Segurança

ONTAP 9

NetApp
January 17, 2025

Índice

Segurança

Autenticação e autorização do cliente

O ONTAP usa métodos padrão para proteger o acesso do cliente e do administrador ao armazenamento e para proteger contra vírus. Tecnologias avançadas estão disponíveis para criptografia de dados em repouso e para storage WORM.

O ONTAP autentica uma máquina cliente e um usuário verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

Autenticação

Você pode criar contas de usuário locais ou remotas:

- Uma conta local é aquela em que as informações da conta residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do ative Directory, um servidor LDAP ou um servidor NIS.

O ONTAP usa serviços de nomes locais ou externos para procurar informações de mapeamento de nome, usuário, grupo, grupo netgroup e nome do host. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Usuários locais
- DNS
- Domínios NIS externos
- Domínios LDAP externos

Uma tabela *name Service switch* especifica as fontes para procurar informações de rede e a ordem na qual pesquisá-las (fornecendo a funcionalidade equivalente do arquivo /etc/nsswitch.conf em sistemas UNIX). Quando um cliente nas se coneta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as informações necessárias.

Kerberos support Kerberos é um protocolo de autenticação de rede que fornece "autenticação de conexão", criptografando senhas de usuário em implementações cliente-servidor. O ONTAP suporta autenticação Kerberos 5 com verificação de integridade (krb5i) e autenticação Kerberos 5 com verificação de privacidade (krb5p).

Autorização

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos níveis de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

  A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

  A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

  A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Autenticação com SAML

O ONTAP suporta a linguagem de marcação de asserção de Segurança (SAML) para autenticação de usuários remotos. Vários provedores de identidade populares (IDPs) são suportados. Para obter mais informações sobre IDPs suportados e instruções para ativar a autenticação SAML, "Configurar a autenticação SAML"consulte .

OAuth 2,0 com clientes API REST do ONTAP

O suporte para a estrutura de autorização aberta (OAuth 2,0) está disponível a partir do ONTAP 9.14. Você só pode usar o OAuth 2,0 para tomar decisões de autorização e controle de acesso quando o cliente usa a API REST para acessar o ONTAP. No entanto, você pode configurar e ativar o recurso com qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI, o Gerenciador de sistema e a API REST.

Os recursos padrão do OAuth 2,0 são suportados juntamente com vários servidores de autorização populares. Você pode aprimorar ainda mais a segurança do ONTAP usando tokens de acesso restritos ao remetente baseados no TLS mútuo. E há uma ampla variedade de opções de autorização disponíveis, incluindo escopos autônomos, bem como integração com as funções REST do ONTAP e definições de usuário local. Consulte "Visão geral da implementação do ONTAP OAuth 2,0" para obter mais informações.

Autenticação de administrador e RBAC

Os administradores usam contas de login locais ou remotas para se autenticar no cluster e na SVM. O controle de acesso baseado em função (RBAC) determina os comandos aos quais um administrador tem acesso.

Autenticação

Você pode criar contas de administrador de cluster local ou remoto e SVM:

- Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento.
- Uma conta remota é aquela em que as informações de conta são armazenadas em um controlador de domínio do ative Directory, um servidor LDAP ou um servidor NIS.

Exceto o DNS, o ONTAP usa os mesmos serviços de nome para autenticar contas de administrador que ele usa para autenticar clientes.

RBAC

A *função* atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Verificação de vírus

Você pode usar a funcionalidade de antivírus integrada no sistema de armazenamento para proteger os dados contra o comprometimento por vírus ou outros códigos maliciosos. A verificação de vírus do ONTAP, chamada *Vscan*, combina o melhor software antivírus de terceiros com recursos do ONTAP que oferecem a flexibilidade necessária para controlar quais arquivos são verificados e quando.

Os sistemas de storage descarregam as operações de verificação para servidores externos que hospedam softwares antivírus de terceiros. O *ONTAP Antivirus Connector*, fornecido pelo NetApp e instalado no servidor externo, lida com as comunicações entre o sistema de armazenamento e o software antivírus.

- Você pode usar *verificação no acesso* para verificar se há vírus quando os clientes abrem, leem, renomeam ou fecham arquivos pelo SMB. A operação do arquivo é suspensa até que o servidor externo comunique o status da digitalização do arquivo. Se o ficheiro já tiver sido lido, o ONTAP permite a operação do ficheiro. Caso contrário, ele solicita uma verificação do servidor.

  A verificação no acesso não é suportada para NFS.

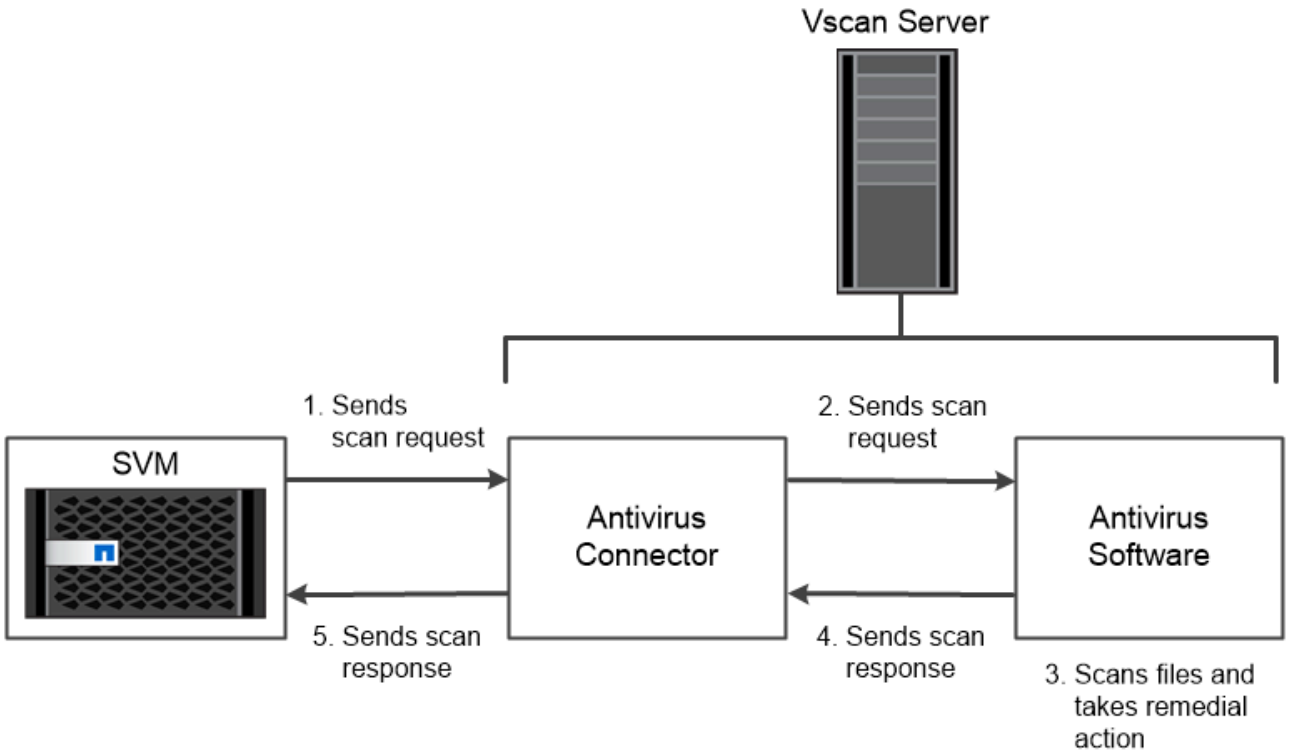
- Você pode usar *On-demand scanning* para verificar arquivos para vírus imediatamente ou em uma programação. Por exemplo, você pode querer executar digitalizações apenas em horas fora de pico. O servidor externo atualiza o status de verificação dos arquivos verificados, de modo que a latência de acesso ao arquivo desses arquivos (supondo que eles não tenham sido modificados) seja normalmente reduzida quando forem acessados pela próxima vez por SMB.

  Você pode usar a verificação sob demanda para qualquer caminho no namespace SVM, até mesmo para volumes exportados somente por NFS.

Normalmente, você ativa ambos os modos de digitalização em um SVM. Em ambos os modos, o software antivírus toma medidas corretivas em arquivos infetados com base em suas configurações no software.

Verificação de vírus na recuperação de desastres e configurações do MetroCluster

Para a recuperação de desastres e configurações do MetroCluster, é necessário configurar servidores Vscan separados para os clusters locais e parceiros.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Criptografia

A ONTAP oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

O ONTAP é compatível com os padrões federais de processamento de informações (FIPS) 140-2 para todas as conexões SSL. Você pode usar as seguintes soluções de criptografia:

- Soluções de hardware:
  - Criptografia de storage do NetApp (NSE)

    O NSE é uma solução de hardware que usa unidades de autocriptografia (SEDs).

  - SEDs NVMe

    O ONTAP fornece criptografia completa de disco para SEDs NVMe que não têm a certificação FIPS 140-2-2.

- Soluções de software:
  - Criptografia de agregados NetApp (NAE)

    NAE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

  - Criptografia de volume NetApp (NVE)

O NVE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade em que ele esteja habilitado com uma chave exclusiva para cada volume.

Use as soluções de criptografia de software (NAE ou NVE) e hardware (NSE ou NVMe SED) para obter criptografia dupla em repouso. A eficiência de storage não é afetada pela criptografia NVE ou NAE.

Criptografia de storage do NetApp

O NetApp Storage Encryption (NSE) é compatível com SEDs que criptografam dados à medida que são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no disco. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

Em uma solicitação de e/S, um nó se autentica em uma SED usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que fornece chaves de autenticação para nós que usam o Key Management Interoperability Protocol (KMIP).
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

O NSE é compatível com HDDs e SSDs com autocriptografia. Você pode usar a criptografia de volume NetApp com NSE para criptografar dados duas vezes em unidades NSE.

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Unidades com autocriptografia NVMe

No entanto, esses discos usam a criptografia de disco transparente AES de 256 bits para proteger os dados em repouso 140-2.

As operações de criptografia de dados, como a geração de uma chave de autenticação, são realizadas internamente. A chave de autenticação é gerada na primeira vez que o disco é acessado pelo sistema de armazenamento. Depois disso, os discos protegem os dados em repouso exigindo autenticação do sistema de storage sempre que as operações de dados forem solicitadas.

Criptografia de agregados NetApp

O NetApp Aggregate Encryption (NAE) é uma tecnologia baseada em software para criptografar todos os dados em um agregado. Um benefício do NAE é que os volumes estão incluídos na deduplicação de nível agregado, enquanto os volumes NVE são excluídos.

Com o NAE ativado, os volumes dentro do agregado podem ser criptografados com chaves agregadas.

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem o "Licença NVE" e gerenciamento de chaves externas ou integradas.

Criptografia de volume do NetApp

O NetApp volume Encryption (NVE) é uma tecnologia baseada em software para criptografar dados em repouso, um volume de cada vez. Uma chave de criptografia acessível apenas para o sistema de

armazenamento garante que os dados de volume não possam ser lidos se o dispositivo subjacente for separado do sistema.

Os dados, incluindo cópias Snapshot, e metadados, são criptografados. O acesso aos dados é dado por uma chave exclusiva XTS-AES-256, uma por volume. Um Gerenciador de chaves integrado protege as chaves no mesmo sistema com seus dados.

Você pode usar o NVE em qualquer tipo de agregado (HDD, SSD, híbrido, LUN de array), com qualquer tipo de RAID e em qualquer implementação de ONTAP com suporte, incluindo ONTAP Select. Você também pode usar o NVE com criptografia de storage NetApp (NSE) para criptografar dados duas vezes em unidades NSE.

quando usar servidores KMIP embora seja menos caro e normalmente mais conveniente usar o Gerenciador de chaves integrado, você deve configurar servidores KMIP se qualquer uma das seguintes situações for verdadeira:

- Sua solução de gerenciamento de chaves de criptografia precisa estar em conformidade com Federal Information Processing Standards (FIPS) 140-2 ou com o padrão OASIS KMIP.
- Você precisa de uma solução de vários clusters. Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

  Os servidores KMIP são compatíveis com vários clusters com gerenciamento centralizado de chaves de criptografia.

- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

  Os servidores KMIP armazenam as chaves de autenticação separadamente dos dados.

Informações relacionadas

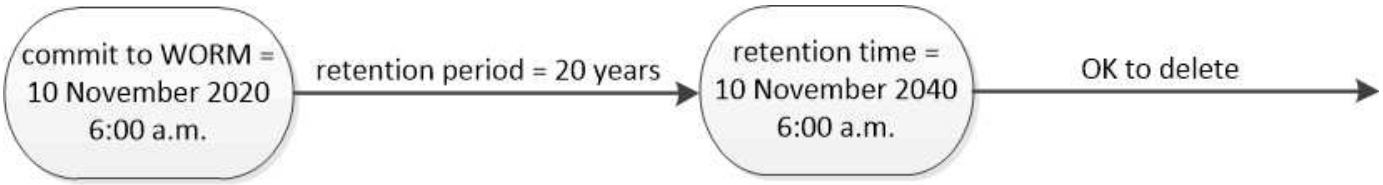
"Perguntas frequentes - encriptação de volume NetApp e encriptação agregada NetApp"

STORAGE WORM

O *SnapLock* é uma solução de conformidade de alto desempenho para organizações que usam o armazenamento *write once, read many (WORM)* para reter arquivos críticos de forma não modificada para fins regulatórios e de governança.

Uma única licença permite que você use o SnapLock no estrito modo *Compliance,* para satisfazer mandatos externos, como a regra SEC 17a-4(f), e um modo *Enterprise mais solto,* para atender aos regulamentos internos exigidos para a proteção de ativos digitais. O SnapLock usa um *ComplianceClock* à prova de violação para determinar quando o período de retenção de um arquivo WORM tiver decorrido.

Use o *SnapLock for SnapVault* para proteger cópias Snapshot WORM no storage secundário. Você pode usar o SnapMirror para replicar arquivos WORM para outro local geográfico para recuperação de desastres e outros fins.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

Informações sobre direitos autorais

Informações sobre marcas comerciais