프로브 및 제공자로서의 **Active Directory**

Active Directory(AD)는 사용자 이름, IP 주소 및 도메인 이름 같은 사용자 ID 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

AD 프로브인 패시브 ID 서비스는 WMI 기술을 이용해 AD에서 사용자 ID 정보를 수신하지만, 다른 프로브는 다른 기술 과 방법을 이용해 AD를 사용자 ID 제공자로 사용합니다. ISE-PIC에서 제공하는 다른 프로브 및 제공자 유형에 관한 자세한 내용은 제공자 항목을 참조하십시오.

Active Directory 프로브를 구성하면 (마찬가지로 Active Directory를 소스로 사용하는) 이러한 다른 프로브를 빠르게 구성하고 활성화할 수 있습니다.

- Active Directory 에이전트

  참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

- SPAN
- 엔드포인트 프로브

또한 사용자 정보를 수집할 때 AD 사용자 그룹을 사용할 수 있도록 Active Directory 프로브를 구성합니다. AD 사용자 그룹을 AD, 에이전트, SPAN 및 Syslog 프로브에 사용할 수 있습니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 7 페이지 항목을 참조하십시오.

Active Directory 작업

패시브 ID 서비스에 대한 Active Directory 프로브를 구성하기 전에 다음을 확인하십시오.

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않습니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았습니다.

- DNS 서버를 올바르게 구성했는지 확인합니다(ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버를 참고하십시오.
- NTP 서버의 시계 설정을 동기화합니다. 자세한 내용은 시스템 시간 및 NTP 서버 설정 지정를 참고하십시오.

참고 Cisco ISE-PIC가 Active Directory에 연결되어 있는 경우 작동 문제가 발생하면 **Reports(**보고서**)** 아래의 AD Connector 운영 보고서를 참고해 주십시오. 자세한 내용은 사용 가능한 보고서의 내용을 참조하십시오.

PassiveID(패시브 ID) 설정 시작하기

ISE-PIC Active Directory를 첫 번째 사용자 ID 제공자로 쉽고 빠르게 구성하여 Active Directory에서 사용자 ID를 수신할 수 있는 마법사를 제공합니다. ISE-PIC용으로 Active Directory를 구성하면, 나중에 다른 제공자 유형도 쉽게 구성할 수 있습니다. Active Directory를 구성한 후에는 가입자(isco FMC(Firepower Management Center) 또는 Stealthwatch 등)를 구성해야 사용자 데이터를 수신할 클라이언트를 정의할 수 있습니다. 가입자에 관한 자세한 내용은 Subscribers(가입자) 항목을 참조하십시오.

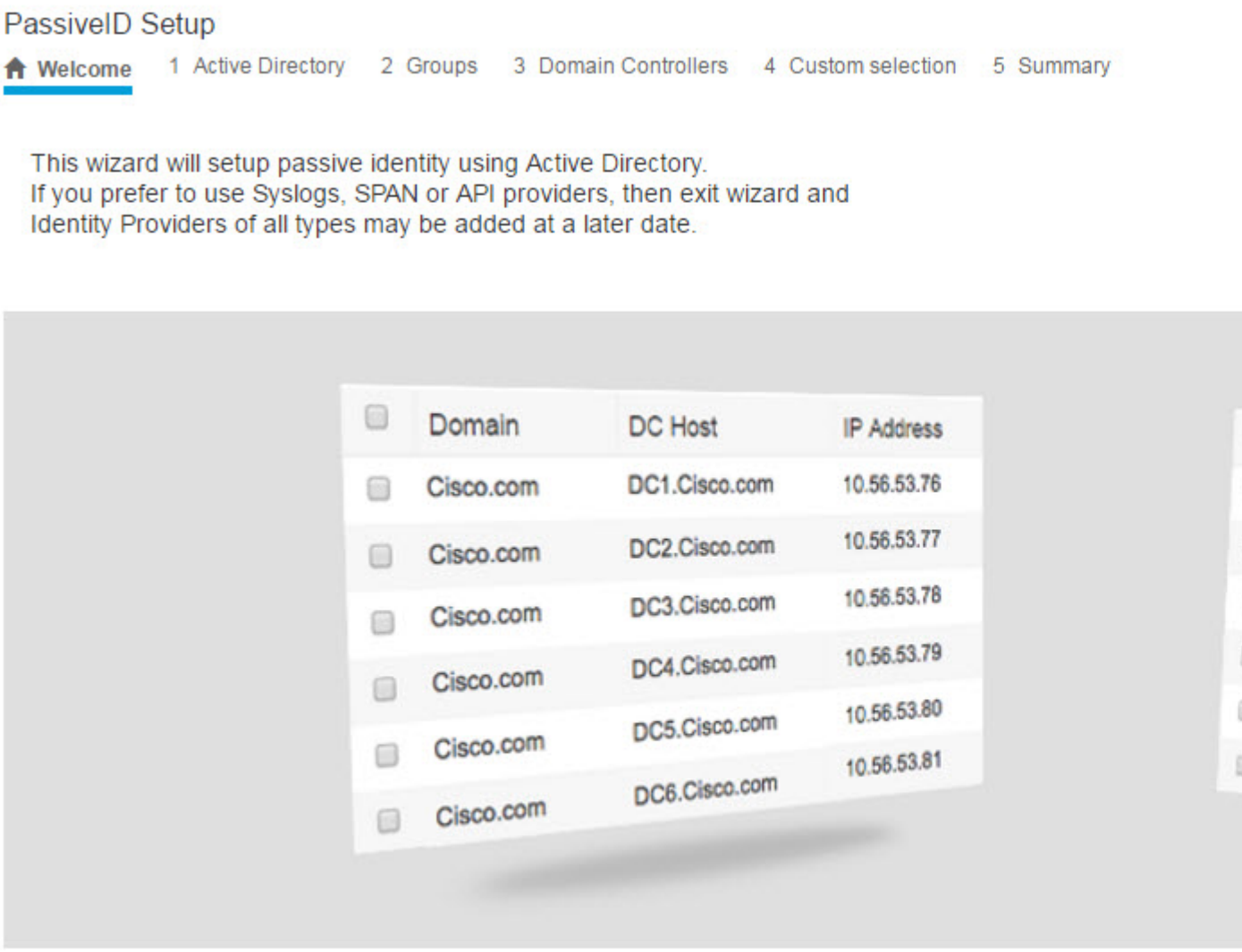
시작하기 전에

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않는지 확인합니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았는지 확인합니다.
- ISE-PIC에 DNS(도메인 이름 서버)의 항목이 있는지 확인합니다. ISE-PIC에서 클라이언트 머신에 대한 역방향 조회를 올바르게 구성했는지 확인합니다. 자세한 내용은 다음을 참조하십시오. DNS 서버

단계 **1** 다음 메뉴를 선택합니다. **Home(**홈**)** > **Introduction(**소개**)**. Passive Identity Connector Overview(패시브 ID 커넥터 개요) 화면에서 **Passive Identity Wizard(**패시브 **ID** 마법사**)**를 클릭합니다.

PassiveID Setup(패시브 ID 설정)이 열립니다.

그림 ***1: PassiveID Setup(***패시브 ***ID*** 설정***)***



단계 **2** **Next(**다음**)**를 클릭하여 마법사를 시작합니다.

단계 **3** 이 Active Directory 조인 포인트의 고유한 이름을 입력합니다. 이 노드가 연결된 Active Directory 도메인의 도메인 이름을 입력하고 Active Directory 관리자의 사용자 이름과 비밀번호를 입력합니다. Active Directory 설정에 관한 자세한 내용은 다음 항목을 참고하십시오. Active Directory 설정, 12 페이지

관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭하여 Active Directory 그룹을 정의하고 포함 및 모니터링할 사용자 그룹을 확인합니다. Active Directory 사용자 그룹은 이전 단계에서 구성한 Active Directory 조인 포인트에 따라 자동으로 표시됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다. 모니터링할 DC를 선택합니다. Custom(사용자 지정)을 선택했다면 다음 화면에서 모니터링할 특정 DC를 선택합니다. 모두 마쳤으면 **Next(**다음**)**를 클릭합니다.

단계 **6** **Exit(**종료**)**를 클릭하여 마법사를 완료합니다.

다음에 수행할 작업

Active Directory를 초기 제공자로 구성하는 작업이 끝나면, 추가 제공자 유형도 쉽게 구성할 수 있습니다. 자세한 내용은 제공자를 참고하십시오. 나아가 정의한 제공자가 수집하는 사용자 ID 정보를 수신하도록 지정된 가입자를 구성할 수도 있습니다. 자세한 내용은 Subscribers(가입자)를 참고하십시오.

Active Directory(WMI) 프로브 단계별 설정

패시브 ID 서비스에 대해 Active Directory 및 WMI를 구성하려면 PassiveID(패시브 ID) 설정 시작하기, 2 페이지를 사용하거나 다음과 같이 이 장의 단계를 수행합니다.

1. Active Directory 도메인을 구성합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입, 4 페이지를 참조하십시오.
2. AD 로그인 이벤트를 수신하는 WMI 구성 노드(또는 노드 모음)에 대한 Active Directory 도메인 컨트롤러 목록을 생성합니다. 도메인 컨트롤러 추가, 6 페이지를 참조하십시오.
3. ISE-PIC와 통합할 수 있도록 Active Directory를 구성합니다. 패시브 ID용 WMI 구성, 8 페이지를 참조하십시오.
4. (선택 사항) Active Directory 제공자 관리, 8 페이지.

Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입

시작하기 전에

Cisco ISE-PIC 노드가 NTP 서버, DNS 서버, 도메인 컨트롤러 및 전역 카탈로그 서버가 있는 네트워크와 통신할 수 있는지 확인합니다.

Active Directory에 더해 의 에이전트, 시스템 로그, SPAN 및 엔드포인트 프로브까지 사용하려면 조인 포인트를 생성해야 합니다.

Active Directory와 통합할 때 IPv6을 사용하려면 관련 ISE-PIC 노드에 대해 IPv6 주소를 구성했는지 확인해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Add(**추가**)**를 클릭하고 **Active Directory Join Point Name(Active Directory** 가입 포인트 이름**)** 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다. 자세한 내용은 표 1: Active Directory 조인 포인트 이름 설정 및 도메인 조인 창, 12 페이지의 내용을 참조하십시오.

단계 **3** **Submit(**제출**)**을 클릭합니다.

새로 생성하는 가입 포인트를 도메인에 가입시킬지를 묻는 팝업 메시지가 표시됩니다. 가입 포인트를 도메인에 즉시 가입시키려면 **Yes(**예**)**를 클릭합니다.

No(아니오**)**를 클릭하고 컨피그레이션을 저장하면 Active Directory 도메인 컨피그레이션이 전역적으로 저장되지만 Cisco ISE-PIC 노드가 도메인에 가입되지는 않습니다.

단계 **4** 새로 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**편집**)**. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다. 자세한 내용은 표 2: Active Directory 가입/탈퇴 창, 13 페이지의 내용을 참조하십시오.

단계 **5** 3단계를 진행하는 도중 가입 포인트가 도메인에 가입되지 않은 경우 관련 Cisco ISE-PIC 노드 옆의 확인란을 선택하고 **Join(**가입**)**을 클릭하여 Cisco ISE-PIC 노드를 Active Directory 도메인에 가입시킵니다.

컨피그레이션을 저장한 경우에도 이 작업을 명시적으로 수행해야 합니다. 단일 작업에서 도메인에 여러 Cisco ISE-PIC 노드를 가입시키려면 모든 가입 작업에 사용할 계정의 사용자 이름 및 비밀번호가 같아야 합니다. 각 Cisco ISE-PIC 노드를 가입시키는 데 필요한 사용자 이름 및 비밀번호가 다른 경우에는 각 Cisco ISE-PIC 노드에 대해 가입 작업을 개별적으로 수행해야 합니다.

단계 **6** **Join Domain(**도메인 가입**)** 대화 상자에서 Active Directory 사용자 이름 및 비밀번호를 입력합니다.

관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

가입 작업에 사용되는 사용자는 도메인 자체에 있어야 합니다. 사용자가 다른 도메인이나 하위 도메인에 있는 경우에는 jdoe@acme.com과 같이 UPN 표기법으로 사용자 이름을 표기해야 합니다.

단계 **7** (선택 사항) **Specify Organizational Unit(**조직 단위 지정**)** 확인란을 선택합니다.

CN=Computers,DC=someDomain,DC=someTLD 이외의 특정 조직 단위에 Cisco ISE-PIC 노드 머신 계정을 배치하려는 경우 이 확인란을 선택해야 합니다. Cisco ISE-PIC는 지정된 조직 단위에 머신 계정을 생성하거나, 머신 계정이 이미 있는 경우 이 위치로 이동합니다. 조직 단위를 지정하지 않으면 Cisco ISE-PIC에서는 기본 위치를 사용합니다. 값은 완전한 DN(Distinguished Name) 형식으로 지정해야 합니다. 구문은 Microsoft 지침을 따라야 합니다. /'+,;=<> 줄 바꿈, 공백, 캐리지 리턴 등의 특수 예약 문자는 백슬래시(\)로 이스케이프 처리해야 합니다. 예를 들면 OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 및 Workstations,DC=someDomain,DC=someTLD와 같습니다. 머신 계정이 이미 생성된 경우에는 이 확인란을 선택하지 않아도 됩니다. Active Directory 도메인에 가입한 후 머신 계정의 위치를 변경할 수도 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Active Directory 도메인에 가입시킬 노드를 두 개 이상 선택할 수 있습니다.

가입 작업이 실패하면 오류 메시지가 나타납니다. 각 노드에 대한 오류 메시지를 클릭하면 해당 노드의 상세 로그를 확인할 수 있습니다.

참고 조인이 완료되면 Cisco ISE-PIC는 자신의 AD 그룹과 대응하는 SIDS를 업데이트합니다. Cisco ISE-PIC는 SID 업데이트 프로세스를 자동으로 시작합니다. 이 프로세스를 완료할 수 있는지를 확인해야 합니다.

참고 DNS SRV 레코드가 없으면 Cisco ISE-PIC를 Active Directory 도메인에 가입시키지 못할 수도 있습니다. 가입시키려는 도메인에 대해 도메인 컨트롤러가 해당 SRV 레코드를 보급하지 않기 때문입니다. 문제 해결 정보는 다음 Microsoft Active Directory 설명서를 참조하십시오.

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

참고 ISE에서 최대 200개의 도메인 컨트롤러를 추가할 수 있습니다. 제한을 초과하면 "Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200(<DC FQDN> 생성 오류 - DC 수가 허용된 최대 200개를 초과)" 오류가 표시됩니다.

다음에 수행할 작업

도메인 컨트롤러 추가, 6 페이지

Active Directory 사용자 그룹 구성, 7 페이지

패시브 ID용 WMI 구성, 8 페이지

도메인 컨트롤러 추가

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다.

단계 **3** 참고 Passive Identity(패시브 ID) 서비스용으로 새 DC(Domain Controller)를 추가하려면 해당 DC의 로그인 자격 증명이 필요합니다.

PassiveID(패시브 ID) 탭으로 이동하여 **Add DCs(DC** 추가**)**를 클릭합니다.

단계 **4** 모니터링을 위해 조인트 포인트에 추가할 도메인 컨트롤러 옆의 확인란을 선택하고 **OK (**확인**)**를 클릭합니다. 도메인 컨트롤러는 PassiveID(패시브 ID) 탭의 Domain Controller(도메인 컨트롤러) 목록에 표시됩니다.

단계 **5** 도메인 컨트롤러를 구성합니다.

a) 도메인 컨트롤러에 체크 표시하고 **Edit(**수정**)**를 클릭합니다. **Edit Item(**항목 수정**)** 화면이 나타납니다.

b) 선택 사항으로, 다른 도메인 컨트롤러 필드를 수정합니다. 자세한 내용은 Active Directory 설정, 12 페이지를 참고하십시오.

c) WMI 프로토콜을 선택했다면 **Configure(**구성**)**를 클릭하여 WMI를 자동으로 구성하고 **Test(**테스트**)**를 클릭하여 연결을 테스트합니다. 자동으로 WMI를 구성하는 방법에 관한 자세한 내용은 패시브 ID용 WMI 구성, 8 페이지 항목을 참조하십시오.

DC 페일오버 메커니즘은 페일오버 시 DC가 선택되는 순서를 지정하는 DC 우선 순위 목록을 기반으로 관리됩니다. DC가 오프라인 상태이거나 오류 때문에 연결할 수 없다면 우선 순위 목록에서 우선

순위가 감소합니다. DC가 다시 온라인 상태가 되면 우선 순위 목록에서 우선 순위가 조정(증가)됩니다.

참고 Cisco ISE는 인증 플로우에 대해 읽기 전용 도메인 컨트롤러를 지원하지 않습니다.

Active Directory 사용자 그룹 구성

Active Directory에서 사용자 ID 정보를 수집하는 다른 프로브로 작업할 때 사용할 수 있도록 Active Directory 사용자 그룹을 구성합니다. Cisco ISE는 내부적으로 SID(Security Identifiers)를 사용하여 모호한 그룹 이름 문제를 해결하고 그룹 매핑을 개선합니다. SID를 통해 정확하게 일치하는 그룹을 할당할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**. 그룹을 추가할 조인 포인트를 클릭합니다.

단계 **2** **Groups(**그룹**)** 탭을 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) 다음 메뉴를 선택합니다. **Add(**추가**)** > **Select Groups From Directory(**디렉터리에서 그룹 선택**)** 그런 다음 기존 그룹을 선택합니다.

b) 다음 메뉴를 선택합니다. **Add(**추가**)** > **Add Group(**그룹 추가**)** 그런 다음 수동으로 그룹을 추가합니다. 그룹 이름과 SID를 모두 입력하거나, 그룹 이름만 입력하고 **Fetch SID(SID** 가져오기**)**를 누를 수 있습니다.

사용자 인터페이스 로그인 시 그룹 이름에 큰따옴표(")를 사용하지 마십시오.

단계 **4** 그룹을 수동으로 선택하는 경우 필터를 사용하여 그룹을 검색할 수 있습니다. 예를 들어 필터 기준으로 **admin***를 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭하면 admin으로 시작하는 사용자 그룹을 확인할 수 있습니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다. 그룹은 한 번에 500개만 검색할 수 있습니다.

단계 **5** 권한 부여 정책에서 사용 가능하도록 지정할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 그룹을 수동으로 추가하도록 선택하는 경우 새 그룹의 이름과 SID를 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고 그룹을 삭제하고 원본과 같은 이름으로 새 그룹을 생성하는 경우에는 **Update SID Values(SID** 값 업데이트**)**를 클릭하여 새로 생성한 그룹에 새 SID를 할당해야 합니다. 업그레이드 후 처음으로 가입하고 나면 SID가 자동으로 업데이트됩니다.

패시브 ID용 WMI 구성

시작하기 전에

AD 도메인 컨피그레이션을 변경하려면 Active Directory 도메인 관리자 자격 증명이 있어야 합니다. **Administration(**관리**) > System(**시스템**) > Deployment(**구축**)**에서 이 노드에 대해 패시브 ID가 활성화되었는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**) > Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다.

단계 **3** Passive ID(패시브 ID) 탭으로 이동하여 관련 도메인 컨트롤러 옆에 있는 확인란을 선택하고 **Config WMI(WMI** 구성**)**를 클릭하여 ISE-PIC가 선택한 도메인 컨트롤러를 자동으로 구성하게 합니다.
Active Directory 및 도메인 컨트롤러를 수동으로 구성하거나 구성 문제를 해결하는 방법은 Active Directory와 Cisco ISE-PIC 통합을 위한 사전 요건 항목을 참조하십시오.

Active Directory 제공자 관리

Active Directory 조인 포인트를 생성하고 구성했다면, 이러한 작업을 이용해 Active Directory 프로브를 관리해야 합니다.

- Test Users for Active Directory(Active Directory 인증을 위해 사용자 테스트)Groups(그룹), 8 페이지
- 노드의 Active Directory 가입 보기, 9 페이지
- Active Directory 문제 진단, 9 페이지
- Active Directory 도메인 탈퇴, 10 페이지
- Active Directory 컨피그레이션 삭제, 11 페이지
- Active Directory 디버그 로그 활성화, 11 페이지

Test Users for Active Directory(Active Directory 인증을 위해 사용자 테스트)Groups(그룹)

Test User(사용자 테스트) 도구를 사용하여 Active Directory에서 사용자 그룹을 확인할 수 있습니다. 단일 가입 포인트 또는 범위에 대해 테스트를 실행할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**) > Active Directory**.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 모든 가입 포인트에서 테스트를 실행하려면 **Advanced Tools(**고급 도구**) > Test User for All Join Points((**모든 가입 포인트에 대해 사용자 테스트**)**.

- 특정 가입 포인트에 대해 테스트를 실행하려면 해당 가입 포인트를 선택하고 **Edit(**편집**)**를 클릭합니다. Cisco ISE-PIC 노드를 선택하고 **Test User(**사용자 테스트**)**를 클릭합니다.

단계 **3** Active Directory에서 사용자 또는 호스트의 사용자 이름 및 비밀번호를 입력합니다.

단계 **4** 인증 유형을 선택합니다. Lookup(조회) 옵션을 선택하는 경우에는 3단계에서 비밀번호를 입력하지 않아도 됩니다.

단계 **5** 모든 가입 포인트에 이 테스트를 실행하는 경우 이 테스트를 실행할 Cisco ISE-PIC 노드를 선택합니다.

단계 **6** Active Directory에서 특성을 Retrieve Groups and Attributes(그룹과 특성 가져오기) 확인란을 선택합니다.

단계 **7** **Test(**테스트**)**를 클릭합니다.
테스트 작업의 결과 및 단계가 표시됩니다. 이러한 단계를 통해 실패 사유 및 문제 해결 상황을 파악할 수 있습니다.

Active Directory에서 각 처리 단계를 수행하는 데 걸린 시간(밀리초)을 볼 수도 있습니다. 작업을 수행한 시간이 임계값을 초과하면 Cisco ISE-PIC에서 경고 메시지가 표시됩니다.

노드의 **Active Directory** 가입 보기

Node View(노드 보기**)** 버튼(**Active Directory** 페이지)을 사용하면 지정된 Cisco ISE-PIC 노드에 대한 모든 Active Directory 가입 포인트의 상태나 모든 Cisco ISE-PIC 노드의 모든 가입 포인트를 확인할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Node View(**노드 보기**)**를 클릭합니다.

단계 **3** **ISE Node(ISE** 노드**)** 드롭다운 목록에서 노드를 선택합니다.
테이블에 노드별 Active Directory 상태가 나열됩니다. 구축에 가입 포인트와 Cisco ISE-PIC 노드가 여러 개 있는 경우 이 테이블이 업데이트되는 데 몇 분 정도 걸릴 수 있습니다.

단계 **4** 가입 포인트 **Name(**이름**)** 링크를 클릭하여 해당 Active Directory 가입 포인트로 이동한 후에 다른 특정 작업을 수행합니다.

단계 **5** **Diagnostic Summary(**진단 요약**)** 열에 있는 링크를 클릭하여 **Diagnostic Tools(**진단 도구**)** 페이지로 이동한 후에 특정 문제를 해결합니다. 진단 도구에는 노드당 각 가입 포인트에 대한 최신 진단 결과가 표시됩니다.

Active Directory 문제 진단

Diagnostic Tool(진단 도구)은 모든 Cisco ISE-PIC 노드에서 실행되는 서비스입니다. Active Directory 구축을 자동으로 테스트 및 진단할 수 있으며, 테스트 집합을 실행하여 Cisco ISE-PIC에서 Active Directory를 사용할 때 기능 또는 성능 오류를 발생시킬 수 있는 문제를 탐지할 수 있습니다.

Cisco ISE-PIC는 여러 이유로 Active Directory에 가입하거나 인증하지 못할 수 있습니다. 이 도구를 사용하면 Cisco ISE-PIC를 Active Directory에 연결하기 위한 사전 요구 사항을 올바르게 구성할 수 있습니다. 그리고 네트워킹, 방화벽 컨피그레이션, 클록 동기화, 사용자 인증 등의 문제를 탐지할 수 있습니다. 이 도구는 단계별 설명서 방식으로 작동하며, 필요한 경우 중간에 모든 레이어의 문제를 해결할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Advanced Tools(**고급 도구**)** 드롭다운을 클릭하고 **Diagnostic Tools(**진단 도구**)**를 선택합니다.

단계 **3** 진단을 실행할 Cisco ISE-PIC 노드를 선택합니다.

Cisco ISE-PIC 노드를 선택하지 않으면 모든 노드에서 테스트가 실행됩니다.

단계 **4** 특정 Active Directory 가입 포인트를 선택합니다.

Active Directory 가입 포인트를 선택하지 않으면 모든 가입 포인트에서 테스트가 실행됩니다.

단계 **5** 진단 보고서는 온디맨드 또는 예약 방식으로 실행할 수 있습니다.

- 테스트를 즉시 실행하려면 **Run Tests Now(**지금 테스트 실행**)**를 선택합니다.
- 예약된 간격으로 테스트를 실행하려면 **Run Scheduled Tests(**예약된 테스트 실행**)** 확인란을 선택하여 테스트를 실행할 시작 시간과 간격(시간, 일 또는 주)을 지정합니다. 이 옵션을 활성화하면 모든 진단 테스트가 모든 노드 및 인스턴스에서 실행되며, **Home(**홈**)** 대시보드의 **Alarms(**알람**)** 데슬렛에서 장애가 보고됩니다.

단계 **6** **View Test Details(**테스트 세부사항 보기**)**를 클릭하여 Warning(경고) 또는 Failed(장애) 상태의 테스트에 대한 세부사항을 확인합니다.
이 테이블을 참조하여 특정 테스트를 다시 실행하고, 실행 중인 테스트를 중지하고, 특정 테스트의 보고서를 확인할 수 있습니다.

Active Directory 도메인 탈퇴

이 Active Directory 도메인이나 이 조인 포인트를 사용하여 사용자 ID를 수집하거나, Active Directory 도메인에서 탈퇴할 수 있습니다.

명령줄 인터페이스에서 Cisco ISE-PIC 애플리케이션 컨피그레이션을 재설정하거나 백업 또는 업그레이드 이후 컨피그레이션을 복원하면 Cisco ISE는 탈퇴 작업을 수행하여 Cisco ISE-PIC 노드가 Active Directory 도메인에 이미 가입되어 있는 경우 해당 도메인에서 노드 연결을 끊습니다. 그러나 Cisco ISE-PIC 노드 계정은 Active Directory 도메인에서 제거되지 않습니다. 관리 포털에서 Active Directory 자격 증명을 사용하여 탈퇴 작업을 수행하는 것이 좋습니다. 이렇게 하면 Active Directory 도메인에서 노드 계정도 제거되기 때문입니다. Cisco ISE-PIC 호스트 이름을 변경할 때도 이 방법을 사용하는 것이 좋습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다. 자세한 내용은 표 2: Active Directory 가입/탈퇴 창, 13 페이지의 내용을 참조하십시오.

단계 **3** Cisco ISE-PIC 노드 옆의 확인란을 선택하고 **Leave(**탈퇴**)**를 클릭합니다.

단계 **4** Active Directory 사용자 이름 및 비밀번호를 입력하고 **OK(**확인**)**를 클릭하여 도메인을 탈퇴시킨 후 Cisco ISE-PIC 데이터베이스에서 머신 계정을 제거합니다.

Active Directory 자격 증명을 입력하는 경우 Active Directory 도메인에서 Cisco ISE-PIC 노드가 탈퇴되며 Active Directory 데이터베이스에서 Cisco ISE-PIC 머신 계정이 삭제됩니다.

참고 Active Directory 데이터베이스에서 Cisco ISE-PIC 머신 계정을 삭제하려면 여기서 입력하는 Active Directory 자격 증명에 도메인에서 머신 계정을 제거할 권한이 있어야 합니다.

단계 **5** Active Directory 자격 증명이 없는 경우에는 **No Credentials Available(**사용 가능한 자격 증명 없음**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

Leave domain without credentials(자격 증명을 사용하지 않고 도메인 탈퇴**)** 확인란을 선택하면 기본 Cisco ISE-PIC 노드가 Active Directory 도메인에서 탈퇴됩니다. 이 경우에는 Active Directory 관리자가 가입 시 Active Directory에서 생성된 머신 계정을 수동으로 제거해야 합니다.

Active Directory 컨피그레이션 삭제

특정 Active Directory 구성을 프로브로 사용하지 않으려는 경우 Active Directory 컨피그레이션을 삭제해야 합니다. 다른 Active Directory 도메인에 가입하려는 경우에는 컨피그레이션을 삭제하지 마십시오. 현재 가입되어 있는 도메인은 그대로 두고 새 도메인에 가입할 수 있습니다. 컨피그레이션이 다음에 있는 유일한 컨피그레이션이라면 삭제해선 안 됩니다. ISE-PIC

시작하기 전에

Active Directory 도메인이 남아 있는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 구성되어 있는 Active Directory 옆의 확인란을 선택합니다.

단계 **3** 로컬 노드 상태가 가입되지 않음으로 나열되어 있는지 확인합니다.

단계 **4** **Delete(**삭제**)**를 클릭합니다.

Active Directory 데이터베이스에서 컨피그레이션이 제거되었습니다. 나중에 Active Directory를 사용하려는 경우 유효한 Active Directory 컨피그레이션을 다시 제출하면 됩니다.

Active Directory 디버그 로그 활성화

Active Directory 디버그 로그는 기본적으로 기록되지 않습니다. Active Directory 디버그 로그를 활성화하는 경우 ISE-PIC 성능에 영향을 줄 수 있습니다.

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

단계 **2** Active Directory 디버그 정보를 가져올 Cisco ISE-PIC 노드 옆의 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** **Active Directory** 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 **4** Active Directory 옆의 드롭다운 목록에서 **DEBUG**를 선택합니다. 여기에는 오류, 경고 및 자세한 정보 표시 로그가 포함됩니다. 전체 로그를 가져오려면 **TRACE**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Active Directory 설정

Active Directory(AD)는 사용자 이름과 IP 주소 같은 사용자 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

조인 포인트를 생성하고 수정하여 Active Directory 프로브를 생성하고 관리하려면 **Providers(**제공자**)** > **Active Directory**.

자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입, 4 페이지를 참고하십시오.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** 그런 다음 수정할 조인 포인트를 체크한 다음 **Edit(**수정**)**를 클릭합니다. Join Domain(도메인 가입) 화면에서 **Providers(**제공자**)** > **Active Directory**를 선택한 다음 수정할 조인 포인트를 선택하고 **Join(**조인**)**을 클릭합니다.

표 ***1: Active Directory*** 조인 포인트 이름 설정 및 도메인 조인 창

필드 이름	설명
조인 포인트 이름	구성한 조인 포인트를 빠르고 쉽게 구분할 수 있는 고유한 이름입니다.
Active Directory 도메인	이 노드가 연결된 Active Directory 도메인의 도메인 이름입니다.
도메인 관리자	관리자 권한이 있는 Active Directory 사용자의 사용자 원이름 또는 사용자 계정 이름입니다.
비밀번호	Active Directory에 구성한 도메인 관리자의 암호입니다.
조직 단위 지정	관리자의 조직 단위 정보를 입력합니다.
자격 증명 저장	관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다. 엔드포인트 프로브의 경우에는 **Store credentials(**자격 증명 저장**)**를 반드시 선택해야 합니다.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory**.

표 ***2: Active Directory*** 가입/탈퇴 창

필드 이름	설명
ISE 노드	설치 내 특정 노드의 URL입니다.
ISE 노드 역할	노드가 설치 내 기본 노드인지 보조 노드인지를 나타냅니다.
상태	노드가 Active Directory 도메인에 적극적으로 가입했는지를 나타냅니다.
도메인 컨트롤러	Active Directory에 가입한 노드의 경우 이 열은 Active Directory 도메인에서 노드가 연결된 특정 도메인 컨트롤러를 나타냅니다.
사이트	전체 ISE 설치에만 적용됩니다. 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드를 참고하십시오.

표 ***3:*** 패시브 ***ID DC(***도메인 컨트롤러***)*** 목록

필드	설명
도메인	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름입니다.
DC 호스트	도메인 컨트롤러가 있는 호스트입니다.
사이트	전체 ISE 설치에만 적용됩니다. 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드를 참고하십시오.
IP 주소	도메인 컨트롤러의 IP 주소.
모니터링	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이저트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트 항목을 참조하십시오.

표 ***4:*** 패시브 ***ID DC(Domain Controller,*** 도메인 컨트롤러***)*** 편집 화면

필드 이름	설명
호스트 **FQDN**	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름을 입력합니다.
설명	쉽게 식별할 수 있도록 이 도메인 컨트롤러에 관한 고유한 설명을 입력합니다.
사용자 이름	Active Directory에 액세스하는 데 사용하는 관리자의 사용자 이름입니다.
비밀번호	Active Directory에 액세스하는 데 사용하는 관리자의 암호입니다.
프로토콜	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이저트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트 항목을 참조하십시오.

Active Directory 그룹은 Active Directory에서 정의하고 관리하며, 이 탭에서는 이 노드에 가입한 Active Directory의 그룹을 확인할 수 있습니다. Active Directory에 관한 자세한 내용은 https://msdn.microsoft.com/en-us/library/bb742437.aspx 항목을 참조하십시오.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** > **Advanced Settings(**고급 설정**)**.

표 ***5: Active Directory*** 고급 설정

필드 이름	설명
기록 간격	이미 수행된 사용자 로그인 정보를 패시브 ID 서비스에서 읽는 시간입니다. 패시브 ID 서비스를 시작하거나 재시작할 때 서비스를 사용할 수 없었던 시간 동안 생성된 이벤트를 확인하려면 이 시간을 설정해야 합니다. 활성 상태인 엔드포인트 프로브는 이 간격의 빈도를 유지합니다.

필드 이름	설명
사용자 세션 에이징 타임	사용자가 로그인할 수 있는 시간입니다. 패시브 ID 서비스는 DC에서 새 사용자 로그인 이벤트를 식별하지만, DC는 사용자가 로그오프할 때는 보고하지 않습니다. 에이징 시간을 설정하면 ISE-PIC는 사용자가 로그인되어 있는 시간 간격을 확인할 수 있습니다.
NTLM 프로토콜 설정	ISE-PIC와 DC 간의 통신 프로토콜로는 NTLMv1 또는 NTLMv2를 선택할 수 있습니다. NTLMv2rk 권장 기본값입니다.