SSL/TLS를 통한 Microsoft AD 인증을 위한 FireSIGHT System의 인증 객체 확인

목차

소개

외부 Active Directory LDAP 사용자가 웹 사용자 인터페이스 및 CLI에 대한 액세스를 인증하도록 FireSIGHT Management Center를 구성할 수 있습니다.이 문서에서는 SSL/TLS를 통한 Microsoft AD 인증을 위한 인증 객체를 구성, 테스트 및 문제 해결하는 방법에 대해 설명합니다.

전제 조건

FireSIGHT Management Center의 사용자 관리 및 외부 인증 시스템에 대한 지식을 보유한 것이 좋습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

절차

1단계. SSL/TLS 암호화 없이 인증 객체를 구성합니다.

1. 인증 객체를 일반적인 방식으로 구성합니다.암호화 및 암호화되지 않은 인증을 위한 기본 컨피그레이션 단계는 동일합니다.
2. 인증 객체가 작동 중이고 AD LDAP 사용자가 암호화되지 않은 인증을 수행할 수 있는지 확인합니다.

2단계. CA 인증서 없이 SSL 및 TLS를 통해 인증 객체를 테스트합니다.

CA 인증서 없이 SSL 및 TLS를 통해 인증 객체를 테스트합니다.문제가 발생한 경우 시스템 관리자에게 문의하여 AD LDS 서버에서 이 문제를 해결하십시오.인증서가 인증 객체에 이전에 업로드된 경우 "**Certificate has been loaded (Select to clear loaded certificate)**"를 선택하여 인증서를 지우고 AO를 다시 테스트하십시오.

인증 개체가 실패하면 다음 단계로 이동하기 전에 시스템 관리자에게 문의하여 AD LDS SSL/TLS

구성을 확인하십시오.그러나 CA 인증서로 인증 객체를 추가로 테스트하려면 다음 단계를 계속 진행하십시오.

3단계. Base**64** CA 인증서를 다운로드합니다.

1. AD LDS에 로그인합니다.
2. 웹 브라우저를 열고 http://localhost/certsrv에 연결합니다.
3. "**Download a CA certificate, certificate chain or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)"을 클릭합니다**.
4. "**CA Certificate**(**CA 인증서**)" 목록에서 CA 인증서를 선택하고 "Encoding Method(**인코딩 방법**)"에서 "**Base64"를 선택합니다**.
5. "**Download CA certificate(CA 인증서 다운로드**)" 링크를 클릭하여 certnew.cer 파일을 다운로드합니다.

4단계. 인증서에서 **Subject** 값을 확인합니다.

1. certnew.cer를 마우스 오른쪽 버튼으로 클릭하고 **열기**를 선택합니다.
2. Details(**세부사항**) 탭을 클릭하고 **Show** 드롭다운 옵션에서 **<All>을** 선택합니다.
3. 각 필드의 값을 확인합니다.특히, Subject(주체) 값이 Authentication Object의 **Primary Server Host** 이름과 일치하는지 확인합니다.

5단계. Microsoft Windows 시스템에서 인증서를 테스트합니다.작업 그룹 또는 도메인에 가입된 Windows 컴퓨터에서 이 테스트를 수행할 수 있습니다.

> **팁:**이 단계는 FireSIGHT Management Center에서 인증 객체를 생성하기 전에 Windows 시스템에서 CA 인증서를 테스트하는 데 사용할 수 있습니다.

1. CA 인증서를 C:\Certficate 또는 원하는 디렉토리에 복사합니다.
2. Windows 명령줄 cmd.exe를 실행합니다.관리자로서
3. Certutil 명령으로 CA 인증서 테스트

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

Windows 시스템이 이미 도메인에 가입되어 있는 경우 CA 인증서가 인증서 저장소에 있어야 하며 cacert.test.txt에 오류가 없어야 합니다.그러나 Windows 시스템이 작업 그룹에 있는 경우 신뢰할 수 있는 CA 목록에 CA 인증서가 있는 경우 두 메시지 중 하나가 표시될 수 있습니다.

a.CA는 신뢰할 수 있지만 CA에 대한 CRL이 없습니다.

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b.CA를 신뢰할 수 없습니다.

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
```

```
CertUtil: -verify command completed successfully.
```
아래와 같은 다른 오류 메시지가 표시되면 시스템 관리자에게 문의하여 AD LDS 및 중간 CA의 문제를 해결하십시오.이러한 오류 메시지는 잘못된 인증서, CA 인증서의 주체, 인증서 체인 누락 등을 나타냅니다.

```
Failed "AIA" Time: 0
Failed "CDP" Time: 0
Error retrieving URL: The specified network resource or d evice is no longer available
```
6단계. CA 인증서가 유효한지 확인하고 5단계에서 테스트를 통과했으면 인증서를 인증 객체에 업로드하고 테스트를 실행합니다.

7단계. 인증 객체를 저장하고 시스템 정책을 다시 적용합니다.