Comunicação de sessão LDAP segura

ONTAP 9

NetApp
January 17, 2025

Índice

Comunicação de sessão LDAP segura 1
Conceitos de assinatura e vedação LDAP 1
Ative a assinatura LDAP e a vedação no servidor CIFS 1
Configurar LDAP em TLS 1

Comunicação de sessão LDAP segura

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você deve configurar as configurações de segurança do servidor CIFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`.

A assinatura LDAP e a vedação no tráfego CIFS são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Ative a assinatura LDAP e a vedação no servidor CIFS

Antes que o servidor CIFS possa usar assinatura e vedação para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor CIFS para habilitar a assinatura e a vedação LDAP.

Antes de começar

Você deve consultar o administrador do servidor AD para determinar os valores de configuração de segurança apropriados.

Passos

1. Configure a configuração de segurança do servidor CIFS que permite o tráfego assinado e selado com servidores LDAP do ative Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

2. Verifique se a configuração de segurança de assinatura e vedação LDAP está definida corretamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX, como usuários, grupos e netgroups, você deverá ativar a configuração correspondente com `-session-security` a opção do `vserver services name-service ldap client modify` comando.

Configurar LDAP em TLS

Exporte uma cópia do certificado de CA raiz autoassinado

Para usar LDAP em SSL/TLS para proteger a comunicação do ative Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ative Directory Service para um arquivo de certificado e convertê-lo em um arquivo de texto ASCII. Esse arquivo de texto é usado pelo ONTAP para instalar o certificado na máquina virtual de storage (SVM).

Antes de começar

O Serviço de certificados do ative Directory já deve estar instalado e configurado para o domínio ao qual o servidor CIFS pertence. Você pode encontrar informações sobre a instalação e configuração dos Serviços de certificados do ative diretor consultando a Biblioteca Microsoft TechNet.

"Microsoft TechNet Library: technet.microsoft.com"

Passo

1. Obtenha um certificado de CA raiz do controlador de domínio que está no `.pem` formato de texto.

   "Microsoft TechNet Library: technet.microsoft.com"

Depois de terminar

Instale o certificado no SVM.

Informações relacionadas

"Microsoft TechNet Library"

Instale o certificado de CA raiz autoassinado no SVM

Se a autenticação LDAP com TLS for necessária ao vincular a servidores LDAP, primeiro você deverá instalar o certificado de CA raiz autoassinado no SVM.

Sobre esta tarefa

Quando o LDAP sobre TLS está ativado, o cliente LDAP do ONTAP no SVM não oferece suporte a certificados revogados no ONTAP 9.0 e 9,1.

A partir do ONTAP 9.2, todos os aplicativos do ONTAP que usam comunicações TLS podem verificar o status do certificado digital usando o protocolo OCSP (Online Certificate Status Protocol). Se o OCSP estiver ativado para LDAP através de TLS, os certificados revogados serão rejeitados e a conexão falhará.

Passos

1. Instale o certificado CA raiz autoassinado:
   a. Inicie a instalação do certificado: `security certificate install -vserver vserver_name -type server-ca`

      A saída do console exibe a seguinte mensagem: `Please enter Certificate: Press <Enter> when done`

   b. Abra o arquivo de certificado `.pem` com um editor de texto, copie o certificado, incluindo as linhas que começam com `-----BEGIN CERTIFICATE-----` e terminam com `-----END CERTIFICATE-----`, e cole o certificado após o prompt de comando.

c. Verifique se o certificado é exibido corretamente.

d. Conclua a instalação pressionando Enter.

2. Verifique se o certificado está instalado: `security certificate show -vserver vserver_name`

Ative LDAP através de TLS no servidor

Antes que o servidor SMB possa usar TLS para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor SMB para ativar o LDAP sobre TLS.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory (AD) e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores AD, use o `-try-channel-binding-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.

Para saber mais, consulte:

- "Visão geral da LDAP"
- "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows".

Passos

1. Configure a configuração de segurança do servidor SMB que permite a comunicação LDAP segura com servidores LDAP do ative Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verifique se a configuração de segurança LDAP sobre TLS está definida como `true`: `vserver cifs security show -vserver vserver_name`

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX (como usuários, grupos e netgroups), você também deve modificar a `-use-start-tls` opção usando o `vserver services name-service ldap client modify` comando.

Informações sobre direitos autorais

Informações sobre marcas comerciais