Verificação do objeto de autenticação no sistema FireSIGHT para autenticação do Microsoft AD sobre SSL/TLS

Contents

Introduction

Você pode configurar um FireSIGHT Management Center para permitir que usuários externos LDAP do Ative Diretory autentiquem o acesso à interface de usuário da Web e à CLI. Este artigo discute como configurar, testar e solucionar problemas do Authentication Object for Microsoft AD Authentication Over SSL/TLS.

Pré-requisito

A Cisco recomenda que você tenha conhecimento sobre o gerenciamento de usuários e o sistema de autenticação externa no FireSIGHT Management Center.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. 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.

Procedimento

Etapa 1. Configure o objeto de autenticação sem criptografia SSL/TLS.

1. Configure o Objeto de Autenticação como faria normalmente. As etapas básicas de configuração para autenticação criptografada e não criptografada são as mesmas.
2. Confirme se o objeto de autenticação está funcionando e se os usuários do AD LDAP podem autenticar sem criptografia.

Etapa 2. Teste o objeto de autenticação sobre SSL e TLS sem certificado CA.

Teste o objeto de autenticação sobre SSL e TLS sem certificado CA. Se você encontrar um problema, consulte o administrador do sistema para resolver esse problema no servidor AD LDS.

Se um certificado tiver sido carregado anteriormente no objeto de autenticação, selecione "**Certificate has been loaded (Select to clear load certificate)**" para limpar o certificado e testar o AO novamente.

Se o objeto de autenticação falhar, consulte o administrador do sistema para verificar a configuração SSL/TLS do AD LDS antes de passar para a próxima etapa. No entanto, sinta-se à vontade para continuar com as etapas a seguir para testar o objeto de autenticação com o certificado CA.

Etapa 3. Baixe o certificado **Base64** CA.

1. Faça login no AD LDS.
2. Abra um navegador da Web e conecte-se a http://localhost/certsrv
3. Clique em "**Baixar um certificado CA, uma cadeia de certificados ou uma CRL**"
4. Escolha o certificado CA na lista "**Certificado CA**" e "**Base64**" em "**Método de codificação**"
5. Clique no link "**Baixar certificado CA**" para baixar o arquivo certnew.cer.

Etapa 4. Verifique o valor **Subject (Assunto)** no certificado.

1. Clique com o botão direito do mouse no certnew.cer e selecione **abrir**.
2. Clique na guia **Detalhes** e selecione **<Todos>** nas opções **Mostrar**
3. Verifique o valor de cada campo. Em particular, verifique se o valor **Subject** corresponde ao nome do **Host do Servidor Primário** do Objeto de Autenticação.

Etapa 5. Teste o certificado em uma máquina do Microsoft Windows. Você pode executar este teste em um grupo de trabalho ou domínio unido a uma máquina do Windows.

> **Dica:** Esta etapa pode ser usada para testar o certificado CA em um sistema Windows antes de criar o objeto de autenticação em um FireSIGHT Management Center.

1. Copie o certificado CA para C:\Certficate ou qualquer diretório preferencial.
2. Execute a linha de comando do Windows, cmd.exe. como administrador
3. Teste o certificado CA com o comando Certutil

```
cd c:\Certificate

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

Se a máquina do Windows já estiver ingressada no domínio, o certificado CA deve estar no repositório de certificados e não deve haver nenhum erro em cacert.test.txt. No entanto, se a máquina do Windows estiver em um grupo de trabalho, você poderá ver uma das duas mensagens dependendo da existência de certificado CA na lista de CAs confiáveis.

a. A CA é confiável, mas não foi encontrada nenhuma CRL para a 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. A AC não é confiável:

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

Se você receber alguma outra mensagem de ERRO como a abaixo, consulte seu administrador do sistema para resolver o problema no AD LDS e CA intermediária. Essas mensagens de erro são um indicativo de certificado incorreto, assunto no certificado CA, cadeia de certificados ausente, etc.

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

Etapa 6. Depois de confirmar que o certificado CA é válido e passou no teste na Etapa 5, carregue o certificado no objeto de autenticação e execute o teste.

Passo 7. Salve o objeto de autenticação e reaplique a política do sistema.