



Configurar LDAP em TLS

ONTAP 9

NetApp
January 17, 2025

Índice

- Configurar LDAP em TLS 1
 - Exporte uma cópia do certificado de CA raiz autoassinado 1
 - Instale o certificado de CA raiz autoassinado no SVM 1
 - Ative LDAP através de TLS no servidor 2

Configurar LDAP em TLS

Exporte uma cópia do certificado de CA raiz autoassinado

Para usar LDAP em SSL/TLS para proteger a comunicação do ativo Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ativo 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 ativo 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 ativo diretor consultando a Biblioteca Microsoft TechNet.

["Microsoft TechNet Library: technet.microsoft.com"](https://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"](https://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 vservice_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 ativo 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 ativo 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 ativo 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

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.