CA SiteMinder Federation Standalone

Agent for Windows Authentication 안내서

r12.52 SP1

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide 에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

CA SiteMinder?Federation Standalone 의 이전 릴리스에서 발견된 문제점으로 인해 12.52 설명서에서 업데이트된 내용은 없습니다.

목차

제 1 장: Federation Agent for Windows Authentication 소개

Federation Agent for Windows 개요

Federation Agent for Windows Authentication 을 사용하는 사용자는 시스템에 IWA(Windows 통합 인증) 프로토콜 중 하나를 구현하여 비즈니스 파트너와 페더레이션할 수 있습니다.

사용자가 보호된 리소스에 대한 액세스를 요청하면 페더레이션 시스템은 타사 WAM(웹 액세스 관리) 시스템의 로그온 아이덴티티 정보를 사용합니다. 이와 같이 타사 WAM 을 사용하는 프로세스를 위임된 인증이라고 합니다. 페더레이션 시스템은 요청을 Federation Agent 로 리디렉션합니다. Federation Agent 는 사용자 아이덴티티를 확인하고, 개방형 쿠키를 생성하고, 쿠키를 페더레이션 시스템에 전달합니다. 그러면 페더레이션 시스템은 SAML 어설션을 생성하여 신뢰 당사자에게 전달합니다.

참고: 위임된 인증에 대한 자세한 내용은 *Federation Standalone 안내서*를 참조하십시오.

IWA 는 Windows NTLM(NT LAN Manager) 및 Kerberos 암호화 프로토콜을 지원합니다. Windows 시스템에서 Federation Agent 는 NTLM 또는 Kerberos 를 사용할 수 있습니다. UNIX 시스템에서 Federation Agent 는 Kerberos 만 사용할 수 있습니다.

Federation Agent 는 CA SiteMinder?Federation Standalone 이 설치된 것과 동일한 Windows 또는 UNIX 시스템에 설치됩니다. 다음 제한이 적용됩니다.

- Federation Agent 는 SiteMinder 커넥터를 사용하는 페더레이션 설치와 호환되지 않습니다.
- SSO(싱글 사인온) 요청을 실행하는 브라우저는 페더레이션 시스템과 동일한 시스템에 있으면 안 됩니다.

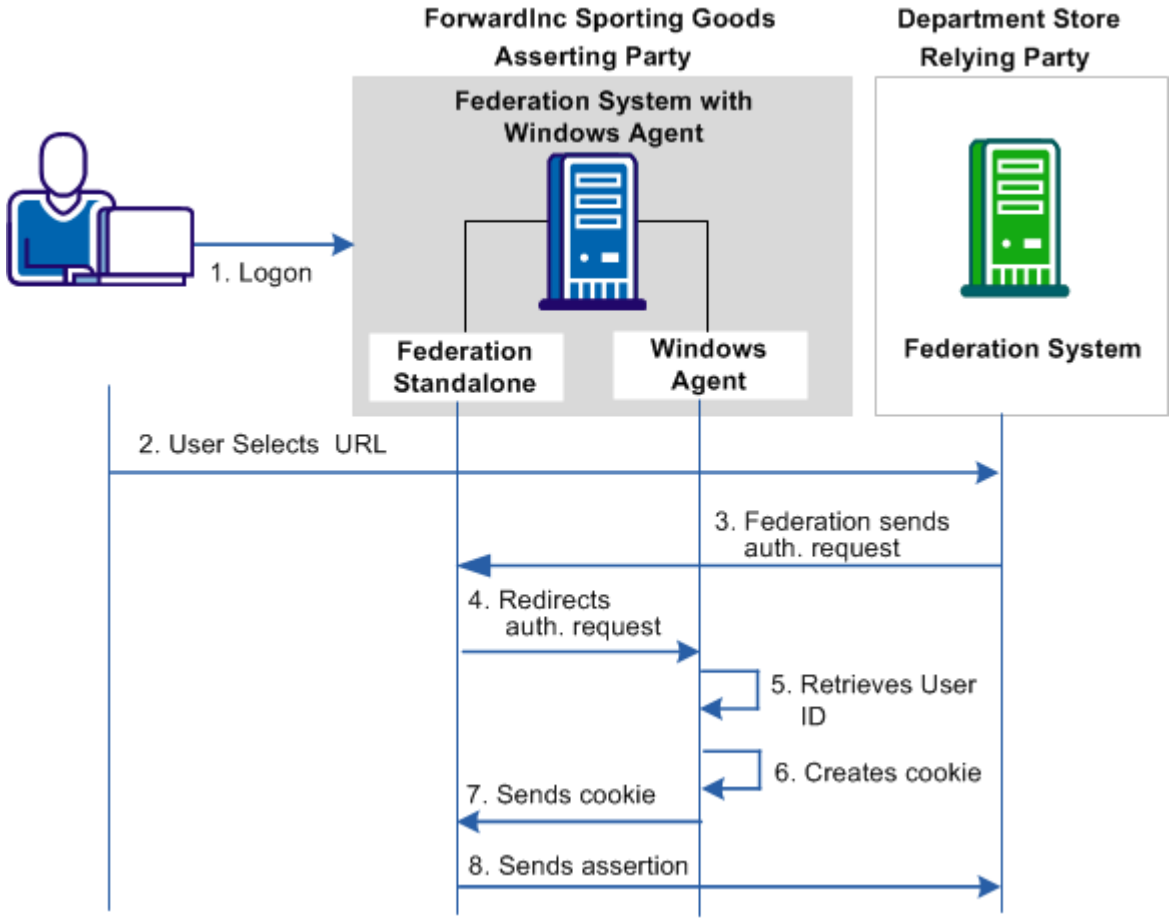
관리자는 Windows 통합 인증 프로토콜(NTLM 및 Kerberos)에 대한 지식이 있어야 합니다. 페더레이션 개념과 CA SiteMinder?Federation Standalone 관리에 대해서도 잘 알고 있어야 합니다.

IWA 를 사용하는 시스템과 비즈니스 파트너 사이의 SSO

위임된 인증 사용 사례에서는 Federation Agent 의 작동 방식을 보여 줍니다. 이 사용 사례에서 한 백화점은 공급업체인 ForwardInc Sporting Goods 의 직원에게 싱글 사인온 액세스 권한을 부여하여 특별 할인을 제공하려고 합니다.

이 백화점 및 ForwardInc Sporting Goods 는 페더레이션된 파트너 관계가 있습니다. ForwardInc Sporting Goods 의 직원은 주로 도메인 사용자 이름과 암호를 사용하여 회사 계정에 로그인합니다. 직원이 이 백화점 웹 사이트를 방문할 때는 인증 요청 없이 IWA 프로토콜 중 하나를 통해 액세스 권한을 부여받습니다.

다음 그림에서는 페더레이션된 파트너 관계에서 Federation Agent 의 역할을 보여 줍니다.



다이어그램에 표시된 트랜잭션은 다음과 같습니다.

1. 사용자가 ForwardInc Sporting Goods 의 WAM(웹 액세스 관리) 시스템에 로그인합니다.
2. 사용자가 브라우저를 열고 신뢰 당사자인 이 백화점의 URL 로 이동합니다.

   참고: 브라우저는 Windows Agent 가 설치된 페더레이션 시스템과 동일한 시스템에 있으면 안 됩니다.
3. 신뢰 당사자가 어설션 당사자로 인증 요청을 보냅니다. 어설션 당사자의 페더레이션 시스템은 이 파트너 관계에 대해 위임된 인증이 구성되었음을 파악합니다.
4. 페더레이션 시스템은 요청을 Federation Agent 로 보냅니다. 에이전트는 사용자에 대한 보안 컨텍스트의 유효성을 검사합니다.
5. Windows Agent 는 이 요청에서 유효성 검사된 정보를 추출합니다.
6. Windows Agent 는 사용자 정보를 개방 형식 쿠키에 저장합니다.
7. Windows Agent 는 쿠키를 페더레이션 시스템으로 보냅니다.
8. 어설션 당사자의 페더레이션 시스템은 사용자 정보를 추출하여 어설션에 저장한 다음 이 어설션을 신뢰 당사자에게 전달합니다.

사용자는 로그인 없이 이 백화점 웹 사이트에 액세스할 수 있게 됩니다.

용어

이 안내서에서는 Windows 인증과 관련하여 다음과 같은 용어를 사용합니다.

인증 서버(AS)

인증 서버는 KDC(Key Distribution Center)의 일부로, 클라이언트의 초기 인증 요청에 응답합니다. 사용자가 인증되면 인증 서버는 TGT(Ticket Granting Ticket)를 발급합니다. TGT 를 사용하여 사용자는 암호를 다시 입력하지 않고도 다른 Kerberos 서비스 티켓을 얻을 수 있습니다.

IWA(Windows 통합 인증)

Windows 통합 인증은 Windows 클라이언트 응용 프로그램에 사용자 로그온 자격 증명의 인증 정보를 제공합니다. 인증 교환에서 사용자를 식별하지 못하는 경우 브라우저에서 Windows ID 와 암호를 묻는 메시지를 표시합니다. Windows 통합 인증은 표준 또는 인증 프로토콜이 아니며 Kerberos 또는 NTLM 프로토콜을 사용합니다.

Kerberos

Kerberos 인증 프로토콜을 사용하면 네트워크를 통해 안전하게 통신할 수 있습니다. Kerberos 는 MIT(Massachusetts Institute of Technology)에서 발표한 무료 소프트웨어 제품군을 의미하기도 하며, 이 소프트웨어에서는 Kerberos 프로토콜이 구현됩니다. Kerberos 는 티켓을 사용하여 사용자 아이덴티티를 확인합니다. Kerberos 프로토콜 메시지는 도청 및 재생 공격으로부터 보호됩니다. Kerberos 는 대칭 키 암호화를 기반으로 구축되며 트러스트된 타사 Key Distribution Center 가 필요합니다.

KDC(Key Distribution Center)

Key Distribution Center 는 암호화 시스템의 일부로, 인증 서버 및 TGS(Ticket Granting Server)를 포함합니다. Key Distribution Center 의 용도는 키 교환 시 내재된 위험을 줄이는 것입니다. Key Distribution Center 는 일부 사용자가 특정 서비스를 특정 시점에만 사용할 수 있고 그 외에는 사용할 수 없는 시스템에서 작동되는 경우가 많습니다.

Keytab

Keytab 은 Kerberos 프린서펄과 Kerberos 암호에서 파생된 암호화된 키가 쌍으로 구성되어 있는 파일입니다. 이 파일은 Key Distribution Center 에 로그인하는 데 사용됩니다.

NTLM

NTLM 은 싱글 사인온을 위한 다양한 Microsoft 네트워크 구현에서 사용되는 인증 프로토콜입니다. NTLM 은 인증을 위해 챌린지-응답 메커니즘을 사용합니다. 이 메커니즘에서는 클라이언트가 서버에 암호를 보내지 않고 자신의 아이덴티티를 증명합니다. NTLM 은 일반적으로 유형 1(협상), 유형 2(챌린지) 및 유형 3(인증)이라고 하는 세 가지 메시지로 구성됩니다. 유형 3 메시지의 응답은 클라이언트 사용자가 계정 암호를 알고 있음을 서버에 증명하는 것이므로 가장 중요합니다.

TGT(Ticket Granting Ticket)

TGT(Ticket Granting Ticket)는 암호화된 작은 ID 파일로, 유효 기간이 제한되어 있습니다. 인증 후 KDC 인증 서버가 데이터 트래픽 보호를 위해 이 파일을 사용자에게 발급합니다. TGT 파일에는 세션 키, 티켓의 만료 날짜 및 사용자 IP 주소가 포함됩니다.

TGS(Ticket Granting Server)

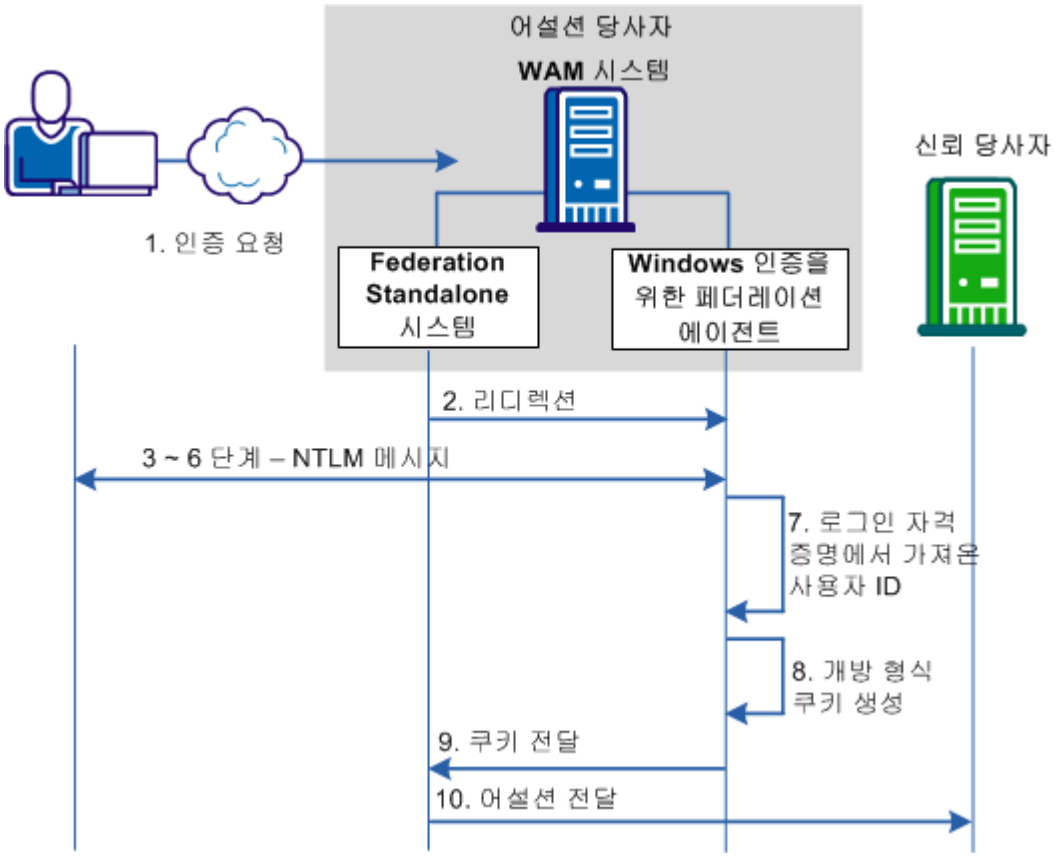
Ticket Granting Server 는 유효한 TGT 가 있는 클라이언트에 서비스 티켓을 배포하는 KDC 구성 요소입니다. Ticket Granting Server 는 응용 프로그램 서버와 마찬가지로 티켓을 서비스로 발급합니다.

NTLM 프로토콜

NTLM 에는 다양한 인증 및 세션 보안 프로토콜이 포함되어 있습니다. NTML 은 챌린지-응답 모델을 기반으로 하며, 이 모델에서는 세 가지 유형의 메시지가 다음과 같은 순서로 교환됩니다.

1. 클라이언트가 유형 1 메시지(협상)를 서버에 보냅니다. 유형 1 메시지는 클라이언트가 지원하는 기능을 지정하고 서버에 요청합니다.
2. 서버가 유형 2 메시지(챌린지)를 클라이언트에 보냅니다. 이 메시지의 기본 기능은 클라이언트 사용자의 아이덴티티를 요청하는 것입니다.
3. 클라이언트가 유형 3 메시지(인증)를 서버에 보냅니다. 유형 3 메시지는 클라이언트 사용자의 사용자 이름 및 도메인을 포함하며 유형 2 메시지의 챌린지에 응답합니다.

다음 그림은 페더레이션 시스템이 Federation Agent 와 함께 NTLM 프로토콜을 사용하는 방법을 보여 줍니다.



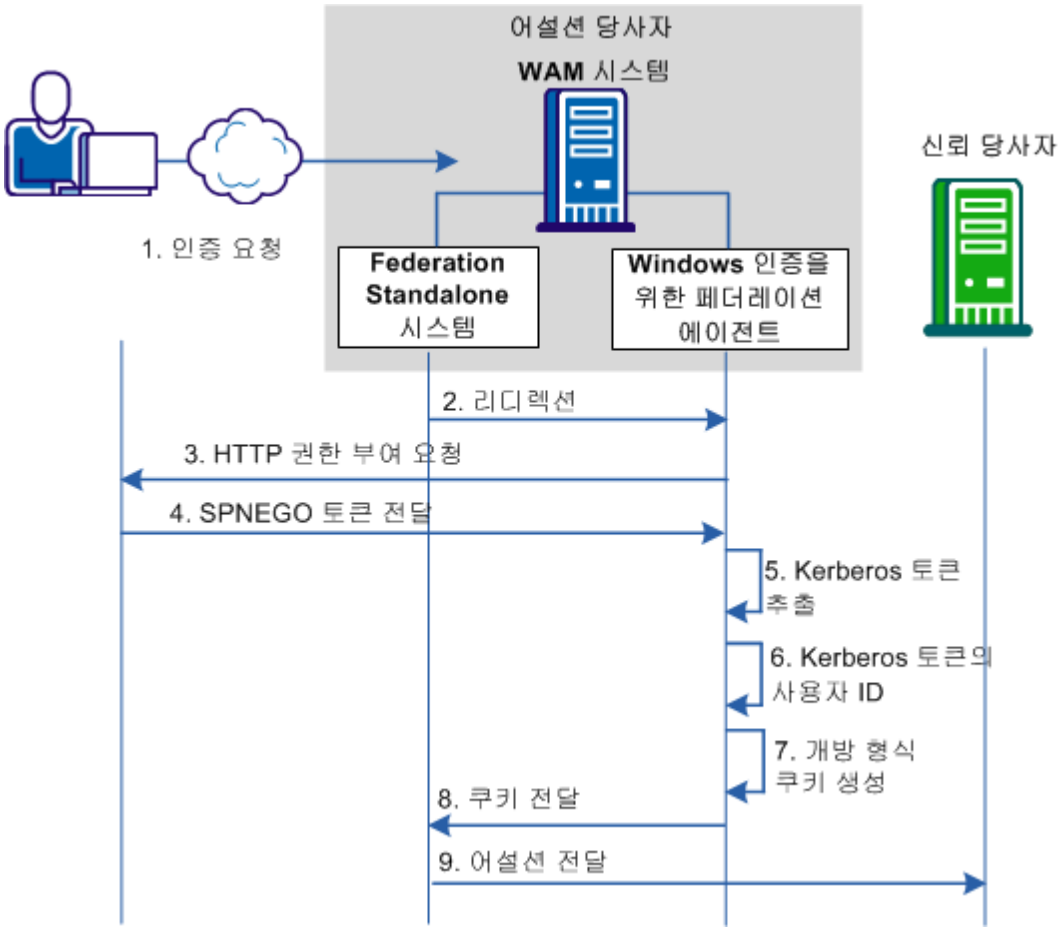
다음 프로세스에서는 앞의 다이어그램에 있는 주석을 참조합니다.

1. 어설션 당사자의 페더레이션 시스템에 대해 인증 요청을 보냅니다.
2. 페더레이션 시스템이 이 요청을 위임된 인증 요청으로 인식하고 Federation Agent 로 리디렉션합니다.
3. Federation Agent 가 응답을 브라우저에 다시 보냅니다.
4. 브라우저가 IWA 를 사용하도록 구성된 경우 브라우저는 권한 부여 헤더의 NTLM 협상 토큰(유형 1 메시지)을 Federation Agent 에 보냅니다.
5. Federation Agent 가 NTLM 챌린지 토큰(유형 2 메시지)을 브라우저에 보냅니다.
6. 브라우저가 NTLM 인증 토큰(유형 3 메시지)을 Federation Agent 에 보냅니다.

7. 보안 컨텍스트가 사용자에 연결된 경우 Federation Agent 가 설정된 컨텍스트에서 사용자 아이덴티티를 검색합니다.
8. 에이전트가 사용자 아이덴티티 정보를 포함하는 개방 형식 쿠키를 생성합니다.
9. Federation Agent 가 쿠키를 페더레이션 시스템으로 보냅니다.
10. 페더레이션 시스템이 어설션을 신뢰 당사자에게 보내 페더레이션 처리를 완료합니다.

Kerberos 프로토콜

다음 그림은 페더레이션 시스템이 Federation Agent 와 함께 Kerberos 프로토콜을 사용하는 방법을 보여 줍니다.



다음 프로세스에서는 앞의 다이어그램에 있는 주석을 참조합니다.

1. 어설션 당사자의 페더레이션 시스템에 대해 인증 요청을 보냅니다.

   페더레이션 시스템이 이 요청을 위임된 인증 요청으로 인식합니다.

2. 페더레이션 시스템은 Federation Agent 로 리디렉션됩니다.
3. Federation Agent 가 브라우저에서 HTTP 권한 부여를 요청합니다.
4. 브라우저가 IWA 를 사용하도록 구성된 경우 SPNEGO 토큰을 Federation Agent 에 보냅니다. 이 토큰을 사용하여 이니시에이터와 승인자는 Kerberos 를 사용할지 또는 NTLM 을 사용할지 협상할 수 있습니다.
5. Federation Agent 가 SPNEGO 토큰에서 Kerberos 토큰을 추출합니다.
6. Kerberos 토큰을 통해 보안 컨텍스트가 설정되고 나면 에이전트가 사용자 아이덴티티 정보를 검색합니다.
7. 에이전트가 개방 형식 쿠키를 생성하고 리디렉션 URL 을 작성합니다.
8. Federation Agent 가 쿠키를 페더레이션 시스템으로 보냅니다.
9. 페더레이션 시스템이 필요한 처리를 수행하여 어설션을 신뢰 당사자에게 보냅니다.

제 2 장: Federation Agent for Windows 에 대한 설치 사전 요구 사항

Federation Agent for Windows 인증은 설치된 동일한 Windows 또는 UNIX 시스템에 설치하십시오. 다음 제한이 적용됩니다.

- Federation Agent 는 CA SiteMinder® 커넥터를 사용하는 페더레이션 설치와 호환되지 않습니다.
- SSO(싱글 사인온) 요청을 실행하는 브라우저는 페더레이션 서버와 동일한 시스템에 있을 수 없습니다.

CA SiteMinder?Federation Windows Agent 의 경우 선택하는 인증 프로토콜에 따라 다음 세 가지 작동 모드가 있습니다.

- NTLM 모드(Windows 에서만 지원)
- Kerberos 모드(Windows 및 UNIX 에서 지원)
- NTLM 에 대한 장애 조치가 적용되는 Kerberos 모드(Windows 에서만 지원)

에이전트 구성 마법사를 실행할 때 운영 모드를 선택합니다.

Federation Windows Agent 의 설치 프로세스는 다음 단계로 구성됩니다.

1. 작동 모드 및 운영 환경에 따라 다음과 같이 다양한 설치 사전 요구 사항을 완료하십시오.
   - Windows 기반 에이전트에서 NTLM 사용
   - Windows 기반 에이전트 및 Windows 기반 KDC 에서 Kerberos 사용
   - Windows 기반 에이전트 및 UNIX 기반 KDC 에서 Kerberos 사용
   - UNIX 기반 에이전트 및 Windows 기반 KDC 에서 Kerberos 사용
   - UNIX 기반 에이전트 및 UNIX 기반 KDC 에서 Kerberos 사용
2. Federation Agent for Windows 를 설치합니다.
3. Federation Agent for Windows 를 구성합니다. (페이지 35)
4. 페더레이션 시스템에 대한 위임된 인증을 구성합니다.

Windows 시스템의 NTLM 모드

NTLM 을 사용하여 Windows 시스템에 Federation Windows Agent 를 설치하기 전에 설치 사전 요구 사항을 완료하십시오.

1. Windows 에서 NTLM 에 대한 도메인 컨트롤러를 설정합니다.
2. Internet Explorer 설정을 구성합니다.

Windows 에서 NTLM 에 대한 도메인 컨트롤러 설정

Windows 2003 SP 1 Active Directory 는 Windows 도메인의 주 도메인 컨트롤러입니다. 이 호스트는 사용자, 서비스 계정, 자격 증명 및 Windows 도메인 서비스에 대한 저장소를 제공합니다.

Federation Agent 는 신뢰 당사자가 보낸 NTML 챌린지 메시지에 대한 NTLM 응답 메시지를 생성합니다. 신뢰 당사자의 서버는 챌린지 및 응답을 도메인 컨트롤러에 전달합니다. 응답은 사용자 암호의 해시를 사용하여 암호화된 챌린지 버전입니다. 도메인 컨트롤러는 암호의 동일한 해시를 사용하여 챌린지를 암호화하고 어설션 당사자 측에서 생성된 응답과 비교합니다. 일치하는 경우 인증이 완료됩니다. 도메인 컨트롤러가 신뢰 당사자의 서버에 알려줍니다.

다음 단계를 수행하십시오.

1. Windows dcpromo 유틸리티를 사용하여 Windows 2003 SP 1 서버를 도메인 컨트롤러로 승격합니다.
2. "관리 도구"에서 "Active Directory 사용자 및 컴퓨터" 대화 상자를 엽니다.
3. "사용자 계정 만들기"를 선택합니다.
4. 이 계정을 생성하기 위한 암호를 입력합니다.
5. "다음 로그온할 때 반드시 암호 변경" 옵션을 선택 취소합니다.

NTLM 에 대한 도메인 컨트롤러가 배포됩니다.

Internet Explorer 에서 싱글 사인온을 구성하십시오. 이 절차는 인증 프로토콜로 NTLM 또는 Kerberos 를 사용하는지 여부에 관계 없이 적용됩니다.

추가 정보:

Internet Explorer 구성 설정 (페이지 25)

Windows KDC 를 사용하는 Windows 시스템에 대한 Kerberos 모드

Kerberos 모드를 사용하는 Windows 시스템에서 Federation Agent 에 대한 설치 사전 요구 사항을 완료하십시오. KDC 는 Windows 시스템에 있습니다. Windows 에서 Kerberos 에 대한 도메인 컨트롤러를 설정합니다.

1. Windows 에서 Kerberos 에 대한 도메인 컨트롤러를 설정합니다.
2. Windows 에서 Kerberos 에 대한 추가 구성 완료
3. Internet Explorer 설정 구성

Windows 의 도메인 컨트롤러에서 Kerberos 설정

Kerberos 를 사용할 경우 도메인 컨트롤러는 Kerberos 영역에 대한 KDC(Key Distribution Centre)가 됩니다. 순수한 Windows 2003 환경에서는 Kerberos 영역이 Windows 도메인에 해당합니다. 도메인 컨트롤러 호스트는 사용자, 서비스 계정, 자격 증명, Kerberos 티켓 서비스 및 Windows 도메인 서비스에 대한 저장소를 제공합니다.

Kerberos 인증에는 keytab 파일이 필요합니다. 이 경우 사용자는 암호를 입력할 필요 없이 KDC 로 사용자를 인증하여 페더레이션 시스템에 로그온할 수 있습니다. keytab 파일은 ktpass 유틸리티를 사용하여 생성합니다. ktpass 명령 도구 유틸리티는 Windows 지원 도구입니다. 기본 암호화 유형은 RC4-HMAC-NT 입니다. 암호화 유형은 명령 프롬프트에서 **ktpass /?**를 실행하여 확인할 수 있습니다. 또한 Kerberos 버전 번호를 확인하십시오.

다음 단계를 수행하십시오.

1. Windows dcpromo 유틸리티를 사용하여 Windows 2003 SP 1 서버를 도메인 컨트롤러로 승격합니다.
2. "관리 도구"에서 "Active Directory 사용자 및 컴퓨터" 대화 상자를 엽니다.
3. "사용자 계정 만들기"를 선택합니다.

4. 이 계정에 대한 암호를 입력합니다.
5. "다음 로그온할 때 반드시 암호 변경" 옵션을 선택 취소합니다.
6. Windows 2003 워크스테이션 계정을 서버 프린서펄 이름(예: HTTP/IWAConnectorHostName.idp.com@IDP.COM)과 연결합니다.
7. 명령 프롬프트 창을 열고 다음 명령을 입력하여 keytab 파일을 만듭니다.

   ktpass -out *output_keytab_location* -princ *SPN_name* -ptype KRB5_NT_PRINCIPAL -mapuser *username* -pass *password*

   4 단계에서 입력한 암호를 사용하십시오.

   Keytab 파일이 생성됩니다.

   예를 들면 다음과 같습니다.

   ```
   ktpass -out c:\workstation.keytab -princ HTTP/
   IWAConnectorHostName.idp.com@IDP.COM
   -ptype KRB5_NT_PRINCIPAL -mapuser testkrb -pass password
   Targeting domain controller: winkdc.idp.com
   Using legacy password setting method
   Successfully mapped HTTP/ IWAConnectorHostName.idp.com to testkrb.
   Key created.
   Output keytab to c:\workstation.keytab:
   Keytab version: 0x502
   keysize 67 HTTP/ IWAConnectorHostName.idp.com@IDP.COM ptype 1 (KRB5_NT_PRINCIPAL)
   vno 2 etype 0x17 (RC4-HMAC) keylength 16 (0xfd77a26f1f5d61d1fafd67a2d88784c7)
   ```

8. 어설션 당사자의 페더레이션 시스템에서 안전한 위치로 keytab 파일을 복사합니다.

   중요! Federation Agent 를 구성할 때 keytab 이름과 전체 경로를 "Keytab Location"(Keytab 위치) 필드에 지정해야 합니다.

Windows 를 실행하는 시스템에 Kerberos 에 대한 도메인 컨트롤러가 배포됩니다.

Windows 에서 Kerberos 에 대한 추가 구성 완료

Windows 에서 Kerberos 를 사용할 경우 페더레이션 시스템에서 다음 작업을 수행해야 합니다.

1. Kerberos 구성 파일(krb5.ini)을 구성합니다. Windows 시스템 루트 경로에 krb5.ini 파일을 넣습니다.
   a. Windows 2003 도메인 컨트롤러를 사용하도록 Windows 2003 Kerberos 영역(도메인)에 대한 KDC 를 구성합니다.
   b. 워크스테이션 프린서펄의 자격 증명이 포함된 Windows 2003 KDC keytab 파일을 사용하도록 krb5.ini 를 구성합니다.

```
[libdefaults]
default_realm = IDP.COM
default_keytab_name = C:\WINDOWS\krb5.keytab
default_tkt_enctypes = des-cbc-md5 rc4-hmac
default_tgs_enctypes = des-cbc-md5 rc4-hmac
[realms]
IDP.COM = {
kdc = winkdc.idp.com:88
default_domain = IDP.COM
}
[domain_realm]
.idp.com = IDP.COM
```

2. krb5.ini 에 대해 설명한 대로 Windows 2003 KDC keytab 파일을 안전한 위치에 배포합니다.

Internet Explorer 에서 싱글 사인온을 구성하십시오. 이 절차는 인증 프로토콜로 NTLM 또는 Kerberos 를 사용하는지 여부에 관계 없이 적용됩니다.

추가 정보:

Internet Explorer 구성 설정 (페이지 25)

UNIX KDC 를 사용하는 Windows 시스템에 대한 Kerberos 모드

Kerberos 모드에서 Windows 를 실행하는 시스템에서 Federation Agent 에 대한 설치 사전 요구 사항을 완료하십시오. KDC 는 UNIX 시스템에 있습니다.

1. UNIX 시스템에서 KDC 를 구성합니다.
2. Windows 에서 Kerberos 에 대한 추가 구성을 완료합니다.
3. Internet Explorer 설정을 구성합니다.

UNIX 시스템에서 KDC 구성

Kerberos KDC(Key Distribution Center)를 호스트하는 UNIX 서버는 페더레이션 시스템을 지원하도록 구성해야 합니다. 이 프로세스의 일부는 keytab 파일을 만들기 위한 것입니다. Kerberos 인증에는 keytab 파일이 필요합니다.

다음 단계를 수행하십시오.

1. 명령 프롬프트 창을 엽니다.
2. 명령줄 프롬프트에 다음 명령을 입력합니다.

   ```
   usr/sbin/kadmin.local
   ```

3. 다음 명령으로 CA SiteMinder® Federation Standalone 시스템 서비스 프린서펄 이름을 추가합니다.

   ```
   addprinc -pw <password> HTTP/AgentHost Name.domainname.com@DOMAINNAME.COM
   ```

4. 명령 프롬프트 창을 열고 다음 명령을 입력하여 keytab 파일을 만듭니다.

   ```
   ktadd -k output_keytab_location SPN name
   ```

   Keytab 파일이 생성됩니다.

5. quit 를 입력합니다.

UNIX KDC 서버에서 페더레이션 구성이 완료되었습니다.

UNIX 에서 Kerberos 에 대한 추가 구성 완료

Kerberos 를 구성하려면 UNIX 시스템의 페더레이션 시스템에 대해 다음 명령이 필요합니다.

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

Kerberos 인증을 사용하도록 UNIX 시스템이 구성되었습니다.

Internet Explorer 에서 싱글 사인온을 구성하십시오. 이 절차는 인증 프로토콜로 NTLM 또는 Kerberos 를 사용하는지 여부에 관계 없이 적용됩니다.

추가 정보:

Internet Explorer 구성 설정 (페이지 25)

Windows KDC 를 사용하는 UNIX 시스템에 대한 Kerberos 모드

Kerberos 모드로 실행되는 UNIX 시스템에서 Federation Agent 설치를 위한 사전 요구 사항을 완료하십시오. KDC 는 Windows 시스템에 있습니다.

1. Windows 에서 Kerberos 에 대한 도메인 컨트롤러를 설정합니다.
2. UNIX 에서 Kerberos 에 대한 추가 구성을 수행합니다.
3. Internet Explorer 설정을 구성합니다.

Windows 의 도메인 컨트롤러에서 Kerberos 설정

Kerberos 를 사용할 경우 도메인 컨트롤러는 Kerberos 영역에 대한 KDC(Key Distribution Centre)가 됩니다. 순수한 Windows 2003 환경에서는 Kerberos 영역이 Windows 도메인에 해당합니다. 도메인 컨트롤러 호스트는 사용자, 서비스 계정, 자격 증명, Kerberos 티켓 서비스 및 Windows 도메인 서비스에 대한 저장소를 제공합니다.

Kerberos 인증에는 keytab 파일이 필요합니다. 이 경우 사용자는 암호를 입력할 필요 없이 KDC 로 사용자를 인증하여 페더레이션 시스템에 로그온할 수 있습니다. keytab 파일은 ktpass 유틸리티를 사용하여 생성합니다. ktpass 명령 도구 유틸리티는 Windows 지원 도구입니다. 기본 암호화 유형은 RC4-HMAC-NT 입니다. 암호화 유형은 명령 프롬프트에서 **ktpass /?**를 실행하여 확인할 수 있습니다. 또한 Kerberos 버전 번호를 확인하십시오.

다음 단계를 수행하십시오.

1. Windows dcpromo 유틸리티를 사용하여 Windows 2003 SP 1 서버를 도메인 컨트롤러로 승격합니다.
2. "관리 도구"에서 "Active Directory 사용자 및 컴퓨터" 대화 상자를 엽니다.
3. "사용자 계정 만들기"를 선택합니다.
4. 이 계정에 대한 암호를 입력합니다.
5. "다음 로그온할 때 반드시 암호 변경" 옵션을 선택 취소합니다.
6. Windows 2003 워크스테이션 계정을 서버 프린서펄 이름(예: HTTP/IWAConnectorHostName.idp.com@IDP.COM)과 연결합니다.
7. 명령 프롬프트 창을 열고 다음 명령을 입력하여 keytab 파일을 만듭니다.

   ```
   ktpass -out output_keytab_location -princ SPN_name -ptype
   KRB5_NT_PRINCIPAL -mapuser username -pass password
   ```

   4 단계에서 입력한 암호를 사용하십시오.

   Keytab 파일이 생성됩니다.

예를 들면 다음과 같습니다.

```
ktpass -out c:\workstation.keytab -princ HTTP/
IWAConnectorHostName.idp.com@IDP.COM
-ptype KRB5_NT_PRINCIPAL -mapuser testkrb -pass password
Targeting domain controller: winkdc.idp.com
Using legacy password setting method
Successfully mapped HTTP/ IWAConnectorHostName.idp.com to testkrb.
Key created.
Output keytab to c:\workstation.keytab:
Keytab version: 0x502
keysize 67 HTTP/ IWAConnectorHostName.idp.com@IDP.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype 0x17 (RC4-HMAC) keylength 16 (0xfd77a26f1f5d61d1fafd67a2d88784c7)
```

8. 어설션 당사자의 페더레이션 시스템에서 안전한 위치로 keytab 파일을 복사합니다.

   중요! Federation Agent 를 구성할 때 keytab 이름과 전체 경로를 "Keytab Location"(Keytab 위치) 필드에 지정해야 합니다.

Windows 를 실행하는 시스템에 Kerberos 에 대한 도메인 컨트롤러가 배포됩니다.

UNIX 에서 Kerberos 에 대한 추가 구성 완료

Kerberos 를 구성하려면 UNIX 시스템의 페더레이션 시스템에 대해 다음 명령이 필요합니다.

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

Kerberos 인증을 사용하도록 UNIX 시스템이 구성되었습니다.

Internet Explorer 에서 싱글 사인온을 구성하십시오. 이 절차는 인증 프로토콜로 NTLM 또는 Kerberos 를 사용하는지 여부에 관계 없이 적용됩니다.

추가 정보:

Internet Explorer 구성 설정 (페이지 25)

UNIX KDC 를 사용하는 UNIX 시스템에 대한 Kerberos 모드

Kerberos 모드로 실행되는 UNIX 시스템에서 Federation Agent 에 대한 설치 사전 요구 사항을 완료하십시오. KDC 는 UNIX 시스템에 있습니다.

1. UNIX 시스템에서 KDC 를 구성합니다.
2. UNIX 에서 Kerberos 에 대한 추가 구성을 수행합니다.
3. Internet Explorer 설정을 구성합니다.

UNIX 시스템에서 KDC 구성

Kerberos KDC(Key Distribution Center)를 호스트하는 UNIX 서버는 페더레이션 시스템을 지원하도록 구성해야 합니다. 이 프로세스의 일부는 keytab 파일을 만들기 위한 것입니다. Kerberos 인증에는 keytab 파일이 필요합니다.

다음 단계를 수행하십시오.

1. 명령 프롬프트 창을 엽니다.
2. 명령줄 프롬프트에 다음 명령을 입력합니다.

   ```
   usr/sbin/kadmin.local
   ```

3. 다음 명령으로 CA SiteMinder® Federation Standalone 시스템 서비스 프린서펄 이름을 추가합니다.

   ```
   addprinc -pw <password> HTTP/AgentHost Name.domainname.com@DOMAINNAME.COM
   ```

4. 명령 프롬프트 창을 열고 다음 명령을 입력하여 keytab 파일을 만듭니다.

   ```
   ktadd -k output_keytab_location SPN name
   ```

   Keytab 파일이 생성됩니다.

5. quit 를 입력합니다.

UNIX KDC 서버에서 페더레이션 구성이 완료되었습니다.

UNIX 에서 Kerberos 에 대한 추가 구성 완료

Kerberos 를 구성하려면 UNIX 시스템의 페더레이션 시스템에 대해 다음 명령이 필요합니다.

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

Kerberos 인증을 사용하도록 UNIX 시스템이 구성되었습니다.

Internet Explorer 에서 싱글 사인온을 구성하십시오. 이 절차는 인증 프로토콜로 NTLM 또는 Kerberos 를 사용하는지 여부에 관계 없이 적용됩니다.

추가 정보:

Internet Explorer 구성 설정 (페이지 25)

Internet Explorer 구성 설정

싱글 사인온 배포로 기능하려면 일부 특정 Internet Explorer 설정을 구성하십시오.

로컬 인트라넷 속성 설정

Internet Explorer 가 싱글 사인온 배포에서 작동하려면 몇 가지 특정 설정이 필요합니다. 브라우저를 설정하려면 로컬 인트라넷 속성과 인트라넷 인증을 구성해야 합니다. 이러한 설정은 사용하는 인증 프로토콜이 Kerberos 이든 NTLM 이든 상관없이 적용됩니다.

다음 단계를 수행하십시오.

1. Internet Explorer 브라우저를 엽니다.
2. Internet Explorer 메뉴 표시줄에서 "도구"를 선택합니다.
3. 드롭다운 메뉴에서 "Internet 옵션"을 선택합니다.
4. "보안" 탭을 클릭합니다.

5. "로컬 인트라넷" 단추를 클릭합니다.
6. "사이트" 단추를 클릭합니다.
7. "프록시 서버를 사용하지 않는 사이트를 모두 포함" 확인란이 선택되어 있는지 확인합니다.
8. "고급" 단추를 클릭합니다.
9. 인트라넷에서 사용되는 모든 도메인 이름을 입력합니다(예: AgentHostName.domainname.com).
10. "고급" 탭을 선택합니다.
11. "보안" 섹션으로 스크롤합니다.
12. "통합된 Windows 인증 사용(다시 시작해야 함)"을 선택합니다.
13. 시스템을 다시 시작합니다.
14. "확인"을 클릭합니다.

로컬 인트라넷 속성이 구성되었습니다.

인트라넷 인증 설정

싱글 사인온 솔루션으로 작동하려면 Internet Explorer 에 대한 몇 가지 특정 설정이 필요합니다. 이러한 클라이언트 브라우저 설정에서는 인트라넷 환경을 사용한다고 가정합니다. 브라우저를 설정하려면 로컬 인트라넷 속성과 인트라넷 인증을 구성해야 합니다.

다음 단계를 수행하십시오.

1. Internet Explorer 브라우저를 엽니다.
2. Internet Explorer 메뉴 표시줄에서 "도구" 메뉴를 선택합니다.
3. 드롭다운 메뉴에서 "Internet 옵션"을 선택합니다.
4. "보안" 탭을 클릭합니다.
5. "로컬 인트라넷" 단추를 클릭합니다.
6. "사용자 지정 수준" 단추를 클릭합니다.
7. "보안" 탭을 선택합니다.
8. 아래로 스크롤하여 "사용자 인증" 섹션을 찾습니다.

9. "인트라넷 영역에서만 자동으로 로그온"을 선택합니다.
10. "확인"을 클릭합니다.

사용자가 인트라넷 영역에서 인증됩니다.

프록시 서버를 통한 브라우저 인증(선택 사항)

어설션 당사자에서 프록시 서버가 에이전트가 있는 페더레이션 시스템과 브라우저 사이에 삽입되면 인증이 더 이상 작동하지 않습니다. 이 경우 상대 도메인 이름을 사용하는 모든 URL 이 프록시 서버를 통과하지 않도록 구성해야 합니다.

다음 단계를 수행하십시오.

1. Internet Explorer 브라우저를 엽니다.
2. Internet Explorer 메뉴 표시줄에서 "도구" 메뉴를 선택합니다.
3. 드롭다운 메뉴에서 "Internet 옵션"을 선택합니다.
4. "고급" 탭을 클릭합니다.
5. 아래로 스크롤하여 "보안" 섹션을 찾습니다.
6. "통합된 Windows 인증 사용"이 선택되어 있는지 확인합니다.
7. "연결" 탭을 클릭합니다.
8. "LAN 설정" 단추를 클릭합니다.
9. 프록시 서버 주소와 포트 번호가 올바른지 확인합니다.
10. "고급" 단추를 클릭합니다.
11. "예외" 필드에 관련 도메인 이름을 나열합니다.
12. "확인"을 클릭합니다.

브라우저가 지정된 도메인에 대해 프록시 서버를 건너뛰도록 구성됩니다.

포트 사양(선택 사항)

Federation Agent 와 도메인 컨트롤러 사이에 방화벽이 있는 구성의 경우 다음과 같은 정적 포트를 열어 통신을 허용해야 합니다.

- Microsoft-DS 트래픽(445/tcp, 445/udp)
- LDAP(Lightweight Directory Access Protocol) ping(389/udp)
- DNS(Domain Name System)(53/tcp, 53/udp)
- Kerberos 인증 프로토콜(88/tcp, 88/udp)
- NetBIOS 데이터그램 서비스(138/tcp, 138/udp)
- NetBIOS-ns 서비스(137/tcp, 137/udp)
- epmap(135/tcp, 135/udp)

또한 다음 로컬 보안 기관(LSA) 포트는 동적 포트이므로 레지스트리 항목을 수정하여 정적으로 만들어야 합니다.

- Local Security Authority Service(NTDS)(1025/tcp, 1025/udp): NTLM 에 필요한 구성 가능한 포트
- Local Security Authority Service(NetLogin)(1026/tcp, 1026/udp): Kerberos 에 필요한 구성 가능한 포트

LSA 포트에 대한 자세한 내용은 다음 사이트를 참조하십시오.

http://support.microsoft.com/kb/224196/

제 3 장: Federation Agent for Windows Authentication 설치

설치 요구 사항

다음 설치 요구 사항을 고려하십시오.

- Federation Agent 는 CA SiteMinder® Federation Standalone 이 이미 설치되어 있는 시스템에 설치해야 합니다.
- CA SiteMinder® Federation Standalone 이 SiteMinder 커넥터를 사용하는 시스템에는 Federation Agent 를 설치하지 마십시오.

중요! 최신 버전으로 CA SiteMinder?Federation Standalone 을 업그레이드하는 경우 에이전트를 동일한 버전으로 업그레이드하십시오. 그렇지 않으면 에이전트가 제대로 작동하지 않습니다.

설치 실행 파일

다음 표에는 Federation Agent 에 대한 설치 실행 파일이 나와 있습니다.

참고: 설치 실행 파일과 폴더 이름에 포함된 **iwa** 문자열은 Windows 통합 인증 기술에 대한 지원을 나타냅니다.

플랫폼	설치 실행 파일
Solaris	ca-fedmgr-iwa-*version*-sol.bin
Linux	ca-fedmgr-iwa-*version*-rhel30.bin
Windows	ca-fedmgr-iwa-*version*-win32.exe

지원되는 운영 체제에 대한 자세한 내용은 기술 지원 사이트의 제품 "Platform Support Matrix"(플랫폼 지원표)를 참조하십시오.

Federation Agent(Windows) 설치

설치 관리자를 실행합니다.

설치 키트를 찾으려면

1. 기술 지원 사이트로 이동합니다.
2. 사이트에 로그온합니다.
3. "Download Center"(다운로드 센터)를 클릭합니다.
4. "Download Center"(다운로드 센터)에서 설치 키트를 검색하고 로컬 시스템으로 다운로드합니다.

Windows 에서 에이전트를 설치하려면

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 실행 파일이 있는 위치로 이동합니다.
3. 운영 플랫폼의 설치 실행 파일을 실행합니다.

   실행 파일 목록은 여기를 참조하십시오.

   설치 마법사가 시작됩니다.
4. 설치 마법사의 지시에 따릅니다.

   Windows Agent 가 시스템에 설치됩니다.
5. 설치가 완료되면 구성 마법사 (페이지 37)를 실행합니다.

Federation Agent 설치(UNIX)

설치 관리자를 실행합니다.

설치 키트를 찾으려면

1. 기술 지원 사이트로 이동합니다.
2. 사이트에 로그온합니다.
3. "Download Center"(다운로드 센터)를 클릭합니다.
4. "Download Center"(다운로드 센터)에서 설치 키트를 검색하고 로컬 시스템으로 다운로드합니다.

UNIX 시스템에서 에이전트를 설치하려면

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 설치 실행 파일이 있는 위치로 이동합니다.
3. 운영 플랫폼의 설치 실행 파일을 실행합니다.

   실행 파일 목록은 여기를 참조하십시오.

   설치 마법사가 시작됩니다.
4. 설치 마법사의 지시에 따릅니다.

   Windows Agent 가 시스템에 설치됩니다.
5. 설치가 완료되면 구성 마법사를 실행합니다.

Federation Agent 무인 설치

Federation Agent 를 수동으로 설치한 후에는 동일한 시스템이나 다른 시스템에서 무인 설치 모드를 사용하여 에이전트를 설치할 수 있습니다. 무인 설치는 사용자 개입이 필요 없습니다. 이 설치는 요구 사항에 맞게 수정할 수 있는 설치 속성 파일이 필요합니다.

무인 설치 프로세스는 모든 플랫폼에서 동일합니다. 실행 파일 이름만 다릅니다.

다음 단계를 수행하십시오.

1. 설치 실행 파일이 있는 디렉터리로 이동합니다.
2. 명령 프롬프트에 다음 명령을 입력합니다.

   ```
   installation_executable -i silent -f
   ca-fedmanager-iwa-installer.properties
   ```

   -f

   Windows Agent 설치 관리자 속성 파일의 이름을 지정합니다. 속성 파일이 설치 실행 파일과 동일한 디렉터리에 없는 경우 속성 파일의 상대 경로를 지정합니다.

   -i

   설치 모드를 지정합니다.

   설치가 실행되고 설정이 속성 파일에 기록됩니다.

무인 설치가 완료되었습니다.

Federation Agent 제거(Windows)

Windows 시스템에서 Federation Agent 가 더 이상 필요하지 않은 경우 제거할 수 있습니다.

다음 단계를 수행하십시오.

1. "시작", "모든 프로그램", "CA", "Federation Standalone", "CA SiteMinder® Federation Standalone Windows Authentication Agent 제거"를 선택합니다.

   마법사가 시작됩니다.
2. 마법사의 지시를 따릅니다.
3. 필요한 경우 Program Files\CA\Federation Standalone\connector 디렉터리로 이동하고 IWA 폴더와 하위 폴더를 모두 삭제합니다.
4. 시스템을 재부팅합니다.

Federation Agent for Windows Authentication 이 시스템에서 제거되었습니다.

Federation Agent 제거(UNIX)

UNIX 시스템에서 Windows Agent 가 더 이상 필요하지 않은 경우 제거할 수 있습니다.

다음 단계를 수행하십시오.

1. 명령 창을 엽니다.
2. Federation Agent for Windows Authentication 홈 디렉터리로 이동합니다.
3. 다음 명령을 입력합니다.

   ./ca-federation-iwa-uninstall.sh
4. 필요한 경우 나머지 폴더와 모든 하위 폴더를 삭제합니다.

Federation Agent 가 시스템에서 제거되었습니다.

Federation Agent 를 r12.52 SP1 로 업그레이드

설치 프로그램은 현재 사용 중인 Federation Agent for Windows Authentication 버전을 업그레이드할 수도 있습니다. CA SiteMinder?Federation Standalone 이 이미 설치되어 있는 시스템에 Federation Agent 를 설치해야 합니다.

중요! Federation Agent 는 CA SiteMinder® Federation Standalone 의 버전과 동일해야 합니다. 페더레이션 시스템을 업그레이드하는 경우 에이전트를 업그레이드하십시오. 그렇지 않으면 에이전트가 제대로 작동하지 않습니다.

다음 단계를 수행하십시오.

1. 기본 페더레이션 시스템의 버전이 업그레이드할 Federation Agent 의 버전과 동일한지 확인합니다. 그렇지 않으면 먼저 CA SiteMinder® Federation Standalone 을 업그레이드합니다.
2. 운영 플랫폼의 Windows Agent 설치 실행 파일을 실행합니다.

   추가 구성이 필요하지 않습니다.
3. 구성 마법사 (페이지 35)를 실행합니다.

제 4 장: Federation Agent for Windows Authentication 구성

구성 마법사에 필요한 정보

Federation Agent 를 설치한 후 구성 마법사를 실행하십시오. Windows 시스템에서는 인증 프로토콜(Kerberos 또는 NTLM)을 선택하십시오. UNIX 시스템에서는 Kerberos 프로토콜만 지원됩니다.

참고: 구성 실행 파일과 폴더 이름에 포함된 **iwa** 문자열은 Windows 통합 인증 기술에 대한 지원을 나타냅니다.

NTLM 및 Kerberos 구성에는 다음 매개 변수가 필요합니다.

중요! 이러한 매개 변수의 값은 관리 UI 의 배포 설정에 지정된 값과 일치해야 합니다. Federation Agent 를 구성하기 전에 먼저 CA SiteMinder?Federation Standalone 관리자에서 이러한 설정 값을 확인하십시오.

쿠키 영역

싱글 사인온 보안 영역 이름을 지정합니다.

기본값: FED

값: 영문자 문자열

쿠키 이름

개방 형식 쿠키의 이름을 지정합니다.

기본값: ""

값: 영문자 문자열

암호화 암호

쿠키를 암호화할 키를 파생시키는 암호를 지정합니다.

기본값: ""

값: 영숫자 문자열

Encryption Transformation type(암호화 변환 유형)

FIPS 호환 암호화 변환을 지정합니다.

기본값: AES128/CBC/PKCS5Padding

제한: AES128/CBC/PKCS5Padding, AES192/CBC/PKCS5Padding, AES256/CBC/PKCS5Padding, 3DES_EDE/CBC/PKCS5Padding

UseHMAC

HMAC(해시 메시지 인증 코드)를 사용할지 여부를 지정합니다.

기본값: false

제한: true 또는 false

참고: Windows 를 실행하는 시스템에서 Kerberos 인증 프로토콜을 선택한 경우 선택적으로 NTLM 을 장애 조치 옵션을 선택할 수 있습니다.

Kerberos 프로토콜을 지정할 경우 다음 매개 변수에 대한 값을 제공하십시오.

KDC 주소

KDC(Key Distribution Center)의 정규화된 도메인 이름을 지정합니다.

KDC realm(KDC 영역)

KDC 가 있는 시스템의 도메인 이름을 지정합니다.

Keytab location(Keytab 위치)

Keytab 파일의 경로를 지정합니다. 이 파일은 KDC 시스템에서 생성된 후 Federation Agent 가 설치된 시스템으로 이동됩니다.

프린서펄

서비스 인스턴스를 고유하게 식별하는 SPN(서비스 프린서펄 이름)을 지정합니다(예: HTTP/host.abc.com). HTTP 는 서비스 이름이고 host.abc.com 은 서비스가 있는 호스트의 이름입니다.

Keytab 위치 및 프린서펄 매개 변수는 login.conf 파일에 기록됩니다. 다른 매개 변수는 IWAConnectorConfig.conf 파일에 기록됩니다.

참고: login.conf 파일을 검토하는 경우 isInitiator 매개 변수 값을 변경하지 마십시오.

Windows 에서 구성 마법사 실행

설치 후 Federation Agent 에 대한 구성 마법사를 실행하십시오. 이 마법사에서는 인증 프로토콜 및 쿠키 사양과 관련된 매개 변수의 값을 설정합니다.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 구성 명령 파일이 있는 다음 위치로 이동합니다.

   federation_installation_dir\connectors\IWA
3. ca-fedmanager-iwa-config.cmd 를 두 번 클릭합니다.

   구성 마법사가 시작됩니다.
4. 마법사에서 제공되는 지시에 따릅니다.

구성이 완료되었습니다.

UNIX 에서 구성 마법사 실행

Federation Agent 의 구성 마법사는 인증 프로토콜 및 쿠키 사양과 관련된 매개 변수 값을 설정합니다.

구성 마법사를 실행하여 설치 프로세스를 완료하십시오.

다음 단계를 수행하십시오.

1. 실행 중인 응용 프로그램을 모두 종료합니다.
2. 구성 명령 파일이 있는 다음 위치로 이동합니다.

   federation_installation_dir/connectors/IWA
3. ca-fedmanager-iwa-config.sh 스크립트를 실행합니다.

   구성 마법사가 시작됩니다.
4. 마법사의 지시에 따라 구성을 완료합니다.

5. 에이전트가 제대로 작동하도록 다음 스크립트의 경로를 수정합니다.
   `. /federation_install_dir/connectors/IWA/ca_fedmgr_iwa_env.ksh`
6. 페더레이션 서비스를 다시 시작합니다.
   a. 명령 창을 엽니다.
   b. 다음 스크립트를 실행합니다.

      federation_install_dir/fedmanager.sh stop

      federation_install_dir/fedmanager.sh start

   참고: 서비스를 중지했다가 루트 사용자로 시작하지 마십시오. 루트가 아닌 사용자여야 합니다.

무인 구성(Windows)

마법사를 사용하여 Federation Agent 를 한 번 구성한 후에는 동일한 시스템이나 다른 시스템에서 무인 모드를 사용하여 Federation Agent 를 구성할 수 있습니다. 무인 모드 구성은 사용자 개입이 필요 없습니다. 이 구성은 구성 속성 파일을 사용합니다. 구성 속성을 요구 사항에 맞게 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. 구성 실행 파일이 있는 다음 디렉터리로 이동합니다.

   federation_installation_dir\connectors\IWA\install_config_info

2. 명령 프롬프트에 다음 명령을 입력합니다.

   `ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties`

   -f

   Federation Agent 구성 속성 파일의 이름을 지정합니다. 속성 파일이 실행 파일과 동일한 디렉터리에 없는 경우 속성 파일의 상대 경로를 지정합니다.

   -i

   구성 모드를 지정합니다. 무인 모드의 경우 값은 silent 입니다.

무인 구성이 완료되었습니다.

무인 구성(UNIX)

마법사를 사용하여 Federation Agent 를 한 번 구성한 후에는 동일한 시스템이나 다른 시스템에서 무인 모드를 사용하여 Federation Agent 를 구성할 수 있습니다. 무인 모드 구성은 사용자 개입이 필요 없습니다. 이 구성은 구성 속성 파일을 사용합니다. 구성 속성 파일을 요구 사항에 맞게 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. 구성 실행 파일이 있는 다음 디렉터리로 이동합니다.

   federation_installation_dir/connectors/IWA/install_config_info

2. 명령 프롬프트에 다음 명령을 입력합니다.

   ```
   ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties
   ```

   -f

   Federation Agent 구성 속성 파일의 이름을 지정합니다. 속성 파일이 실행 파일과 동일한 디렉터리에 없는 경우 속성 파일의 상대 경로를 지정합니다.

   -i

   구성 모드를 지정합니다. 무인 모드의 경우 값은 silent 입니다.

무인 구성이 완료되었습니다.

Federation Agent 구성 파일 수정(선택 사항)

구성 마법사를 실행한 후에는 지정한 값이 IWAConnectorConfig.conf 파일에 기록됩니다. 언제든 마법사를 다시 실행하여 거의 모든 매개 변수 값을 수정할 수 있습니다.

몇몇 매개 변수 값은 구성 마법사에서 설정되지 않습니다. 다음 값을 업데이트하려면 파일을 직접 수정하십시오.

context_cleanup_interval

정리 스레드가 만료된 컨텍스트의 삭제를 시작하는 간격을 지정합니다. 이 값을 줄이면 정리 간격이 짧아지므로 메모리 가용성이 향상됩니다.

기본값: 30,000 밀리초

값: 불완전한 요청이 많이 발생할 것으로 예상되는 경우 값을 낮게 지정하는 것이 좋습니다.

context_expiration_interval

컨텍스트가 만료되기까지의 시간을 지정합니다. NTLM 의 경우 컨텍스트가 최대 1 분 동안 유효합니다.

기본값: 60,000 밀리초

값: 이 매개 변수 값은 1 분 미만으로 설정할 수 없습니다. 값이 크면 오래된 컨텍스트가 정리되지 않을 수 있습니다.

context_cleanup_thread_priority

컨텍스트 정리 스레드의 우선 순위를 지정합니다.

기본값: 5

값: 불완전한 요청이 많이 발생할 것으로 예상되는 경우 우선 순위를 높게 지정하는 것이 좋습니다.

제 5 장: 위임된 인증 설정

Federation Agent 는 CA SiteMinder?Federation Standalone 과 함께 작동하므로 사용자는 IWA 컨텍스트에서 인증을 수행할 수 있습니다. Federation Agent 는 타사 인증 서비스로 작동하므로 위임된 인증을 사용하도록 페더레이션 시스템을 구성하십시오.

다음 단계를 수행하십시오.

1. 관리 UI 에 로그인합니다.
2. 편집할 SAML 1.1 또는 SAML 2.0 파트너 관계를 선택합니다. 생산자 -> 소비자 파트너 관계 또는 IdP -> SP 파트너 관계를 편집합니다.
3. 파트너 관계 마법사에서 다음 단계 중 하나로 이동합니다.
   - SAML1.1: 싱글 사인온
   - SAML 2.0: SSO 및 SLO
4. "인증 모드"를 "위임됨"으로 설정합니다.
5. "위임된 인증 유형"을 "개방 형식 쿠키"로 설정합니다.

   다음 정보에 주의하십시오.

   - Federation Agent 에는 개방 형식 쿠키를 기반으로 하는 위임된 인증이 필요합니다. SiteMinder 커넥터를 사용하도록 페더레이션 시스템을 구성한 경우에는 이 옵션을 사용할 수 없습니다.
   - Federation Agent 구성 시 지정한 쿠키 설정 값은 관리 UI 의 배포 설정 값과 일치해야 합니다.
6. 위임된 인증 URL 을 입력합니다.

   예: http://*hostname:portnum*/iwa/IWARedirect

위임된 인증이 사용되도록 설정되었습니다.

참고: 위임된 인증에 대한 자세한 내용은 *CA SiteMinder® Federation Standalone 안내서*를 참조하십시오.

제 6 장: 에이전트 추적 로그 파일을 사용한 문제 해결

추적 로그 파일인 IWAConnectorTrace.log 를 참조하여 Federation Agent 문제를 해결할 수 있습니다.

추적 로그 파일을 설정하려면

1. %FEDROOT%\connectors\IWA\Config\login.conf 로 이동합니다.
2. login.conf 파일을 열고 다음과 같이 변경합니다.

   debug=true
3. 페더레이션 서비스를 다시 시작합니다.

로그 파일이 %FEDROOT%\logs\connectors\IWA\IWAConnectorTrace.log 디렉터리에 기록됩니다.

로그 파일에는 다음과 같은 메시지가 포함되어 있을 수 있습니다.

증상

구성 파일을 찾을 수 없습니다.

해결 방법

IWAConnectorConfig.conf 파일이 *federation_install_dir*\connectors\IWA\config 폴더에 있는지 확인하십시오.

증상

잘못된 authtype 을 지정했습니다.

해결 방법

인증 유형이 NTLM 또는 Kerberos 로 지정되어 있는지 확인하십시오. 필요한 경우 구성 마법사를 다시 실행하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

Windows 가 아닌 플랫폼에서는 NTLM 이 지원되지 않습니다.

해결 방법

구성 마법사를 다시 실행하고 Kerberos 를 인증 유형으로 지정하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

IWAEncryptPassword 유틸리티를 사용하여 암호를 암호화해야 합니다.

해결 방법

구성 마법사를 다시 실행하고 암호를 입력하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

AuthType 은 비워 둘 수 없습니다.

해결 방법

구성 마법사를 다시 실행하고 인증 유형을 선택하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

암호화 키는 비워 둘 수 없습니다.

해결 방법

구성 마법사를 다시 실행하고 암호화 키를 선택하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

잘못된 암호화 변환을 지정했습니다.

해결 방법

구성 마법사를 다시 실행하고 다른 암호화 변환을 지정하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

잘못된 HMAC 값을 지정했습니다. true 또는 false 만 지정할 수 있습니다.

해결 방법

구성 마법사를 다시 실행하고 true 또는 false 를 선택하여 HMAC 를 사용할지 여부를 지정하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

Kerberos 구성이 잘못되었습니다.

해결 방법

다음 매개 변수가 올바로 지정되어 있는지 확인하십시오.

- Kerberos 영역
- KDC 주소
- Kerberos 구성 파일 위치(login.conf 파일)

필요한 경우 구성 마법사를 다시 실행하십시오. 구성 파일을 수동으로 편집하여 이러한 값을 변경하지 마십시오.

증상

컨텍스트 만료 간격은 1 분 미만으로 설정할 수 없습니다.

해결 방법

구성 마법사를 다시 실행하고 컨텍스트 만료 간격을 1 분 이상으로 지정하십시오. 구성 파일을 수동으로 편집하여 이 값을 변경하지 마십시오.

증상

구성이 잘못되었습니다. 서버가 초기화되지 않았습니다.

해결 방법

다음 값이 올바로 지정되어 있는지 확인하십시오.

- 인증 유형
- 암호화 키
- 암호화 변환
- Kerberos 영역
- KDC 주소
- Kerberos 구성 파일 위치(login.conf 파일)

필요한 경우 구성 마법사를 다시 실행하십시오. 구성 파일을 수동으로 편집하여 이러한 값을 변경하지 마십시오.

증상

요청이 IP 주소로 시작되었으므로 요청을 중단합니다.

해결 방법

SSO 요청이 항상 정규화된 도메인 이름으로 시작되는지 확인하십시오.

증상

Kerberos 를 초기화하지 못했습니다. 구성 매개 변수를 확인하십시오.

해결 방법

다음 값이 올바로 지정되어 있는지 확인하십시오.

- 인증 유형
- 암호화 키
- 암호화 변환
- Kerberos 영역
- KDC 주소
- Kerberos 구성 파일 위치(login.conf 파일)

필요한 경우 구성 마법사를 다시 실행하십시오. 구성 파일을 수동으로 편집하여 이러한 값을 변경하지 마십시오.

증상

쿠키를 찾을 수 없습니다. 만료되었거나 삭제되었습니다.

해결 방법

이러한 내용의 메시지는 브라우저가 잘못 구성된 경우에 나타납니다. NTLM 에 대한 브라우저 구성이 완료되었으며 쿠키를 사용할 수 있는지 확인하십시오.

증상

NTLM 자격 증명 쿠키를 찾을 수 없습니다.

해결 방법

이러한 내용의 메시지는 브라우저가 잘못 구성된 경우에 나타납니다. NTLM 에 대한 브라우저 구성이 완료되었으며 쿠키를 사용할 수 있는지 확인하십시오.

증상

사용자 도메인 또는 워크스테이션 정보를 찾을 수 없습니다.

해결 방법

이러한 내용의 메시지는 NTLM 유형 3 메시지에 도메인 이름 또는 워크스테이션 이름이 없는 경우에 나타납니다. 해당 유형의 메시지가 변경되지 않았는지 확인하십시오.

증상

사용자가 도메인 정보를 입력하지 않았습니다.

해결 방법

NTLM 인증에 대한 브라우저 구성이 완료되었는지 확인하십시오. 프롬프트 기반 인증을 사용하는 경우 사용자 이름과 함께 도메인 이름을 제공해야 합니다.

증상

Keytab *keytab_path* 의 키를 사용하여 *SPN_Name* 프린서펄을 KDC *KDC_address* 에 인증하려고 할 때 인증이 실패했습니다.

해결 방법

다음 매개 변수가 올바른지 확인하십시오.

- 프린서펄 이름
- KDC 주소
- Keytab 경로

증상

사용자 이름을 찾을 수 없습니다. 브라우저가 페더레이션 서버가 아닌 다른 시스템에 있는지 확인하십시오.

해결 방법

SSO 요청이 항상 어설션 당사자의 페더레이션 서버가 아닌 다른 시스템에서 발생하는지 확인하십시오.