Cisco ISE 네트워크 구축

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

Cisco ISE 네트워크 아키텍처

Cisco ISE 아키텍처는 다음 구성 요소를 포함합니다.

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

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

Cisco ISE 구축 용어

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

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

분산 구축의 노드 유형 및 페르소나

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

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

관리 노드

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

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

정책 서비스 노드

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

분산 설정에서 하나 이상의 노드가 정책 서비스 페르소나를 맡아야 합니다.

모니터링 노드

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

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

pxGrid 노드

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

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

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

독립형 및 분산 ISE 구축

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

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

분산 구축 시나리오

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

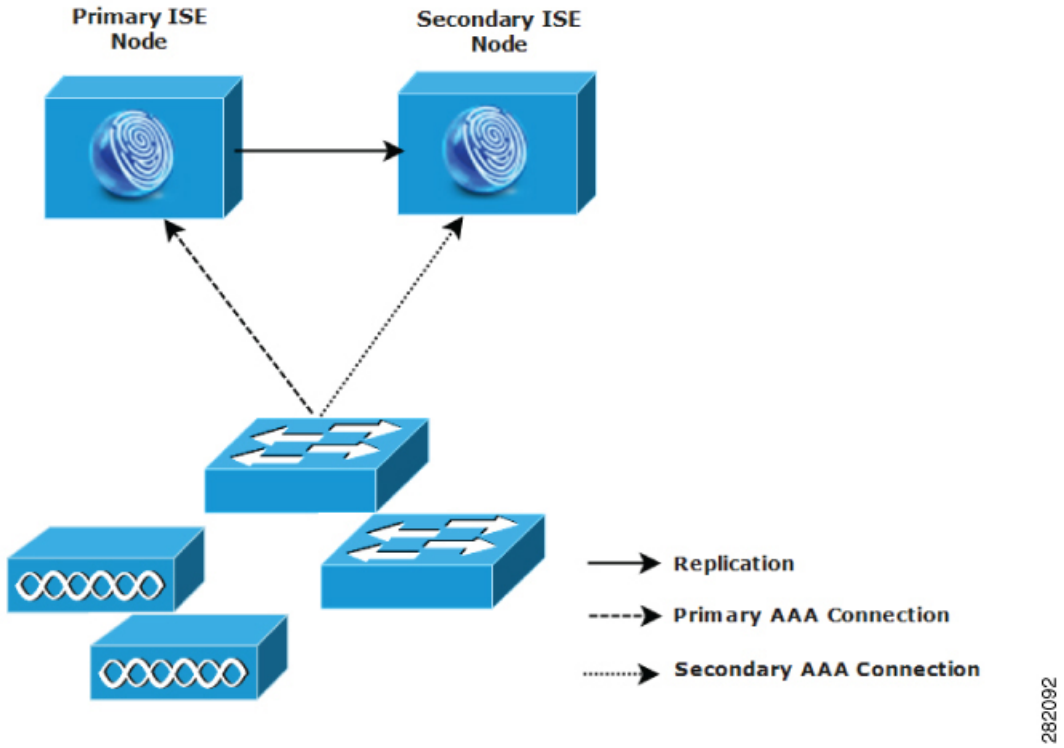
소형 네트워크 구축

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

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

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

그림 *1:* 소형 네트워크 구축



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

분할 구축

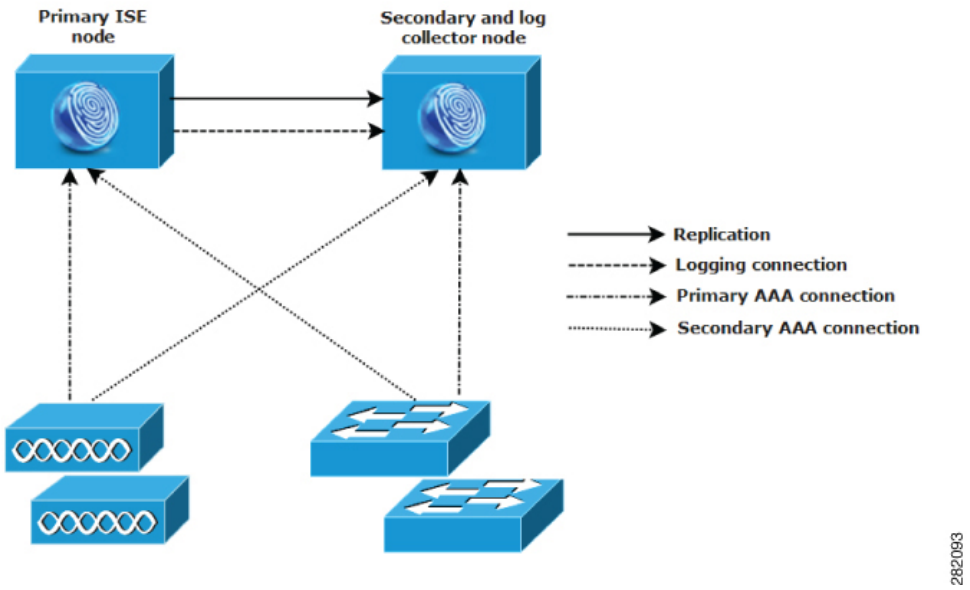
분할 Cisco ISE 구축에서는 소형 Cisco ISE 구축에서 설명한 기본 노드와 보조 노드를 계속 유지합니다. 그러나 AAA 워크플로 최적화를 위해 두 Cisco ISE 노드 간에 AAA 로드가 분할됩니다. 각 Cisco ISE 어플라이언스(기본 또는 보조)는 AAA 연결에 문제가 생길 경우 전체 워크로드를 처리할 수 있어야 합니다. 정상적인 네트워크 운영 상태에서는 기본 노드와 보조 노드 모두 모든 AAA 요청을 처리하지는 않습니다. 이 워크로드가 두 노드에 분산되어 있기 때문입니다.

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

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

또한 분할 Cisco ISE 구축 설계는 확장을 허용하기 때문에 유리합니다.

그림 2: 분할 네트워크 구축



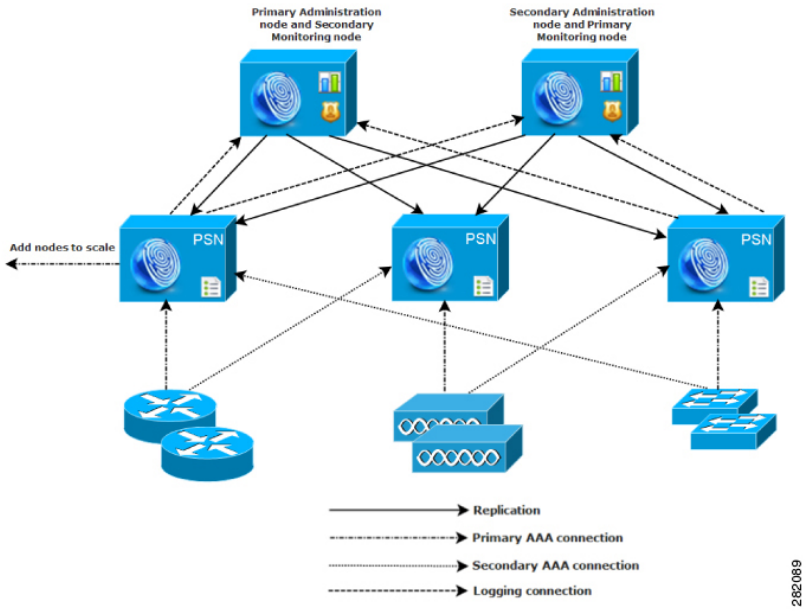
중형 네트워크 구축

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

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

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

그림 *3:* 중형 네트워크 구축



대형 네트워크 구축

중앙 집중식 로깅

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

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

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

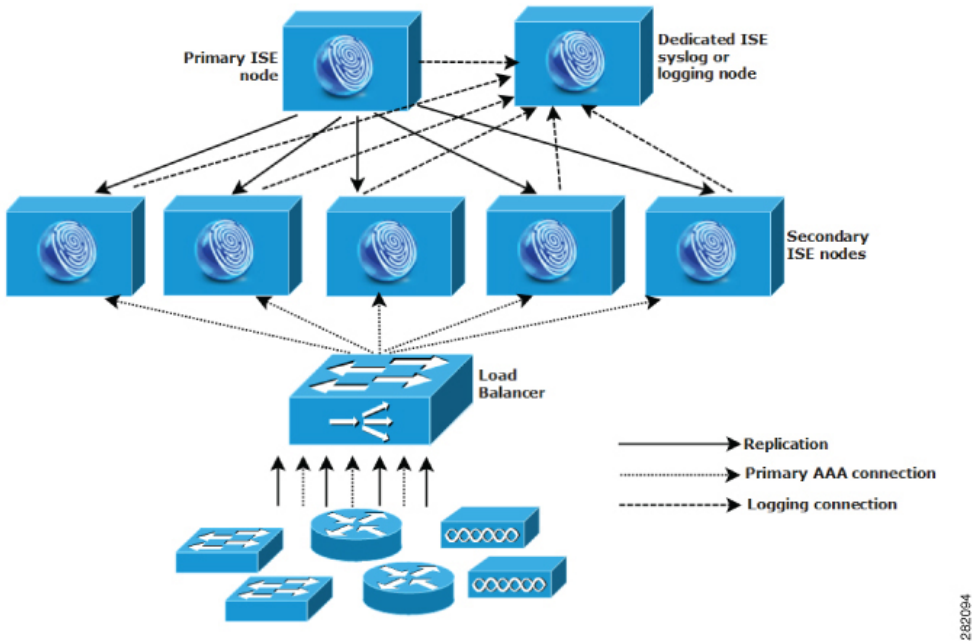
로드 밸런서

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

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

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

그림 *4:* 대규모 네트워크 구축

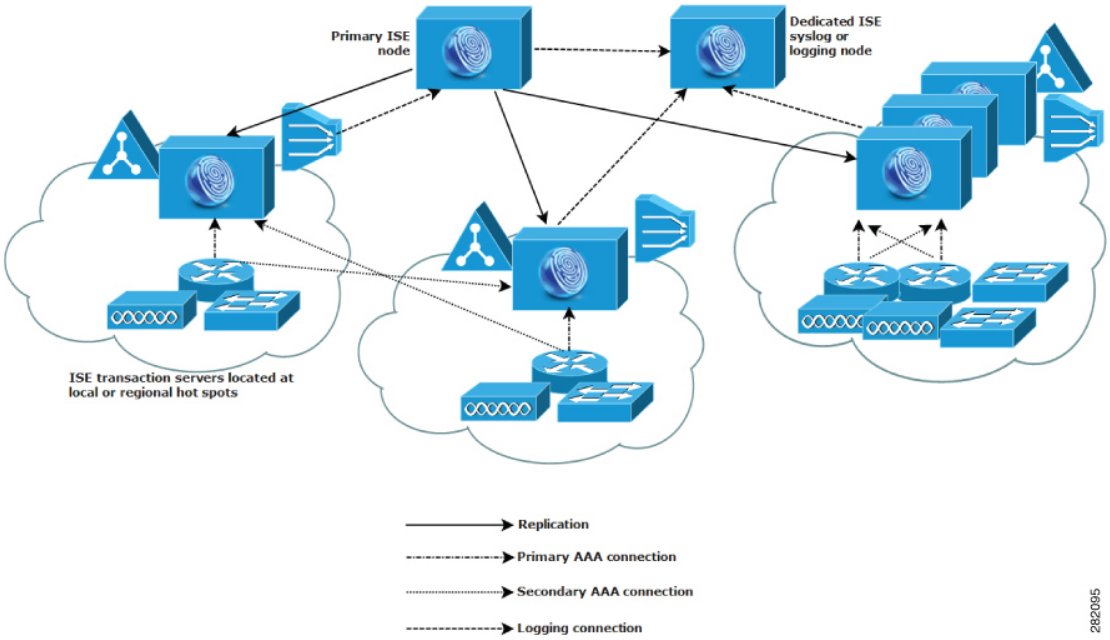


분산 네트워크 구축

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

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

그림 5: 분산 구축



여러 원격 사이트가 있는 네트워크 계획 시 고려 사항

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

각 구축 모델에 지원되는 최대 세션 수

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

표 *1:* 구축 모델별로 지원되는 최대 세션 수

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

표 *2: PSN*당 최대 활성 세션 수

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

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

[1] 전용 정책 노드별 확장(총 구축 크기로 제어하는 최대 세션)

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

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

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

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

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

ISE 커뮤니티 리소스

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