PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 ISE-PIC

모니터링 및 문제 해결 서비스는 모든 Cisco ISE-PIC 런타임 서비스에 사용할 수 있는 포괄적인 ID 솔루션으로, 다음과 같은 구성 요소를 사용합니다.

- 모니터링 - 네트워크에 대한 액세스 활동의 상태를 나타내는 의미 있는 데이터를 실시간으로 표시합니다. 이 정보는 쉽게 해석할 수 있으며 작동 조건에 영향을 미칠 수 있습니다.
- 문제 해결 - 네트워크의 액세스 문제를 해결하기 위한 상황별 지침을 제공합니다. 그러면 관리자는 사용자의 문제를 해결하고 시기 적절하게 해결 방법을 제공할 수 있습니다.
- 보고 - 관리자가 트렌드를 분석하고 시스템 성능 및 네트워크 활동을 모니터링하는 데 사용할 수 있는 표준 보고서 카탈로그를 제공합니다. 다양한 방법으로 보고서를 맞춤화하고 나중에 사용하기 위해 저장할 수 있습니다. Identity(ID), Endpoint ID(엔드포인트 ID) 및 ISE Node(ISE 노드) 필드 관련 와일드카드와 여러 값을 사용하여 레코드를 검색할 수 있습니다.

이 섹션에서는 모니터링, 문제 해결 및 보고 도구를 사용하여 ISE-PIC를 관리하는 방법을 확인할 수 있습니다.

Live Sessions(라이브 세션)

다음 표에서는 라이브 세션을 표시하는, **Live Sessions(**라이브 세션**)** 창의 필드를 설명합니다. 메인 메뉴 막대에서 **Live Sessions(**라이브 세션**)**를 선택합니다.

표 *1:* 라이브 세션

필드 이름	설명
Initiated(시작됨**)**	세션이 시작된 타임스탬프를 표시합니다.
업데이트됨	변경으로 인해 세션이 마지막으로 업데이트된 타임스탬프를 표시합니다.
Account Session Time(계정 세션 시간**)**	사용자 세션의 시간 범위를 초 단위로 표시합니다.
Session Status(세션 상태**)**	엔드포인트 디바이스의 현재 상태를 표시합니다.
조치	Actions(작업) 아이콘을 클릭하여 **Actions(**작업**)** 팝업창을 엽니다. 다음을 수행할 수 있습니다. • 세션 지우기 • 현재 사용자의 세션 상태 확인
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
ID	엔드포인트 디바이스의 사용자 이름을 표시합니다.
IP 주소	엔드포인트 디바이스의 IP 주소를 표시합니다.
서버	로그가 생성된 PIC 노드를 나타냅니다.
Auth Method(인증 방법**)**	PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Session Source(세션 소스**)**	RADIUS 세션인지 PassiveID 세션인지를 나타냅니다.
User Domain Name(사용자 도메인 이름**)**	사용자의 등록된 DNS 이름을 표시합니다.
User NetBIOS Name(사용자 **NetBIOS** 이름**)**	사용자의 NetBIOS 이름을 표시합니다.

필드 이름	설명
사업자	엔드포인트 이벤트는 다양한 시스템 로그 소스에서 학습됩니다. 이러한 시스템 로그 소스를 제공자라고 합니다. • WMI(Windows Management Instrumentation)—WMI는 운영 체제, 장치, 애플리케이션 및 서비스 관련 관리 정보에 액세스하기 위한 공통 인터페이스와 개체 모델을 제공하는 Windows 서비스입니다. • Agent(에이전트)-클라이언트나 다른 프로그램을 대신하여 클라이언트에서 실행되는 프로그램입니다. • Syslog(시스템 로그)—클라이언트가 메시지를 전송하는 로깅 서버입니다. • REST—터미널 서버를 통해 인증한 클라이언트입니다. 이 시스템 로그 소스에 대한 TS Agent ID(TS 에이전트 ID), Source Port Start(소스 포트 시작), Source Port End(소스 포트 끝), Source First Port(소스 최초 포트) 값이 표시됩니다. • Span—네트워크 정보는 span 프로브를 이용해 검색합니다. • DHCP—DHCP 이벤트입니다. • 엔드포인트 엔드포인트 세션에서 서로 다른 제공자에서 발생한 두 이벤트를 파악하면, 제공자는 라이브 세션 페이지에 쉼표로 구분된 값으로 표시됩니다.
MAC Address(MAC 주소)	클라이언트의 MAC 주소를 표시합니다.
엔드포인트 확인 시간	엔드포인트 프로브가 엔드포인트를 마지막으로 확인한 시간을 표시합니다.
엔드포인트 확인 결과	엔드포인트 프로브의 결과를 표시합니다. 가능한 값은 다음과 같습니다. • 연결 불가 • 사용자 로그아웃 • 활성 사용자

필드 이름	설명
Source Port Start(소스 포트 시작**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 첫 번째 포트 번호를 표시합니다.
Source Port End(소스 포트 종료**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 마지막 포트 번호를 표시합니다.
Source First Port(소스 첫 번째 포트**)**	(값은 REST 제공자에 대해서만 표시됨) TS(Terminal Server) 에이전트가 할당한 첫 번째 포트를 표시합니다. TS(Terminal Server)는 모뎀이나 네트워크 인터페이스 없이도 여러 엔드포인트가 연결될 수 있고 여러 엔드포인트와 LAN 네트워크 간의 연결을 촉진하는 서버 또는 네트워크 장치를 말합니다. 여러 엔드포인트가 같은 IP 주소를 이용하는 것처럼 보이기 때문에 특정 사용자의 IP 주소를 식별하기가 어렵습니다. 따라서 특정 사용자를 식별하기 위해 각 사용자에 포트 범위를 할당하는 TS 에이전트가 서버에 설치됩니다. 이렇게 하면 IP 주소-포트-사용자 매핑을 만들 수 있습니다.
TS 에이전트 **ID**	(값은 REST 제공자에 대해서만 표시됨) 엔드포인트에 설치된 TS(Terminal Server) 에이전트의 고유 ID를 표시합니다.
AD 사용자가 확인한 **ID**	(값은 AD 사용자에 대해서만 표시됨) 일치하는 잠재적 계정을 표시합니다.
AD 사용자가 확인한 **DN**	(값은 AD 사용자에 대해서만 폿시됨) AD 사용자의 Distinguished Name(고유 이름) 을 표시합니다 (예: CN=chris,CN=Users,DC=R1,DC=com).

사용 가능한 보고서

다음 표에는 미리 구성된 보고서가 범주에 따라 그룹화되어 있습니다. 보고서 기능 및 로깅 범주에 대한 설명도 제공됩니다.

보고서 이름	설명	로깅 범주
IDC 보고서		

보고서 이름	설명	로깅 범주
AD Connector 운영	AD Connector 운영 보고서에서는 ISE-PIC 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 관리 관리 등 AD Connector에서 수행된 작업 로그를 제공합니다. 일부 AD 장애가 발생하면 이 보고서의 세부사항을 검토하여 가능한 원인을 식별할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 AD 커넥터를 선택합니다.
관리자 로그인	관리자 로그인 보고서는 모든 GUI 기반 관리자 로그인 이벤트와 성공한 CLI 로그인 이벤트에 대한 정보를 제공합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
컨피그레이션 변경 감사	컨피그레이션 변경 감사 보고서에서는 지정된 기간 내의 컨피그레이션 변경 사항에 대한 세부사항을 제공합니다. 특정 기능 문제를 해결해야 하는 경우 이 보고서를 통해 최근의 컨피그레이션 변경이 문제에 영향을 미쳤는지 확인할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
현재 활성 세션	현재 활성 세션 보고서를 사용하면 지정된 기간 내에 현재 네트워크에 있는 사용자에 대한 세부사항이 포함된 보고서를 내보낼 수 있습니다. 사용자가 네트워크에 액세스하지 않은 경우에는 세션이 인증 또는 종료되었는지 확인하거나 세션에 다른 문제가 있는지 확인할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 로깅 범주인 Accounting(계정 관리) 및 Radius Accounting(Radius 계정 관리)을 선택합니다.

보고서 이름	설명	로깅 범주
상태 요약	상태 요약 보고서에서는 대시보드와 유사한 세부사항을 제공합니다. 그러나 대시보드에는 지난 24시간 동안의 데이터만 표시되지만 이 보고서에서는 더 자세한 기록 데이터를 검토할 수 있습니다. 이 데이터를 평가하여 데이터의 일관된 패턴을 확인할 수 있습니다. 예를 들어 대부분의 직원이 하루 일과를 시작하는 시점에 CPU 사용량이 증가할 것을 예측할 수 있습니다. 이러한 트렌드의 불일치가 발견되는 경우 잠재적 문제를 식별할 수 있습니다. CPU 사용량 표에는 다양한 ISE-PIC 기능의 CPU 사용량 백분율이 나열됩니다. **show cpu usage** CLI 명령의 출력이 이 표에 나와 있으며, 이러한 값을 구축 내 문제와 연결하여 문제 원인을 식별할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 로깅 범주인 Administrative and Operational Audit(관리 및 운영 감사), System Diagnostics(시스템 진단), System Statistics(시스템 통계)를 선택합니다.
운영 감사	운영 감사 보고서에서는 백업 실행, ISE-PIC 노드 등록 또는 애플리케이션 다시 시작 등 작동 변경에 대한 세부사항을 제공합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
PassiveID	Passive ID(패시브 ID) 보고서에서는 도메인 컨트롤러에 대한 WMI 연결의 상태를 모니터링하고 그와 관련된 통계(예: 수신된 알림 개수, 초당 사용자 로그인/로그아웃 수 등)를 수집할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Identity Mapping(ID 매핑)을 선택합니다.

보고서 이름	설명	로깅 범주
pxGrid 관리자 감사	pxGrid 관리자 감사 보고서에서는 클라이언트 등록, 클라이언트 등록 취소, 클라이언트 승인, 항목 생성, 항목 삭제, 게시자-구독자 추가 및 게시자-구독자 삭제 등의 pxGrid 관리 작업에 대한 세부사항을 제공합니다. 각 레코드에는 노드에 대한 작업을 수행한 관리자 이름이 있습니다. 관리자 및 메시지 기준에 따라 pxGrid 관리자 감사 보고서를 필터링할 수 있습니다.	—
시스템 진단	시스템 진단 보고서에서는 ISE-PIC 노드의 상태에 대한 세부사항을 제공합니다. ISE-PIC 노드를 등록할 수 없는 경우 이 보고서를 검토하여 문제를 해결할 수 있습니다. 이 보고서를 사용하려면 먼저 여러 진단 로깅 범주를 활성화해야 합니다. 이러한 로그를 수집하면 ISE-PIC 성능에 부정적 영향을 줄 수 있습니다. 그러므로 이러한 범주는 기본적으로 활성화되어 있지 않으므로 데이터를 수집하는 기간 동안만 활성화해야 합니다. 그렇지 않으면, 30분 후에 자동으로 비활성화됩니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Internal Operations Diagnostics(내부 운영 진단), Distributed Management(분산형 관리), Administrator Authentication and Authorization(관리자 인증 및 권한 부여) 기록 범주를 선택합니다.
사용자 변경 비밀번호 감사	사용자 변경 비밀번호 감사 보고서에서는 직원의 비밀번호 변경에 대한 확인을 표시합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.

Cisco ISE-PIC 알람

알람은 네트워크의 조건에 대해 알리며 알람 dashlet에 표시됩니다. 세 가지 알람 심각도, 즉 중요, 경고 및 정보가 있습니다. 또한 데이터 제거 이벤트와 같은 시스템 활동에 대한 정보도 제공합니다. 시스템 활동에 대한 알림을 어떤 식으로 받으려는지 구성할 수 있습니다. 아니면 경보를 완전히 비활성화할 수도 있습니다. 특정 경보에 대한 임계값도 구성할 수 있습니다.

대부분의 경보에는 일정이 연결되어 있지 않으며 이벤트가 발생한 직후에 경보가 전송됩니다. 특정한 시점에 보존되는 경보 수는 최신 경보를 기준으로 15,000개입니다.

이벤트가 다시 발생하는 경우 약 1시간 동안 동일한 경보가 표시되지 않습니다. 이벤트가 다시 발생하는 기간 동안에는 트리거에 따라 경보가 다시 표시되려면 약 1시간이 소요될 수 있습니다.

다음 표에는 모든 Cisco ISE-PIC 경보, 설명 및 해당 해결 방법이 나와 있습니다.

표 ***2: Cisco ISE-PIC*** 알람

경보 이름	경보 설명	경보 해결 방법
관리 및 운영 관리 감사		
구축 업그레이드 장애	ISE PIC 노드에서 업그레이드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 장애 이유와 정정 작업을 확인해 주십시오.
업그레이드 번들 다운로드 장애	ISE-PIC 노드에서 업그레이드 번들 다운로드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 장애 이유와 정정 작업을 확인해 주십시오.
CRL에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	CRL 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	OCSP 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CRL에서 취소된 인증서를 발견하여 보안 syslog 연결이 다시 연결됨	CRL 확인 결과 syslog 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. syslog 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 syslog 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 syslog 연결이 다시 연결됨	OCSP 확인 결과 syslog 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. syslog 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 syslog 서버에 설치해 주십시오.
관리자 계정 잠금/비활성화	비밀번호 만료 또는 잘못된 로그인 시도로 인해 관리자 계정이 잠기거나 비활성화되었습니다. 자세한 내용은 관리자 비밀번호 정책을 참고해 주십시오.	관리자 비밀번호는 다른 관리자가 GUI 또는 CLI를 사용하여 재설정할 수 있습니다.
ERS에서 더 이상 사용되지 않는 URL을 식별함	ERS에서 더 이상 사용되지 않는 URL을 식별함	요청 URL이 더 이상 사용되지 않으므로 해당 URL을 사용하지 않는 것이 좋습니다.
ERS에서 오래된 URL을 식별함	ERS에서 오래된 URL을 식별함	요청한 URL이 오래되었으므로 최신 URL을 사용하는 것이 좋습니다. 이 URL는 향후 릴리스에서 제거되지 않습니다.
ERS 요청 content-type 헤더가 오래되었습니다.	ERS 요청 content-type 헤더가 오래되었습니다.	요청 content-type 헤더에 나와 있는 요청 리소스 버전이 오래되었습니다. 이는 리소스 스키마가 수정되었음을 의미합니다. 하나 이상의 특성이 추가되었거나 제거되었을 수 있습니다. 오래된 스키마 문제를 해결하기 위해 ERS Engine은 기본값을 사용합니다.
ERS XML 입력에서 XSS 또는 삽입 공격이 의심됨	ERS XML 입력에서 XSS 또는 삽입 공격이 의심됩니다.	xml 입력을 검토하십시오.

경보 이름	경보 설명	경보 해결 방법
백업 실패	Cisco ISE-PIC 백업 작업이 실패했습니다.	Cisco ISE-PIC와 리포지토리 사이의 네트워크 연결을 확인해 주십시오. 다음 사항을 확인해 주십시오. • 리포지토리에 사용되는 자격 증명이 올바릅니다. • 리포지토리에 충분한 디스크 공간이 있습니다. • 리포지토리 사용자에게 쓰기 권한이 있습니다.
CA 서버 작동 중지됨	CA 서버가 작동 중지되었습니다.	CA 서비스가 CA 서버에서 작동되어 실행 중인지 확인해 주십시오.
CA 서버 작동	CA 서버가 작동합니다.	관리자에게 CA 서버가 작동하고 있음을 알리는 알림입니다.
인증서 만료	이 인증서가 곧 만료됩니다. 인증서가 만료되면 ISE-PIC가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE-PIC를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 취소됨	관리자가 내부 CA에 의해 엔드포인트로 발급된 인증서를 취소했습니다.	처음부터 새 인증서로 프로비저닝될 때까지 ISE-PIC 흐름을 진행해 주십시오.
인증서 프로비저닝 초기화 오류	인증서 프로비저닝 초기화에 실패했습니다.	주체에서 동일한 CN(CommonName) 속성 값을 가진 여러 인증서가 발견된 경우 인증서 체인을 작성할 수 없습니다. 시스템의 모든 인증서를 확인하십시오.

경보 이름	경보 설명	경보 해결 방법
인증서 복제 실패	보조 노드에 대한 인증서 복제에 실패했습니다.	보조 노드의 인증서가 유효하지 않거나 다른 영구적인 오류 조건이 있습니다. 보조 노드에 기존의 충돌하는 인증서가 있는지 확인해 주십시오. 충돌하는 인증서가 있는 경우, 보조 노드에서 기존 인증서를 삭제하고 기본 노드에서 새 인증서를 내보내고 인증서를 삭제한 다음 가져와 복제를 다시 시도하도록 해 주십시오.
인증서 복제 일시적 실패	보조 노드에 대한 인증서 복제가 일시적으로 실패했습니다.	네트워크 중단과 같은 일시적 상태로 인해 인증서가 보조 노드로 복제되지 않았습니다. 복제가 성공할 때까지 재시도됩니다.
인증서 만료됨	이 인증서가 만료되었습니다. Cisco ISE-PIC가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다. 노드 간 통신에도 영향을 미칠 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE-PIC를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 요청 전달 실패	인증서 요청 전달에 실패했습니다.	들어오는 인증 요청이 발신자의 특성과 일치하는지 확인해 주십시오.
컨피그레이션 변경됨	Cisco ISE 컨피그레이션이 업데이트되었습니다. 이 경보는 사용자 및 엔드포인트에서 컨피그레이션이 변경된 경우에는 트리거되지 않습니다.	컨피그레이션 변경이 예상되는지 확인해 주십시오.
CRL 검색 실패	서버에서 CRL을 검색할 수 없습니다. 지정된 CRL을 사용할 수 없는 경우에 발생할 수 있습니다.	다운로드 URL이 올바르고 서비스에 사용할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
DNS 확인 실패	노드에서 DNS 확인에 실패했습니다.	명령 **ip name-server** 로 구성한 DNS 서버에 연결할 수 있는지 확인해 주십시오. 'CNAME <노드의 호스트 이름>에 대한 DNS 확인 장애'라는 경보가 나타나면 각 Cisco ISE 노드에 대해 A 레코드와 함께 CNAME RR을 생성해야 합니다.
펌웨어 업데이트 필요	이 호스트에서 펌웨어를 업데이트해야 합니다.	펌웨어 업데이트를 받으려면 Cisco Technical Assistance Center(TAC)에 문의해 주십시오.
불충분한 가상 머신 리소스	이 호스트에서 CPU, RAM, 디스크 공간 또는 IOPS와 같은 VM(Virtual Machine) 리소스가 충분하지 않습니다.	Cisco ISE 하드웨어 설치 설명서에 명시된 VM 호스트에 대한 최소 요구사항을 확인해 주십시오.
NTP 서비스 실패	이 노드에서 NTP 서비스 작동이 중지되었습니다.	이는 NTP 서버와 Cisco ISE-PIC 노드 사이의 시간 차이가 크기 때문에(1,000초 이상) 발생할 수 있습니다. NTP 서버가 적절히 작동 중인지 확인하고 **ntp server** <서버 이름> CLI 명령을 사용하여 NTP 서비스를 재시작하고 시간 격차 문제를 해결해 주십시오.
NTP 동기화 실패	이 노드에 구성된 모든 NTP 서버에 연결할 수 없습니다.	실행 **show ntp** 명령을 실행해 주십시오. Cisco ISE-PIC에서 NTP 서버에 연결할 수 있는지 확인해 주십시오. NTP 인증이 구성된 경우 키 ID와 값이 서버의 값과 일치하는지 확인해 주십시오.
예약된 컨피그레이션 백업 없음	Cisco ISE-PIC 컨피그레이션 백업이 예약되지 않았습니다.	컨피그레이션 백업에 대한 일정을 생성해 주십시오.
작업 DB 제거 실패	작업 데이터베이스에서 오래된 데이터를 제거할 수 없습니다. 이는 M&T 노드가 사용 중인 경우에 발생할 수 있습니다.	데이터 제거 감사 보고서에서 used_space가 threshold_space보다 작은지 확인해 주십시오. CLI를 사용하여 M&T 노드에 로그인하고 제거 작업을 수동으로 수행해 주십시오.

경보 이름	경보 설명	경보 해결 방법
복제 실패	보조 노드에서 복제된 메시지를 사용하지 못했습니다.	Cisco ISE-PIC GUI에 로그인하고 구축 페이지에서 수동 동기화를 수행해 주십시오. 영향을 받는 Cisco ISE-PIC 노드를 등록 취소했다가 다시 등록해 주십시오.
복원 실패	Cisco ISE-PIC 복원 작업에 실패했습니다.	Cisco ISE-PIC와 리포지토리 사이의 네트워크 연결을 확인해 주십시오. 리포지토리에 사용된 자격 증명이 올바른지 확인해 주십시오. 백업 파일이 손상되지 않았는지 확인해 주십시오. CLI에서 **reset-config** 명령을 실행하고 마지막으로 알려진 안전한 백업을 복원해 주십시오.
패치 실패	서버에서 패치 프로세스가 실패했습니다.	서버에서 패치 프로세스를 다시 실행해 주십시오.
패치 성공	서버에서 패치 프로세스가 성공했습니다.	-
복제 중지됨	ISE-PIC 노드가 PAN에서 컨피그레이션 데이터를 복제할 수 없습니다.	Cisco ISE-PIC GUI에 로그인하여 구축 페이지에서 수동 동기화를 수행하거나, 필수 필드를 사용하여 영향을 받는 ISE-PIC 노드를 등록 취소했다가 다시 등록해 주십시오.
엔드포인트 인증서 만료됨	엔드포인트 인증서가 일별 예약 작업에서 만료된 상태로 표시되었습니다.	새 엔드포인트 인증서를 받으려면 엔드포인트 디바이스를 다시 등록해 주십시오.
엔드포인트 인증서 제거됨	일별 예약 작업에서 만료된 엔드포인트 인증서가 제거되었습니다.	추가 작업 필요 없음 - 이는 관리자가 시작한 정리 작업입니다.
느린 복제 오류	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 정보	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
느린 복제 경고	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
EST 서비스 중단	EST 서비스가 중단되었습니다.	CA 및 EST 서비스가 실행 중이고 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완전한지 확인하십시오.
EST 서비스 작동 중	EST 서비스가 작동 중입니다.	관리자에게 EST 서비스가 작동하고 있음을 알리는 알림입니다.
Smart Call Home 통신 실패	Smart Call Home 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE-PIC와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
원격 분석 통신 장애	원격 분석 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
ISE 서비스		
AD Connector를 다시 시작해야 함	AD Connector가 예기치 않게 중지되었으므로 다시 시작해야 합니다.	이 문제가 계속되면 Cisco TAC에 지원을 요청해 주십시오.
Active Directory 포리스트를 사용할 수 없음	Active Directory 포리스트 GC(Global Catalog)를 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
인증 도메인을 사용할 수 없음	인증 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 매핑. 인증 비활성	ID 매핑 서비스에서 최근 15분간 사용자 인증 이벤트를 수집하지 않았습니다.	사용자 인증이 필요한 시점이라면(예: 근무 시간) Active Directory 도메인 컨트롤러에 대한 연결을 확인해 주십시오.
구성된 네임서버 작동 중지됨	구성된 네임서버가 작동 중지되었거나 사용 불가능합니다.	DNS 컨피그레이션 및 네트워크 연결을 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
AD: 머신 TGT 새로 고침 실패	ISE-PIC 서버 TGT(Ticket Granting Ticket) 새로 고침에 실패했습니다. 해당 TGT는 AD 연결 및 서비스에 사용됩니다.	Cisco ISE-PIC 머신 계정이 있으며 유효한지 확인해주십시오. 또한 가능한 클럭 오차, 복제, Kerberos 컨피그레이션 및/또는 네트워크 오류가 있는지도 확인해 주십시오.
AD: ISE 계정 비밀번호 업데이트 실패	ISE-PIC 서버에서 AD 머신 계정 비밀번호를 업데이트하지 못했습니다.	Cisco ISE-PIC 머신 계정 비밀번호가 변경되지 않았는지, 그리고 머신 계정이 비활성화되었거나 제한되어 있지 않은지 확인해 주십시오. KDC에 대한 연결을 확인해 주십시오.
가입한 도메인 사용 불가능	가입한 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 저장소 사용 불가능	Cisco ISE-PIC 정책 서비스 노드를 구성한 ID 저장소에 연결할 수 없습니다.	Cisco ISE-PIC와 ID 저장소 사이의 네트워크 연결을 확인해 주십시오.
AD: ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE-PIC 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE-PIC 머신 계정에 Active Directory에서 사용자 그룹을 가져올 권한이 있는지 확인 합니다.
시스템 상태		
높은 디스크 I/O 사용률	Cisco ISE-PIC 시스템의 디스크 I/O사용률이 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 디스크 공간 사용률	Cisco ISE-PIC 시스템의 디스크 공간사용률이 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.

경보 이름	경보 설명	경보 해결 방법
높은 로드 평균	Cisco ISE-PIC 시스템의 로드 평균이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 메모리 사용률	Cisco ISE-PIC 시스템의 메모리 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 작업 DB 사용률	Cisco ISE-PIC 모니터링 노드의 syslog 데이터 볼륨이 예상보다 많습니다.	작업 데이터에 대한 컨피그레이션 제거 창을 확인하고 줄이십시오.
상태 사용 불가능	모니터링 노드가 Cisco ISE-PIC 노드에서 상태를 받지 못했습니다.	Cisco ISE-PIC 노드가 작동되어 실행 중인지 확인해 주십시오. Cisco ISE-PIC 노드가 모니터링 노드와 통신할 수 있는지 확인해 주십시오.
프로세스 작동 중지	Cisco ISE-PIC 프로세스 중 하나가 실행되고 있지 않습니다.	Cisco ISE-PIC 애플리케이션을 다시 시작해 주십시오.
OCSP 트랜잭션 임계값에 도달함	OCSP 트랜잭션 임계값에 도달했습니다. 이 경보는 내부 OCSP 서비스에서 많은 양의 트래픽이 발생하는 경우에 트리거됩니다.	시스템의 리소스가 충분한지 확인해 주십시오.
라이센싱		
PIC 라이센스 만료됨	Cisco ISE-PIC 노드에 설치된 라이센스가 만료되었습니다.	새 라이센스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
30일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 30일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.
60일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 60일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.

경보 이름	경보 설명	경보 해결 방법
90일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 90일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.
시스템 오류		
로그 수집 오류	Cisco ISE-PIC 모니터링 컬렉터 프로세스가 정책 서비스 노드에서 생성된 감사 로그를 유지할 수 없습니다.	이는 정책 서비스 노드의 실제 기능에는 영향을 미치지 않습니다. 추가적인 해결 방법은 TAC에 문의해 주십시오.
예약된 보고서 내보내기 실패	내보낸 보고서(CSV 파일)를 구성한 리포지토리에 복사할 수 없습니다.	구성한 리포지토리를 확인해 주십시오. 리포지토리가 삭제되었으면 다시 추가해 주십시오. 리포지토리를 사용할 수 없거나 리포지토리에 연결할 수 없는 경우 리포지토리를 유효한 리포지토리로 다시 구성해 주십시오.

사용자 또는 엔드포인트를 Cisco ISE-PIC에 추가하는 경우에는 경보가 트리거되지 않습니다.

알람 설정

다음 표에서는 **Alarm Settings(**알람 설정**)** 창(**Settings(**설정**)** > **Alarm Settings(**알람 설정**))**에 대해 설명합니다.

필드 이름	설명
알람 유형	알람 유형입니다.
경보 이름	알람의 이름입니다.
설명	알람에 대한 설명입니다.
제안 조치	알람이 트리거될 때 수행할 작업입니다.
상태	알람 규칙을 활성화하거나 비활성화합니다.
심각도	알람의 심각도 레벨을 선택합니다. 유효한 옵션은 다음과 같습니다. • Critical(위험) : 심각한 오류 상태를 나타냅니다. • Warning(경고): 정상적이기는 하지만 중요한 상태를 나타냅니다. 기본 상태입니다. • Info(정상): 정보 메시지를 나타냅니다.

필드 이름	설명
시스템 로그 메시지 보내기	Cisco ISE-PIC에서 생성하는 각 시스템 알람에 대해 시스템 로그 메시지를 보냅니다.
쉼표로 구분하여 여러 이메일 입력	이메일 주소 또는 ISE-PIC 관리자 이름 또는 둘 다의 목록입니다.
이메일 메모**(0 ~ 4,000**자**)**	시스템 알람과 연결하려는 맞춤형 텍스트 메시지.

맞춤형 경보 추가

Cisco ISE-PIC에는 5개의 기본 알람 유형(컨피그레이션 변경됨, 높은 디스크 I/O 사용률, 높은 디스크 공간 사용률, 높은 메모리 사용률 및 ISE 인증 비활성 등)이 포함되어 있습니다. Cisco에서 정의한 시스템 알람은 Alarms Settings(알람 설정) 페이지(Settings(설정) > Alarms Settings(알람 설정))에 나열됩니다. 시스템 알람만 편집할 수 있습니다.

기존 시스템 알람 외에도 기존 알람 유형에서 사용자 지정 알람을 추가, 수정 또는 삭제할 수 있습니다.

각 경보 유형에 대해 경보를 최대 5개까지 생성할 수 있으며 총 경보 수는 200개로 제한됩니다.

경보를 추가하려면 다음을 수행합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings (**설정**)> Alarm Settings (**알람 설정**)**를 선택합니다.

단계 **2** **Alarm Configuration(**알람 구성**)** 탭 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부사항을 입력합니다. 자세한 내용은 알람 설정 섹션을 참고하십시오.

알람 유형에 따라 Alarm Configuration(알람 컨피그레이션) 페이지에 추가 특성이 표시됩니다. 예를 들어 구성 변경 알람에 대해서는 Object Name(개체 이름), Object Type(개체 유형) 및 Admin Name(관리자 이름) 필드가 표시됩니다. 각기 기준이 다른 동일 경보의 여러 인스턴스를 추가할 수 있습니다.

단계 **4** 제출을 클릭합니다.

들어오는 트래픽을 검증하는 **TCP** 덤프 유틸리티

TCP 덤프 유틸리티는 패킷을 스니핑합니다. 이 패킷을 사용하여 예상 패킷이 노드에 도달했는지 확인할 수 있습니다. 예를 들어 보고서에 들어오는 인증 또는 로그인이 나타나 있지 않은 경우 들어오는 트래픽이 없거나 들어오는 트래픽이 Cisco ISE에 도달되지 않는다는 의심이 있을 수 있습니다. 이 경우 이 도구를 실행하여 검증할 수 있습니다.

네트워크 문제를 해결하는 데 도움이 되도록 TCP 덤프 옵션을 구성한 다음 네트워크 트래픽에서 데이터를 수집할 수 있습니다.

TCP 덤프를 사용하여 네트워크 트래픽 모니터링

TCP Dump(TCP 덤프) 페이지에는 사용자가 생성하는 TCP 덤프 프로세스 파일이 나열됩니다. 각기 다른 용도로 다른 파일을 생성하고 필요에 따라 실행한 다음 필요하지 않은 경우 삭제할 수 있습니다.

크기, 파일 수 및 프로세스 실행 기간을 지정하여 수집되는 데이터를 제어할 수 있습니다. 프로세스가 제한 시간 전에 완료되고 최대 크기보다 작은 파일 둘 이상을 활성화한 경우 프로세스가 계속 진행되고 다른 덤프 파일이 생성됩니다.

결합된 인터페이스를 포함하여 더 많은 인터페이스에서 TCP 덤프를 실행할 수 있습니다.

사람이 읽을 수 있는 형식은 더 이상 옵션으로 제공되지 않며, 덤프 파일은 항상 원시 형식입니다.

저장소에 대한 IPv6 연결을 지원합니다.

시작하기 전에

TCP 덤프 페이지의 네트워크 인터페이스 드롭다운 목록에는 IPv4 또는 IPv6 주소가 구성되어 있는 NIC(Network Interface Cards)만 표시됩니다. 기본적으로 VMware에서는 모든 NIC가 연결되어 있으므로 모든 NIC에 IPv6 주소가 있으며 네트워크 인터페이스 드롭다운 목록에 표시됩니다.

단계 **1** TCP 덤프 유틸리티의 소스로 **Host Name(**호스트 이름**)**을 선택합니다.

단계 **2** 드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다.

단계 **3** Filter(필터) 필드에 필터 기준으로 사용할 부울 식을 입력합니다.

다음과 같은 표준 tcpdump 필터 식이 지원됩니다.

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 및 not 10.77.122.119

단계 **4** 이 TCP 덤프 프로세스의 파일 이름을 입력합니다.

단계 **5** TCP 덤프 로그 파일을 저장할 저장소를 선택합니다.

단계 **6** **File Size(**파일 크기**)**—최대 파일 크기를 선택합니다.

덤프가 이 파일 크기를 초과하면 새 파일이 열려 덤프를 계속합니다. 덤프가 새 파일을 계속 사용할 수 있는 횟수는 **Limit to(**다음으로 제한**)** 설정을 기준으로 제한됩니다.

단계 **7** **Limit to(**다음으로 제한**)**—덤프가 확장 할 수 있는 파일의 수를 제한합니다.

단계 **8** **Time Limit(**시간 제한**)**—종료 전에 덤프가 실행되는 기간을 설정합니다.

단계 **9** 라디오 버튼을 클릭해 On(켜기) 또는 Off(끄기)로 설정하여 Promiscuous Mode(무차별 모드)를 설정합니다. 기본값은 On(켜기)입니다.

무차별 모드는 네트워크 인터페이스가 시스템 CPU로 모든 트래픽을 전달하는 기본 패킷 스니핑 모드입니다. 이 모드는 On(켜기)으로 설정해 두는 것이 좋습니다.

참고 Cisco ISE는 1500MTU(점보 프레임)보다 큰 프레임을 지원하지 않습니다.

TCP 덤프 파일 저장

시작하기 전에

TCP 덤프를 사용하여 네트워크 트래픽 모니터링 섹션의 설명에 따라 작업을 정상적으로 완료한 상태여야 합니다.

참고 Cisco ISE CLI를 통해 TCP 덤프에 액세스할 수도 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI* 참조 설명서를 참고해 주십시오.

단계 **1** **Format(**형식**)** 드롭다운 목록에서 옵션을 선택합니다. **Human Readable(**사람이 읽을 수 있음**)**이 기본값입니다.

단계 **2** **Download(**다운로드**)**를 클릭하고 원하는 위치로 이동한 후에 **Save(**저장**)**를 클릭합니다.

단계 **3** 이전 덤프 파일을 먼저 저장하지 않고 제거하려면 **Delete(**삭제**)**를 클릭합니다.

TCP 덤프 설정

다음 표에서는 네트워크 인터페이스에서 패킷의 내용을 모니터링하고 네트워크에서 나타나는 문제를 해결하는 데 사용할 수 있는 **tcpdump** 유틸리티 페이지의 필드에 대해 설명합니다. 이 페이지의 탐색 경로는 **Troubleshoot(**문제 해결**)**.

표 ***3: TCP*** 덤프 설정

옵션	사용 지침
상태	• Stopped(중지됨) - tcpdump 유틸리티가 실행되고 있지 않습니다. • Start(시작) - tcpdump 유틸리티의 네트워크 모니터링을 시작하려면 클릭합니다. • Stop(중지) - tcpdump 유틸리티를 중지하려면 클릭합니다.
Host Name(호스트 이름)	드롭다운 목록에서 모니터링할 호스트 이름을 선택합니다.

옵션	사용 지침
Network Interface(네트워크 인터페이스)	드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다. 참고 모든 NIC(Network Interface Cards)가 Cisco ISE 관리 포털에 표시되도록 IPv4 또는 IPv6 주소를 사용하여 구성해야 합니다.
Promiscuous Mode(무차별 모드)	• On(켜기) - 무차별 모드를 켜려면 클릭합니다(기본값). • Off(켜기) - 무차별 모드를 끄려면 클릭합니다. 무차별 모드는 기본 패킷 스니핑 모드로, On(켜기)으로 설정해 두는 것이 좋습니다. 이 모드에서는 네트워크 인터페이스가 모든 트래픽을 시스템 CPU로 전달합니다.
Filter(필터)	필터 기준으로 사용할 부울 식을 입력합니다. 지원되는 표준 tcpdump 필터 식: ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123
Format(형식)	tcpdump 파일의 형식을 선택합니다.
Dump File(덤프 파일)	다음과 같은 마지막 덤프 파일에 대한 데이터를 표시합니다. 관리자가 2011년 4월 27일 수요일 20:42:38(UTC)에 마지막으로 생성함 `파일 크기: 3,744바이트 형식: 원시 패킷 데이터 호스트 이름: Positron 네트워크 인터페이스: GigabitEthernet 0 무차별 모드: 설정` • Download(다운로드) - 최신 덤프 파일을 다운로드하려면 클릭합니다. • Delete(삭제) - 최신 덤프 파일을 삭제하려면 클릭합니다.

로깅 메커니즘

Cisco ISE-PIC 로깅 메커니즘

시스템 로그 제거 설정 구성

다음 프로세스를 사용하여 로컬 로그 저장 기간을 설정하고 특정 기간이 지난 후 로컬 로그를 삭제합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Logging(**기록**)** > **Local Log Settings(**로컬 로그 설정**)**.

단계 **2** **Local Log Storage Period(**로컬 로그 저장 기간**)** 필드에 로그 엔트리를 컨피그레이션 소스에 보관할 최대 기간을 일 단위로 입력합니다.

localStore 폴더의 크기가 97GB에 도달하면 구성된 **Local Log Storage Period(**로컬 로그 저장 기간**)**가 끝나기 전에 일찍 로그가 삭제될 수 있습니다.

단계 **3** 저장 기간이 만료되기 전에 언제든지 기존 로그 파일을 삭제하려면 **Delete Logs Now(**지금 로그 삭제**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

디버그 로그

디버그 로그에서는 부트스트랩, 애플리케이션 컨피그레이션, 런타임, 구축, 모니터링, 보고 및 PKI(Public Key Infrastructure) 정보를 캡처합니다. 지난 30일 동안의 위험 및 경고 경보와 지난 7일 동안의 정보 경보가 디버그 로그에 포함됩니다.

개별 구성 요소에 대한 디버깅 로그 심각도 수준을 구성할 수 있습니다.

노드 또는 구성 요소에 대해 Reset to Default(기본값으로 재설정) 옵션을 사용하여 로그 레벨을 공장에서 제공한 기본값으로 다시 재설정할 수 있습니다.

로컬 서버에 디버그 로그를 저장할 수 있습니다.

참고 시스템이 백업 또는 업그레이드에서 복원된 경우 디버그 로그 컨피그레이션은 저장되지 않습니다.

디버그 로그 심각도 수준 구성

디버그 로그의 심각도 레벨을 구성할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration** > **Logging(로깅)** > **Debug Log Configuration(디버그 로그 구성)**.

단계 **2** 노드를 선택하고 **Edit(편집)**를 클릭합니다.

Debug Log Configuration(디버그 로그 컨피그레이션) 페이지에는 선택한 노드에서 실행 중인 서비스를 기준으로 하는 구성 요소 목록과 개별 구성 요소에 대해 설정된 현재 로그 레벨이 표시됩니다.

노드 또는 구성 요소에 대해 **Reset to Default(기본값으로 재설정)** 옵션을 사용하여 로그 레벨을 공장에서 제공한 기본값으로 다시 재설정할 수 있습니다.

단계 **3** 로그 심각도 수준을 구성하려는 구성 요소를 선택하고 **Edit(편집)**를 클릭합니다. **Log Level(로그 레벨)** 드롭다운 목록에서 원하는 로그 심각도 수준을 선택하고 **Save(저장)**를 클릭합니다.

참고 런타임 AAA 구성 요소의 로그 심각도 수준을 변경하면 해당 하위 구성 요소 prrt-JNI의 로그 레벨도 변경됩니다. 하위 구성 요소 로그 레벨을 변경해도 부모 구성 요소에는 영향을 주지 않습니다.

Active Directory 문제 해결

Active Directory와 Cisco ISE-PIC 통합을 위한 사전 요건

이 섹션에서는 Cisco ISE-PIC와 통합되도록 Active Directory를 구성하는 데 필요한 수동 단계를 설명합니다. 그러나 대부분의 경우 Cisco ISE-PIC가 Active Directory를 자동으로 구성할 수 있습니다. Active Directory와 Cisco ISE-PIC 통합의 사전 요구 사항은 다음과 같습니다.

- Active Directory 도메인 구성을 변경하는 데 필요한 AD 도메인 관리자 자격 증명이 있어야 합니다.
- NTP(Network Time Protocol) 서버 설정을 사용하여 Cisco ISE-PIC 서버와 Active Directory 간에 시간을 동기화합니다. Cisco ISE-PIC CLI에서 NTP 설정을 구성할 수 있습니다.
- Cisco ISE-PIC를 가입시키는 도메인에 Cisco ISE-PIC에서 액세스할 수 있으며 작동 가능한 글로벌 카탈로그 서버가 하나 이상 있어야 합니다.

다양한 작업을 수행하는 데 필요한 **Active Directory** 계정 권한

가입 작업	탈퇴 작업	**Cisco ISE-PIC** 머신 계정
가입 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE-PIC 머신 계정이 있는지 확인하는 용도) • 도메인에 Cisco ISE-PIC 머신 계정 생성(머신 계정이 아직 없는 경우) • 새 머신 계정에서 속성 설정(예: Cisco ISE-PIC 머신 계정 비밀번호, SPN, dnsHostname)	탈퇴 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE-PIC 머신 계정이 있는지 확인하는 용도) • 도메인에서 Cisco ISE-PIC 머신 계정 제거 강제 탈퇴를 수행하는 경우(비밀번호 없이 탈퇴) 도메인에서 머신 계정이 제거되지 않습니다.	Active Directory 연결과의 통신에 사용되는 ISE-PIC 머신 계정에는 다음 권한이 필요합니다. • 비밀번호 변경 • 연락된 사용자 및 머신에 해당하는 사용자 및 머신 개체 읽기 • 정보(예: 신뢰할 수 있는 도메인, 대체 UPN 접미사 등)를 확인하기 위한 Active Directory 쿼리 • tokenGroups 속성 읽기 Active Directory에서 머신 계정을 미리 생성할 수 있습니다. SAM 이름이 Cisco ISE-PIC 어플라이언스 호스트 이름과 일치하는 경우 가입 작업 중에 해당 항목을 찾아서 재사용해야 합니다. 여러 가입 작업이 수행되는 경우 Cisco ISE-PIC 내에서 가입별로 하나씩 여러 머신 계정이 유지 관리됩니다.

참고 가입 또는 탈퇴 작업에 사용하는 크리덴셜은 Cisco ISE-PIC에 저장되지 않습니다. 새로 생성된 Cisco ISE-PIC 머신 계정 크리덴셜만 저장됩니다.

Microsoft Active Directory에서 네트워크 액세스**: SAM**에 대한 원격 호출을 허용하는 클라이언트 제한 보안 정책이 수정되었습니다. 이로 인해 Cisco ISE는 15일마다 머신 계정 암호를 업데이트하지 못할 수 있습니다. 머신 계정 암호가 업데이트되지 않으면 Cisco ISE는 Microsoft Active Directory를 통해 더 이상 사용자를 인증하지 않습니다. 이 이벤트에 대해 알 수 있도록 Cisco ISE 대시보드에서 **AD: ISE password update failed(AD: ISE** 암호 업데이트 실패**)** 알람을 받게 됩니다.

사용자는 보안 정책을 통해 로컬 SAM(Security Accounts Manager) 데이터베이스 및 Microsoft Active Directory의 사용자 및 그룹을 열거할 수 있습니다. Cisco ISE가 머신 계정 암호를 업데이트할 수 있도록 하려면 Microsoft Active Directory의 컨피그레이션이 정확한지 확인하십시오. 영향을 받는 Windows 운영체제 및 Windows Server 버전, 네트워크에 미치는 영향 및 필요한 변경 사항에 대한 자세한 내용은 다음을 참조하십시오.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

통신을 위해 열어 두어야 하는 네트워크 포트

프로토콜	포트(원격-로컬)	대상	참고
DNS(TCP/UDP)	49,152 이상의 난수	DNS 서버/AD 도메인 컨트롤러	—
MSRPC	445	도메인 컨트롤러	—
Kerberos(TCP/UDP)	88	도메인 컨트롤러	MS AD/KDC
LDAP(TCP/UDP)	389	도메인 컨트롤러	—
LDAP(GC)	3268	글로벌 카탈로그 서버	—
NTP	123	NTP 서버/도메인 컨트롤러	—
IPC	80	보조 ISE-PIC 노드용	—

Easy Connect ISE-PIC

ISE-PIC Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. Active Directory 서버를 올바르게 구성해야 ISE 사용자가 서버에 연결하여 사용자 로그인 정보를 가져올 수 있습니다. 다음 섹션에서는 ISE-PIC를 지원하도록 Active Directory 도메인 컨트롤러를 구성하는 방법을 확인할 수 있습니다(Active Directory 측에서의 구성).

를 지원하도록 Active Directory 도메인 컨트롤러를 구성하려면(Active Directory 측에서의 구성) 다음 단계를 따르십시오.

참고 모든 도메인에서 모든 도메인 컨트롤러를 구성해야합니다.

1. ISE-PIC에서 Active Directory 조인 포인트 및 도메인 컨트롤러를 설정합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입 및 도메인 컨트롤러 추가를 참조하십시오.
2. 도메인 컨트롤러별 WMI를 구성합니다. 패시브 ID용 WMI 구성를 참조하십시오.
3. Active Directory에서 다음 단계를 수행합니다.
   - 다음에 대한 Active Directory 설정 구성 패시브 ID 서비스, 26 페이지
4. (선택 사항) 다음 단계를 수행하여 Active Directory에서 ISE로 수행하는 자동 구성 문제를 해결합니다.
   - Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정, 29 페이지

• 도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한, 29 페이지
• 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 31 페이지
• WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 32 페이지
• AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여, 33 페이지

다음에 대한 Active Directory 설정 구성 패시브 ID 서비스

ISE-PIC Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. ISE-PIC는 Active Directory에 연결하여 사용자 로그인 정보를 가져옵니다.

Active Directory 도메인 컨트롤러에서 다음 단계를 수행해야 합니다.

단계 **1** 관련 Microsoft 패치가 Active Directory 도메인 컨트롤러에 설치되어 있는지 확인합니다.

a) Windows Server 2008에는 다음 패치가 필요합니다.

- http://support.microsoft.com/kb/958124

  이 패치는 Microsoft의 WMI에서 메모리 누수를 수정하여, ISE가 도메인 컨트롤러와의 성공적인 연결을 설정할 수 없게 합니다.

- http://support.microsoft.com/kb/973995

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 다른 메모리 유출을 수정합니다.

b) Windows Server 2008 R2에는 다음 패치가 필요합니다(SP1이 설치되어 있지 않은 경우).

- http://support.microsoft.com/kb/981314

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 메모리 유출을 수정합니다.

- http://support.microsoft.com/kb/2617858

  이 패치는 Windows Server 2008 R2에서 예기치 않게 발생하는 느린 시작 또는 로그인 프로세스를 수정합니다.

c) Windows 플랫폼의 WMI 관련 문제의 경우 다음 링크에 나열되어 있는 패치가 필요합니다.

- http://support.microsoft.com/kb/2591403

이러한 핫픽스는 WMI 서비스 및 관련 구성 요소의 작동 및 기능과 연관되어 있습니다.

단계 **2** Active Directory가 Windows 보안 로그에 사용자 로그인 이벤트를 기록하는지 확인합니다.

Audit Policy(감사 정책) 설정(Group Policy Management(그룹 정책 관리) 설정의 일부분)의 설정이 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 정상 로그온을 허용하는지 확인합니다(이는 기본 Windows 설정이지만 이 설정이 올바른지를 명시적으로 확인해야 함).

단계 **3** ISE-PIC가 Active Directory에 연결하려면 Active Directory 사용자에게 충분한 권한이 있어야 합니다. 다음 지침에서는 관리 도메인 그룹 사용자 또는 비관리 도메인 그룹 사용자에 대한 권한을 정의하는 방법을 보여줍니다.

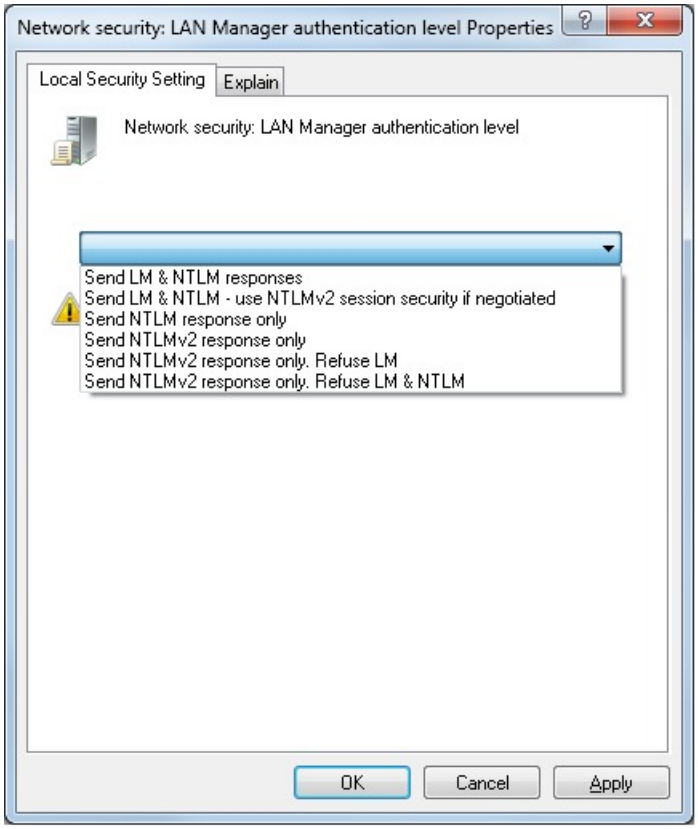
- Active Directory 사용자가 도메인 관리자 그룹의 멤버인 경우 필요한 권한
- Active Directory 사용자가 도메인 관리자 그룹의 멤버가 아닌 경우 필요한 권한

단계 **4** ISE-PIC에서 사용하는 Active Directory 사용자는 NTLM(NT LAN Manager) v1 또는 v2로 인증할 수 있습니다. ISE-PIC와 Active Directory 도메인 컨트롤러 간에 정상적으로 인증된 연결을 위해 Active Directory NTLM 설정이 ISE-PIC NTLM 설정과 일치하는지를 확인해야 합니다. 다음 표에는 모든 Microsoft NTLM 옵션과 지원되는 ISE-PIC NTLM 작업이 나와 있습니다. ISE-PIC가 NTLMv2로 설정되어 있으면 설명된 6개 옵션이 모두 지원됩니다. ISE-PIC가 NTLMv1을 지원하도록 설정되어 있으면 처음 5개 옵션만 지원됩니다.

표 *4: ISE-PIC* 및 *AD NTLM* 버전 설정에 따라 지원되는 인증 유형

ISE-PIC NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM response(LM 및 NTLM 응답 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send LM & NTLM - use NTLMv2 session security if negotiated(LM 및 NTLM 전송 - 협상 시 NTLMv2 세션 보안 사용) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLM response only(NTLM 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only(NTLMv2 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM(NTLMv2 응답만 전송하고 LM은 거부) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM & NTLM(NTLMv2 응답만 전송하고 LM 및 NTLM은 거부) 연결이 거부됨 연결이 허용됨	연결이 거부됨	연결이 허용됨

그림 *1: MS NTLM* 인증 유형 옵션



단계 **5** Active Directory 도메인 컨트롤러에서 `dllhost.exe`에 대한 트래픽을 허용하는 방화벽 규칙을 생성했는지 확인합니다.

방화벽을 끄거나, 특정 IP(ISE-PIC IP 주소)에서의 다음 포트에 대한 액세스를 허용할 수 있습니다.

- TCP 135: 일반 RPC 포트입니다. 비동기 RPC 호출을 수행하는 경우, 이 포트에서 수신 대기하는 서비스는 이 요청을 서비스하는 구성 요소에서 사용 중인 포트를 클라이언트에 알립니다.
- UDP 137: Netbios 이름 확인
- UDP 138: Netbios 데이터그램 서비스
- TCP 139: Netbios 세션 서비스
- TCP 445: SMB

더 많은 포트를 동적으로 할당되거나 수동으로 구성할 수 있습니다. 대상으로 %SystemRoot%\System32\dllhost.exe를 추가하는 방법을 권장합니다. 이 프로그램은 포트를 동적으로 관리합니다.

모든 방화벽 규칙을 특정 IP(ISE-PIC IP)에 할당할 수 있습니다.

Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정

Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2의 경우 도메인 관리자 그룹에는 기본적으로 Windows 운영체제의 특정 레지스트리 키에 대한 모든 권한이 없습니다. Microsoft Active Directory 관리자는 Microsoft Active Directory 사용자에게 다음 레지스트리 키에 대한 모든 권한을 부여해야 합니다.

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

다음 Microsoft Active Directory 버전의 경우에는 레지스트리를 변경할 필요가 없습니다.

- Windows 2003
- Windows 2003R2
- Windows 2008

모든 권한을 부여하려면 Microsoft Active Directory 관리자가 먼저 다음과 같이 키 소유권을 가져와야 합니다.

단계 **1** 키 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Owner(**소유자**)** 탭을 선택합니다.

단계 **2** **Permissions(**권한**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한

Windows 2012 R2의 경우 Microsoft AD 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여합니다.

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell에서 다음 명령을 사용하여 레지스트리 키에 대한 전체 권한이 부여되었는지 확인합니다.

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD 사용자가 도메인 관리자 그룹에는 없지만 도메인 사용자 그룹에는 있으면 다음 권한이 필요합니다.

- ISE-PIC가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

• 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 31 페이지
• WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 32 페이지

이러한 권한은 다음 Microsoft AD 버전에만 필요합니다.

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE-PIC가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

ISE-PIC가 도메인 사용자로 연결하여 로그인 인증 이벤트를 검색할 수 있게 하려면 도메인 컨트롤러에 일부 레지스트리 키를 수동으로 추가해야 합니다. 도메인 컨트롤러 또는 도메인의 머신에서 에이전트는 필요하지 않습니다.

다음 레지스트리 스크립트에는 추가할 키가 나와 있습니다. 이 스크립트를 복사하여 텍스트 파일에 붙여 넣고 파일을 .reg 확장자로 저장한 다음 파일을 더블 클릭하여 레지스트리를 변경합니다. 레지스트리 키를 추가하려면 사용자가 루트 키의 소유자여야 합니다.

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

DllSurrogate 키의 값에는 공백이 두 개 포함되어야 합니다. 레지스트리를 수동으로 업데이트하는 경우 두 개의 공백만 포함하고 따옴표는 포함하지 않아야 합니다. 레지스트리를 수동으로 업데이트하는 동안 AppID, DllSurrogate 및 해당 값에 따옴표가 포함되지 않았는지 확인하십시오.

파일 맨 끝의 빈 줄을 포함하여 위 스크립트에 나와 있는 빈 줄은 그대로 유지합니다.

Windows 명령 프롬프트에서 다음 명령을 사용하여 레지스트리 키가 생성되었고 올바른 값을 가지고 있는지 확인합니다.

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

도메인 컨트롤러에서 **DCOM**을 사용하기 위한 권한

ISE-PIC 패시브 ID 서비스에 사용되는 Active Directory 사용자는 도메인 컨트롤러에서 DCOM을 사용할 권한이 있어야 합니다. **dcomcnfg** 명령줄 툴을 사용하여 권한을 구성하십시오.

단계 **1** 명령줄에서 **dcomcnfg** 툴을 실행합니다.

단계 **2** **`Component Services`**(구성 요소 서비스)를 펼칩니다.

단계 **3** 확장 컴퓨터 > 내 컴퓨터 .

단계 **4** 메뉴 모음에서 **Action(**작업**)**을 선택하고 **properties(**속성**)**를 클릭한 후 **COM Security(COM** 보안**)**를 클릭합니다.

단계 **5** Cisco ISE가 Access(액세스) 및 Launch(실행)에 모두 사용할 계정에 Allow(허용) 권한이 있는지 확인합니다. 해당 AMicrosoft Active Directory 사용자를 4개 옵션(**Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 모두에 대한 **Edit Limits(**제한 편집**)**와 **Edit Default(**기본값 편집**))**에 모두 추가해야 합니다.

단계 **6** **Access Permission(**액세스 권한**)** 및 **Launch and Activation Permission(**실행 및 활성화 권한**)** 둘 다에 대해 Local Access(로컬 액세스) 및 Remote Access를 모두 Allow(허용)합니다.

그림 ***2:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

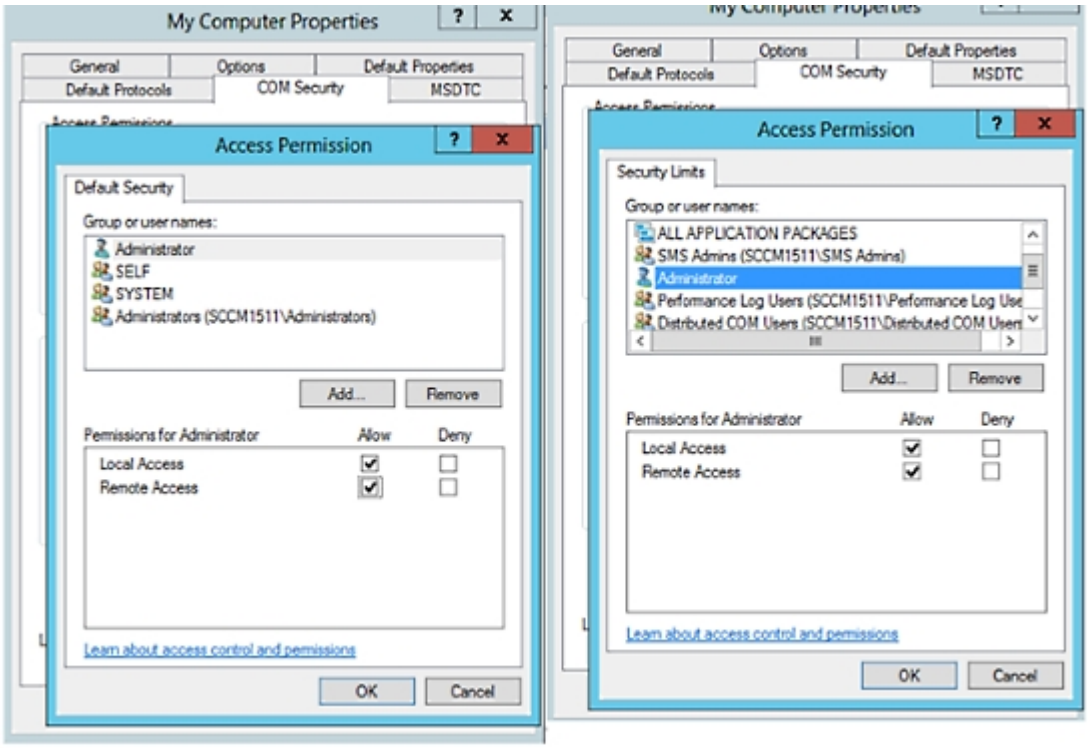
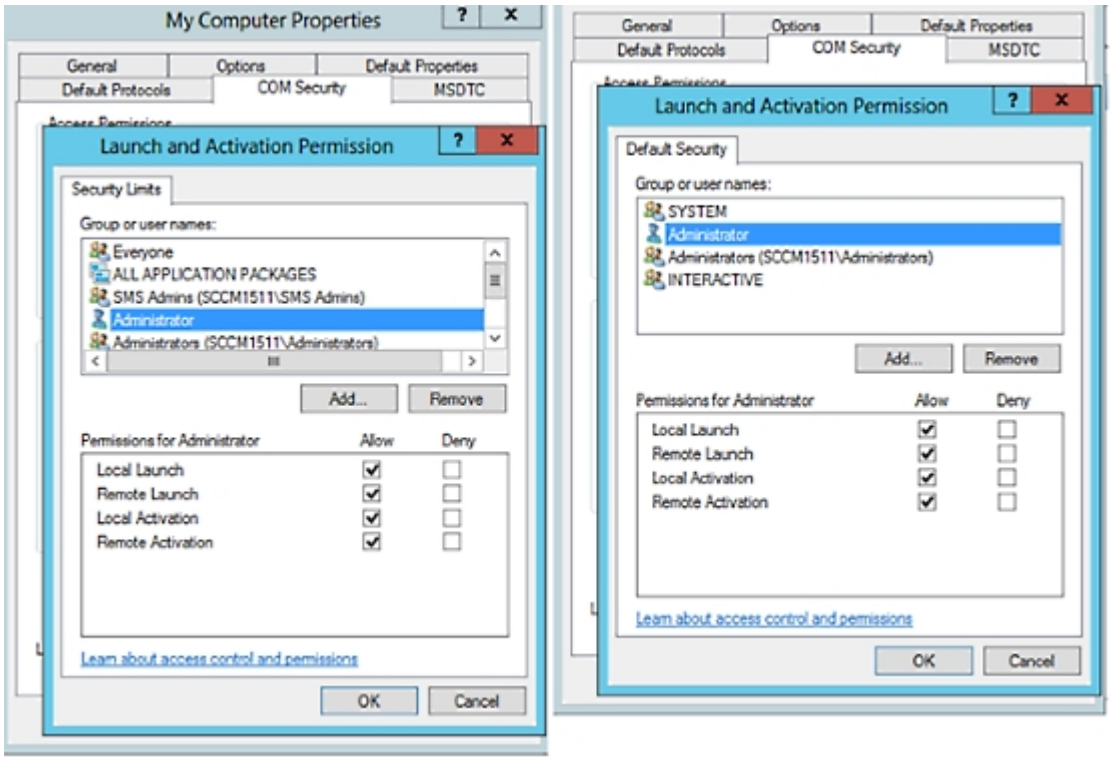


그림 *3:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

기본적으로 Microsoft Active Directory 사용자에게는 방법 실행 및 원격 활성화에 대한 권한이 없습니다. wmimgmt.msc MMC 콘솔을 사용하여 액세스 권한을 부여할 수 있습니다.

단계 **1** 다음 메뉴를 선택합니다. **Start(**시작**)** > **Run(**실행**)** 그런 다음 `wmimgmt.msc`를 입력합니다.

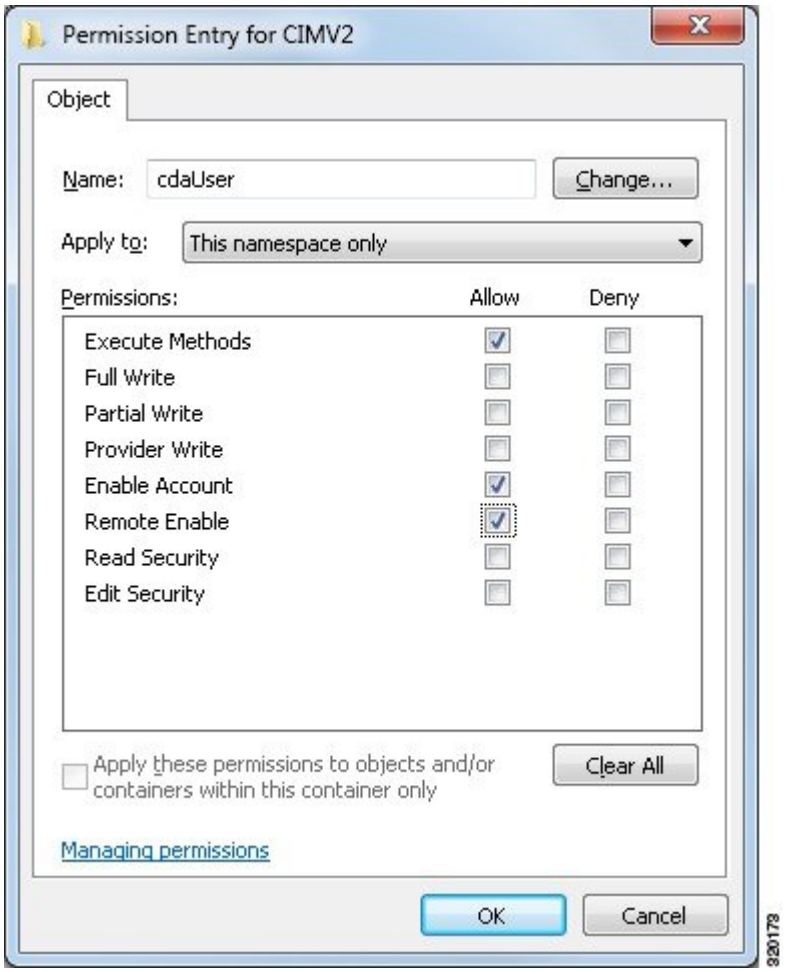
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

단계 **3** **Security(**보안**)** 탭에서 **Root(**루트**)**를 펼치고 **CIMV2**를 선택합니다.

단계 **4** **Security(**보안**)**를 클릭합니다.

단계 **5** Active Directory 사용자를 추가하고 아래 이미지에 나와 있는 대로 필요한 권한을 구성합니다.

그림 *4: WMI Root\CIMv2* 이름 공간에 필요한 권한



AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여

Windows 2008 이상에서는 Event Log Readers라는 그룹에 ISE-PIC ID 매핑 사용자를 추가하여 AD 도메인 컨트롤러 로그에 대한 액세스 권한을 부여할 수 있습니다.

모든 이전 버전 Windows에서는 아래에 나와 있는 것처럼 레지스트리 키를 편집해야 합니다.

단계 **1** 보안 이벤트 로그에 대한 액세스 권한을 위임하려면 계정의 SID를 찾습니다.

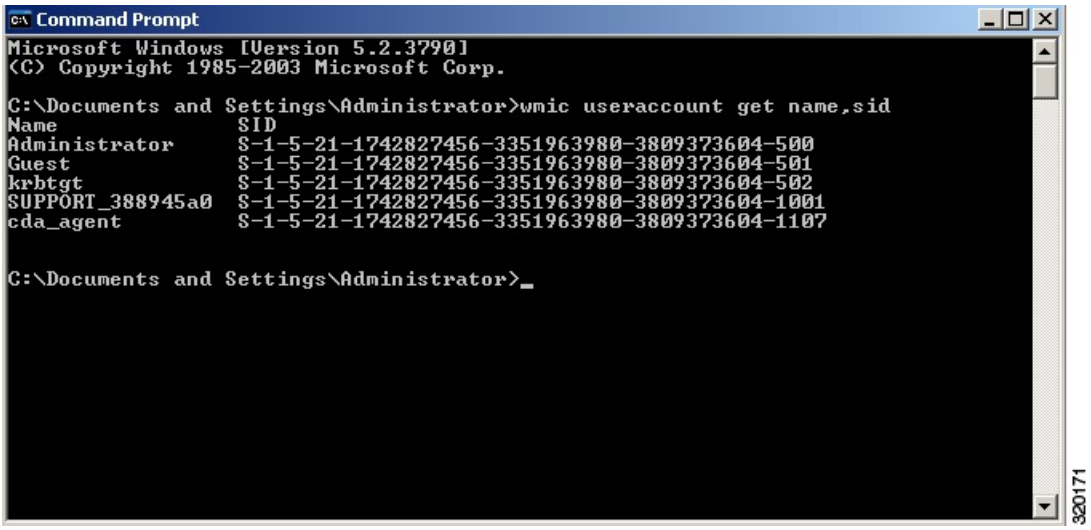
단계 **2** 명령줄에서 다음 명령을 사용하여 모든 SID 계정을 나열합니다. 이 명령은 아래 다이어그램에도 나와 있습니다.

```
wmic useraccount get name,sid
```

특정 사용자 이름 및 도메인의 경우 다음 명령을 사용할 수도 있습니다.

```
wmic useraccount where name="iseUser" get domain,name,sid
```

그림 *5:* 모든 ***SID*** 계정 나열



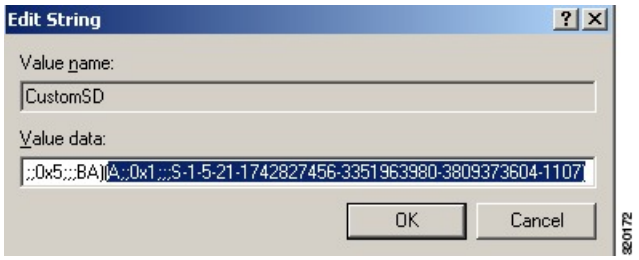
단계 **3** SID를 찾고 레지스트리 편집기를 연 후에 다음 위치로 이동합니다.

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

단계 **4** **Security(**보안**)**를 클릭하고 **CustomSD**를 두 번 클릭합니다.

예를 들어 ise_agent 계정 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`에 읽기 권한을 허용하려면 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`을 입력합니다.

그림 *6:* ***CustomSD*** 문자열 편집



단계 **5** 도메인 컨트롤러에서 WMI 서비스를 다시 시작합니다. 다음과 같이 두 가지 방법으로 WMI 서비스를 다시 시작할 수 있습니다.

a) CLI에서 다음 명령을 실행합니다.

net stop winmgmt

net start winmgmt

b) `Services.msc`를 실행합니다. 그러면 Windows 서비스 관리 툴이 열립니다. Windows 서비스 관리 윈도우에서 **Windows Management Instrumentation** 서비스를 찾아 마우스 오른쪽 버튼으로 클릭한 후에 **Restart(**다시 시작**)**를 선택합니다.

추가 문제 해결 정보 얻기

Cisco ISE-PIC에서는 관리 포털에서 지원 및 문제 해결 정보를 다운로드할 수 있습니다. 지원 번들을 사용하면 Cisco TAC(Technical Assistance Center)가 Cisco ISE-PIC의 문제 해결을 위한 진단 정보를 준비할 수 있습니다.

참고 TAC용 고급 문제 해결 정보를 제공하는 지원 번들과 디버그 로그는 해석하기가 어렵습니다. Cisco ISE-PIC에서 제공하는 다양한 보고서 및 문제 해결 도구를 사용하여 네트워크에서 발생하는 문제를 진단하고 해결할 수 있습니다.

Cisco ISE-PIC 지원 번들

지원 번들에 포함시킬 로그를 구성할 수 있습니다. 예를 들어 디버그 로그에 포함되도록 특정 서비스의 로그를 구성할 수 있습니다. 날짜를 기준으로 로그를 필터링할 수도 있습니다.

다운로드할 수 있는 로그는 다음과 같이 분류될 수 있습니다.

- 전체 구성 데이터베이스: 사람이 읽을 수 있는 XML 형식의 Cisco ISE-PIC 구성 데이터베이스를 포함합니다. 문제를 해결할 때 이 데이터베이스 구성을 다른 Cisco ISE 노드로 가져와 시나리오를 다시 생성할 수 있습니다.
- 디버그 로그: 부트스트랩, 애플리케이션 구성, 런타임, 구축, PKI(Public Key Infrastructure) 정보와 모니터링 및 보고 로그를 캡처합니다.

  디버그 로그는 특정 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그를 사용하려면 11장, "로깅"을 참고해 주십시오. 디버그 로그를 사용하지 않으면 모든 정보 메시지(INFO)가 지원 번들에 포함됩니다. 자세한 내용은 Cisco ISE-PIC 디버그 로그, 37 페이지를 참고하십시오.
- 로컬 로그: Cisco ISE에서 실행되는 다양한 프로세스의 시스템 로그 메시지를 포함합니다.
- 코어 파일: 크래시의 원인을 식별하는 데 도움이 되는 중요한 정보를 포함합니다. 이 로그는 애플리케이션이 크래시될 때 생성되며 힙 덤프를 포함합니다.
- 모니터링 및 보고 로그: 알림 및 보고서에 대한 정보를 포함합니다.
- 시스템 로그: Cisco ADE(Application Deployment Engine) 관련 정보를 포함합니다.
- 정책 구성: Cisco ISE에서 사람이 읽을 수 있는 형식으로 구성된 정책을 포함합니다.

Cisco ISE CLI에서 **backup-logs** 명령을 사용하여 이러한 로그를 다운로드할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI* 참조 설명서를 참고해 주십시오.

관리 포털에서 이러한 로그를 다운로드하도록 선택하는 경우 다음과 같이 해 주십시오.

- 디버그 로그 또는 시스템 로그 등의 로그 유형에 따라 로그 하위 집합만 다운로드합니다.

- 선택한 로그 유형에 대한 마지막 *n* 번호 파일만 다운로드합니다. 이 옵션을 사용하면 지원 번들의 크기와 다운로드에 소요되는 시간을 제어할 수 있습니다.

모니터링 로그는 모니터링, 보고 및 문제 해결 기능에 대한 정보를 제공합니다. 로그 다운로드에 대한 자세한 내용은 Cisco ISE-PIC 로그 파일 다운로드, 36 페이지를 참고하십시오.

지원 번들

지원 번들을 단순 tar.gpg 파일로 로컬 컴퓨터에 다운로드할 수 있습니다. 지원 번들은 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 형식으로 날짜 및 타임스탬프를 사용하여 이름이 지정됩니다. 브라우저에서 지원 번들을 적절한 위치에 저장하도록 메시지를 표시합니다. 지원 번들 내용을 추출하여 README.TXT 파일을 볼 수 있습니다. 이 파일에는 지원 번들의 내용과 함께 지원 번들에 포함되어 있는 ISE 데이터베이스의 내용을 가져오는 방법이 설명되어 있습니다.

Cisco ISE-PIC 로그 파일 다운로드

네트워크에서 문제를 해결하는 동안 자세한 정보를 확인하기 위해 Cisco ISE-PIC 로그 파일을 다운로드할 수 있습니다.

설치 및 업그레이드 문제를 해결하기 위해 ADE-OS가 포함된 시스템 로그 및 기타 로그 파일을 다운로드할 수도 있습니다.

시작하기 전에

- 디버그 로그 및 디버그 로그 레벨을 구성해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Logging(기록)** > **Download Logs(로그 다운로드)** > **Appliance node list(어플라이언스 노드 목록)**.

단계 **2** 지원 번들을 다운로드할 노드를 클릭합니다.

단계 **3** **Support Bundle(지원 번들)** 탭에서 지원 번들에 입력할 매개변수를 선택합니다.

모든 로그를 포함하는 경우 지원 번들이 매우 커지며 다운로드 시간이 오래 걸립니다. 다운로드 프로세스를 최적화하려면 최근 *n*개 파일만 다운로드하도록 선택합니다.

단계 **4** 지원 번들을 생성할 시작 및 종료 날짜를 입력합니다.

단계 **5** 다음 중 하나를 선택합니다.

- Public Key Encryption(공개 키 암호화): 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 선택합니다.
- Shared Key Encryption(공유 키 암호화): 온프레미스에서 로컬로 문제를 해결하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 지원 번들의 암호화 키를 입력해야 합니다.

단계 **6** **Create Support Bundle(지원 번들 생성)**을 클릭합니다.

단계 **7** **Download(다운로드)**를 클릭하여 새로 생성한 지원 번들을 다운로드합니다.

지원 번들은 애플리케이션 브라우저를 실행 중인 클라이언트 시스템에 다운로드되는 tar.gpg 파일입니다.

다음에 수행할 작업

특정 구성 요소에 대한 디버그 로그를 다운로드합니다.

Cisco ISE-PIC 디버그 로그

디버그 로그는 다양한 Cisco ISE-PIC 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그에는 최근 30일 내에 생성된 위험 및 경고 경보와 함께 최근 7일 내에 생성된 정보 경보가 포함됩니다. 문제를 보고하는 동안 이러한 디버그 로그를 사용하고 문제 진단 및 확인을 위해 해당 로그를 보낼지 묻는 메시지가 표시될 수 있습니다.

참고 디버그 로그의 모니터링 등 로드가 많은 디버그 로그를 활성화하면 높은 로드에 대한 알람이 생성될 수 있습니다.

디버그 로그 가져오기

단계 **1** 디버그 로그를 가져올 구성 요소를 구성합니다.

단계 **2** 디버그 로그를 다운로드합니다.

Cisco ISE-PIC 구성 요소 및 해당 디버그 로그

참고 아래 목록은 ISE에서 사용 가능한 전체 구성 요소 목록입니다. 표에 나열된 일부 구성 요소는 ISE-PIC

와 관련이 없을 수 있습니다.

표 ***5:*** 구성 요소 및 해당 디버그 로그

구성 요소	디버그 로그
Active Directory	ad_agent.log
Cache Tracker	tracking.log
EDF(Entity Definition Framework)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log

구성 요소	디버그 로그
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
게스트 액세스 관리자	guest.log
게스트 액세스	guest.log
MyDevices	guest.log
포털	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log

구성 요소	디버그 로그
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

디버그 로그 다운로드

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Logging(**기록**)** > **Download Logs(**로그 다운로드**)**.

단계 **2** Appliance node(어플라이언스 노드) 목록에서 디버그 로그를 다운로드할 노드를 클릭합니다.

단계 **3** **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

디버그 로그 유형 및 디버그 로그의 목록이 표시됩니다. 이 목록은 디버그 로그 컨피그레이션을 기반으로 합니다.

단계 **4** 다운로드하려는 로그 파일을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에 저장합니다.

필요에 따라 이 프로세스를 반복하여 다른 로그 파일을 다운로드할 수 있습니다. **Debug Logs(**디버그 로그**)** 창에서 다운로드할 수 있는 추가 디버그 로그는 다음과 같습니다.

- isebootstrap.log: 부트스트래핑 로그 메시지를 제공합니다.
- monit.log: Watchdog 메시지를 제공합니다.
- pki.log - 타사 암호화 라이브러리 로그를 제공합니다.
- iseLocalStore.log: 로컬 저장소 파일에 대한 로그를 제공합니다.
- ad_agent.log: Microsoft Active Directory 타사 라이브러리 로그를 제공합니다.

• catalina.log: 타사 로그를 제공합니다.