듈 업데이트: TCP/8905(HTTPS)</li> <li>• 평가 - 포스처 협상 및 에이전트 보고서: TCP/8905(HTTPS)</li> <li>• 평가 - PRA/Keep-alive: UDP/8905(SWISS)</li> </ul> |
| BYOD(Bring Your Own Device)/NSP(Network Service Protocol)<br>- 리디렉션<br>- 프로비저닝<br>- SCEP |                |                |                | <ul style="list-style-type: none"> <li>• 프로비저닝 - URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• 프로비저닝 - Active-X 및 Java Applet 설치(마법사 설치 시작 포함): 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• 프로비저닝 - Cisco ISE에서 마법사 설치(Windows, Mac OS): TCP/8443</li> <li>• 프로비저닝 - Google Play에서 마법사 설치(Android): TCP/443</li> <li>• 프로비저닝 - 신청자 프로비저닝 프로세스: TCP/8905</li> <li>• SCEP 프록시-CA: TCP/80 또는 TCP/443(SCEP RA URL 컨피그레이션 기반)</li> </ul>                                                                                                                                                                                                                                       |
| MDM(Mobile Device Management) API 통합                                                     |                |                |                | <ul style="list-style-type: none"> <li>• URL 리디렉션: 웹 포털 서비스: 게스트 포털 및 클라이언트 프로비저닝 참조</li> <li>• API: 벤더별</li> <li>• 에이전트 설치 및 디바이스 등록: 벤더별</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Cisco ISE Service | 기가비트 이더넷 0의 포트                                                                                                                                                                                                                                                                                                                                                                             | 기가비트 이더넷 1의 포트 | 기가비트 이더넷 2의 포트 | 기가비트 이더넷 3의 포트 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|----------------|----------------|
| 프로파일링             | <ul style="list-style-type: none"> <li>• NetFlow: UDP/9996<br/>참고 이 포트는 구성 가능합니다.</li> <li>• DHCP: UDP/67<br/>참고 이 포트는 구성 가능합니다.</li> <li>• DHCP SPAN Probe: UDP/68</li> <li>• HTTP: TCP/80, 8080</li> <li>• DNS: UDP/53(lookup)<br/>참고 이 포트는 라우트 테이블에 따라 달라집니다.</li> <li>• SNMP 쿼리: UDP/161<br/>참고 이 포트는 라우트 테이블에 따라 달라집니다.</li> <li>• SNMP 트랩: UDP/162<br/>참고 이 포트는 구성 가능합니다.</li> </ul> |                |                |                |

## 인라인 포스처 노드 포트



참고 인라인 포스처 노드가 관리 페르소나를 지원하지 않으므로 포트 TCP 80 및 443에 액세스할 수 없습니다. 인라인 포스처 노드 고가용성은 다른 어떤 Cisco ISE 노드 유형에도 적용되지 않습니다.

| Cisco ISE Service | 기가비트 이더넷 0<br>의 포트                                                                                                                                                                                                                                                                                    | 기가비트 이더넷 1<br>의 포트                                                                                                                                                                                                        | 기가비트 이더넷 2<br>의 포트 | 기가비트 이더넷 3<br>의 포트 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------|
| 관리                | <ul style="list-style-type: none"> <li>• HTTPS:<br/>TCP/8443</li> <li>참고 TCP:<br/>8443<br/>은 관<br/>리 노<br/>드에<br/>서 사<br/>용 합<br/>니다.</li> <li>• SSH 서버:<br/>TCP/22</li> </ul>                                                                                                                        | —                                                                                                                                                                                                                         | —                  | —                  |
| 인라인 포스처           | <ul style="list-style-type: none"> <li>• RADIUS 인증<br/>프록시:<br/>UDP/1645,<br/>1812</li> <li>• RADIUS 계정<br/>관리 프록시:<br/>UDP/1646,<br/>1813</li> <li>• RADIUS<br/>CoA:<br/>UDP/1700,<br/>3799</li> <li>참고 UDP<br/>포트<br/>3799<br/>는 구<br/>성 불<br/>가 합<br/>니다.</li> <li>• 리디렉션:<br/>TCP/9090</li> </ul> | <ul style="list-style-type: none"> <li>• RADIUS 인증<br/>프록시:<br/>UDP/1645,<br/>1812</li> <li>• RADIUS 계정<br/>관리 프록시:<br/>UDP/1646,<br/>1813</li> <li>• RADIUS<br/>CoA: 해당 없<br/>음</li> <li>• 리디렉션:<br/>TCP/9090</li> </ul> | —                  | —                  |
| 로깅(아웃바운드)         | Syslog: UDP/20154<br>참고 이 포트는<br>구성 가능<br>합니다.                                                                                                                                                                                                                                                        | Syslog: UDP/20154<br>참고 이 포트는<br>구성 가능<br>합니다.                                                                                                                                                                            | —                  | —                  |

| Cisco ISE Service | 기가비트 이더넷 0<br>의 포트 | 기가비트 이더넷 1<br>의 포트 | 기가비트 이더넷 2<br>의 포트         | 기가비트 이더넷 3<br>의 포트 |
|-------------------|--------------------|--------------------|----------------------------|--------------------|
| 고가용성              | —                  | —                  | 하트비트:<br>UDP/694(하트비<br>트) | 하트비트:UDP/694       |

## Cisco ISE pxGrid Service 포트

| Cisco ISE Service | 기가비트 이더넷 0<br>의 포트                                                                                                              | 기가비트 이더넷 1<br>의 포트 | 기가비트 이더넷 2<br>의 포트 | 기가비트 이더넷 3<br>의 포트 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------|--------------------|
| 관리                | <ul style="list-style-type: none"> <li>• SSL:<br/>TCP/5222(노<br/>드 간 통신)</li> <li>• SSL:<br/>TCP/7400(노<br/>드 그룹 통신)</li> </ul> | —                  | —                  | —                  |
| 복제 및 동기화          | 데이터 동기화/복<br>제(JGroups):<br>TCP/12001(글로벌)                                                                                      | —                  | —                  | —                  |

## 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 노드, 모니터링 노드, 인라인 포스처 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.





색 인

## A

고정 IP, 설정 [22](#)

## D

DHCP, 활성화 [22](#)

## G

사양 [75, 76](#)

물리적 [75](#)

전원 [76](#)

환경 [75](#)

설치 [21, 22, 29](#)

IP 설정 [22](#)

NIC 모드 [21](#)

NIC 이중화 [22](#)

확인 [29](#)

설치 후 작업 [61](#)

## H

업그레이드 [61](#)

설치 후 작업 [61](#)

## I

전원 [76](#)

사양 [76](#)

절차 [43](#)

제품 외장 사양 [75](#)

## V

VMWare [31, 33, 43, 45](#)

Cisco ISE Appliance 설치 [45](#)

구성 [43](#)

설치 [31](#)

하드웨어 요구 사항 [33](#)

## W

환경 사양 [75](#)

