Verificación del Objeto de Autenticación en FireSIGHT System para la Autenticación de Microsoft AD sobre SSL/TLS

Contenido

Introducción

Puede configurar un FireSIGHT Management Center para permitir a los usuarios LDAP externos de Active Directory autenticar el acceso a la interfaz de usuario web y a la CLI. En este artículo se explica cómo configurar, probar y resolver problemas del objeto de autenticación para la autenticación de Microsoft AD a través de SSL/TLS.

Requisito previo

Cisco recomienda que tenga conocimientos sobre la gestión de usuarios y el sistema de autenticación externo en FireSIGHT Management Center.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Procedimiento

Paso 1. Configure el objeto de autenticación sin cifrado SSL/TLS.

1. Configure el objeto de autenticación como lo haría normalmente. Los pasos de configuración básicos para la autenticación cifrada y no cifrada son los mismos.
2. Confirme que el objeto de autenticación funcione y que los usuarios de AD LDAP puedan autenticarse sin cifrar.

Paso 2. Pruebe el objeto de autenticación sobre SSL y TLS sin certificado CA.

Pruebe el objeto de autenticación a través de SSL y TLS sin certificado de CA. Si detecta un problema, consulte con el administrador del sistema para resolverlo en el servidor AD LDS. Si un certificado se ha cargado previamente en el objeto de autenticación, seleccione "**Se ha cargado el**

certificado (Seleccione para borrar el certificado cargado)" para borrar el certificado y probar AO de nuevo.

Si el objeto de autenticación falla, consulte al administrador del sistema para verificar la configuración de AD LDS SSL/TLS antes de continuar con el siguiente paso. Sin embargo, no dude en continuar con los siguientes pasos para probar el objeto de autenticación con el certificado CA.

Paso 3. Descargue **Base64** CA Cert.

1. Inicie sesión en AD LDS.
2. Abra un explorador Web y conéctese a http://localhost/certsrv
3. Haga clic en "**Descargar un certificado de CA, cadena de certificado o CRL**"
4. Elija el certificado CA de la lista "**Certificado CA**" y "**Base64**" de "**Método de codificación**"
5. Haga clic en el enlace "**Descargar certificado de CA**" para descargar el archivo certnew.cer.

Paso 4. Verifique el valor **Subject** en el certificado.

1. Haga clic con el botón derecho del ratón en certnew.cer y seleccione **open**.
2. Haga clic en la pestaña **Detalles** y seleccione **<Todos>** en las opciones del menú desplegable **Mostrar**.
3. Verifique el valor para cada campo. En particular, verifique que el valor **Subject** coincida con el nombre **Primary Server Host** del objeto Authentication.

Paso 5. Pruebe el certificado en un equipo de Microsoft Windows. Puede realizar esta prueba en un equipo Windows unido a Workgroup o Domain.

> **Consejo:** Este paso se puede utilizar para probar el certificado CA en un sistema Windows antes de crear el objeto de autenticación en un FireSIGHT Management Center.

1. Copie el certificado de CA en C:\Certficate o en cualquier directorio preferido.
2. Ejecute la línea de comandos de Windows, cmd.exe. como administrador
3. Pruebe el certificado de CA con el comando Certutil

```
cd c:\Certificate

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

Si la máquina de Windows ya está unida al dominio, el certificado de CA debe estar en el almacén de certificados y no debe haber error en cacert.test.txt. Sin embargo, si el equipo de Windows está en un grupo de trabajo, es posible que vea uno de los dos mensajes dependiendo de la existencia de certificado de CA en la lista de CA de confianza.

a. La CA es de confianza pero no se ha encontrado ninguna CRL para la CA:

```
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. La CA no es de confianza:

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

Si obtiene cualquier otro mensaje de ERROR como el siguiente, consulte con el administrador del sistema para resolver el problema en AD LDS y CA intermedia. Estos mensajes de error son un indicativo de certificado incorrecto, asunto en el certificado de CA, falta cadena de certificado, etc.

```
Failed "AIA" Time: 0
Failed "CDP" Time: 0
Error retrieving URL: The specified network resource or d evice is no longer available
```

Paso 6. Una vez que confirme que el certificado de CA es válido y ha pasado la prueba en el paso 5, cargue el certificado en el objeto de autenticación y ejecute la prueba.

Paso 7. Guarde el objeto de autenticación y vuelva a aplicar la directiva del sistema.