



Relatórios técnicos do ONTAP

ONTAP Technical Reports

NetApp
August 07, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/ontap-technical-reports/index.html> on August 07, 2026. Always check docs.netapp.com for the latest.

Índice

Relatórios técnicos do ONTAP	1
ONTAP e relatórios técnicos de aplicativos e bancos de dados	2
Microsoft SQL Server	2
MySQL	2
Oracle	2
PostgreSQL	4
SAP HANA	4
Épico	4
Relatórios técnicos de continuidade dos negócios	5
SnapMirror ativo Sync (anteriormente SM-BC)	5
MetroCluster	5
Relatórios técnicos de proteção de dados e recuperação de desastres da ONTAP	6
SnapMirror	6
Aplicações e infraestrutura com o SnapMirror	6
Ciber Vault da ONTAP	6
Relatórios técnicos de volume ONTAP FlexCache e FlexGroup	8
FlexCache	8
FlexCache write-back	8
Volumes FlexGroup	8
Relatórios técnicos de rede da ONTAP	9
Roteamento	9
Serviços de nomes	9
NFS	10
Relatórios técnicos do ONTAP NFS	10
NFS	10
Multiprotocolo	10
NFS sobre TLS	10
Visão geral do NFS sobre TLS	10
Casos de uso e cargas de trabalho	11
Arquitetura	12
Configurar NFS sobre TLS	15
Segurança	25
Monitorar NFS sobre TLS	27
Desempenho	28
Interoperabilidade e limites	30
Relatórios técnicos da SAN ONTAP	32
Segurança	33
Relatórios técnicos de segurança da ONTAP	33
Ciber Vault da ONTAP	33
Ransomware	33
Confiança zero	33
Autenticação de vários fatores	33
Alocação a vários clientes	34

Padrões	34
Controle de acesso baseado em atributos	34
Solução NetApp para ransomware	34
Portfólio de proteção de ransomware e NetApp	34
SnapLock e snapshots à prova de violações para proteção contra ransomware	37
Bloqueio de arquivos FPolicy	38
Data Infrastructure Insights , armazenamento, carga de trabalho, segurança	39
Deteção e resposta incorporadas baseada em IA on-box da NetApp ONTAP	40
Proteção WORM com uso de cofres cibernéticos no ONTAP	41
Proteção contra ransomware do Digital Advisor	42
Resiliência abrangente com proteção contra ransomware da NetApp	43
NetApp e confiança zero	44
NetApp e confiança zero	44
Projete uma abordagem centrada em dados para zero confiança com o ONTAP	46
Controles de orquestração e automação de segurança da NetApp externos ao ONTAP	50
Implantações de nuvem híbrida e de confiança zero	51
Controle de acesso baseado em atributos	51
Controle de acesso baseado em atributos com ONTAP	52
Abordagens para controle de acesso baseado em atributos (ABAC) no ONTAP	52
Endurecimento da segurança	65
Guias de proteção de segurança da ONTAP	65
Guias de endurecimento	65
Diretrizes de fortalecimento da segurança do ONTAP	65
Visão geral do fortalecimento da segurança do ONTAP	65
Validação de imagem ONTAP	66
Contas de administrador de armazenamento local	66
Métodos de administração do sistema	83
Proteção autônoma contra ransomware da ONTAP	89
Auditoria de sistema administrativo de storage	89
Criptografia de storage no ONTAP	91
Criptografia de replicação de dados	93
Criptografia de dados em trânsito IPsec	94
Modo FIPS e gerenciamento TLS e SSL no ONTAP	96
Crie um certificado digital assinado pela CA	98
Protocolo de estado do certificado online	98
Gerenciamento do SSHv2	98
NetApp AutoSupport	100
Protocolo de hora de rede	101
Contas locais do sistema de arquivos nas (grupo de trabalho CIFS)	101
Auditoria do sistema de arquivos nas	101
Configure e ative a assinatura e a vedação CIFS SMB	103
Proteção do NFS	104
Ative a assinatura e a vedação do protocolo Lightweight Directory Access	107
Crie e use um FPolicy do NetApp	107
Caraterísticas de segurança das funções de LIF no ONTAP	109

Segurança de protocolo e porta	110
Relatórios técnicos do ONTAP nas	114
ONTAP S3	114
Relatórios técnicos do ONTAP SMB	115
SMB	115
Multiprotocolo	115
Sistemas de armazenamento	116
AFX	116
NetApp AFX visão geral: saiba mais sobre NetApp AFX	116
O que há de novo no NetApp AFX	120
Como a arquitetura AFX da NetApp difere do ONTAP unificado	120
Desempenho	139
Ferramentas de gerenciamento	147
Rede, segurança e operações	150
Detalhes do hardware	152
Máximos e limites	156
Onde encontrar informações adicionais	157
Relatórios técnicos da ONTAP SnapCenter	158
SnapCenter para Oracle	158
SnapCenter para Microsoft SQL Server	158
SnapCenter para Microsoft Exchange Server	158
SnapCenter para SAP HANA	158
Guia de endurecimento SnapCenter	159
Relatórios técnicos de disposição em camadas do ONTAP	160
Relatórios técnicos de virtualização da ONTAP	161
Avisos legais	163
Direitos de autor	163
Marcas comerciais	163
Patentes	163
Política de privacidade	163
Código aberto	163
ONTAP	163
ONTAP Mediador para configurações MetroCluster IP	163

Relatórios técnicos do ONTAP

ONTAP e relatórios técnicos de aplicativos e bancos de dados

O ONTAP é a base para o gerenciamento e a proteção de dados em muitas tecnologias de banco de dados e aplicações empresariais. Os relatórios técnicos a seguir fornecem orientação sobre as práticas recomendadas e os procedimentos de implementação do NetApp para Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA e Epic.

Microsoft SQL Server

O SQL Server é a base da plataforma de dados da Microsoft, fornecendo desempenho de missão crítica com tecnologias in-memory e insights mais rápidos sobre quaisquer dados, seja no local ou na nuvem.

"[Prática recomendada para Microsoft SQL Server com ONTAP](#)" Saiba como os administradores de storage e os administradores de banco de dados podem implantar com sucesso o Microsoft SQL Server no armazenamento ONTAP.



Esta documentação substitui o relatório técnico publicado anteriormente *TR-4590: Guia de práticas recomendadas para Microsoft SQL Server com ONTAP*.

"[TR-4976: Desempenho virtualizado do Microsoft SQL Server em sistemas NetApp AFF A-Series e C-Series](#)" Saiba mais sobre as características de desempenho do Microsoft SQL Server usando sistemas NetApp AFF A-Series e C-Series, bem como orientações sobre como selecionar o sistema certo com base na carga de trabalho.

"[TR-4714: Práticas recomendadas para Microsoft SQL Server usando SnapCenter](#)" Saiba agora para implantar com sucesso o Microsoft SQL Server no armazenamento ONTAP usando a tecnologia SnapCenter para proteção de dados.

MySQL

Este documento descreve os requisitos de configuração e fornece orientações sobre ajuste e configuração de armazenamento para a implantação do MySQL no ONTAP.

"[Banco de dados MySQL sobre as melhores práticas do NetApp ONTAP](#)" MySQL e suas variantes, incluindo MariaDB e Percona, são amplamente utilizados para muitas aplicações empresariais. Esses aplicativos variam de sites globais de redes sociais e sistemas massivos de comércio eletrônico a sistemas de hospedagem SMB que contêm milhares de instâncias de banco de dados. Saiba mais sobre os requisitos de configuração e orientação sobre ajuste e configuração de armazenamento para a implantação do MySQL no ONTAP.



Esta documentação substitui o relatório técnico publicado anteriormente *TR-4722: Banco de dados MySQL sobre as melhores práticas do NetApp ONTAP*.

Oracle

O ONTAP foi projetado para bancos de dados Oracle. Por décadas, o ONTAP foi otimizado para as demandas exclusivas de e/S de banco de dados relacional e vários recursos do ONTAP foram criados especificamente para atender às necessidades dos bancos de dados Oracle e até mesmo a pedido da própria Oracle Inc..

["Bancos de dados Oracle no ONTAP"](#) Saiba mais sobre as práticas recomendadas que permitem que administradores de armazenamento e administradores de banco de dados implantem com sucesso o Oracle no armazenamento ONTAP.

["Proteção de dados Oracle com ONTAP"](#) Saiba mais sobre as práticas recomendadas que permitem que administradores de storage e administradores de banco de dados façam backup, recuperem, repliquem e forneçam recuperação de desastres para o Oracle no armazenamento ONTAP.

["Recuperação de desastres Oracle com o ONTAP"](#) Saiba mais sobre as práticas recomendadas, procedimentos de teste e outras considerações para a operação de bancos de dados Oracle em um MetroCluster e SnapMirror Business Continuity.

["Migração de bancos de dados Oracle para sistemas de storage ONTAP"](#) Saiba mais sobre as considerações gerais para o Planejamento de uma estratégia de migração, os três níveis diferentes em que a movimentação de dados ocorre e detalha alguns dos vários procedimentos disponíveis.



A documentação vinculada acima substitui esses relatórios técnicos publicados anteriormente *TR-3633: Bancos de dados Oracle no ONTAP*; *TR-4591: Proteção de dados Oracle: Backup, recuperação, replicação*; *TR-4592: Oracle no MetroCluster*; e *TR-4534: Migração de bancos de dados Oracle para sistemas de armazenamento NetApp*

["TR-4969: Desempenho do banco de dados Oracle no AFF A-Series e C-Series"](#) O ONTAP é uma plataforma avançada de gerenciamento de dados com funcionalidades nativas que incluem compactação in-line, atualizações de hardware sem interrupções e a capacidade de importar um LUN de um array de storage estrangeiro. É possível agrupar até 24 nós, fornecendo dados simultaneamente por meio dos protocolos Network File System (NFS), Server Message Block (SMB), iSCSI, Fibre Channel (FC) e Nonvolatile Memory Express (NVMe). Além disso, a tecnologia Snapshot é a base para a criação de dezenas de milhares de backups online e clones totalmente operacionais de bancos de dados. Além do conjunto avançado de recursos do ONTAP, há uma grande variedade de requisitos do usuário, incluindo tamanho do banco de dados, requisitos de desempenho e necessidades de proteção de dados. Saiba mais sobre o desempenho do banco de dados bare metal usando os sistemas de armazenamento AFF, incluindo a série A e a série C, e abrange os máximos e a diferença prática entre as duas opções do AFF.

["TR-4971: Desempenho de banco de dados Oracle virtualizado no AFF Série A e série C."](#) O ONTAP é uma plataforma avançada de gerenciamento de dados com funcionalidades nativas que incluem compactação in-line, atualizações de hardware sem interrupções e a capacidade de importar um LUN de um array de storage estrangeiro. É possível agrupar até 24 nós, fornecendo dados simultaneamente por meio dos protocolos Network File System (NFS), Server Message Block (SMB), iSCSI, Fibre Channel (FC) e Nonvolatile Memory Express (NVMe). Além disso, a tecnologia Snapshot é a base para a criação de dezenas de milhares de backups online e clones totalmente operacionais de bancos de dados. Além do conjunto avançado de recursos do ONTAP, há uma grande variedade de requisitos do usuário, incluindo tamanho do banco de dados, requisitos de desempenho e necessidades de proteção de dados. Saiba mais sobre o desempenho do banco de dados virtualizado usando sistemas de armazenamento AFF, incluindo o série A e o série C, e abrange tanto os máximos quanto a diferença prática entre as duas opções do AFF.

["TR-4695: Disposição em camadas de storage de banco de dados com FabricPool"](#) Saiba mais sobre os benefícios e opções de configuração do FabricPool com vários bancos de dados, incluindo o Oracle Relational Database Management System (RDBMS).

["TR-4899: Failover de aplicativos transparente de banco de dados Oracle com sincronização ativa do SnapMirror"](#) O SnapMirror ativo Sync (anteriormente SM-BC) e o Oracle Real Application Cluster (RAC) podem fornecer failover transparente de aplicativos (TAF) e continuidade diante de interrupções de site e desastres reais. Saiba mais sobre as orientações de configuração e as práticas recomendadas de um storage array do AFF com o SnapMirror ativo Sync como o componente de armazenamento do Oracle RAC.

["TR-4876: Multitenancy Oracle com solução ONTAP e práticas recomendadas de implantação"](#) Saiba mais sobre as práticas recomendadas de solução sobre como provisionar, gerenciar e proteger bancos de dados multitenant Oracle usando o armazenamento ONTAP para maximizar os benefícios dos bancos de dados multitenant Oracle e dos recursos do software ONTAP.

PostgreSQL

PostgreSQL vem com variantes que incluem PostgreSQL, PostgreSQL Plus e EDB Postgres Advanced Server (EPAS). O PostgreSQL é normalmente implantado como banco de dados back-end para aplicativos de várias camadas. O NetApp ONTAP é uma excelente escolha para executar bancos de dados PostgreSQL de acordo com sua confiabilidade, alto desempenho e recursos eficientes de gerenciamento de dados.

["Banco de dados PostgreSQL sobre as melhores práticas do ONTAP"](#) PostgreSQL vem com variantes que incluem PostgreSQL, PostgreSQL Plus e EDB Postgres Advanced Server (EPAS). O PostgreSQL é normalmente implantado como banco de dados back-end para aplicativos de várias camadas. Ele é suportado por pacotes de middleware comuns (como PHP, Java, Python, Tcl/Tk, ODBC e JDBC) e tem sido historicamente uma escolha popular para sistemas de gerenciamento de banco de dados de código aberto. Saiba mais sobre os requisitos de configuração e orientação sobre ajuste e configuração de armazenamento para a implantação do PostgreSQL no ONTAP.



Esta documentação substitui o relatório técnico publicado anteriormente *TR-4770: Banco de dados PostgreSQL sobre as melhores práticas do ONTAP*.

SAP HANA

["Soluções de banco de dados SAP HANA no ONTAP"](#) As práticas recomendadas para configuração, gerenciamento e automação de soluções SAP podem ser encontradas na página soluções SAP da NetApp.

Épico

["Épico sobre as melhores práticas da ONTAP"](#) Um guia para entender as práticas recomendadas de implantação da Epic no local e na nuvem, atendendo aos padrões de configuração para implantação adequada no ONTAP.



Esta documentação substitui o relatório técnico publicado anteriormente *TR-3923: Melhores práticas da NetApp para a Epic*.

Relatórios técnicos de continuidade dos negócios

A NetApp oferece uma ampla gama de soluções que racionalizam onde os aplicativos e dados residem para melhorar o desempenho de forma econômica. Proteção de dados, replicação e disponibilidade contínua: O gerenciamento de dados do ONTAP pode simplificar a proteção de dados com o gerenciamento de políticas "configurar e esquecer", enquanto fornece continuidade dos negócios com o MetroCluster e o SnapMirror active Sync.



Esses relatórios técnicos expandem a "[Sincronização ativa do ONTAP SnapMirror](#)" documentação do produto e "[ONTAP MetroCluster](#)".

SnapMirror ativo Sync (anteriormente SM-BC)

"[TR-4878: Sincronização ativa do SnapMirror](#)" O SnapMirror active Sync é uma solução de storage continuamente disponível com granularidade no nível do aplicativo, disponível para ONTAP executado no AFF ou em todos os sistemas de storage de array SAN (ASA), para atender às necessidades de RPO 0 e rto 0 das aplicações mais essenciais aos negócios.

MetroCluster

"[TR-4705: Arquitetura e design da solução NetApp MetroCluster](#)" Este documento descreve conceitos de arquitetura e design de alto nível para recursos do MetroCluster no ONTAP.

IP do MetroCluster

"[TR-4689: IP NetApp MetroCluster](#)" MetroCluster é uma solução de storage continuamente disponível para ONTAP em sistemas FAS e AFF. MetroCluster IP é a evolução mais recente que utiliza uma estrutura de armazenamento de back-end baseada em Ethernet. MetroCluster IP oferece uma configuração altamente redundante para atender às necessidades das aplicações de negócios mais críticas. MetroCluster IP está incluído no ONTAP e fornece conectividade NAS e SAN para clientes e servidores que utilizam o armazenamento ONTAP.

FC do MetroCluster

"[TR-4375: NetApp MetroCluster FC](#)" O MetroCluster fornece disponibilidade contínua de dados em data centers separados geograficamente para aplicações de missão crítica. Saiba mais sobre as práticas recomendadas, decisões de design e configurações compatíveis do MetroCluster FC.

Relatórios técnicos de proteção de dados e recuperação de desastres da ONTAP

O SnapMirror é uma solução de replicação unificada econômica e fácil de usar no Data Fabric. Ele replica dados em alta velocidade em LAN ou WAN. Você obtém alta disponibilidade de dados e rápida replicação de dados para suas aplicações essenciais aos negócios, como Microsoft Exchange, Microsoft SQL Server e Oracle, em ambientes virtuais e tradicionais. Quando você replica os dados para um ou mais sistemas de storage da ONTAP e atualiza os dados secundários continuamente, eles permanecem atualizados e disponíveis sempre que você precisar. Não são necessários servidores de replicação externos.



Esses relatórios técnicos expandem a "[Proteção de dados e recuperação de desastres da ONTAP](#)" documentação do produto.

SnapMirror

SnapMirror assíncrono

["TR-4015: Configuração assíncrona do SnapMirror e práticas recomendadas"](#) Saiba mais sobre as práticas recomendadas para configurar a replicação assíncrona do SnapMirror (SM-A) de volumes, grupos de consistência e máquinas virtuais de storage (recuperação de desastres da SVM).

["TR-4678: Proteção de dados e backup de volumes ONTAP FlexGroup"](#) Saiba mais sobre a proteção de dados e o backup recomendados para volumes FlexGroup. Os tópicos incluem cópias Snapshot, SnapMirror e outras soluções de proteção de dados e backup.

SnapMirror síncrono

["TR-4733: Configuração síncrona do SnapMirror e práticas recomendadas"](#) Saiba mais sobre as práticas recomendadas para configurar a replicação síncrona do SnapMirror (SM-S).

SnapMirror Three-Data-Center DR

["TR-4832: Recuperação de desastres de três data centers usando o NetApp SnapMirror para ONTAP 9.7"](#) Saiba mais sobre uma configuração de recuperação de desastres de três data centers usando a tecnologia ONTAP SnapMirror para replicação.

Aplicações e infraestrutura com o SnapMirror

["TR-4900: Gerente de recuperação de site da VMware com ONTAP"](#) A ONTAP é uma solução de storage líder para ambientes VMware vSphere desde sua introdução ao data center moderno em 2002 e continua adicionando recursos inovadores para simplificar o gerenciamento e reduzir custos. Saiba mais sobre a solução ONTAP recomendada para o VMware Site Recovery Manager (SRM), o software de recuperação de desastres (DR) líder do setor da VMware, incluindo as informações mais recentes do produto e práticas recomendadas para simplificar a implantação, reduzir riscos e simplificar o gerenciamento contínuo.

Ciber Vault da ONTAP

["Ciber Vault da ONTAP"](#) O Cyber Vault baseado em ONTAP da NetApp oferece às organizações uma solução abrangente e flexível para proteger seus ativos de dados mais críticos. Ao utilizar metodologias de

fortalecimento lógicas com metodologias robustas, o ONTAP permite que você crie ambientes de storage seguros e isolados que sejam resilientes contra ameaças cibernéticas em evolução. Com o ONTAP, você garante a confidencialidade, integridade e disponibilidade dos dados, mantendo a agilidade e a eficiência da infraestrutura de storage.

Relatórios técnicos de volume ONTAP FlexCache e FlexGroup

As soluções nas da NetApp simplificam o gerenciamento de dados e ajudam você a acompanhar o ritmo do crescimento e, ao mesmo tempo, otimizam os custos. As soluções nas da ONTAP oferecem operações ininterruptas, eficiência comprovada e escalabilidade aprimorada em uma arquitetura unificada. Equipado com ONTAP, o nas com escalabilidade horizontal aproveita o enorme ecossistema ONTAP, com uma visão e uma liderança de inovação significativas para inovações futuras agressivas.



Esses relatórios técnicos expandem a ["Volume ONTAP FlexCache"](#) documentação do produto e ["Volume ONTAP FlexGroup"](#).

FlexCache

["TR-4743: FlexCache em ONTAP"](#) O FlexCache é uma tecnologia de armazenamento em cache que cria réplicas esparsas e graváveis de volumes no mesmo ou em diferentes clusters do ONTAP. Ele pode aproximar dados e arquivos do usuário para obter uma taxa de transferência mais rápida com um espaço físico menor. Saiba como o FlexCache pode ser usado, as práticas recomendadas, limites e considerações para o projeto e implementação.

FlexCache write-back

["FlexCache write-back"](#) Introduzido no ONTAP 9.15.1, o FlexCache write-back é um modo alternativo de operação para escrever em um cache. Write-back permite que a gravação seja comprometida com o armazenamento estável no cache e reconhecida ao cliente sem esperar que os dados cheguem à origem. Os dados são escoados assincronamente de volta à origem. Como resultado, um sistema de arquivos distribuído globalmente permite que as gravações sejam executadas em velocidades quase locais para workloads e ambientes específicos, oferecendo benefícios significativos de performance.

Volumes FlexGroup

["TR-4571: Guia de práticas recomendadas e implementação do NetApp ONTAP FlexGroup volumes"](#) Saiba mais sobre o FlexGroup volumes, práticas recomendadas e dicas de implementação. Os volumes FlexGroup são uma evolução de contêineres nas ONTAP com escalabilidade horizontal que combina capacidade quase infinita com performance previsível e de baixa latência em workloads com uso intenso de metadados.

["TR-4678: Proteção de dados e backup de volumes FlexGroup"](#) Saiba mais sobre a proteção de dados e o backup para volumes FlexGroup, incluindo cópias Snapshot, SnapMirror e outras soluções de proteção e backup de dados.

Relatórios técnicos de rede da ONTAP

O ONTAP fornece uma variedade de configurações e recursos de rede diferentes para atender aos aplicativos de escalabilidade horizontal mais exigentes. Usando os recursos e recursos de rede, as empresas podem criar acesso confiável e seguro aos seus dados.



Esses relatórios técnicos expandem a "[Gerenciamento de rede ONTAP](#)" documentação do produto.

Roteamento

["TR-4949: BGP/VIP com ONTAP no data center"](#) Saiba como implantar rapidamente uma configuração básica de BGP no ONTAP.

Serviços de nomes

["TR-4523: Balanceamento de carga DNS no ONTAP"](#) Saiba como configurar o ONTAP para uso com metodologias de balanceamento de carga DNS, incluindo DNS no ONTAP, vários métodos de configuração e práticas recomendadas.

["TR-4668: Guia de melhores práticas de serviços de nomes"](#) Saiba mais sobre práticas recomendadas, limites e considerações ao implementar soluções nas (Network-Attached Storage), como CIFS/SMB e NFS no ONTAP.

["TR-4835: Como configurar LDAP no gerenciamento de identidade nas multiprotocolo ONTAP"](#) Saiba como configurar o gerenciamento de identidade LDAP (Lightweight Directory Access Protocol) no ONTAP para nas multiprotocolo.

NFS

Relatórios técnicos do ONTAP NFS

NetApp NFS simplifica o gerenciamento de dados e ajuda você a acompanhar o crescimento enquanto otimiza custos.

NFS

["TR-4067: Guia de práticas recomendadas e implementação de NFS em ONTAP"](#) Saiba mais sobre conceitos básicos, informações de suporte, dicas de configuração e práticas recomendadas para NFS no ONTAP.

["TR-4962: NFSv4,2 atributos estendidos"](#) Saiba mais sobre como ativar e usar atributos estendidos do NFSv4,2 no ONTAP 9.12,1 e posterior.

Multiprotocolo

["TR-4887: Visão geral e melhores práticas de nas multiprotocolo na ONTAP"](#) Saiba como o acesso nas multiprotocolo funciona no ONTAP e as práticas recomendadas para ambientes multiprotocolo.

NFS sobre TLS

Visão geral do NFS sobre TLS

ONTAP 9.19.1 introduz NFS sobre TLS, o tão aguardado "botão fácil" para criptografar seu tráfego NFS.

Antes desse recurso, criptografar sua carga NFS em trânsito era limitado ao IPsec ou Kerberos. Embora ambos sejam eficazes, a configuração era trabalhosa e as penalidades de desempenho podiam ser altas. Ambos os métodos eram soluções "adicionais" — soluções não definidas em uma RFC especificamente para NFS. ["RFC 9289"](#), intitulado "Toward Remote Procedure Call Encryption by Default", mudou isso. Agora NFSv3 e NFSv4.x podem criptografar o tráfego RPC NFS em trânsito usando TLS 1.3. Kerberos não é necessário. IPsec não é necessário.

Pré-requisitos

Para usar ONTAP NFS sobre TLS, você deve atender aos seguintes requisitos.

- ...estar executando ONTAP 9.19.1
 - Personalidades de nuvem ONTAP não são suportadas neste momento
- ...possuem licença NFS
- ...encontrou um cliente NFS no ["NetApp Matriz de interoperabilidade"](#)

O que não faz

NFS sobre TLS protege a camada de transporte; ele não altera a forma como NFS autentica os usuários.

Autenticação de usuário baseada em certificado. NFS sobre TLS **não fornece um novo mecanismo de autenticação de usuário.** Você ainda precisa de `auth_sys` ou `krb5` para autenticação de usuário. Você

ainda pode usar `krb5i` e `krb5p`, mas o TLS torna suas proteções de integridade e privacidade redundantes e você ainda terá o impacto na performance.

Casos de uso e cargas de trabalho

NFS sobre TLS é uma boa opção para três cenários de implementação comuns: criptografia em trânsito sem uma infraestrutura Kerberos, aplicação de TLS por cliente em uma exportação compartilhada e autenticação mútua de cliente.

Nem todas as cargas de trabalho se beneficiam da mesma forma — conhecer os padrões que se encaixam e os que não se encaixam ajudará você a planejar sua implantação.

Casos de uso

Criptografia NFS em trânsito sem uma infraestrutura Kerberos. Se você precisa de criptografia NFS para dados em trânsito, mas não quer implantar e operar um Centro de Distribuição de Chaves (KDC), distribuir keytabs para clientes ou estender um domínio Kerberos para abranger seus clientes NAS, NFS sobre TLS resolve isso diretamente. Você instala um certificado de servidor por Storage Virtual Machine (SVM), habilita NFS sobre TLS em cada Interface Lógica (LIF) de dados que deve transportar NFS criptografado, e os clientes negociam TLS 1.3 em banda na porta NFS padrão. Nenhum novo serviço de autenticação é necessário.

Imposição de TLS somente por cliente em uma exportação NFS compartilhada. Se você tiver uma combinação de clientes que exigem criptografia e clientes que não precisam de criptografia, você precisa de uma maneira de forçar os clientes regulamentados a usar o caminho criptografado sem afetar os outros. A opção de regra de política de exportação `-allow-nfs-tls-only true` faz exatamente isso. Ela impede montagens não TLS de clientes correspondentes via TCP, enquanto deixa as outras regras de política de exportação intactas.

Autenticação mútua de cliente (mTLS) para confiança entre armazenamento e cliente. Se você está operando sob princípios de rede de confiança zero ou possui requisitos de reforço que exigem que o controlador de armazenamento verifique a identidade do host de cada cliente que se conecta, use a opção de TLS mútuo por LIF. Defina `-enforce-host-auth true` em `vserver nfs tls interface enable` ou `vserver nfs tls interface modify`. O ONTAP então valida o certificado X.509 de cada cliente que se conecta em relação à cadeia de confiança da Autoridade Certificadora (CA) instalada na SVM no momento do handshake TLS e rejeita clientes que não apresentem um certificado confiável. Isso oferece a você a aplicação criptográfica de "somente minha frota de hosts registrados pode acessar este NFS LIF" e funciona em conjunto com os filtros de host da política de exportação já existentes.

Cargas de trabalho

A criptografia não é gratuita. O handshake TLS tem um custo mensurável e a criptografia de registro TLS adiciona sobrecarga a cada RPC. O impacto no desempenho varia bastante dependendo da carga de trabalho, da plataforma e da disponibilidade de descarregamento de hardware. Para obter detalhes, consulte ["Desempenho"](#).

Padrões de carga de trabalho

Montagens NFS de longa duração com uma população de clientes estável são uma ótima opção. O handshake TLS tem um custo por conexão, pago no momento da montagem e no restabelecimento da sessão. Se você tiver um conjunto pequeno e estável de clientes que montam uma vez e permanecem montados por horas ou dias, você absorverá esse custo sem problemas.

Se você já gerencia o mapeamento de LIF para nome de host de forma organizada, por exemplo, com

registros DNS sob seu controle, você achará o provisionamento de NFS sobre TLS simples. O recurso é configurado por LIF: você instala um certificado de servidor cujo Common Name (CN) corresponde ao Fully Qualified Domain Name (FQDN) da LIF e cuja lista de Subject Alternative Name (SAN) contém o endereço IP da LIF.

NFS sobre TLS é a ferramenta certa quando a confidencialidade na transmissão, a identidade do servidor e, opcionalmente, a identidade do host do cliente são seus requisitos de segurança, exatamente as propriedades que o TLS oferece.

Antipadrões de carga de trabalho

Alta rotatividade de conexões ou grandes tempestades de montagens não são uma boa opção. Cada nova conexão TLS paga o custo do handshake TLS 1.3, incluindo criptografia assimétrica, validação de certificado e validação opcional da cadeia mTLS. Se muitos clientes montarem, fizerem uma pequena quantidade de trabalho, desmontarem e reconectarem repetidamente, você pagará esse custo de handshake várias vezes em vez de amortizá-lo.

Arquitetura

NFS sobre TLS é um recurso de segurança de transporte por LIF do servidor NFS do ONTAP. Ele aplica proteção TLS ao tráfego NFS entre o cliente e o servidor NFS do ONTAP. A configuração é gerenciada por meio da família de comandos `vserver nfs tls interface` e do recurso REST correspondente `/api/protocols/nfs/tls/interfaces`.

A configuração é específica para cada SVM, aplicada por LIF e replicada em todo o cluster. Qualquer nó que hospeda a LIF aplica as mesmas configurações de TLS. Não há opção de ativação/desativação para todo o cluster. Habilitar e desabilitar são operações realizadas por LIF.

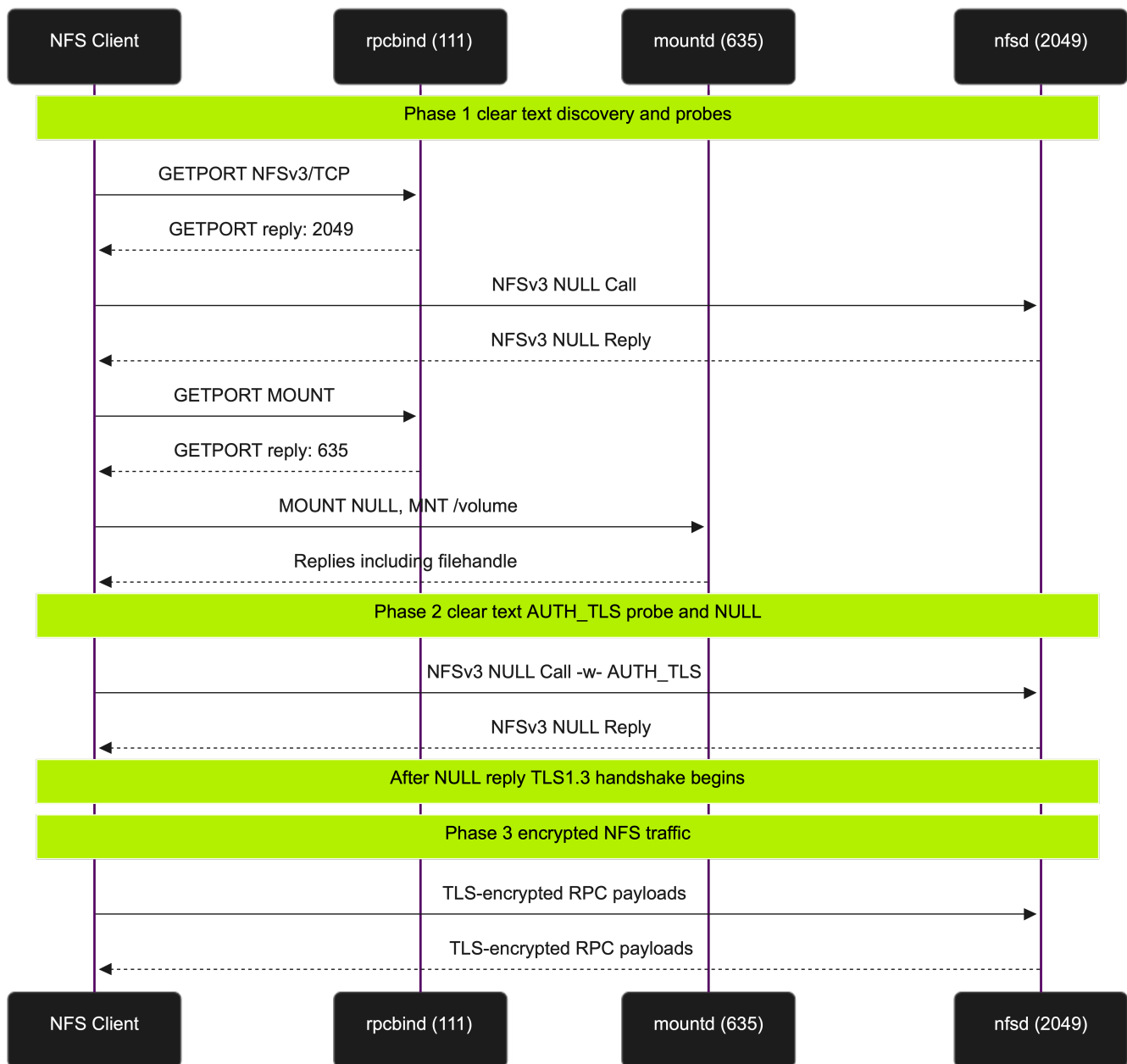
Dependências externas

Nenhuma chamada de saída para uma Autoridade Certificadora (CA) externa ou respondedor OCSP é feita a partir do caminho de handshake TLS do NFS na versão 9.19.1. A validação da cadeia e do Subject Alternative Name (SAN) é realizada localmente em relação ao material de certificado instalado no SVM.

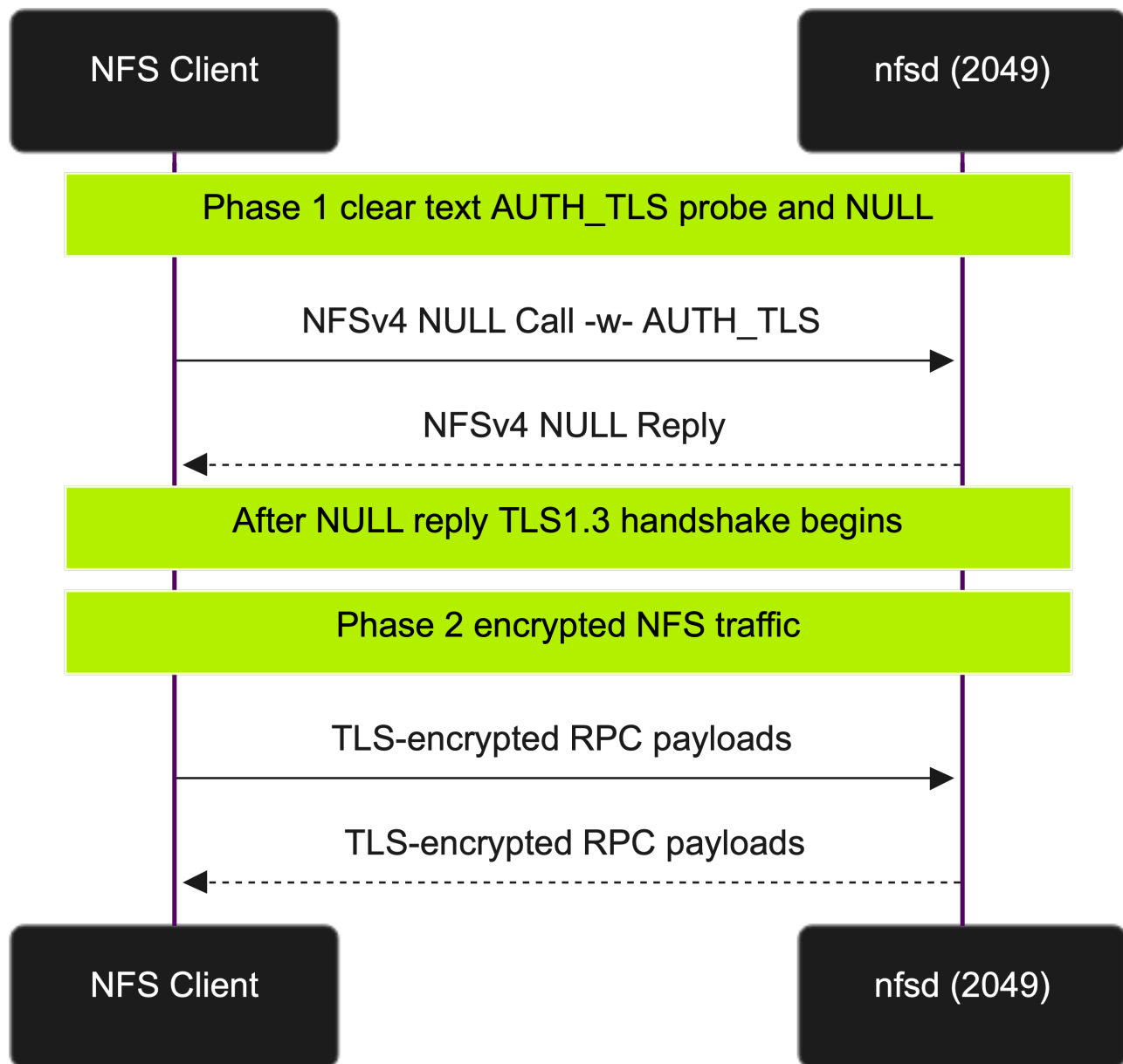
Fluxo de dados

Tanto o NFSv3 quanto o NFSv4 criptografam toda a carga NFS após o primeiro par de chamada/resposta NULL para a porta TCP 2049. A chamada NULL possui o novo `AUTH_TLS` tipo de credencial definido na RFC 9289, que sinaliza a intenção do cliente de usar TLS. O servidor responde com uma resposta NULL que aceita ou rejeita a atualização para TLS. Se o cliente receber aceitação, ele prossegue com o handshake TLS 1.3 na mesma conexão TCP. Se o handshake for concluído com sucesso, todas as chamadas RPC NFS subsequentes são encapsuladas em registros TLS e criptografadas em trânsito.

Existe uma diferença entre NFSv3 e NFSv4.x: o NFSv3 depende de protocolos auxiliares `-rpcbind` (portmapper), `mountd`, `NLM` (Network Lock Manager) e `NSM` (Network Status Monitor), que não são transmitidos pela conexão protegida por TLS e são enviados em texto não criptografado. Organizações com requisitos de conformidade que exigem criptografia total do tráfego de armazenamento devem considerar isso ao escolher entre NFSv3 e NFSv4.x. O NFSv4.x elimina esses protocolos de canal lateral; todo o tráfego NFSv4.x é consolidado na porta 2049 e criptografado após o handshake TLS.



O NFSv4.x não utiliza protocolos auxiliares, portanto, todas as RPCs do NFSv4.x são criptografadas após o handshake TLS.



ONTAP encerra o TLS no servidor NFS do nó que atualmente hospeda a LIF. Acima da camada de transporte, o servidor NFS processa as chamadas de procedimento remoto (RPCs) de forma idêntica a uma conexão NFS sem TLS.

Comportamento de takeover de HA

Sessões NFS sobre TLS existentes não sobrevivem a uma transição de alta disponibilidade (HA) ou a um pânico inesperado de nó. TLS é um transporte em nível de sessão construído sobre TCP. Quando as conexões TCP caem com o nó, as sessões TLS caem junto.

Após a aquisição, os clientes se reconectam e realizam um novo handshake TLS 1.3. O nó parceiro utiliza a mesma configuração TLS replicada — vinculação de certificado, configuração de autenticação de host e configuração de validação SAN — porque o registro de configuração é replicado em todo o cluster.

Os tickets de sessão TLS e as chaves pré-compartilhadas (PSKs) são locais ao nó e não são transferidos

para o parceiro. Espere uma tempestade de reconexões com handshakes TLS completos na tomada de controle.

MetroCluster e comportamento SVM-DR

O certificado da interface TLS e a configuração são replicados com a SVM por meio do caminho de replicação padrão SVM-DR e de replicação em nível de SVM do MetroCluster. Após um switchover com preservação de identidade, a SVM de destino mantém a mesma configuração TLS por LIF.

O `-allow-nfs-tls-only` campo na regra de política de exportação é replicado juntamente com o restante da regra de política de exportação pelo caminho padrão de replicação de política de exportação. No SVM-DR, a regra acompanha a política quando a política é replicada com o SVM.

Configurar NFS sobre TLS

NFS sobre TLS é configurado por LIF usando a ``vserver nfs tls interface`` família de comandos, os ``/api/protocols/nfs/tls/interfaces`` endpoints REST ou as configurações de NFS do System Manager.

As regras de política de exportação ganham um campo complementar que permite impor acesso somente TLS para clientes correspondentes. Para referências de comandos, consulte "netapp.com/br/". Você pode explorar a API REST interativamente por meio da documentação Swagger incorporada — basta acessar <https://<cluster-mgmt-ip>/api/docs>.

Pré-requisitos do ONTAP

O procedimento descrito abaixo pressupõe que os seguintes pré-requisitos sejam atendidos:

- ONTAP 9.19.1 ou posterior
- Uma SVM com o protocolo NFS habilitado
- Pelo menos uma LIF de dados configurada para acesso NFS básico

Etapa 1: criar uma CA raiz no ONTAP



Opção de CA externa. Se sua organização utiliza uma CA externa, ignore esta etapa. Você enviará as solicitações de assinatura de certificado (CSRs) das etapas 2 e 5 para sua CA externa e instalará os certificados assinados resultantes no ONTAP. O restante do procedimento permanece o mesmo.

ONTAP pode atuar como uma Autoridade Certificadora (CA) interna para implantações em laboratório e internas. Esta etapa cria uma CA raiz autoassinada na SVM que será usada para assinar o certificado do servidor (e, opcionalmente, certificados de cliente para TLS mútuo).

```
ontap9::> security certificate create -vserver <svm> -common-name <ca-name> -type root-ca -size 2048 -hash-function SHA256 -expire-days 3652 -country US -state <state> -locality <city> -organization <org> -unit <unit>
```

Após a conclusão do comando, recupere e anote o número de série da CA. Ele é necessário na etapa 2 e, se estiver usando mutual TLS, na etapa 5.

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields serial
```

Anote o número de série: isso se torna <ca-serial> em etapas posteriores.

Etapa 2: gere o certificado do servidor para o LIF de dados

ONTAP apresenta este certificado aos clientes NFS durante o handshake TLS. O Nome Comum (CN) e o Nome Alternativo do Assunto (SAN) do certificado devem corresponder ao FQDN e ao endereço IP da LIF, pois o `tlshd` no cliente valida a identidade do servidor em relação a ambos.



Requisito de SAN IP. Se você planeja configurar trunking de sessão NFSv4.1 com NFS sobre TLS, ou se qualquer comando de montagem usar um endereço IP em vez de um nome de host, o certificado deve incluir uma entrada de SAN IP para cada endereço IP de LIF ao qual os clientes irão se conectar. Sem isso, o handshake TLS falha com "Certificate owner unexpected" para caminhos com endereços IP.

O gerador de CSR do ONTAP (`security certificate generate-csr`) suporta SAN IP diretamente via `-ipaddr`, que aceita uma lista de endereços IP separados por vírgulas.

2a. Gerar a CSR e a chave privada.

Inclua `-ipaddr` uma lista separada por vírgulas de todos os endereços IP da LIF que transportarão tráfego NFS sobre TLS. Inclua `-dns-name` o nome ou nomes de host usados nos comandos de montagem.

```
ontap9::> security certificate generate-csr -common-name <lif-fqdn>
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name <lif-fqdn> -ipaddr <lif-ip>[,<lif-ip-2>,...] -country
US -state <state> -locality <city> -organization <org> -unit <unit>
```

Exemplo, para uma única LIF:

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130 -country US
-state CA -locality SanJose -organization "MyOrg" -unit "Storage"
```

Para o trunking de sessão entre dois endereços IP de LIF, forneça ambos em uma lista separada por vírgulas:

```
ontap9::> security certificate generate-csr -common-name nfs.example.com
-security-strength 128 -hash-function SHA256 -extended-key-usage
serverAuth -dns-name nfs.example.com -ipaddr 192.0.2.130,192.0.2.131
-country US -state CA -locality SanJose -organization "MyOrg" -unit
"Storage"
```

O comando gera um bloco PEM de Solicitação de Assinatura de Certificado (CSR) e um bloco PEM de chave privada. Copie ambos e salve-os — a chave privada é exibida apenas uma vez.

Para verificar se o CSR contém os SANs esperados antes da assinatura, execute em qualquer cliente com OpenSSL:

```
echo <paste CSR PEM> | openssl req -noout -text | grep -A3 "Subject  
Alternative"
```

Saída esperada:

```
X509v3 Subject Alternative Name: critical  
DNS:nfs.example.com, IP Address:192.0.2.130
```

2b. Assine o CSR com a CA do ONTAP.

```
ontap9::> security certificate sign -vserver <svm> -ca <ca-name> -ca  
-serial <ca-serial> -expire-days 365 -hash-function SHA256
```

Cole o bloco PEM do CSR quando solicitado. Copie o certificado PEM assinado da saída.

2c. Instale o certificado de servidor assinado.

```
ontap9::> security certificate install -vserver <svm> -type server -cert  
-name <cert-name>
```

Quando solicitado:

- Cole o certificado PEM assinado.
- Cole a chave privada PEM.
- Quando solicitado a inserir certificados intermediários ou raiz, cole o arquivo PEM do certificado da CA e pressione Enter, depois responda n para interromper a adição de certificados.

2d. Verifique o certificado instalado.

```
ontap9::> security certificate show -vserver <svm> -type server -common  
-name <cert-name>
```

Confirme a data de validade e se o registro está presente.

Etapa 3: habilite NFS sobre TLS na LIF de dados

Com o certificado do servidor instalado, habilite NFS sobre TLS na LIF de destino.

```
ontap9::> vserver nfs tls interface enable -vserver <svm> -lif <lif>
-certificate-name <cert-name>
```

Verifique se o LIF está habilitado para TLS.

```
ontap9::> vserver nfs tls interface show -vserver <svm>
```

Saída esperada:

```
Vserver:                <svm>
Logical Interface:      <lif>
IP Address:             <lif-ip>
TLS Status:             enabled
TLS Certificate Name:   <cert-name>
Enforce Host Authentication: false
```

‘TLS Status: enabled’ confirma que ONTAP negociará TLS na porta 2049 para esta LIF. Clientes que utilizam ‘xprtsec=tls’ ou ‘xprtsec=mtls’ agora receberão uma conexão protegida por TLS. Clientes que não solicitam TLS ainda se conectam em texto não criptografado, a menos que a imposição seja adicionada na Etapa 7.

Etapa 4: instale o certificado da CA no cliente Linux

O cliente Linux deve confiar na Autoridade Certificadora (CA) que assinou o certificado do servidor ONTAP. Sem isso, `tlshd` rejeita o handshake TLS porque o certificado do servidor não é confiável.

Se você utilizou o ONTAP CA (Etapa 1)

Exporte o certificado da CA do ONTAP:

```
ontap9::> security certificate show -vserver <svm> -common-name <ca-name>
-type root-ca -fields cert
```

Copie o certificado PEM da saída e salve-o em um arquivo (por exemplo, `nfs-ca.crt`). Transfira este arquivo para o cliente Linux.

Se você utilizou uma CA externa

Obtenha o certificado PEM da sua infraestrutura de CA externa e salve-o em um arquivo (por exemplo, `nfs-ca.crt`). Transfira este arquivo para o cliente Linux.

Instale o certificado da CA no repositório de confiança do sistema

RHEL / Rocky / AlmaLinux / Fedora:

```
sudo cp nfs-ca.crt /etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
sudo update-ca-trust
```

Debian / Ubuntu:

```
sudo cp nfs-ca.crt /usr/local/share/ca-certificates/nfs-tls-ca.crt
sudo update-ca-certificates
```

Configure o tlshd para usar esta CA como seu repositório de confiança

Editar /etc/tlshd.conf:

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
```

Ajuste o `x509.truststore` caminho para corresponder ao local onde você colocou o certificado da CA.

Reinicie o tlshd para aplicar a configuração:

```
sudo systemctl restart tlshd
```

Verifique se o tlshd foi iniciado corretamente:

```
journalctl -u tlshd -n 20 --no-pager
```

Não deve haver linhas de erro na saída.

Etapa 5: Resolver o FQDN do LIF no cliente

tlshd valida o certificado do servidor em relação ao nome do host usado no comando de montagem. Confirme que `<lif-fqdn>` resolve para `<lif-ip>` no cliente antes de montar.

```
getent hosts <lif-fqdn>
```

Se o nome do host não for resolvido via DNS, adicione uma entrada estática:

```
echo <lif-ip> <lif-fqdn> | sudo tee -a /etc/hosts
```

Etapa 6: Montar com NFS sobre TLS

Carregue o módulo TLS do kernel caso ainda não esteja carregado:

```
sudo modprobe tls
```

Crie o ponto de montagem e monte:

```
sudo mkdir -p <mountpoint>
sudo mount -t nfs \
  -o vers=4.1,xprtsec=tls \
  <lif-fqdn>:<export-path> <mountpoint>
```

Etapa 7: verifique a conexão TLS

Lado do cliente

Confirme se a montagem está ativa e exibe xprtsec=tls:

```
mount | grep nfs
```

Saída esperada (linha contendo o ponto de montagem):

```
<lif-fqdn>:<export-path> on <mountpoint> type nfs4
(rw,...,xprtsec=tls,...)
```

Confirme `tlshd` que um handshake TLS foi concluído com sucesso:

```
journalctl -u tlshd -n 10 --no-pager
```

Procure uma linha que contenha:

```
Handshake with '<lif-fqdn>' (...) was successful
```

Lado ONTAP

Confirme se a conexão está listada como TLS/nfs (gere uma pequena quantidade de E/S primeiro, caso a

conexão tenha sido estabelecida recentemente):

```
ontap9::> network connections active show -vserver <svm>
```

Entrada esperada:

```
<lif>:2049 <client-fqdn>:<port> TLS/nfs
```

Verifique se não ocorreram erros de handshake TLS:

```
ontap9::> event log show -severity error -message-name  
Nblade.TLSHandshakeFailed
```

A ausência de novas entradas desde a tentativa de montagem significa que o handshake foi bem-sucedido.

Opcional: exigir TLS para clientes específicos (aplicação da política de exportação)

Por padrão, NFS sobre TLS é opcional: clientes que não solicitam TLS ainda podem se conectar em texto não criptografado em uma LIF habilitada para TLS. Para impor TLS para uma regra de exportação específica, defina `-allow-nfs-tls-only true`.

```
ontap9::> vserver export-policy rule modify -vserver <svm> -policyname  
<policy-name> -ruleindex <rule-index> -allow-nfs-tls-only true
```

Após configurar isso, qualquer cliente NFS correspondente a essa regra que **não** utilize TLS será rejeitado no ponto de avaliação da regra de exportação. Conexões TLS existentes não são afetadas.

Verifique:

```
ontap9::> vserver export-policy rule show -vserver <svm> -policyname  
<policy-name> -fields allow-nfs-tls-only
```

Opcional: TLS mútuo (autenticação de cliente)

O NFS padrão sobre TLS autentica o servidor para o cliente (TLS somente no servidor). O TLS mútuo (`xprtsec=mtls` exige adicionalmente que o cliente apresente um certificado que o ONTAP valida. Isso fornece autenticação criptográfica do host em ambos os lados.



Requisito do sistema operacional do cliente. O TLS mútuo requer `ktls-utils` 0.12 ou posterior. A versão fornecida com RHEL 9.7 (`ktls-utils` 0.11 não funciona — ela nunca envia o certificado do cliente, independentemente da configuração. RHEL 10.1 (`ktls-utils` 1.2.1 é validado. Verifique sua `ktls-utils` versão antes de prosseguir.



Opção de montagem. Use `xprtsec=mtls`, **não** `xprtsec=tls`. Com `xprtsec=tls`, o kernel envia o modo de autenticação `HANDSHAKE_AUTH_UNAUTH` para `tlshd`, que segue o caminho de handshake anônimo e não apresenta um certificado de cliente, mesmo que um esteja configurado.

Etapa 1: criar uma CA para certificados de cliente (ONTAP)

Pode ser a mesma CA da Etapa 1 ou uma diferente. Recomenda-se o uso de uma CA diferente para produção, para que as cadeias de certificados do servidor e do cliente sejam distintas.

```
ontap9::> security certificate create -vserver <svm> -common-name "NFS-
mTLS-CA" -type root-ca -expire-days 3652 -hash-function SHA256
```

Anote o número de série como `<mtls-ca-serial>`.

Etapa 2: instale a CA como uma âncora de confiança cliente-CA (ONTAP)

Exporte o certificado da CA:

```
ontap9::> security certificate show -vserver <svm> -common-name "NFS-mTLS-
CA" -type root-ca -fields cert
```

Instale-o como tipo `client-ca`:

```
ontap9::> security certificate install -vserver <svm> -type client-ca
```

Cole o certificado CA em formato PEM quando solicitado. Verifique:

```
ontap9::> security certificate show -vserver <svm> -type client-ca
```

Etapa 3: Habilite o `enforce-host-auth` no LIF (ONTAP)

```
ontap9::> vserver nfs tls interface modify -vserver <svm> -lif <lif>
-enforce-host-auth true
```

Verifique:

```
ontap9::> vserver nfs tls interface show -vserver <svm> -instance
```

Confirme: `Enforce Host Authentication: true`.

Etapa 4: Gere a chave do cliente e o CSR (cliente Linux)

```
sudo mkdir -p /etc/nfs
sudo openssl genrsa -out /etc/nfs/client.key 2048
sudo chmod 600 /etc/nfs/client.key

sudo openssl req -new \
  -key /etc/nfs/client.key \
  -subj "/CN=<client-fqdn>/C=US" \
  -addext "subjectAltName=DNS:<client-fqdn>,IP:<client-ip>" \
  -out /tmp/client.csr

cat /tmp/client.csr
```

Etapa 5: Assine o CSR do cliente com a CA do ONTAP

No cluster ONTAP:

```
ontap9::> security certificate sign -vserver <svm> -ca "NFS-mTLS-CA" -ca
-serial <mtls-ca-serial> -expire-days 365 -hash-function SHA256
```

Cole o conteúdo `/tmp/client.csr` quando solicitado. Copie o certificado PEM assinado da saída.

Etapa 6: criar o arquivo da cadeia de certificados do cliente (cliente Linux)

Salve o certificado assinado em `/tmp/client-signed.crt`. Obtenha também o certificado da CA PEM (`nfs-mtls-ca.crt`). Concatene-os em um arquivo de cadeia:

```
sudo bash -c "cat /tmp/client-signed.crt /path/to/nfs-mtls-ca.crt \
  > /etc/nfs/client-chain.crt"
sudo chmod 600 /etc/nfs/client-chain.crt
```



Por que um arquivo de cadeia? `tlshd` A versão 1.2.1 usa

`gnutls_pcert_list_import_x509_raw` e exige a cadeia completa de certificados (folha seguida pela CA) para que o GnuTLS resolva corretamente o emissor durante o callback `find_x509_client_cert`. Um arquivo contendo apenas o certificado folha causa uma falha de asserção no GnuTLS.

Passo 7: Atualize o arquivo `/etc/tlshd.conf` com o certificado do cliente (cliente Linux)

```
[debug]
loglevel=1
tls=1
nl=0

[authenticate]

[authenticate.client]
x509.truststore=/etc/pki/ca-trust/source/anchors/nfs-tls-ca.crt
x509.certificate=/etc/nfs/client-chain.crt
x509.private_key=/etc/nfs/client.key
```

Reinicie tlshd:

```
sudo systemctl restart tlshd
```

Etapla 8: Monte com xprtsec=mtls

```
sudo mount -t nfs \
-o vers=4.1,xprtsec=mtls \
<lif-fqdn>:<export-path> <mountpoint>
```

Etapla 9: Verifique o TLS mútuo

Cliente:

```
mount | grep nfs
# Confirm: xprtsec=mtls in mount options

journalctl -u tlshd -n 5 --no-pager
# Confirm: "Handshake with '<lif-fqdn>' (...) was successful"
```

ONTAP:

```
ontap9::> network connections active show -vserver <svm>
# Confirm: <lif>:2049 <client-fqdn>:<port> TLS/nfs

ontap9::> event log show -severity error -message-name
Nblade.TLSHandshakeFailed
# No new entries = success
```

Configurações padrão que importam

- `-enforce-host-auth = false` NFS sobre TLS não impõe autenticação baseada em host por padrão. Essa é a postura mais flexível. Configurar para `true` rejeitar conexões TLS cuja identidade do certificado não corresponda à identidade do host da LIF.
- `-skip-san-validation = false` A verificação SAN é realizada por padrão. Definir esse parâmetro para `true` relaxa a vinculação de identidade entre certificado e LIF. Este parâmetro é somente para gravação: chamadas subsequentes de `show` ou `GET` não exibem o valor, portanto, os administradores não podem determinar posteriormente se a validação SAN foi ignorada no momento da ativação ou modificação.
- `-allow-nfs-tls-only = false` Uma regra de export-policy não exige TLS por padrão. Habilitar NFS sobre TLS em uma LIF não rejeita NFS em texto simples por si só. Se você deseja uma postura rígida de uso exclusivo de TLS, opte por essa configuração em cada regra e certifique-se de que o TLS esteja habilitado em todas as LIFs de dados que atendem esses clientes primeiro, caso contrário, você negará o acesso.

Os comandos `vserver export-policy rule create` e `vserver export-policy rule modify` ganham um novo campo, `-allow-nfs-tls-only`, que restringe os clientes correspondentes apenas a conexões NFS sobre TLS.

Endpoints REST

Você pode explorar a API REST interativamente por meio da documentação Swagger incorporada — basta acessar no seu navegador <https://<cluster-mgmt-ip>/api/docs>. Os endpoints NFS sobre TLS estão no caminho `/api/protocols/nfs/tls/interfaces` para a configuração do LIF e em `/api/protocols/nfs/export-policies/{policy.id}/rules` para o campo da regra de export-policy.

Segurança

Esta página aborda os requisitos de RBAC, validação de certificados, parâmetros de criptografia, auditoria e limitações de segurança conhecidas para NFS sobre TLS no ONTAP 9.19.1.

Requisitos de função e RBAC

A família de comandos `vserver nfs tls interface-enable, disable, modify` e `show` é com escopo de SVM. Ela pode ser executada pela função de cluster `admin` ou pelo `vsadmin` da SVM proprietária.

O campo `-allow-nfs-tls-only`on`` `vserver export-policy rule` é um campo de escrita no objeto de regra de exportação existente. Ele usa o RBAC padrão da regra de política de exportação.

Os endpoints REST `/api/protocols/nfs/tls/interfaces`` correspondem diretamente aos comandos da CLI acima. Eles utilizam o RBAC padrão de administração do NAS. Nenhuma função REST separada é definida.

Autenticação e autorização

Habilitar NFS sobre TLS em uma LIF requer um certificado X.509 de servidor instalado na SVM via `security certificate install`. O certificado é vinculado por LIF no momento da habilitação usando `-certificate-name`.

ONTAP aplica duas verificações ao certificado do servidor fornecido:

1. O Nome Comum (CN) do certificado deve corresponder ao Nome de Domínio Totalmente Qualificado (FQDN) da LIF.
2. O endereço IP da LIF deve constar na lista de Nomes Alternativos do Assunto (SAN) do certificado.

Uma opção `-skip-san-validation` booleana (padrão `false`) suprime a verificação SAN no momento da ativação ou modificação.

Cada falha na verificação retorna um erro distinto.

A autenticação de host mútua TLS (mTLS) é opcional. Defina `-enforce-host-auth true` como `vserver nfs tls interface enable` `on` `modify` para habilitá-la. O padrão é `false`, o que significa autenticação apenas do servidor. Os certificados do cliente são validados em relação à cadeia de confiança da CA instalada na SVM, cujo provisionamento é de sua responsabilidade.

Autenticação de usuário

A autenticação de usuário permanece inalterada pelo TLS. O TLS adiciona confidencialidade no tráfego e autenticação do host. `AUTH_SYS` O UID/GID do UNIX ou `RPCSEC_GSS` Kerberos ainda devem ser usados para autenticação de usuário RPC. A RFC 9289 é explícita sobre isso: o TLS protege o transporte, enquanto os tipos de autenticação NFS existentes lidam com a autenticação de usuário exatamente como sempre fizeram.

Criptografia

Em trânsito

Quando NFS sobre TLS está habilitado em uma LIF, somente a versão TLS 1.3 é utilizada. Os seguintes conjuntos de cifras são suportados:

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`
- `TLS_CHACHA20_POLY1305_SHA256`

A troca de chaves utiliza ECDHE na `secp384r1` curva. A criptografia se aplica ao tráfego NFSv3 e NFSv4.x transportado pela LIF habilitada para TLS.

Auditoria

Todas as alterações de configuração do NFS sobre TLS são registradas no log de auditoria padrão do ONTAP (`security audit log show`). As seguintes operações são registradas:

- `vserver nfs tls interface enable`
- `vserver nfs tls interface modify`
- `vserver nfs tls interface disable`
- `vserver export-policy rule create -allow-nfs-tls-only`
- `vserver export-policy rule modify -allow-nfs-tls-only`

As operações somente leitura `show` e `GET` seguem a política de log de auditoria padrão do ONTAP e normalmente não são registradas, a menos que a auditoria esteja configurada para registrá-las.

Três eventos EMS visíveis ao cliente são emitidos no caminho de dados NFS-over-TLS. Para detalhes do evento, condições de ativação e limites de taxa, consulte ["Mensagens EMS"](#).

Limite de locatário

A configuração NFS-over-TLS é feita por SVM. Um administrador de SVM pode visualizar e gerenciar apenas a configuração TLS nas LIFs pertencentes à sua própria SVM. Os administradores do cluster visualizam todas as SVMs.

As referências aos certificados do servidor são locais ao SVM. A configuração é replicada em todo o cluster, de modo que qualquer nó que atenda a uma determinada LIF aplique a mesma configuração TLS.

Limitações conhecidas relevantes para a segurança

Aviso sobre certificados autoassinados. A CLI `enable` e `modify` comandos alertam que certificados autoassinados expõem você a ataques do tipo "man-in-the-middle". Use um certificado assinado por uma CA instalado via `security certificate install`.

O TLS mútuo é opcional. Com o padrão `-enforce-host-auth false`, NFS sobre TLS protege a confidencialidade e a integridade na transmissão e autentica o servidor para o cliente, mas não autentica criptograficamente o host do cliente. Se você precisar disso, habilite o mTLS explicitamente.

A aplicação exclusiva de TLS é feita por regra de política de exportação, não globalmente. Até que você configure `-allow-nfs-tls-only true` na regra de política de exportação relevante, a mesma LIF ainda poderá aceitar conexões NFS sem TLS de clientes que, de outra forma, seriam permitidos pela regra.

Monitorar NFS sobre TLS

NFS sobre TLS expõe contadores do Counter Manager no `nfs_tls` objeto e quatro eventos do EMS que você pode usar para monitorar a integridade da conexão e o comportamento de aplicação de regras.

Contadores do Counter Manager

Todos os contadores do Gerenciador de Contadores NFS sobre TLS residem no objeto com escopo de administrador `nfs_tls`. Visualize-os com `statistics show -object nfs_tls`. Use `-counter <name>` para filtrar para um único contador ou `-instance` para restringir a uma linha específica de SVM ou nó.

Contadores de identificador/rótulo (string):

- `nfs_tls:instance_name`--nome da instância (nome da SVM constituinte) para a linha.
- `nfs_tls:instance_uuid`--UUID da instância para a linha (identificador SVM constituinte).
- `nfs_tls:vserver_id`--Rótulo identificador SVM para uma linha agregada.
- ``nfs_tls:vserver_name``--Rótulo do nome SVM para uma linha agregada.
- `nfs_tls:node_name`--rótulo do nome do nó para uma linha agregada.

Contadores de volume de conexão (taxa):

- `nfs_tls:tls_total_connection_requests`--total de solicitações de conexão NFS-over-TLS processadas (sucesso + falha).

- ``nfs_tls:tls_connection_success`` conexões NFS sobre TLS bem-sucedidas.
- `nfs_tls:tls_disabled_connection_failures`--Conexões rejeitadas porque NFS sobre TLS está desativado na SVM.
- `nfs_tls:tls_connection_handshake_failures`--conexões que falharam durante o handshake TLS.
- `nfs_tls:tls_configuration_not_found`--tentativas de conexão rejeitadas porque não existe configuração TLS para o par SVM/LIF.
- `nfs_tls:tls_connection_mismatch`--conexões que falharam porque o identificador de conexão na memória não correspondeu à conexão observada durante a conclusão do handshake.

Contador de latência (média):

- `nfs_tls:tls_handshake_average_latency`` latência média de handshake TLS em microssegundos. Contador base: ``tls_connection_success``.

Mensagens do Sistema de Gerenciamento de Eventos (EMS)

Quatro eventos EMS visíveis para o cliente são emitidos pelo servidor NFS no caminho de dados NFS-over-TLS. Visualize-os com `event log show`.

Nblade.TLSConfigError

Severidade ERR, com limite de taxa de 10 minutos. Acionado quando um cliente tenta usar NFS sobre TLS em uma SVM/LIF que não possui configuração TLS. Campos registrados: endereço IP do cliente, nome da SVM, endereço IP da LIF. Para resolver, habilite a configuração com `vserver nfs tls interface enable`.

Nblade.TLSHandshakeFailed

Gravidade ERR, taxa limitada a 10 minutos. Acionado quando o handshake TLS entre o cliente e o servidor falha. Campos registrados: nome da SVM, endereço IP da LIF, endereço IP do cliente (remoto), UUID do certificado do servidor. Para resolver, verifique a configuração TLS na LIF e a integridade da rede. Se o problema persistir, entre em contato com o suporte da NetApp.

Nblade.NfsTlsDisabled

Severidade ALERT, com limite de taxa de 24 horas. Acionada quando um cliente tenta usar NFS sobre TLS em uma SVM onde o recurso está desativado. Campos registrados: nome da SVM.

Nblade.nfsTLSSuccessErr

Gravidade ERR. Acionado quando um cliente correspondente a uma regra de política de exportação com `-allow-nfs-tls-only true` tenta montar ou acessar o caminho NFS sem TLS. Use este evento para confirmar que clientes sem TLS estão sendo bloqueados conforme o esperado.

Desempenho

O TLS aumenta o custo em três dimensões de recursos: CPU, memória e rede.

Visão geral dos custos de recursos

CPU é o principal custo. O handshake TLS 1.3 é uma despesa única por conexão, cobrindo criptografia assimétrica, análise de certificados e troca de chaves. Depois que a conexão é estabelecida, a sobrecarga em estado estacionário é a criptografia simétrica de registros usando AES-GCM ou ChaCha20-Poly1305. Em

plataformas equipadas com Mellanox ConnectX-6 Dx (CX6-Dx) ou ConnectX-7 (CX7) NICs, a própria NIC realiza a criptografia e a descriptografia por meio do descarregamento do kernel TLS (KTLS), reduzindo significativamente o custo da CPU em estado estacionário.

O impacto na **memória** é baixo. O TLS adiciona um estado de sessão por conexão e um cache de configuração TLS por nó. O tamanho do cache é limitado; as entradas são atualizadas de acordo com o Time-To-Live (TTL) e atualizadas em segundo plano.

O overhead de **rede** é pequeno. O enquadramento de registro TLS 1.3 adiciona um overhead fixo por registro e uma tag de autenticação. O handshake adiciona transferências de ida e volta apenas na configuração da conexão, não por RPC.

Penalidade de desempenho do TLS

Existem dois caminhos distintos para NFS sobre TLS no ONTAP: o caminho de descarregamento por hardware e o caminho TLS por software. O caminho de descarregamento por hardware está disponível em plataformas com NICs CX6-Dx ou CX7. O caminho TLS por software é usado em plataformas sem NICs com capacidade de descarregamento.

Em plataformas com NICs com capacidade de offload, o desempenho observado ficou dentro de aproximadamente 10% do NFS em texto simples em uma variedade de cargas de trabalho. Em plataformas sem NICs com capacidade de offload, o caminho TLS por software é mais sensível à carga de trabalho e pode apresentar reduções de throughput de aproximadamente 30% em comparação com NFS em texto simples, no pior caso. Esses são números de caracterização, não especificações garantidas. Seus resultados vão variar dependendo do tipo de carga de trabalho, tamanho de E/S e número de conexões. Se você estiver misturando tráfego TLS e não-TLS no mesmo nó, espere algum impacto no throughput do tráfego não-TLS também.

Fatores de escala

Os seguintes fatores aumentam o custo agregado de CPU do TLS ou a latência do handshake:

Troca de conexões. Cada nova conexão acarreta o custo do handshake. Cargas de trabalho que abrem e fecham conexões TCP com o servidor NFS apresentam um uso agregado de CPU TLS maior do que cargas de trabalho com conexões de longa duração.

Tempestades de montagem após uma tomada de controle ou evento de rede. Cargas de trabalho em que muitos clientes se reconectam simultaneamente, como após uma tomada de controle de HA, pagam o custo total do handshake TLS 1.3 por conexão. Monitore `nfs_tls:tls_handshake_average_latency` e planeje a capacidade de conexão de acordo.

Grande número de identidades de clientes distintas (TLS mútuo). As implementações de TLS mútuo (mTLS) escalam a CPU do handshake de acordo com o número de certificados de cliente exclusivos que estão sendo validados.

mTLS vs. TLS somente no servidor. Habilitar autenticação de host (mTLS) adiciona a validação do certificado do cliente no lado do servidor, tornando cada handshake moderadamente mais caro do que o TLS somente no servidor. O custo por RPC em estado estável permanece inalterado.

Churn de configuração TLS. Alterações frequentes na configuração da interface TLS, como rotação de certificados e ciclos de ativação/desativação, invalidam o cache de configuração TLS por nó e forçam consultas de volta ao host de gerenciamento, aumentando brevemente a latência do handshake.

Interoperabilidade e limites

NFS sobre TLS é compatível com os controles de política de exportação padrão do ONTAP, replica por meio do SVM-DR e MetroCluster, e apresenta um pequeno conjunto de limitações de plataforma e recomendações operacionais que você deve conhecer antes da implementação.

Interoperabilidade

Funcionalidades coexistentes suportadas

Políticas de exportação, exportações de qtree e caminhos de junção. A regra de política de exportação ganha o campo `-allow-nfs-tls-only`, que pode exigir TLS individualmente para cada regra. Ela se integra aos controles de segurança existentes, como `client-match`, protocolo, somente leitura/leitura e gravação, superusuário, anônimo, modo `chown`, `allow-suid` e NTFS-UNIX. As exportações de qtree e as montagens de caminhos de junção herdam a exigência de TLS por meio do mesmo mecanismo de política de exportação. System Manager exibe a configuração `-allow-nfs-tls-only` no seletor de acesso NFS.

A replicação NFS sobre TLS e o suporte a DR estão resumidos na tabela abaixo. Para obter informações sobre o mecanismo de replicação, consulte ["Arquitetura"](#).

Replicação / DR	NFS sobre TLS na 9.19.1
SVM-DR	Compatível. A linha da interface TLS é replicada no escopo SVM (status, nome do certificado e UUID, impor autenticação de host). O campo <code>-allow-nfs-tls-only</code> regra de exportação é replicado com a política de exportação.
MetroCluster (replicação em nível SVM)	Compatível. Mesmo caminho de replicação que o SVM-DR. O ciclo de vida do material do certificado na SVM de destino é gerenciado pelo administrador de certificados.
SnapMirror (replicação de volume)	Compatível. Ortogonal ao transporte TLS do lado do cliente.
Variantes do ONTAP hospedadas na nuvem	Não suportado na 9.19.1.

Recursos com restrições

Requisitos do cliente. O cliente NFS deve implementar TLS para ONC RPC conforme ["RFC 9289"](#). No Linux, isso é fornecido por um cliente NFS no kernel que suporta a opção de montagem `xprtsec=tls` (ou `xprtsec=mtls`), usada em conjunto com o auxiliar de handshake TLS do espaço do usuário `tlshd` do pacote `ktls-utils`. Para a matriz definitiva de clientes — incluindo versões mínimas do kernel, versões de pacotes do espaço do usuário e distribuições Linux suportadas — consulte a Ferramenta de Matriz de Interoperabilidade (IMT).

Limitações e ressalvas

- **Variantes do ONTAP hospedadas na nuvem.** Cloud Volumes ONTAP e outras variantes do ONTAP hospedadas na nuvem não são compatíveis com o ONTAP 9.19.1.
- **NFS sobre Acesso Direto à Memória Remota (RDMA).** NFS sobre RDMA e NFS sobre TLS são mutuamente exclusivos na mesma LIF.

Limites por nó



Atualmente, não existem limites de conexão fixos para NFS-over-TLS no ONTAP. Para obter as informações mais recentes sobre os limites suportados, consulte ["Hardware Universe"](#).

MELHOR PRÁTICA: Mantenha o número de conexões NFS sobre TLS por nó abaixo de 10.000 para garantir margem de segurança para tempestades de montagem e retomadas de alta disponibilidade.

Limites por cluster

Não existe um limite agregado separado para todo o cluster imposto no código.

Limites por LIF e por objeto

- A tabela de configuração é indexada pela (SVM, LIF) tupla. Cada LIF contém zero ou uma linha de configuração NFS-over-TLS.
- Exatamente um certificado de servidor é vinculado a cada LIF com NFS sobre TLS habilitado. O certificado é especificado no `vserver nfs tls interface enable` momento e pode ser alterado com `... modify -certificate-name`.
- `-allow-nfs-tls-only` é um único valor booleano por regra de política de exportação. Este recurso não adiciona um limite máximo separado de regras; os limites máximos padrão por política e por SVM para regras de exportação se aplicam.

Comportamento de aplicação

`-allow-nfs-tls-only true` aplicação. Quando este campo está `true` em uma regra de política de exportação correspondente, as tentativas de conexão NFS de clientes correspondentes que não estejam usando TLS para ONC RPC conforme RFC 9289 são rejeitadas na avaliação da regra de exportação. As conexões TLS existentes desses clientes não são afetadas.

`-enforce-host-auth true` aplicação. Quando `true` em um (SVM, LIF), handshakes TLS cujo certificado de identidade do cliente não corresponde à identidade do host configurada para a LIF são rejeitados durante o handshake TLS. O evento `EMS Nblade.TLSHandshakeFailed` (gravidade ERR, limitado a uma vez a cada 10 minutos por fonte de evento) é emitido para cada handshake com falha.

Limites de taxa do EMS.

`Nblade.TLSConfigError` e `Nblade.TLSHandshakeFailed` têm a taxa limitada a uma vez a cada 10 minutos por fonte de evento. `Nblade.NfsTlsDisabled` tem a taxa limitada a uma vez a cada 24 horas por fonte de evento. Esses são limites intencionais para o volume de logs de eventos durante condições de falha sustentada. Durante uma rajada, apenas a primeira ocorrência dentro de cada janela de limite de taxa é registrada.

Limites flexíveis e recomendações

As seguintes são recomendações, não valores máximos rígidos.

- **Mantenha a margem de segurança abaixo de 10.000 conexões NFS-over-TLS por nó.** Não há um limite fixo, mas mantenha o número de conexões NFS-over-TLS por nó em 10.000 ou menos.
- **Planeje um novo handshake TLS completo após a tomada de controle do HA.** As sessões TLS têm escopo TCP e não sobrevivem a uma tomada de controle. Cada cliente se reconectará com um novo handshake TLS 1.3 no nó sobrevivente ou de destino, portanto, planeje uma tempestade de montagens. Manter o número de conexões bem abaixo de 10.000 oferece margem para absorver esse pico.

Relatórios técnicos da SAN ONTAP

O storage SAN ONTAP oferece uma experiência de SAN simplificada que fornece alta disponibilidade para os bancos de dados essenciais da sua organização e outros workloads de SAN. Com a melhor integração de serviços de dados da categoria com os bancos de dados Oracle, SAP e Microsoft SQL Server, além de VMware e outros hipervisores líderes, o ONTAP SAN oferece um retorno acelerado do investimento para aplicações de banco de dados empresariais.



Esses relatórios técnicos expandem a "[Gerenciamento de storage SAN ONTAP](#)" documentação do produto.

["TR-4080: Melhores práticas para SAN moderna em ONTAP"](#) Saiba mais sobre protocolos de bloqueio no ONTAP, bem como práticas de recomendações.

["TR-4684: Implementando e configurando SANs modernas com NVMe sobre Fabrics \(NVMe-of\)"](#) Saiba como implementar e configurar o NVMe sobre Fabrics Transports (NVMe sobre Fibre Channel e NVMe sobre TCP). Os tópicos incluem design, implementação, configuração, diretrizes de gerenciamento e práticas recomendadas para criar soluções SAN modernas de alta performance e altamente disponíveis usando protocolos e transportes NVMe.

["TR-4968: Disponibilidade e integridade de dados de array all-SAN NetApp"](#) Saiba como os vários recursos de proteção de dados e integridade de dados de todos os sistemas de storage SAN funcionam para alcançar o máximo de tempo de atividade da aplicação, além de práticas recomendadas para projetar, implementar e gerenciar uma rede SAN.

["Solução flash moderna conectada à nuvem SAN"](#) Esta arquitetura verificada do NetApp foi projetada e verificada em conjunto pela NetApp, VMware e Broadcom. Ele usa as mais recentes soluções de tecnologia Brocade, Emulex e VMware vSphere, juntamente com o storage all-flash NetApp, que estabelece um novo padrão para armazenamento SAN empresarial e proteção de dados que gera valor comercial superior.

Segurança

Relatórios técnicos de segurança da ONTAP

A ONTAP continua a evoluir, com a segurança como parte integrante da solução. As versões mais recentes do ONTAP contêm muitos novos recursos de segurança que são inestimáveis para sua organização proteger seus dados na nuvem híbrida, prevenir ataques de ransomware e aderir às práticas recomendadas pelo setor. Esses novos recursos também dão suporte ao movimento da sua organização em direção a um modelo Zero Trust.



Esses relatórios técnicos expandem a "[Segurança e criptografia de dados do ONTAP](#)" documentação do produto.

Ciber Vault da ONTAP

["Ciber Vault da ONTAP"](#) O Cyber Vault baseado em ONTAP da NetApp oferece às organizações uma solução abrangente e flexível para proteger seus ativos de dados mais críticos. Ao utilizar metodologias de fortalecimento lógicas com metodologias robustas, o ONTAP permite que você crie ambientes de storage seguros e isolados que sejam resilientes contra ameaças cibernéticas em evolução. Com o ONTAP, você garante a confidencialidade, integridade e disponibilidade dos dados, mantendo a agilidade e a eficiência da infraestrutura de storage.

Ransomware

["TR-4572: A solução NetApp para ransomware"](#) Saiba como o ransomware evoluiu e como identificar ataques, prevenir a propagação e se recuperar o mais rápido possível usando a solução NetApp para ransomware. As orientações e as soluções fornecidas neste documento são projetadas para ajudar as organizações a ter soluções de resiliência cibernética, ao mesmo tempo em que cumprem seus objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informação.

["TR-4526: Storage WORM em conformidade com NetApp SnapLock"](#) Muitas empresas usam o storage de dados WORM (uma gravação, muitas leituras) para atender a requisitos de conformidade regulamentar ou simplesmente adicionar outra camada à estratégia de proteção de dados. Saiba como integrar o SnapLock, a solução WORM em ONTAP, em ambientes que exigem storage de dados WORM.

Confiança zero

["NetApp e confiança zero"](#) O Zero Trust tradicionalmente tem sido uma abordagem centrada na rede de arquitetura de micro núcleo e perímetro (MCAP) para proteger dados, serviços, aplicativos ou ativos com controles conhecidos como gateway de segmentação. A ONTAP adota uma abordagem centrada em dados para a confiança zero, na qual o sistema de gerenciamento de storage se torna o gateway de segmentação para proteger e monitorar o acesso aos dados de nossos clientes. Em particular, o mecanismo FPolicy Zero Trust e o ecossistema parceiro da FPolicy se tornam um centro de controle para obter uma compreensão detalhada dos padrões de acesso a dados normais e aberrantes e identificar ameaças internas.

Autenticação de vários fatores

["TR-4647: Autenticação multifator nas práticas recomendadas e guia de implementação do ONTAP"](#) Saiba mais sobre o recurso de autenticação multifator do ONTAP para acesso administrativo usando o Gerenciador

de sistema, Active IQ Unified Manager e autenticação de CLI de shell seguro (SSH) do ONTAP.

["TR-4717: Autenticação ONTAP SSH com um cartão de acesso comum"](#) Saiba como configurar e testar clientes SSH de terceiros, em conjunto com o software ActivClient, para autenticar um administrador de armazenamento ONTAP através da chave pública armazenada em um cartão de acesso comum (CAC) quando configurado no ONTAP.

Alocação a vários clientes

["TR-4160: Alocação segura a vários clientes no ONTAP"](#) Saiba como implementar a alocação segura a vários clientes usando VMs de storage no ONTAP, incluindo considerações de design e práticas recomendadas.

Padrões

["TR-4401: PCI-DSS 4,0 e ONTAP"](#) Saiba como validar um sistema em relação ao padrão PCI DSS 4,0 e atender aos requisitos dos controles que você aplica a um sistema NetApp ONTAP.

Controle de acesso baseado em atributos

["Controle de acesso baseado em atributos com ONTAP"](#) Saiba como configurar rótulos de segurança NFSv4,2 e atributos estendidos (xattrs) para suportar o controle de acesso baseado em função (RBAC) e o controle de acesso baseado em atributos (ABAC), uma estratégia de autorização que define permissões com base em atributos de usuário, recurso e ambiente.

Solução NetApp para ransomware

Portfólio de proteção de ransomware e NetApp

O ransomware continua sendo uma das ameaças mais significativas que causam interrupções nos negócios na organização em 2024. De acordo com o ["Sophos State of ransomware 2024"](#), os ataques de ransomware afetaram 72% do público pesquisado. Os ataques de ransomware evoluíram para serem mais sofisticados e direcionados, com os agentes de ameaças empregando técnicas avançadas como inteligência artificial para maximizar seu impactos e lucros.

As organizações devem examinar toda a postura de segurança de perímetro, rede, identidade, aplicativo e onde os dados estão no nível de storage e proteger essas camadas. A adoção de uma abordagem centrada em dados à proteção cibernética na camada de storage é crucial no cenário de ameaças atual. Embora nenhuma solução única possa impedir todos os ataques, o uso de um portfólio de soluções, incluindo parcerias e terceiros, oferece uma defesa em camadas.

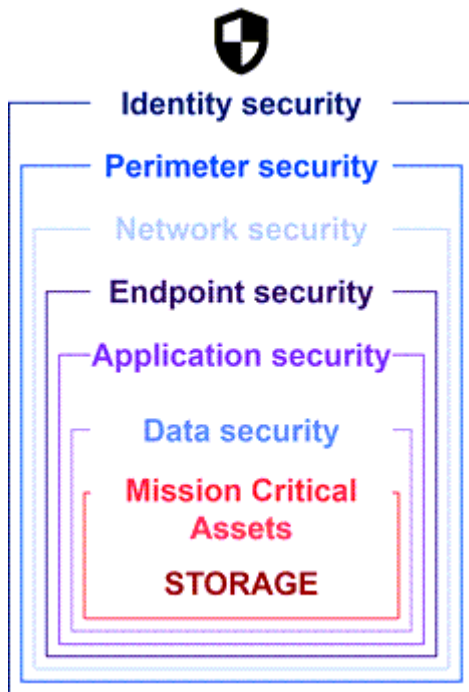
O [Portfólio de produtos NetApp](#) oferece várias ferramentas eficazes de visibilidade, detecção e correção, ajudando você a identificar ransomware com antecedência, prevenir propagação e se recuperar rapidamente, se necessário, para evitar tempo de inatividade caro. As soluções tradicionais de defesa em camadas continuam prevalecendo, assim como as soluções de terceiros e parceiros para visibilidade e detecção. A correção eficaz continua sendo uma parte crucial da resposta a qualquer ameaça. A abordagem exclusiva do setor que utiliza a tecnologia imutável Snapshot da NetApp e a solução SnapLock Logical AIR GAP é um diferencial do setor e a prática recomendada do setor para recursos de correção de ransomware.



A partir de julho de 2024, o conteúdo do relatório técnico *TR-4572: NetApp ransomware Protection*, que foi publicado anteriormente em PDF, está disponível em docs.netapp.com.

Os dados são o alvo principal

Os cibercriminosos segmentam cada vez mais os dados diretamente, reconhecendo seu valor. Embora a segurança de perímetro, rede e aplicativos sejam importantes, eles podem ser ignorados. Com o foco na proteção de dados em sua origem, a camada de storage, fornece uma última linha de defesa crítica. Obter acesso aos dados de produção e criptografá-los ou torná-los inacessíveis é o objetivo dos ataques de ransomware. Para chegar lá, os invasores já devem ter perfurado as defesas existentes implantadas pelas organizações hoje, do perímetro à segurança do aplicativo.



Infelizmente, muitas organizações não aproveitam os recursos de segurança na camada de dados. É aqui que entra o portfólio de proteção contra ransomware da NetApp, protegendo você na última linha de defesa.

O custo real do ransomware

O pagamento de resgate em si não é o maior efeito monetário em um negócio. Embora o pagamento não seja insignificante, ele fica pálido em comparação com o custo do tempo de inatividade de sofrer um incidente de ransomware.

Os pagamentos de resgate são apenas um elemento dos custos de recuperação ao lidar com eventos de ransomware. Excluindo quaisquer resgates pagos, em 2024 as organizações relataram um custo médio para se recuperar de um ataque de ransomware de 2,73M dólares, um aumento de quase 1M dólares em relação aos 1,82M dólares relatados em 2023, de acordo com o "[2024 Sophos State of ransomware](#)" relatório. Para organizações que dependem muito da DISPONIBILIDADE DE TI, como e-commerce, negociação de ações e cuidados de saúde, os custos podem ser 10 vezes maiores ou mais.

Os custos do seguro cibernético também continuam a aumentar, dada a probabilidade muito real de um ataque de ransomware a empresas seguradas.

Proteção contra ransomware na camada de dados

A NetApp entende que sua postura de segurança é ampla e profunda em toda a organização, desde o perímetro até o local onde os dados estão na camada de storage. Sua pilha de segurança é complexa e deve fornecer segurança em todos os níveis de sua pilha de tecnologia.

A proteção em tempo real na camada de dados é ainda mais importante e tem requisitos exclusivos. Para serem eficazes, as soluções nessa camada devem oferecer esses atributos críticos:

- **Segurança por design** para minimizar a chance de ataque bem-sucedido
- **Deteção e resposta em tempo real** para minimizar o impactos de um ataque bem-sucedido
- **Proteção WORM com ar-gapped** para isolar backups de dados críticos
- * Um único plano de controle* para uma defesa abrangente contra ransomware

A NetApp pode oferecer tudo isso e muito mais.

Secure by Design
Data-centric on-box protection


Immutable backups & snapshots


Multi-user verification and authentication


Malicious file blocking

Real-time Detection & Response
99% detection accuracy to minimize attack impact


AI-powered detection


Actional intelligence for insider threats

Air-gapped WORM protection with cyber vaulting
Layered approach to further fortify data against ransomware attacks


Isolated, immutable & indelible WORM snapshots

Single control plane for comprehensive ransomware defense
BlueXP Ransomware Protection


PROTECT
Recommends workload protection policies and applies them with one-click.


DETECT
Detects potential attacks on your workload data in near real-time using industry leading AI/ML.


RESPOND
Automatically responds by taking immutable and indelible Snapshots when a potential attack is suspected. Integrates with popular SIEMs.


RECOVER
Rapidly restores workloads with application consistency, through simplified orchestrated recovery.


GOVERN
Implements your ransomware protection strategy and policies, and monitors outcomes.

Ransomware Recovery Guarantee
No data loss with NetApp Snapshots, guaranteed.

Portfólio de proteção contra ransomware da NetApp

A NetApp "proteção incorporada contra ransomware"oferece defesa em tempo real, robusta e multifacetada para seus dados críticos. Na sua essência, os algoritmos avançados de detecção habilitados por IA monitoram continuamente os padrões de dados, identificando rapidamente possíveis ameaças de ransomware com precisão de 99%. Reagir rapidamente a ataques permite que nosso storage snapshots rapidamente os dados e proteja as cópias, garantindo uma recuperação rápida.

Para fortalecer ainda mais os dados, a capacidade do NetApp "vaulting cibernético"isola os dados com uma lacuna de ar lógica. Ao proteger os dados essenciais, garantimos a rápida continuidade dos negócios.

NetApp"Proteção contra ransomware da NetApp" reduz os encargos operacionais com um único plano de controle para coordenar e executar de forma inteligente uma defesa de ransomware centrada na carga de trabalho de ponta a ponta, para que você possa identificar e proteger dados críticos da carga de trabalho em risco com um único clique, detectar e responder com precisão e automaticamente para limitar o impacto de um ataque potencial e recuperar cargas de trabalho em minutos, não dias, protegendo seus valiosos dados de carga de trabalho e minimizando interrupções dispendiosas.

36

Como uma solução ONTAP nativa e integrada para proteger o acesso não autorizado aos seus dados, ["Verificação multi-admin \(MAV\)"](#) tem um conjunto robusto de recursos que garante que operações como exclusão de volumes, criação de usuários administrativos adicionais ou exclusão de snapshots possam ser executadas somente após aprovações de pelo menos um segundo administrador designado. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados. Você pode configurar quantos aprovadores de administrador designados desejar antes que um snapshot possa ser excluído.



NetApp ONTAP atende à necessidade de acesso baseado na Web ["Autenticação multifator \(MFA\)"](#) no System Manager e de autenticação SSH CLI.

A proteção contra ransomware da NetApp oferece tranquilidade em um cenário de ameaças em constante evolução. Sua abordagem abrangente não só defende as variantes atuais de ransomware, mas também se adapta a ameaças emergentes, fornecendo segurança em longo prazo para sua infraestrutura de dados.

Saiba mais sobre outras opções de proteção

- ["Proteção contra ransomware do Digital Advisor"](#)
- ["Data Infrastructure Insights , armazenamento, carga de trabalho, segurança"](#)
- ["FPolicy"](#)
- ["SnapLock e snapshots à prova de violações"](#)

Garantia de recuperação de ransomware

A NetApp oferece a garantia de restaurar dados snapshot se ocorrer um ataque de ransomware. Nossa garantia: Se não pudermos ajudá-lo a restaurar seus dados de snapshot, faremos isso certo. A garantia está disponível em novas aquisições de sistemas AFF A-Series, AFF C-Series, ASA e FAS.

Saiba mais

- ["Descrição do serviço de garantia de recuperação"](#)
- ["Blog de garantia de recuperação de ransomware"](#).

Informações relacionadas

- ["Página de recursos do site de suporte da NetApp"](#)
- ["Segurança do produto NetApp"](#)

SnapLock e snapshots à prova de violações para proteção contra ransomware

Uma arma vital no arsenal de NetApp Snap é o SnapLock, que provou ser altamente eficaz na proteção contra ameaças de ransomware. Ao impedir a exclusão não autorizada de dados, o SnapLock fornece uma camada adicional de segurança, garantindo que os dados críticos permaneçam intactos e acessíveis, mesmo em caso de ataques mal-intencionados.

SnapLock Compliance

O SnapLock Compliance (SLC) fornece proteção indelével para seus dados. O SLC proíbe que os dados sejam excluídos mesmo quando um administrador tenta reinicializar a matriz. Ao contrário de outros produtos competitivos, o SnapLock Compliance não é vulnerável a ataques de engenharia social por meio das equipes de suporte desses produtos. Os dados protegidos por volumes do SnapLock Compliance são recuperáveis até que esses dados atinjam a data de expiração.

Para ativar o SnapLock, é necessária uma ["ONTAP One"](#) licença.

Saiba mais

- ["Documentação do SnapLock"](#)

Snapshots à prova de violações

As cópias Snapshot (TPS) à prova de violações fornecem uma maneira conveniente e rápida de proteger os dados de atos maliciosos. Ao contrário do SnapLock Compliance, o TPS é normalmente usado em sistemas primários onde o usuário pode proteger os dados por um determinado tempo e deixado localmente para recuperações rápidas ou onde os dados não precisam ser replicados fora do sistema primário. O TPS usa tecnologias SnapLock para impedir que o snapshot primário seja excluído mesmo por um administrador do ONTAP que use o mesmo período de expiração de retenção do SnapLock. A exclusão de snapshot é impedida mesmo que o volume não esteja habilitado para SnapLock, embora os snapshots não tenham a mesma natureza indelével dos volumes SnapLock Compliance.

Para fazer snapshots à prova de violações, é necessária uma ["ONTAP One"](#) licença.

Saiba mais

- ["Bloqueie um snapshot para proteção contra ataques de ransomware"](#).

Bloqueio de arquivos FPolicy

O FPolicy impede que arquivos indesejados sejam armazenados em seu dispositivo de armazenamento de nível empresarial. O FPolicy também oferece uma maneira de bloquear extensões de arquivo ransomware conhecidas. Um usuário ainda tem permissões de acesso total à pasta inicial, mas o FPolicy não permite que um usuário armazene arquivos que suas marcas de administrador como bloqueados. Não importa se esses arquivos são arquivos MP3 ou extensões de arquivo ransomware conhecidas.

Bloqueie arquivos maliciosos com o modo nativo FPolicy

O modo nativo do NetApp FPolicy (uma evolução do nome, Política de arquivos) é uma estrutura de bloqueio de extensão de arquivo que permite bloquear extensões de arquivo indesejadas de entrar em seu ambiente. Faz parte do ONTAP há mais de uma década e é incrivelmente útil para ajudar você a proteger contra ransomware. Esse mecanismo de confiança zero é valioso porque você obtém medidas de segurança extras além das permissões da lista de controle de acesso (ACL).

No ONTAP System Manager e no NetApp Console, uma lista de mais de 3.000 extensões de arquivo está disponível para referência.



Algumas extensões podem ser legítimas em seu ambiente e bloqueá-las pode levar a problemas inesperados. Crie sua própria lista apropriada para o seu ambiente antes de configurar o FPolicy nativo.

O modo nativo FPolicy está incluído em todas as licenças do ONTAP.

Saiba mais

- ["Blog: Fighting ransomware: Parte três - ONTAP FPolicy, outra ferramenta nativa poderosa \(também conhecida como gratuita\)"](#)

Ative a análise de comportamento do usuário e da entidade (UEBA) com o modo externo FPolicy

O modo externo FPolicy é uma estrutura de notificação e controle de atividade de arquivo que fornece visibilidade da atividade de arquivo e do usuário. Essas notificações podem ser usadas por uma solução externa para executar análises baseadas em IA para detectar comportamentos maliciosos.

O modo externo FPolicy também pode ser configurado para aguardar a aprovação do servidor FPolicy antes de permitir que atividades específicas passem. Várias políticas como essa podem ser configuradas em um cluster, o que proporciona grande flexibilidade.



Os servidores FPolicy devem ser responsivos às solicitações FPolicy se configurados para fornecer aprovação; caso contrário, o desempenho do sistema de storage pode ser afetado negativamente.

O modo externo FPolicy está incluído no ["Todas as licenças ONTAP"](#).

Saiba mais

- ["Blog: Fighting ransomware: Parte quatro - UBA e ONTAP com o modo externo FPolicy."](#)

Data Infrastructure Insights , armazenamento, carga de trabalho, segurança

O Storage Workload Security (SWS) é um recurso do NetApp Data Infrastructure Insights que aprimora muito a postura de segurança, a capacidade de recuperação e a responsabilidade de um ambiente ONTAP . O SWS adota uma abordagem centrada no usuário, rastreando todas as atividades de arquivo de cada usuário autenticado no ambiente. Ele usa análises avançadas para estabelecer padrões de acesso normais e sazonais para cada usuário. Esses padrões são usados para identificar rapidamente comportamentos suspeitos sem a necessidade de assinaturas de ransomware.

Quando o SWS detecta um possível ransomware ou exclusão de dados, ele pode tomar ações automáticas como:

- Tire um instantâneo do volume afetado.
- Bloqueie a conta de utilizador e o endereço IP suspeito de atividade maliciosa.
- Envie um alerta para administradores.

Como pode tomar medidas automatizadas para parar rapidamente uma ameaça privilegiada, bem como rastrear todas as atividades de arquivos, o SWS torna a recuperação de um evento de ransomware muito mais simples e rápida. Com ferramentas avançadas de auditoria e forense integradas, os usuários podem ver imediatamente quais volumes e arquivos foram afetados por um ataque, de qual conta de usuário o ataque veio e de que ação maliciosa foi realizada. Instantâneos automáticos mitigam os danos e aceleram a restauração de arquivos.

Total Attack Results

5	0	1,488
Affected Volumes	Deleted Files	Encrypted Files

1,488 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of Ransomware Attack.

The extension ".wanna" was added to each file.

Alertas da proteção autônoma contra ransomware (ARP) da ONTAP também são visíveis no SWS, fornecendo uma única interface para clientes que usam ARP e SWS para proteger contra ataques de ransomware.

Saiba mais

- ["Data Infrastructure Insights da NetApp"](#)

Detecção e resposta incorporadas baseada em IA on-box da NetApp ONTAP

À medida que as ameaças de ransomware se tornam cada vez mais sofisticadas, os seus mecanismos de defesa também devem ser aplicados. A proteção autônoma contra ransomware (ARP) da NetApp é baseada em AI com detecção inteligente de anomalias incorporada ao ONTAP. Ative-o para adicionar mais uma camada de defesa à sua resiliência cibernética.

ARP e ARP/AI são configuráveis por meio da interface de gerenciamento integrada do ONTAP, do Gerenciador de sistema e habilitados por volume.

Proteção autônoma contra ransomware (ARP)

A proteção autônoma contra ransomware (ARP), outra solução nativa da ONTAP incorporada desde 9.10.1, analisa a atividade do arquivo de workload de volume de storage nas e a entropia de dados para detectar automaticamente possíveis ransomwares. O ARP fornece aos administradores detecção, insights e um ponto de recuperação de dados em tempo real para detecção on-box de ransomware sem precedentes.

Para o ONTAP 9.15.1 e versões anteriores que suportam ARP, o ARP começa no modo de aprendizado para aprender a atividade típica de dados de carga de trabalho. Isso pode levar sete dias para a maioria dos ambientes. Depois que o modo de aprendizado estiver concluído, o ARP mudará automaticamente para o modo ativo e começará a procurar atividade anormal da carga de trabalho que possa potencialmente ser ransomware.

Se for detetada atividade anormal, um instantâneo automático é imediatamente tomado, o que fornece um ponto de restauração o mais próximo possível do momento do ataque com dados infetados mínimos. Simultaneamente, é gerado um alerta automático (configurável) que permite que os administradores vejam a atividade anormal do arquivo para que possam determinar se a atividade é realmente maliciosa e tomar as medidas apropriadas.

Se a atividade for uma carga de trabalho esperada, os administradores podem marcá-la facilmente como um falso positivo. O ARP aprende essa mudança como atividade normal de carga de trabalho e não a sinaliza mais como um ataque potencial no futuro.

Para ativar o ARP, é necessária uma ["ONTAP One"](#) licença.

Saiba mais

- ["Proteção autônoma contra ransomware"](#)

Proteção autônoma contra ransomware/AI (ARP/AI)

Apresentado como uma prévia técnica no ONTAP 9.15.1, o ARP/AI leva a detecção em tempo real dos sistemas de armazenamento nas on-box para o próximo nível. A nova tecnologia de detecção habilitada por AI é treinada em mais de um milhão de arquivos e vários ataques de ransomware conhecidos. Além dos sinais usados no ARP, o ARP/AI também detecta criptografia de cabeçalho. A potência de IA e os sinais adicionais permitem que o ARP/AI forneça uma precisão de detecção superior a 99%. Isso foi validado pelo se Labs, um laboratório de testes independente que deu à ARP/AI a sua maior classificação AAA.

Como o treinamento dos modelos acontece continuamente na nuvem, o ARP/AI não requer um modo de aprendizado. Ele está ativo no momento em que é ligado. O treinamento contínuo também significa que o ARP/AI sempre é validado contra novos tipos de ataque de ransomware à medida que eles surgem. O ARP/AI também vem com recursos de atualização automática que fornecem novos parâmetros a todos os clientes para manter a detecção de ransomware atualizada. Todos os outros recursos de detecção, insight e ponto de recuperação de dados do ARP são mantidos para ARP/AI.

Para ativar o ARP/AI, é necessária uma ["ONTAP One"](#) licença.

Saiba mais

- ["Blog: A solução de detecção de ransomware em tempo real baseada em IA da NetApp atinge a classificação AAA"](#)

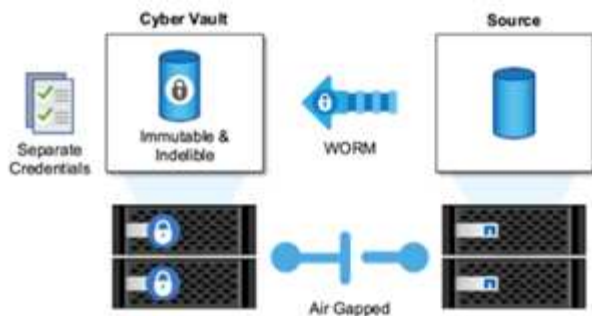
Proteção WORM com uso de cofres cibernéticos no ONTAP

A abordagem da NetApp a um cofre cibernético é uma arquitetura de referência criada especificamente para um cofre cibernético com conexão lógica. Essa abordagem aproveita as tecnologias de fortalecimento da segurança e conformidade, como o SnapLock, para permitir snapshots imutáveis e indelévels.

Cyber vaulting com SnapLock Compliance e uma lacuna de ar lógica

Uma tendência crescente é que os invasores destruam as cópias de backup e, em alguns casos, até as criptografem. É por isso que muitos no setor de cibersegurança recomendam o uso de backups Air Gap como parte de uma estratégia geral de resiliência cibernética.

O problema é que as lacunas de ar tradicionais (fita e Mídia off-line) podem aumentar significativamente o tempo de restauração, aumentando assim o tempo de inatividade e os custos associados gerais. Mesmo uma abordagem mais moderna de uma solução de abertura de ar pode ser problemática. Por exemplo, se o cofre de backup for temporariamente aberto para receber novas cópias de backup e, em seguida, desconectar e fechar sua conexão de rede com dados primários para que mais uma vez sejam "trocados", um invasor pode aproveitar a abertura temporária. Durante o tempo em que a conexão está online, um invasor pode atacar para comprometer ou destruir os dados. Esse tipo de configuração geralmente também adiciona complexidade indesejada. Uma lacuna de ar lógica é um excelente substituto para uma lacuna de ar tradicional ou moderna, porque tem os mesmos princípios de proteção de segurança, mantendo o backup online. Com o NetApp, você pode resolver a complexidade do gapping de ar em fita ou disco com gapping de ar lógico, o que pode ser alcançado com snapshots imutáveis e NetApp SnapLock Compliance.



A NetApp lançou o recurso SnapLock há mais de 10 anos para atender aos requisitos de conformidade de dados, como a Lei de portabilidade e responsabilidade de seguros de Saúde (HIPAA), a Sarbanes-Oxley e outras regras de dados regulatórios. Você também pode armazenar snapshots primários nos volumes do SnapLock para que as cópias possam ser comprometidas com WORM, impedindo a exclusão. Existem duas versões de licença SnapLock: SnapLock Compliance e SnapLock Enterprise. Para proteção contra ransomware, a NetApp recomenda o SnapLock Compliance porque você pode definir um período de retenção específico durante o qual os snapshots são bloqueados e não podem ser excluídos, mesmo pelos administradores do ONTAP ou pelo suporte da NetApp.

Saiba mais

- ["Blog: Visão geral do ONTAP Cyber Vault"](#)

Snapshots à prova de violações

Embora a utilização do SnapLock Compliance como uma lacuna lógica forneça a melhor proteção para impedir que atacantes excluam suas cópias de backup, isso exige que você mova os snapshots usando o SnapVault para um volume secundário habilitado para SnapLock. Como resultado, muitos clientes implantam essa configuração em storage secundário na rede. Isso pode levar a tempos de restauração mais longos versus a restauração de um Snapshot de volume primário no storage primário.

A partir do ONTAP 9.12.1, os snapshots à prova de violações fornecem proteção perto do nível SnapLock Compliance para seus snapshots no storage primário e em volumes primários. Não há necessidade de armazenar o snapshot usando o SnapVault em um volume secundário SnapLocked. Os snapshots à prova de violações usam a tecnologia SnapLock para impedir que o snapshot principal seja excluído, mesmo por um administrador completo do ONTAP usando o mesmo período de expiração de retenção do SnapLock. Isso possibilita tempos de restauração mais rápidos e o backup de um volume FlexClone por um snapshot protegido e à prova de violações, algo que você não pode fazer com um snapshot abobadado do SnapLock Compliance tradicional.

A principal diferença entre os instantâneos SnapLock Compliance e invioláveis é que o SnapLock Compliance não permite que o array ONTAP seja inicializado e apagado se existirem volumes SnapLock Compliance com snapshots abobadados que ainda não atingiram sua data de expiração. Para fazer snapshots à prova de violações, é necessária uma licença do SnapLock Compliance.

Saiba mais

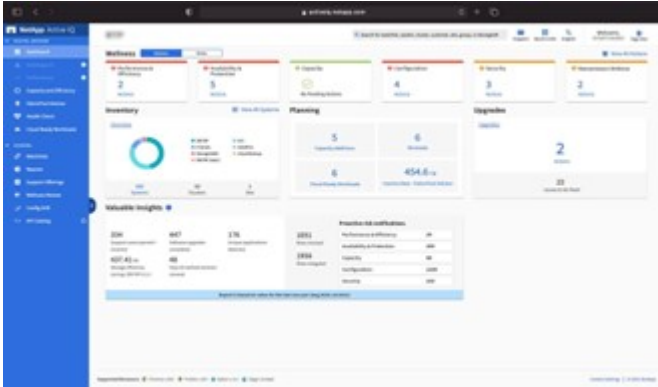
- ["Bloqueie um snapshot para proteção contra ataques de ransomware"](#)

Proteção contra ransomware do Digital Advisor

Digital Advisor, com tecnologia Active IQ, simplifica o cuidado proativo e a otimização do armazenamento NetApp com informações práticas para uma gestão de dados ideal. Alimentado por dados de telemetria da nossa base instalada, ele utiliza técnicas

avançadas de IA e ML para descobrir oportunidades de reduzir riscos e melhorar o desempenho e a eficiência do seu ambiente de storage.

Além de "[Consultor digital da NetApp](#)" ajudar "[eliminar vulnerabilidades de segurança](#)", também fornece informações e orientações específicas para proteger contra ransomware. Um cartão de integridade dedicado mostra as ações necessárias e os riscos abordados, para que você tenha certeza de que seus sistemas estão atendendo às recomendações de melhores práticas.



Os riscos e ações rastreados na página de bem-estar da Defesa do ransomware incluem o seguinte (e muito mais):

- A contagem de snapshot de volume é baixa, diminuindo a possível proteção contra ransomware.
- O FPolicy não está habilitado para todas as máquinas virtuais de armazenamento (SVMs) configuradas para protocolos nas.

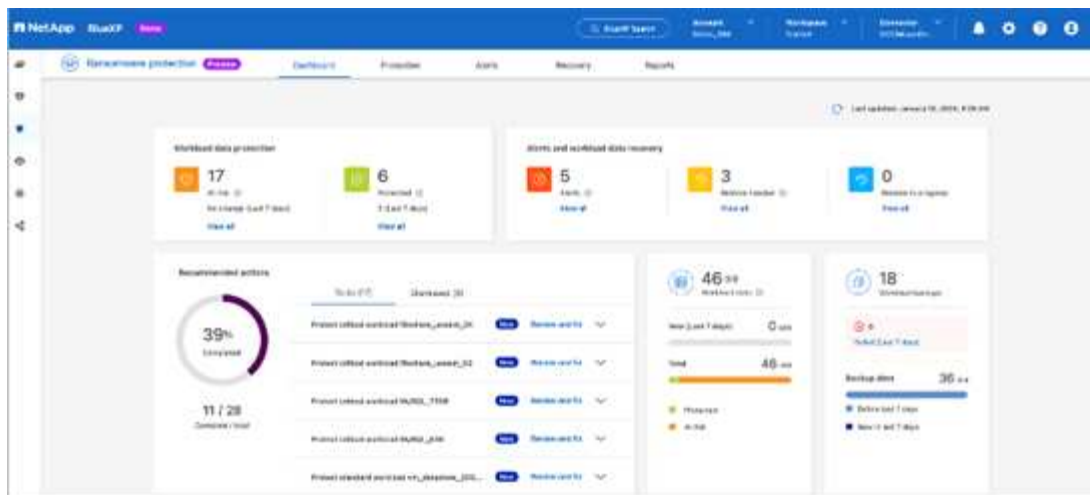
Para ver a proteção contra ransomware em ação, veja "[Consultor digital](#)".

Resiliência abrangente com proteção contra ransomware da NetApp

É importante que a detecção de ransomware ocorra o mais cedo possível para que você possa evitar a propagação e evitar tempo de inatividade dispendioso. Uma estratégia eficaz de detecção de ransomware, no entanto, deve incluir mais de uma camada de proteção. A proteção contra ransomware da NetApp adota uma abordagem abrangente que inclui recursos prontos para uso em tempo real, que se estendem aos serviços de dados usando o NetApp Console e uma solução isolada e em camadas para proteção cibernética.

Proteção contra ransomware da NetApp

O NetApp Console é um único plano de controle para orquestrar de forma inteligente uma defesa abrangente e centrada na carga de trabalho contra ransomware. A proteção contra ransomware da NetApp reúne os poderosos recursos de resiliência cibernética do ONTAP, como ARP, FPolicy e snapshots à prova de violação, e serviços de dados da NetApp, como NetApp Backup and Recovery. Ele também adiciona recomendações e orientações com fluxos de trabalho automatizados para fornecer uma defesa de ponta a ponta por meio de uma única interface de usuário. Ele opera no nível da carga de trabalho para garantir que os aplicativos que executam seu negócio estejam protegidos e possam ser recuperados o mais rápido possível em caso de um ataque.



Benefícios para o cliente:

- A preparação assistida para ransomware reduz a sobrecarga operacional e melhora a eficácia
- A detecção de anomalias alimentada por IA/ML oferece maior precisão e resposta mais rápida para conter riscos
- A restauração orientada consistente com aplicações permite recuperar workloads com mais facilidade e em poucos minutos

"Proteção contra ransomware da NetApp" torna essas funções do NIST mais fáceis de serem alcançadas:

- **Descubra** e priorize dados automaticamente no armazenamento NetApp **com foco nas principais cargas de trabalho baseadas em aplicativos**.
- * Proteção com um clique* do backup de dados da carga de trabalho superior, configuração imutável e segura, bloqueio de arquivos maliciosos e domínio de segurança diferente.
- * Detecte com precisão* ransomware o mais rápido possível usando **detecção de anomalias baseada em IA de última geração**.
- Resposta automatizada e fluxos de trabalho e integração com as principais soluções **SIEM e XDR**.
- Restaure rapidamente os dados usando uma recuperação simplificada **orquestrada** para acelerar o tempo de atividade da aplicação.
- Implemente sua proteção contra ransomware * estratégia* e **políticas e monitore os resultados**.

NetApp e confiança zero

NetApp e confiança zero

O Zero Trust tradicionalmente tem sido uma abordagem centrada na rede de arquitetura de micro núcleo e perímetro (MCAP) para proteger dados, serviços, aplicativos ou ativos com controles conhecidos como gateway de segmentação. A NetApp ONTAP está adotando uma abordagem centrada em dados para a confiança zero, na qual o sistema de gerenciamento de storage se torna o gateway de segmentação para proteger e monitorar o acesso aos dados de nossos clientes. Em particular, o mecanismo FPolicy Zero Trust e o ecossistema parceiro da FPolicy se tornam um centro de controle para obter uma compreensão detalhada dos padrões de acesso a dados normais e aberrantes e identificar ameaças internas.



A partir de julho de 2024, o conteúdo do relatório técnico *TR-4829: NetApp e confiança zero: Habilitando um modelo de confiança zero centrado em dados*, que foi publicado anteriormente como PDF, está disponível em docs.netapp.com.

Os dados são o ativo mais importante da sua organização. Ameaças internas são responsáveis por 18% das violações de dados, segundo o relatório de 2022 "[Relatório de investigações de violação de dados da Verizon](#)". As organizações podem aumentar sua vigilância implementando controles de Zero Trust líderes do setor em torno dos dados com o software de gerenciamento de dados NetApp ONTAP.

O que é Zero Trust?

O modelo Zero Trust foi desenvolvido pela primeira vez por John Kindervag na Forrester Research. A abordagem Zero Trust de dentro para fora identifica um micronúcleo e um perímetro (MCAP). O MCAP é uma definição interior de dados, serviços, aplicativos e ativos a serem protegidos com um conjunto abrangente de controles. O conceito de um perímetro externo seguro é obsoleto. As entidades que são confiáveis e têm permissão para se autenticar com êxito através do perímetro podem então tornar a organização vulnerável a ataques. Insiders, por definição, já estão dentro do perímetro seguro. Funcionários, contratados e parceiros são membros da equipe e precisam estar habilitados a operar com controles apropriados para desempenhar suas funções na infraestrutura da organização.

Zero Trust foi mencionado como uma tecnologia que oferece promessa ao DoD em setembro de 2019 "[FY19-23 Estratégia de modernização Digital DoD](#)". Ele define Zero Trust como "Uma estratégia de segurança cibernética que incorpora segurança em toda a arquitetura com o objetivo de impedir violações de dados. Esse modelo de segurança centrado em dados elimina a ideia de redes, dispositivos, personas ou processos confiáveis ou não confiáveis e muda para níveis de confiança baseados em múltiplos atributos que permitem políticas de autenticação e autorização sob o conceito de acesso menos privilegiado. A implementação de confiança zero requer repensar como usamos a infraestrutura existente para implementar a segurança por meio do design de uma maneira mais simples e eficiente, ao mesmo tempo em que permite operações sem obstáculos."

Em agosto de 2020, o NIST publicou "[Especial Pub 800-207 arquitetura Zero Trust](#)" (ZTA). O ZTA se concentra em proteger recursos, não segmentos de rede, porque a localização da rede não é mais vista como o principal componente da postura de segurança do recurso. Os recursos são dados e computação. As estratégias ZTA são para arquitetos de rede empresarial. O ZTA introduz uma nova terminologia dos conceitos originais da Forrester. Os mecanismos de proteção chamados de ponto de decisão de política (PDP) e ponto de aplicação de políticas (PEP) são análogos a um gateway de segmentação da Forrester. A ZTA apresenta quatro modelos de implantação:

- Implantação baseada em agente de dispositivo ou gateway
- Implantação baseada em enclave (um pouco análoga ao Forrester MCAP)
- Implantação baseada em portal de recursos
- Aplicação do dispositivo sandboxing

Para os fins desta documentação, usamos os conceitos e a terminologia da Forrester Research em vez do ZTA NIST.

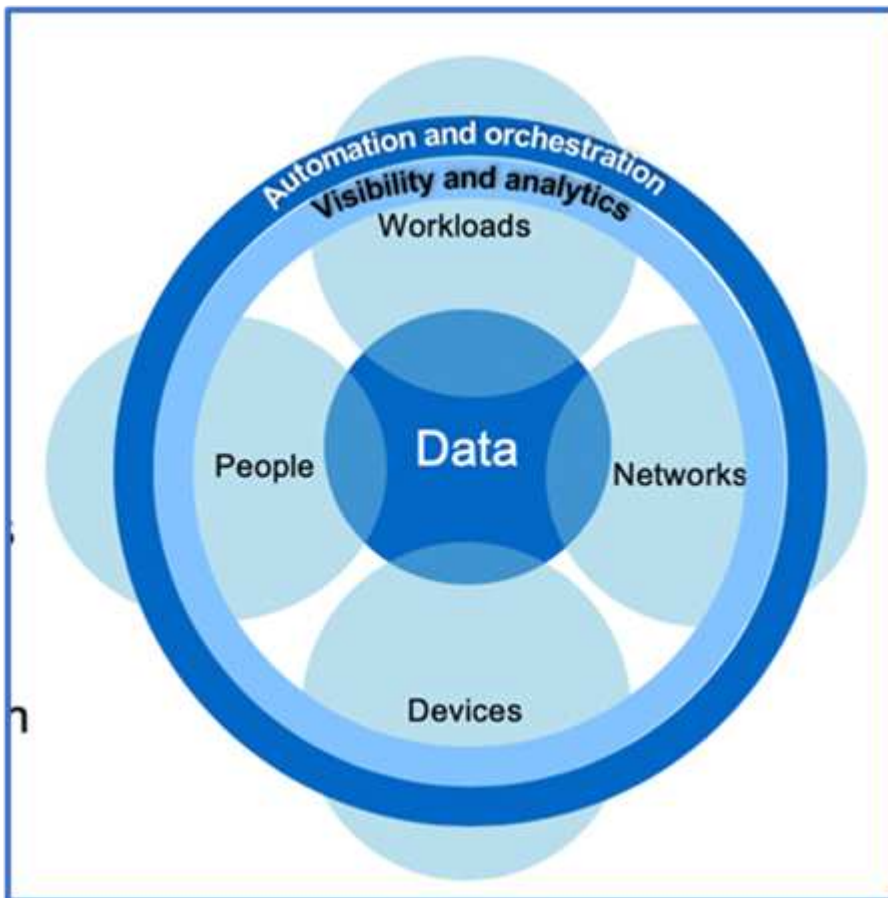
Recursos de segurança

Para obter informações sobre como reportar vulnerabilidades e incidentes, respostas de segurança do NetApp e confidencialidade do cliente, consulte o "[Portal de segurança da NetApp](#)".

Projete uma abordagem centrada em dados para zero confiança com o ONTAP

Uma rede Zero Trust é definida por uma abordagem centrada em dados, na qual os controles de segurança devem estar o mais próximo possível dos dados. As funcionalidades do ONTAP, somadas ao ecossistema parceiro do NetApp FPolicy, podem fornecer os controles necessários para o modelo de confiança zero centrado em dados.

O ONTAP é um software de gerenciamento de dados seguro da NetApp, e o mecanismo de confiança zero da FPolicy é um recurso ONTAP líder do setor que oferece uma interface de notificação granular com eventos baseados em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP.



Crie um MCAP centrado em dados Zero Trust

Para arquitetar um MCAP Zero Trust centrado em dados, siga estas etapas:

1. Identificar a localização de todos os dados organizacionais.
2. Classificar os dados.
3. Elimine com segurança os dados que já não necessita.
4. Entenda quais funções devem ter acesso às classificações de dados.
5. Aplique o princípio de privilégio mínimo para aplicar controles de acesso.
6. Use a autenticação multifator para acesso administrativo e acesso aos dados.

7. Uso de criptografia para dados em repouso e dados em trânsito.
8. Monitore e Registre todo o acesso.
9. Alertar acessos ou comportamentos suspeitos.

Identificar a localização de todos os dados organizacionais

O recurso FPolicy do ONTAP, juntamente com o ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. Mais detalhes sobre a análise comportamental do usuário são discutidos no Monitor e log todo o acesso. Se você não entender onde seus dados estão e quem tem acesso a eles, a análise comportamental do usuário pode fornecer uma linha de base para criar classificação e política a partir de observações empíricas.

Classificar os dados

Na terminologia do modelo Zero Trust, a classificação de dados envolve a identificação de dados tóxicos. Dados tóxicos são dados confidenciais que não devem ser expostos fora de uma organização. A divulgação de dados tóxicos pode violar a conformidade regulamentar e prejudicar a reputação de uma organização. Em termos de conformidade regulamentar, dados tóxicos incluem dados de titulares de cartão para o ["Padrão de segurança de dados do setor de cartões de pagamento \(PCI-DSS\)"](#), dados pessoais para a UE ["Regulamento Geral de proteção de dados \(GDPR\)"](#) ou dados de saúde para o ["Lei de portabilidade e responsabilidade de seguros de saúde \(HIPAA\)"](#). Você pode usar NetApp ["NetApp Data Classification"](#) (anteriormente conhecido como Cloud Data Sense), um kit de ferramentas orientado por IA, para escanear, analisar e categorizar automaticamente seus dados.

Elimine com segurança os dados que já não necessita

Depois de classificar os dados da sua organização, você pode descobrir que alguns dos seus dados não são mais necessários ou relevantes para a função da sua organização. A retenção de dados desnecessários é uma responsabilidade, e esses dados devem ser excluídos. Para obter um mecanismo avançado para apagar dados criptograficamente, consulte a descrição da limpeza segura na criptografia dados em repouso.

Entenda quais funções devem ter acesso às classificações de dados e aplique o princípio de menor privilégio para impor controles de acesso

Mapear o acesso a dados confidenciais e aplicar o princípio do menor privilégio significa dar às pessoas em sua organização acesso apenas aos dados necessários para executar seus trabalhos. Esse processo envolve controle de acesso baseado em função ("[RBAC](#)"), que se aplica ao acesso a dados e acesso administrativo.

Com o ONTAP, uma máquina virtual de storage (SVM) pode ser usada para segmentar o acesso a dados organizacionais por locatários em um cluster do ONTAP. O RBAC pode ser aplicado ao acesso aos dados, bem como ao acesso administrativo ao SVM. O RBAC também pode ser aplicado no nível administrativo do cluster.

Além do RBAC, você pode usar o ONTAP ["verificação multi-admin"](#)(MAV) para exigir que um ou mais administradores aprovem comandos como `volume delete` ou `volume snapshot delete`. Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

Outra maneira de proteger snapshots é com o ONTAP ["bloqueio instantâneo"](#). O bloqueio de snapshot é um recurso do SnapLock no qual os snapshots são tornados indelévels manual ou automaticamente com um período de retenção na política de snapshot de volume. O bloqueio de snapshot também é conhecido como bloqueio de snapshot à prova de violação. O objetivo do bloqueio de snapshot é impedir que administradores desonestos ou não confiáveis excluam snapshots nos sistemas ONTAP primário e secundário. A recuperação rápida de snapshots bloqueados em sistemas primários pode ser obtida a fim de restaurar volumes

corrompidos por ransomware.

Use a autenticação multifator para acesso administrativo e acesso aos dados

Além do RBAC administrativo do cluster, ["Autenticação de vários fatores \(MFA\)"](#) pode ser implementado para acesso administrativo via web do ONTAP e acesso via linha de comando SSH (Secure Shell). A autenticação multifator (MFA) para acesso administrativo é um requisito para organizações do setor público dos EUA ou para aquelas que precisam seguir o PCI-DSS. A MFA torna impossível que um invasor comprometa uma conta usando apenas um nome de usuário e senha. A MFA exige dois ou mais fatores independentes para autenticação. Um exemplo de autenticação de dois fatores é algo que o usuário possui, como uma chave privada, e algo que o usuário sabe, como uma senha. O acesso à Web administrativo ao ONTAP System Manager ou ao Active IQ Unified Manager é habilitado pelo Security Assertion Markup Language (SAML) 2.0. O acesso via linha de comando SSH utiliza autenticação em cadeia de dois fatores com uma chave pública e uma senha.

Você pode controlar o acesso de usuário e máquina por meio de APIs com os recursos de gerenciamento de identidade e acesso no ONTAP:

- Utilizador:
 - **Autenticação e autorização.** Por meio de funcionalidades de protocolo nas para SMB e NFS.
 - **Auditoria.** Syslog de acessos e eventos. Registro de auditoria detalhado do protocolo CIFS para testar políticas de autenticação e autorização. Auditoria granular fina de FPolicy de acesso detalhado nas no nível do arquivo.
- Dispositivo:
 - **Autenticação.** Autenticação baseada em certificado para acesso à API.
 - **Autorização.** Controle de acesso padrão ou personalizado baseado em função (RBAC).
 - **Auditoria.** Syslog de todas as ações tomadas.

Uso de criptografia para dados em repouso e dados em trânsito

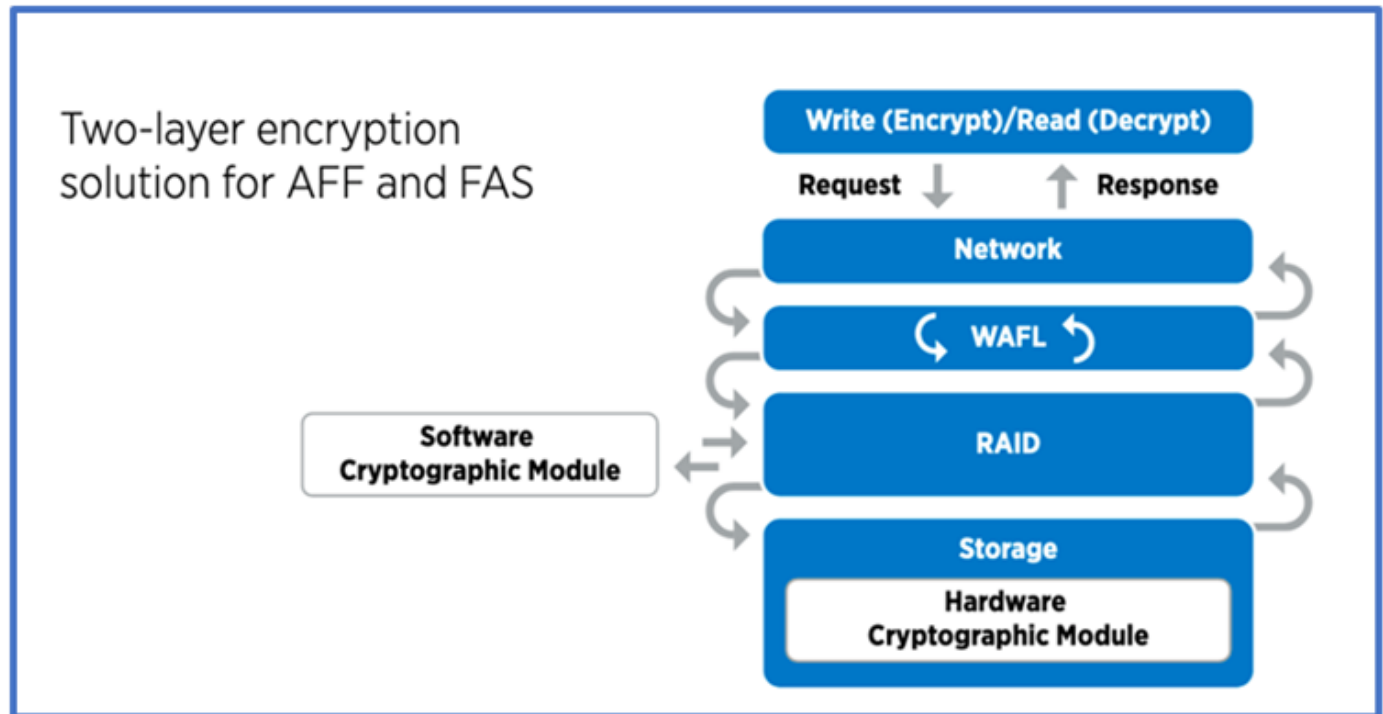
Criptografia de dados em repouso

A cada dia, surgem novos requisitos para mitigar riscos em sistemas de storage e lacunas de infraestrutura quando uma organização reutiliza unidades, devolve unidades defeituosas ou faz upgrade para unidades maiores, vendendo-as ou trocando-as. Como administradores e operadores de dados, espera-se que os engenheiros de storage gerenciem e mantenham os dados com segurança durante todo o seu ciclo de vida. ["NetApp Storage Encryption \(NSE\) n.o 44; NetApp volume Encryption \(NVE\) n.o 44; e NetApp Aggregate Encryption"](#) ajudam você a criptografar todos os seus dados em repouso o tempo todo, sejam eles tóxicos ou não, e sem afetar as operações diárias. "NSE" é uma solução de hardware ONTAP ["dados em repouso"](#) que utiliza unidades de autocriptografia validadas pelo FIPS 140-2 nível 2. "NVE e NAE" são uma solução de software ONTAP ["dados em repouso"](#) que utilizam o ["Módulo criptográfico NetApp validado FIPS 140-2 nível 1"](#). Com NVE e NAE, tanto discos rígidos quanto unidades de estado sólido podem ser usados para criptografia de dados em repouso. Além disso, as unidades NSE podem ser usadas para fornecer uma solução de criptografia nativa e em camadas, que oferece redundância de criptografia e segurança adicional. Se uma camada for violada, a segunda camada ainda protegerá os dados. Esses recursos tornam o ONTAP bem posicionado para ["criptografia pronta para quantum"](#).

O NVE também fornece uma funcionalidade chamada ["purga segura"](#) que remove criptograficamente dados tóxicos de derramamentos de dados quando arquivos confidenciais são gravados em um volume não classificado.

O ["Gerenciador de chaves integrado \(OKM\)"](#), que é o gerenciador de chaves integrado ao ONTAP, ou

"aprovado" terceiros ["gestores de chaves externos"](#) podem ser usados com NSE e NVE para armazenar com segurança material de codificação.



Como visto na figura acima, a criptografia baseada em hardware e software pode ser combinada. Essa capacidade levou ao ["Validação do ONTAP nas soluções comerciais da NSA para o programa classificado"](#) que permite o armazenamento de dados secretos principais.

Criptografia de dados em trânsito

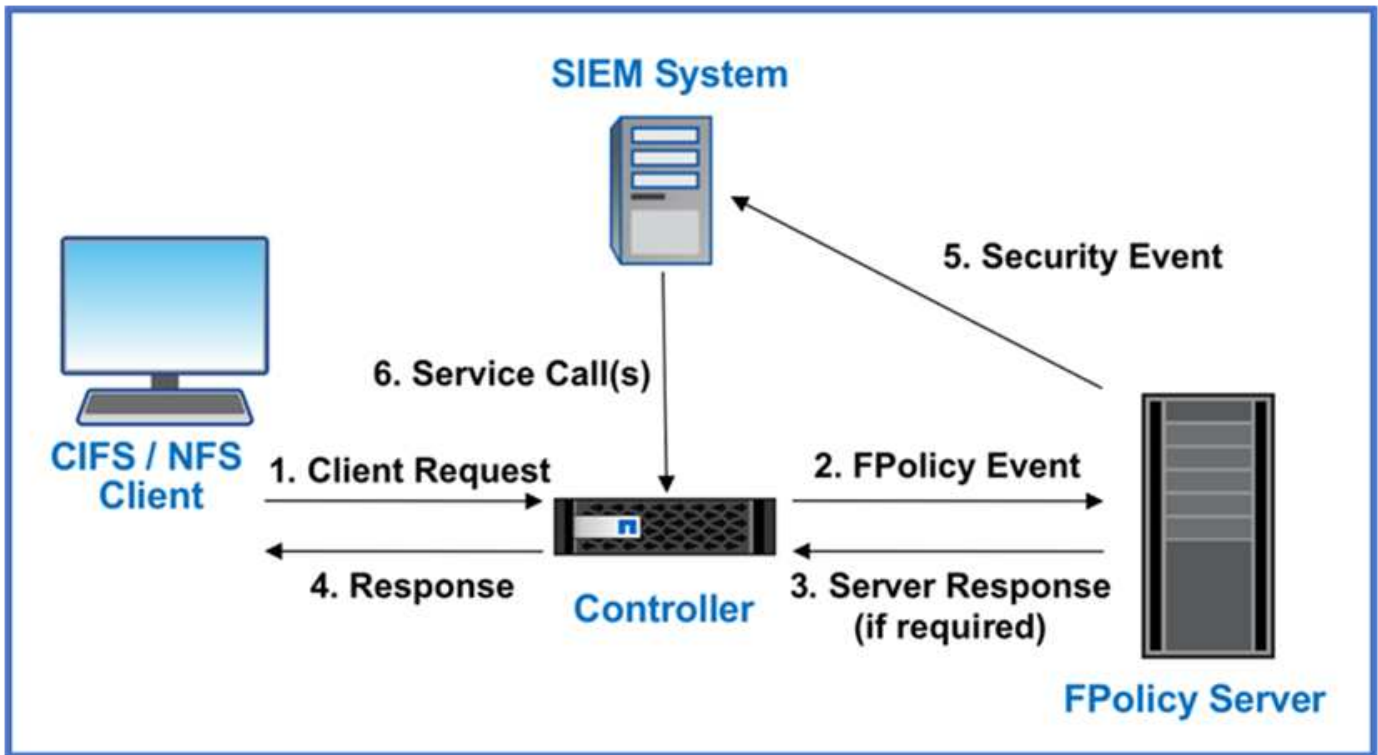
A criptografia de dados em trânsito do ONTAP protege o acesso aos dados do usuário e o acesso ao plano de controle. O acesso aos dados do usuário pode ser criptografado pela criptografia SMB 3,0 para o Microsoft CIFS Share Access ou pelo krb5P para NFS Kerberos 5. O acesso aos dados do usuário também pode ser criptografado com ["IPsec"](#)CIFS, NFS e iSCSI. O acesso ao plano de controle é criptografado com Transport Layer Security (TLS). O ONTAP fornece ["FIPS"](#) modo de conformidade para acesso ao plano de controle, o que habilita algoritmos aprovados pela FIPS e desabilita algoritmos que não são aprovados pela FIPS. A replicação de dados é criptografada com ["criptografia por peer de cluster"](#)o . Isso fornece criptografia para as tecnologias ONTAP SnapVault e SnapMirror.

Monitore e Registre todo o acesso

Depois que as políticas RBAC estiverem em vigor, você precisará implantar monitoramento, auditoria e alertas ativos. O mecanismo de confiança zero de FPolicy da NetApp ONTAP, juntamente com o ["Ecossistema de parceiros do NetApp FPolicy"](#), fornece os controles necessários para o modelo de confiança zero centrado em dados. O NetApp ONTAP é um software de gerenciamento de dados seguro e ["FPolicy"](#) é um recurso ONTAP líder do setor que oferece uma interface granular de notificação de eventos baseada em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP. O recurso FPolicy do ONTAP, associado ao ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. A análise comportamental do usuário pode ser usada para alertar para acesso a dados suspeitos ou aberrantes que estejam fora do padrão normal e, se necessário, tomar medidas para negar acesso.

Os parceiros do FPolicy estão indo além da análise comportamental do usuário em direção ao aprendizado de

máquina (ML) e à inteligência artificial (AI) para maior fidelidade de eventos e menos, se houver, falsos positivos. Todos os eventos devem ser registrados em um servidor syslog ou em um sistema de gerenciamento de informações e eventos de segurança (SIEM) que também pode empregar ML e IA.



da NetApp "[Segurança de carga de trabalho de armazenamento DII](#)" utiliza a interface FPolicy e análises comportamentais do usuário em sistemas de armazenamento ONTAP locais e na nuvem para fornecer alertas em tempo real sobre comportamento malicioso do usuário. O Storage Workload Security protege os dados organizacionais contra uso indevido por usuários mal-intencionados ou comprometidos por meio de aprendizado de máquina avançado e detecção de anomalias. O Storage Workload Security pode identificar ataques de ransomware ou outros comportamentos maliciosos, invocar snapshots e colocar usuários mal-intencionados em quarentena. O Storage Workload Security também tem um recurso forense para visualizar detalhadamente as atividades de usuários e entidades. A segurança da carga de trabalho de armazenamento faz parte do NetApp Data Infrastructure Insights.

Além da segurança de workload de storage, o ONTAP tem uma funcionalidade de detecção de ransomware integrada conhecida como ARP (Onboard ransomware "[Proteção autônoma contra ransomware](#)"). O ARP usa aprendizado de máquina para determinar se uma atividade anormal de arquivos indica que um ataque de ransomware está em andamento e invoca um snapshot e um alerta para os administradores. A segurança do workload de storage se integra ao ONTAP para receber eventos ARP e fornece uma camada adicional de análise e respostas automáticas.

Saiba mais sobre os comandos descritos neste procedimento no "[Referência do comando ONTAP](#)".

Controles de orquestração e automação de segurança da NetApp externos ao ONTAP

A automação permite que você execute um processo ou procedimento com o mínimo de assistência humana. A automação permite que as organizações escalem implantações Zero Trust muito além dos procedimentos manuais para se defenderem de atividades maliciosas que também são automatizadas.

O Ansible é uma ferramenta de software livre para provisionamento, gerenciamento de configuração e implantação de aplicações. Ele roda em diversos sistemas do tipo Unix e pode configurar tanto sistemas Unix quanto Microsoft Windows. Inclui sua própria linguagem declarativa para descrever a configuração do sistema. O Ansible foi escrito por Michael DeHaan e adquirido pela Red Hat em 2015. O Ansible não utiliza agentes, conectando-se temporariamente de forma remota por meio de SSH ou Gerenciamento Remoto do Windows (permitindo execução remota do PowerShell) para realizar tarefas. NetApp desenvolveu mais de ["150 módulos do Ansible para o software ONTAP"](#), possibilitando maior integração com a estrutura de automação do Ansible. Os módulos Ansible para NetApp fornecem um conjunto de instruções sobre como definir o estado desejado e transmiti-lo ao ambiente de destino NetApp. Os módulos são criados para suportar tarefas como configuração de licenciamento, criação de agregados e máquinas virtuais de armazenamento, criação de volumes e restauração de snapshots, entre outras. Uma função Ansible foi ["Publicado no GitHub"](#) desenvolvida especificamente para o NetApp DoD Unified Capabilities (UC) Deployment Guide.

Ao usar a biblioteca de módulos disponíveis, os usuários podem facilmente desenvolver playbooks do Ansible e personalizá-los de acordo com suas próprias aplicações e necessidades empresariais para automatizar tarefas mundanas. Depois que um manual é escrito, você pode executá-lo para executar a tarefa especificada, o que economiza tempo e melhora a produtividade. A NetApp criou e compartilhou exemplos de playbooks que podem ser usados diretamente ou personalizados para suas necessidades.

O Data Infrastructure Insights é uma ferramenta de monitoramento de infraestrutura que oferece visibilidade de toda a sua infraestrutura. Com o Data Infrastructure Insights, você pode monitorar, solucionar problemas e otimizar todos os seus recursos, incluindo suas instâncias de nuvem pública e seus data centers privados. O Data Infrastructure Insights pode reduzir o tempo médio de resolução em 90% e evitar que 80% dos problemas de nuvem afetem os usuários finais. Ele também pode reduzir os custos de infraestrutura de nuvem em uma média de 33% e diminuir sua exposição a ameaças internas protegendo seus dados com inteligência acionável. O recurso de segurança de carga de trabalho de armazenamento do Data Infrastructure Insights permite análises comportamentais do usuário com IA e ML para alertar quando comportamentos anormais do usuário ocorrem devido a uma ameaça interna. Para o ONTAP, o Storage Workload Security utiliza o mecanismo Zero Trust FPolicy.

Implantações de nuvem híbrida e de confiança zero

A NetApp é a autoridade em dados para a nuvem híbrida. A NetApp oferece uma variedade de opções para estender sistemas de gerenciamento de dados locais para a nuvem híbrida com Amazon Web Services (AWS), Microsoft Azure, Google Cloud e outros provedores de nuvem líderes. As soluções de nuvem híbrida da NetApp oferecem suporte aos mesmos controles de segurança Zero Trust disponíveis nos sistemas ONTAP locais e no armazenamento definido por software ONTAP Select .

Você pode expandir facilmente a capacidade em nuvens públicas sem as restrições típicas de CAPEX usando serviços de arquivo nativos em nuvem de nível empresarial para AWS (FSxN), Google Cloud (GCNV) e Azure NetApp Files para Microsoft Azure. Ideais para cargas de trabalho com uso intensivo de dados, como análise e DevOps, esses serviços de dados em nuvem combinam armazenamento elástico e sob demanda como serviço da NetApp com gerenciamento de dados ONTAP em uma oferta totalmente gerenciada.

O ONTAP permite a movimentação de dados entre seus sistemas ONTAP locais e o ambiente de armazenamento AWS, Google Cloud ou Azure com o software de replicação de dados NetApp SnapMirror .

Controle de acesso baseado em atributos

Controle de acesso baseado em atributos com ONTAP

A partir do 9.12.1, você pode configurar o ONTAP com rótulos de segurança NFSv4,2 e atributos estendidos (xattrs) para dar suporte ao controle de acesso baseado em função (RBAC) com atributos e controle de acesso baseado em atributos (ABAC).

ABAC é uma estratégia de autorização que define permissões com base em atributos de usuário, atributos de recursos e condições ambientais. A integração da ONTAP com etiquetas de segurança NFS v4,2 e xattrs está em conformidade com os padrões NIST para soluções ABAC, conforme estabelecido na publicação especial NIST 800-162.

Você pode usar rótulos de segurança NFS v4,2 e xattrs para atribuir atributos e rótulos definidos pelo usuário aos arquivos. O ONTAP pode se integrar com o software de gerenciamento de identidade e acesso orientado ao ABAC para impor políticas de controle de acesso granular a arquivos e pastas com base nesses atributos e rótulos.

Informações relacionadas

- ["Abordagens para ABAC com ONTAP"](#)
- ["NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"](#)

Abordagens para controle de acesso baseado em atributos (ABAC) no ONTAP

O ONTAP fornece várias abordagens que você pode usar para obter controle de acesso baseado em atributos de arquivo (ABAC), incluindo rótulos de segurança NFS v4,2 e atributos estendidos (xattrs) usando NFS.

Etiquetas de segurança NFS v4,2

A partir do ONTAP 9,9.1, o recurso NFS v4,2 chamado rotulado NFS é suportado.

Os rótulos de segurança NFS v4,2 são uma maneira de gerenciar o acesso granular a arquivos e pastas usando rótulos SELinux e Controle de Acesso obrigatório (MAC). Esses rótulos MAC são armazenados com arquivos e pastas e funcionam em conjunto com permissões UNIX e ACLs NFS v4.x.

O suporte para rótulos de segurança NFS v4,2 significa que a ONTAP agora reconhece e compreende as configurações de rótulo SELinux do cliente NFS. Os rótulos de segurança NFS v4,2 são cobertos no RFC-7204.

Os casos de uso de etiquetas de segurança NFS v4,2 incluem o seguinte:

- MAC rotulagem de imagens de máquina virtual (VM)
- Classificação de segurança de dados para o setor público (segredo, segredo principal e outras classificações)
- Conformidade de segurança
- Linux sem disco

Habilite rótulos de segurança NFS v4,2

Você pode ativar ou desativar rótulos de segurança NFS v4,2 com o seguinte comando (privilégio avançado necessário):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Saiba mais sobre `vserver nfs modify` o ["Referência do comando ONTAP"](#) na .

Modos de aplicação para rótulos de segurança NFS v4,2

A partir do ONTAP 9,9.1, o ONTAP suporta os seguintes modos de aplicação:

- **Modo de servidor limitado:** O ONTAP não pode impor as etiquetas, mas pode armazená-las e transmiti-las.



A capacidade de alterar etiquetas MAC depende do cliente para impor.

- **Modo convidado:** Se o cliente não estiver identificado como NFS-Aware (v4,1 ou inferior), os rótulos MAC não serão transmitidos.



Atualmente, o ONTAP não suporta o modo completo (armazenamento e aplicação de etiquetas MAC).

Exemplos de rótulos de segurança NFS v4,2

A configuração de exemplo a seguir demonstra conceitos usando o Red Hat Enterprise Linux versão 9,3 (Plow).

O usuário `jrsmith`, criado com base nas credenciais de John R. Smith, tem o seguinte Privileges de conta:

- Nome de utilizador `jrsmith`
- Privileges `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith)`
`context=user_u:user_r:user_t:s0`

Há duas funções: A conta de administrador que é um usuário privilegiado e usuário `jrsmith`, conforme descrito na seguinte tabela MLS Privileges:

Usuários	Função	Tipo	Níveis
admins	sysadm_r	sysadm_t	t:s0
jrsmith	user_r	user_t	t:s1 - t:s4

Neste ambiente de exemplo, o usuário `jrsmith` tem acesso a arquivos nos níveis `s0` `s3` de . Podemos aprimorar as classificações de segurança existentes, conforme descrito abaixo, para garantir que os administradores não tenham acesso a dados específicos do usuário.

- `s0`: dados de usuário do administrador de privilégios
- `s0`: dados não classificados
- `s1`: confidencial
- `s2`: dados secretos

- s3: dados secretos principais

Exemplo de etiquetas de segurança NFS v4,2 com MCS

Além do MLS (Multi-Level Security), outro recurso chamado MCS (Multi-Category Security) permite definir categorias como projetos.

Etiqueta de segurança NFS	Valor
entitySecurityMark	t:s01 = UNCLASSIFIED

Atributos estendidos (xattrs)

A partir do ONTAP 9.12.1, o ONTAP suporta xattrs. Os xattrs permitem que os metadados sejam associados a arquivos e diretórios além do que é fornecido pelo sistema, como listas de controle de acesso (ACLs) ou atributos definidos pelo usuário.

Para implementar o xattrs, você pode usar `setfattr` e `getfattr` utilitários de linha de comando no Linux. Essas ferramentas fornecem uma maneira poderosa de gerenciar metadados adicionais para arquivos e diretórios. Eles devem ser usados com cuidado, pois o uso inadequado pode levar a comportamentos inesperados ou problemas de segurança. Consulte sempre as `setfattr` páginas de manual e `getfattr` ou outra documentação fiável para obter instruções de utilização detalhadas.

Quando o xattrs está habilitado em um sistema de arquivos ONTAP, os usuários podem definir, modificar e recuperar atributos arbitrários em arquivos. Esses atributos podem ser usados para armazenar informações adicionais sobre o arquivo que não é capturado pelo conjunto padrão de atributos de arquivo, como informações de controle de acesso.

Existem vários requisitos e limites para o uso de xattrs no ONTAP:

- Red Hat Enterprise Linux 8,4 ou posterior
- Ubuntu 22,04 ou posterior
- Cada arquivo pode ter até 128 xattrs
- As chaves xattr estão limitadas a 255 bytes
- O tamanho combinado da chave ou do valor é de 1.729 bytes por xattr
- Diretórios e arquivos podem ter xattrs
- Para definir e recuperar xattrs `w`, ou bits de modo de gravação devem estar ativados para o usuário e grupo

Os Xattrs são utilizados dentro do namespace do usuário e não carregam nenhum significado intrínseco para o próprio ONTAP. Em vez disso, suas aplicações práticas são determinadas e gerenciadas exclusivamente pelo aplicativo do lado do cliente que interage com o sistema de arquivos.

Exemplos de casos de uso do xattr:

- Gravando o nome do aplicativo responsável pela criação de um arquivo
- Manter uma referência à mensagem de e-mail a partir da qual um arquivo foi obtido
- Estabelecendo uma estrutura de categorização para organizar objetos de arquivo

- Rotular arquivos com o URL de sua fonte de download original

Comandos para gerenciar xattrs

- `setfattr` define um atributo estendido de um arquivo ou diretório:

```
setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
```

Exemplo de comando:

```
setfattr -n user.comment -v test example.txt
```

- `getfattr` recupera o valor de um atributo estendido específico ou lista todos os atributos estendidos de um arquivo ou diretório:

Atributo específico:

```
getfattr -n <attribute_name> <file or directory name>
```

Todos os atributos:

```
getfattr <file or directory name>
```

Exemplo de comando:

```
getfattr -n user.comment example.txt
```

Exemplos de pares de valores de chave xattr

A tabela a seguir mostra dois exemplos de pares de valores de chave xattr:

xattr	Valor
user.digitalIdentifier	CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US
user.countryOfAffiliations	USA

Permissões de usuário com ACE para xattrs

Uma entrada de controle de acesso (ACE) é um componente dentro de uma ACL que define os direitos de acesso ou permissões concedidas a um usuário individual ou a um grupo de usuários para um recurso específico, como um arquivo ou diretório. Cada ACE especifica o tipo de acesso permitido ou negado e está associado a um responsável de segurança específico (identidade de usuário ou grupo).

Entrada de controle de acesso (ACE) necessária para xattrs

- Recuperar xattr: As permissões necessárias para um usuário ler os atributos estendidos de um arquivo ou diretório. O "R" significa que a permissão de leitura é necessária.
- Definir xattrs: As permissões necessárias para modificar ou definir os atributos estendidos. "A", "W" e "T"

representam diferentes exemplos de permissões, como anexar, escrever e uma permissão específica relacionada ao xattrs.

- Arquivos: Os usuários precisam anexar, escrever e potencialmente uma permissão especial relacionada ao xattrs para definir atributos estendidos.
- Diretórios: Uma permissão específica "T" é necessária para definir atributos estendidos.

Tipo de ficheiro	Recuperar xattr	Definir xattrs
Ficheiro	R	A, W, T
Diretório	R	T

Integração com software de controle de acesso e identidade ABAC

Para aproveitar totalmente os recursos do ABAC, o ONTAP pode se integrar com um software de gerenciamento de identidade e acesso orientado ao ABAC.

Em um sistema ABAC, o ponto de aplicação da Política (PEP) e o ponto de Decisão da Política (PDP) desempenham papéis cruciais. O PEP é responsável pela aplicação de políticas de controle de acesso, enquanto o PDP toma a decisão de conceder ou negar acesso com base nas políticas.

Em um ambiente prático, uma organização empregaria uma mistura de rótulos de segurança NFS e xattrs. Estes são usados para representar uma variedade de metadados, incluindo classificação, segurança, aplicação e conteúdo, que são todos fundamentais na tomada de decisões ABAC.xattrs, por exemplo, pode ser usado para armazenar os atributos de recursos que o PDP usa para seu processo de tomada de decisão. Um atributo pode ser definido para representar o nível de classificação de um arquivo (por exemplo, "não classificado", "confidencial", "segredo" ou "segredo superior"). O PDP poderia então utilizar este atributo para impor uma política que restringe os utilizadores a aceder apenas a ficheiros que tenham um nível de classificação igual ou inferior ao nível de autorização.



Este conteúdo pressupõe que os serviços de identidade, autenticação e acesso do cliente incluem, no mínimo, um PEP e um PDP que atuam como intermediários para o acesso ao sistema de arquivos.

Exemplo de fluxo de processo para ABAC

1. O usuário apresenta credenciais (por exemplo, PKI, OAuth, SAML) para acesso ao sistema ao PEP e obtém resultados do PDP.

A função do PEP é interceptar a solicitação de acesso do usuário e encaminhá-la para o PDP.

2. Em seguida, o PDP avalia essa solicitação em relação às políticas estabelecidas da ABAC.

Essas políticas consideram vários atributos relacionados ao usuário, ao recurso em questão e ao ambiente circundante. Com base nessas políticas, o PDP toma uma decisão de acesso para permitir ou negar e, em seguida, comunica essa decisão de volta ao PEP.

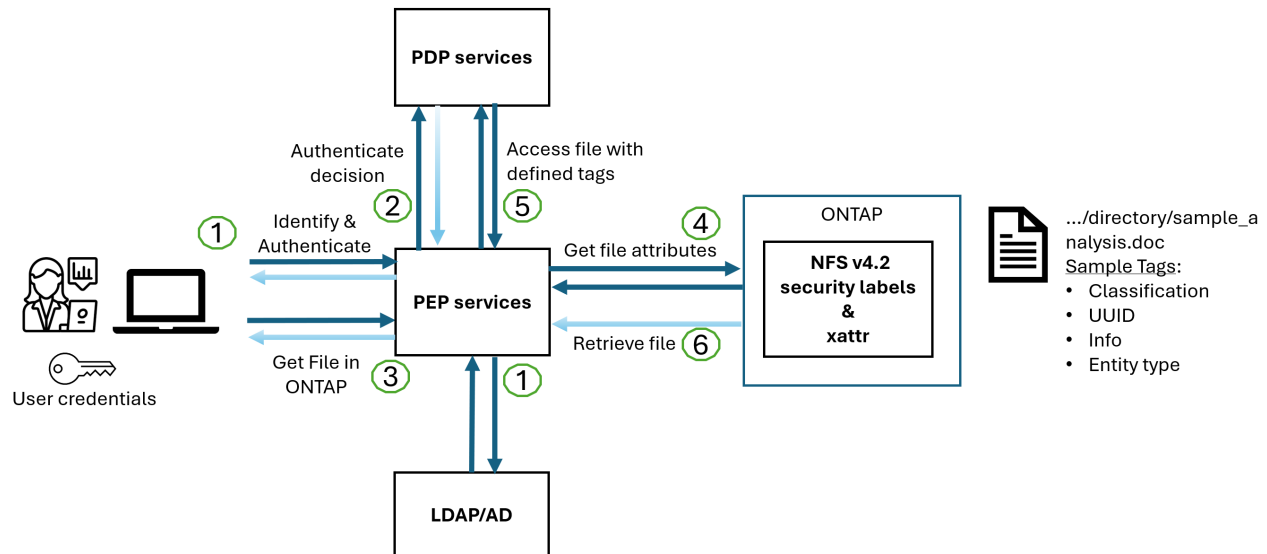
PDP fornece política para PEP para fazer cumprir. O PEP então impõe essa decisão, concedendo ou negando o pedido de acesso do usuário conforme decisão do PDP.

3. Após uma solicitação bem-sucedida, o usuário solicita um arquivo armazenado no ONTAP (AFF, AFF-C, por exemplo).
4. Se a solicitação for bem-sucedida, o PEP obtém tags de controle de acesso de grãos finos do documento.

5. PEP solicita política para o utilizador com base nos certificados desse utilizador.
6. O PEP toma uma decisão com base na política e nas tags se o usuário tiver acesso ao arquivo e permitir que o usuário recupere o arquivo.



O acesso real pode ser feito usando tokens.



Clonagem de ONTAP e SnapMirror

As tecnologias de clonagem e SnapMirror da ONTAP foram projetadas para fornecer recursos de replicação e clonagem de dados eficientes e confiáveis, garantindo que todos os aspectos dos dados de arquivos, incluindo xattrs, sejam preservados e transferidos juntamente com o arquivo. Os xattrs são críticos, pois armazenam metadados adicionais associados a um arquivo, como rótulos de segurança, informações de controle de acesso e dados definidos pelo usuário, essenciais para manter o contexto e integridade do arquivo.

Quando um volume é clonado usando a tecnologia FlexClone da ONTAP, uma réplica gravável exata do volume é criada. Esse processo de clonagem é instantâneo e eficiente em espaço, e inclui todos os dados e metadados de arquivos, garantindo que os xattrs sejam totalmente replicados. Da mesma forma, o SnapMirror garante que os dados sejam espelhados para um sistema secundário com fidelidade total. Isso inclui xattrs, que são cruciais para aplicativos que dependem desses metadados para funcionar corretamente.

Ao incluir xattrs nas operações de clonagem e replicação, o NetApp ONTAP garante que todo o conjunto de dados, com todas as suas características, esteja disponível e consistente em sistemas de storage primário e secundário. Essa abordagem abrangente ao gerenciamento de dados é vital para organizações que exigem proteção de dados consistente, recuperação rápida e adesão a padrões regulatórios e de conformidade. Ele também simplifica o gerenciamento de dados em diferentes ambientes, seja no local ou na nuvem, fornecendo aos usuários a confiança de que seus dados estão completos e inalterados durante esses processos.



As etiquetas de segurança NFS v4,2 têm as ressalvas definidas no 2.

Auditoria de alterações em rótulos

A auditoria de alterações em rótulos de segurança xattrs ou NFS é um aspecto crítico do gerenciamento e da segurança do sistema de arquivos. As ferramentas padrão de auditoria do sistema de arquivos permitem o monitoramento e o Registro de todas as alterações em um sistema de arquivos, incluindo modificações em

xattrs e rótulos de segurança.

Em ambientes Linux, o `auditd` daemon é comumente usado para estabelecer auditoria para eventos de sistema de arquivos. Ele permite que os administradores configurem regras para observar chamadas específicas do sistema relacionadas a alterações xattr, como `setxattr`, `lsetxattr` e `fsetxattr` para definir atributos e, `lremovexattr` e `fremovexattr` para `removexattr` remover atributos.

O ONTAP FPolicy amplia esses recursos fornecendo uma estrutura robusta para monitoramento e controle em tempo real de operações de arquivos. O FPolicy pode ser configurado para oferecer suporte a vários eventos xattr, oferecendo controle granular sobre as operações de arquivos e a capacidade de aplicar políticas abrangentes de gerenciamento de dados.

Para usuários que utilizam xattrs, especialmente em ambientes NFS v3 e NFS v4, apenas determinadas combinações de operações de arquivos e filtros são suportadas para monitoramento. A lista de combinações de filtro e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFS v3 e NFS v4 é detalhada abaixo:

Operações de arquivos compatíveis	Filtros suportados
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

Exemplo de um snippet de log auditd para uma operação setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Habilitar ["Política de ONTAP"](#) para usuários que trabalham com xattrs fornece uma camada de visibilidade e controle que é essencial para manter a integridade e a segurança do sistema de arquivos. Ao aproveitar os recursos avançados de monitoramento da FPolicy, as organizações podem garantir que todas as alterações aos xattrs sejam rastreadas, auditadas e alinhadas com seus padrões de segurança e conformidade. Essa abordagem proativa para o gerenciamento do sistema de arquivos é por isso que habilitar o ONTAP FPolicy é altamente recomendado para qualquer organização que queira aprimorar suas estratégias de governança e proteção de dados.

Exemplos de controle do acesso aos dados

A seguinte entrada de exemplo para dados armazenados no cert PKI de John R. Smith mostra como a abordagem do NetApp pode ser aplicada a um arquivo e fornecer controle de acesso refinado.



Esses exemplos são para fins ilustrativos, e é responsabilidade do cliente determinar os metadados associados a etiquetas de segurança NFS v4,2 e xattrs. Detalhes sobre a atualização e retenção de rótulos são omitidos para simplificar.

Exemplo de valores de cert PKI

Chave	Valor
EntitySecurityMark	t:S01 NÃO CLASSIFICADO
Informações	<pre>{ "commonName": { "value": "Smith John R jrsmith" }, "emailAddresses": [{ "value": "jrsmith@dod.mil" }], "employeeId": { "value": "00000387835" }, "firstName": { "value": "John" }, "lastName": { "value": "Smith" }, "telephoneNumber": { "value": "938/260-9537" }, "uid": { "value": "jrsmith" } }</pre>
especificação	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15
AdminOrganization	<pre>{ "value": "DoD" }</pre>

Chave	Valor
briefings	<pre>[{ "value": "ABC1000" }, { "value": "DEF1001" }, { "value": "EFG2000" }]</pre>
CitizensaStatus	<pre>{ "value": "US" }</pre>
folgas	<pre>[{ "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" }]</pre>
CountryOfAffiliations	<pre>[{ "value": "USA" }]</pre>

Chave	Valor
DigitalIdentifier	<pre>{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }</pre>
It is always	<pre>{ "value": "DoD" }</pre>
DutyOrganization	<pre>{ "value": "DoD" }</pre>
Tipo de entidade	<pre>{ "value": "GOV" }</pre>
FineAccessControls	<pre>[{ "value": "SI" }, { "value": "TK" }, { "value": "NSYS" }]</pre>

Esses direitos PKI mostram os detalhes de acesso de John R. Smith, incluindo acesso por tipo de dados e atribuição.

Em cenários em que os metadados IC-TDF são armazenados separadamente do arquivo, o NetApp defende uma camada adicional de controle de acesso refinado. Isso envolve o armazenamento de informações de controle de acesso tanto no nível de diretório quanto em associação com cada arquivo. Como exemplo, considere as seguintes tags vinculadas a um arquivo:

- Rótulos de segurança NFS v4,2: Utilizados para tomar decisões de segurança
- Xattrs: Fornecer informações complementares pertinentes ao arquivo e aos requisitos do programa organizacional

Os pares chave-valor a seguir são exemplos de metadados que podem ser armazenados como xattrs e oferecer informações detalhadas sobre o criador do arquivo e classificações de segurança associadas. Esses metadados podem ser aproveitados por aplicativos clientes para tomar decisões de acesso informado e organizar arquivos de acordo com os padrões e requisitos organizacionais.

- Exemplo de pares de chave-valor xattr*

Chave	Valor
user.uuid	"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"
user.entitySecurityMark	"UNCLASSIFIED"
user.specification	"INFO"

Chave	Valor
user.Info	<pre> { "commonName": { "value": "Smith John R jrsmith" }, "currentOrganization": { "value": "TUV33" }, "displayName": { "value": "John Smith" }, "emailAddresses": ["jrsmith@example.org"], "employeeId": { "value": "00000405732" }, "firstName": { "value": "John" }, "lastName": { "value": "Smith" }, "managers": [{ "value": "" }], "organizations": [{ "value": "TUV33" }, { "value": "WXY44" }], "personalTitle": { "value": "" }, "secureTelephoneNumber": { "value": "506-7718" }, "telephoneNumber": { "value": "264/160-7187" }, "title": { "value": "Software Engineer" }, </pre>

Chave	Valor
user.geo_point	[-78.7941, 35.7956]

}

Informações relacionadas

- ["NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"](#)
- ["Referência do comando ONTAP"](#)
- Pedido de comentários (RFC)
 - ["RFC 7204: Requisitos para NFS rotulado"](#)
 - ["RFC 2203: Especificação do protocolo RPCSEC_GSS"](#)
 - ["RFC 3530: Protocolo NFS \(Network File System\) versão 4"](#)

Endurecimento da segurança

Guias de proteção de segurança da ONTAP

Esses relatórios técnicos fornecem orientação sobre como endurecer o NetApp ONTAP, bem como outros produtos NetApp.



Esses relatórios técnicos expandem a ["Segurança e criptografia de dados do ONTAP"](#) documentação do produto.

Guias de endurecimento

["TR-4569: Guia de proteção de segurança para NetApp ONTAP"](#) Saiba como configurar o NetApp ONTAP para ajudar as organizações a cumprir os objetivos de segurança prescritos para a confidencialidade, integridade e disponibilidade do sistema de informações.

["Guia de fortalecimento da segurança para as ferramentas do ONTAP para VMware vSphere"](#) Saiba como configurar as ferramentas do ONTAP para o VMware vSphere para ajudar as organizações a cumprir os objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

["TR-4957: Guia de proteção de segurança para NetApp SnapCenter"](#) Saiba como configurar o software NetApp SnapCenter para ajudar as organizações a cumprir os objetivos de segurança prescritos para a confidencialidade, integridade e disponibilidade do sistema de informações.

["TR-4963: Guia de reforço de segurança: NetApp Backup and Recovery for Applications"](#) Aprenda a configurar o NetApp Cloud Backup for Applications para ajudar as organizações a atingir os objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

["TR-4943: Guia de proteção de segurança para NetApp Active IQ Unified Manager"](#) Saiba como configurar o NetApp Active IQ Unified Manager para ajudar as organizações a cumprir os objetivos de segurança prescritos para a confidencialidade, integridade e disponibilidade do sistema de informações.

["TR-4945: Guia de proteção de segurança para SDK de gerenciamento do NetApp"](#) Saiba como configurar o NetApp Manageability SDK (NMSDK) para ajudar as organizações a cumprir os objetivos de segurança prescritos para a confidencialidade, integridade e disponibilidade do sistema de informações.

["Guia de proteção de segurança para host e banco de dados do MetroCluster tiebreaker"](#) Saiba como configurar o host e o banco de dados do NetApp MetroCluster tiebreaker para ajudar as organizações a atender aos objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

Diretrizes de fortalecimento da segurança do ONTAP

Visão geral do fortalecimento da segurança do ONTAP

O ONTAP fornece um conjunto de controles que permitem proteger o sistema operacional de storage ONTAP, o software de gerenciamento de dados líder do setor. Use as orientações e as configurações do ONTAP para ajudar sua organização a cumprir os objetivos de segurança prescritos para confidencialidade, integridade e

disponibilidade do sistema de informações.

A evolução do cenário atual de ameaças apresenta uma organização com desafios únicos para proteger seus ativos mais valiosos: Dados e informações. As ameaças e vulnerabilidades avançadas e dinâmicas que enfrentamos estão cada vez mais aumentando em sofisticação. Juntamente com um aumento na eficácia das técnicas de ofuscação e reconhecimento por parte de potenciais intrusos, os gestores de sistemas devem abordar a segurança de dados e informações de forma proativa.



A partir de julho de 2024, o conteúdo do relatório técnico *TR-4569: Guia de proteção de segurança para ONTAP*, que foi publicado anteriormente em PDF, está disponível em docs.netapp.com.

Validação de imagem ONTAP

O ONTAP fornece mecanismos para garantir que a imagem ONTAP seja válida na atualização e no momento da inicialização.

Atualizar validação de imagem

A assinatura de código ajuda a verificar se as imagens ONTAP instaladas por meio de atualizações de imagem sem interrupções ou atualizações automatizadas de imagem sem interrupções, CLIs ou APIs ONTAP são autenticamente produzidas pela NetApp e não foram adulteradas. A validação da imagem de atualização foi introduzida no ONTAP 9.3.

Esse recurso é um aprimoramento de segurança sem toque para atualização ou reversão do ONTAP. Não se espera que o usuário faça nada de diferente, exceto para opcionalmente verificar a assinatura de nível `superior image.tgz`.

Validação de imagem no momento da inicialização

A partir do ONTAP 9.4, a inicialização segura da interface de firmware extensível unificada (UEFI) é ativada para sistemas NetApp AFF A800, AFF A220, FAS2750 e FAS2720 e sistemas subsequentes de próxima geração que utilizam BIOS UEFI.

Durante a ativação, o bootloader valida o banco de dados da lista de permissões de chaves de inicialização seguras com a assinatura associada a cada módulo carregado. Depois que cada módulo é validado e carregado, o processo de inicialização continua com a inicialização do ONTAP. Se a validação da assinatura falhar para qualquer módulo, o sistema será reiniciado.



Esses itens se aplicam às imagens do ONTAP e ao BIOS da plataforma.

Contas de administrador de armazenamento local

Funções, aplicativos e autenticação do ONTAP

O ONTAP fornece à empresa com consciência de segurança a capacidade de fornecer acesso granular a diferentes administradores por meio de diferentes aplicativos e métodos de login. Isso ajuda os clientes a criar um modelo de confiança zero centrado nos dados.

Estas são as funções disponíveis para administradores de máquinas virtuais de administração e

armazenamento. Os métodos de aplicação de início de sessão e os métodos de autenticação de início de sessão são especificados.

Funções

Com o controle de acesso baseado em funções (RBAC), os usuários têm acesso apenas aos sistemas e opções necessários para suas funções e funções de trabalho. A solução RBAC no ONTAP limita o acesso administrativo dos usuários ao nível concedido para sua função definida, o que permite que os administradores gerenciem os usuários por função atribuída. O ONTAP fornece várias funções predefinidas. Os operadores e administradores podem criar, modificar ou excluir funções de controle de acesso personalizadas e podem especificar restrições de conta para funções específicas.

Funções predefinidas para administradores de cluster

Esta função...	Tem este nível de acesso...	Para os seguintes comandos ou diretórios de comandos
admin	Tudo	Todos os diretórios de comando (DEFAULT)
admin-no-fsa (Disponível a partir do ONTAP 9.12.1)	Leitura/escrita	• Todos os diretórios de comando (DEFAULT) • security login rest-role • security login role

Somente leitura	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	Nenhum
volume file show-disk-usage	autosupport	Tudo
• set • system node autosupport	Nenhum	Todos os outros diretórios de comando (DEFAULT)
backup	Tudo	vserver services ndmp
Somente leitura	volume	Nenhum
Todos os outros diretórios de comando (DEFAULT)	readonly	Tudo

• security login password Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves • set	Nenhum	security
Somente leitura	Todos os outros diretórios de comando (DEFAULT)	none



A autosupport função é atribuída à conta predefinida autosupport, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a autosupport conta. O ONTAP também impede que você atribua autosupport a função a outras contas de usuário.

Funções predefinidas para administradores de máquina virtual de storage (SVM)

Nome da função	Recursos
vsadmin	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, snapshots e arquivos • Gerenciar LUNs • Executar operações SnapLock, exceto exclusão privilegiada • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede • Monitorar a integridade do SVM

vsadmin-volume	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, snapshots e arquivos • Gerenciar LUNs • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede • Monitorar a integridade do SVM
vsadmin-protocol	• Gerencie a senha local da própria conta de usuário e as informações chave • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Gerenciar LUNs • Monitorar a interface de rede • Monitorar a integridade do SVM
vsadmin-backup	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerenciar operações NDMP • Faça uma leitura/gravação de volume restaurada • Gerenciar relacionamentos e snapshots do SnapMirror • Exibir volumes e informações de rede
vsadmin-snaplock	• Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, snapshots e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurar protocolos: NFS e SMB • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede

vsadmin-readonly	• Gerencie a senha local da própria conta de usuário e as informações chave • Monitorar a integridade do SVM • Monitorar a interface de rede • Visualizar volumes e LUNs • Exibir serviços e protocolos
------------------	---

Métodos de aplicação

O método de aplicação especifica o tipo de acesso do método de início de sessão. Os valores possíveis incluem `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, e `telnet`.

Definir este parâmetro para `service-processor` conceder ao utilizador acesso ao processador de serviço. Quando este parâmetro está definido como `service-processor`, o `-authentication-method` parâmetro tem de ser definido como `password` porque o processador de serviço suporta apenas `password` a autenticação. As contas de usuário do SVM não podem acessar o processador de serviços. Portanto, os operadores e administradores não podem usar o `-vserver` parâmetro quando este parâmetro está definido como `service-processor`.

Para restringir ainda mais o acesso ao `service-processor` use o comando `system service-processor ssh add-allowed-addresses`. O comando `system service-processor api-service` pode ser usado para atualizar as configurações e certificados.

Por motivos de segurança, o Telnet e o Shell remoto (RSH) são desativados por padrão porque o NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro. Se houver um requisito ou necessidade exclusiva para Telnet ou RSH, eles devem ser ativados.

O `security protocol modify` comando modifica a configuração existente em todo o cluster do RSH e Telnet. Ative o RSH e o Telnet no cluster definindo o campo ativado para `true`.

Métodos de autenticação

O parâmetro método de autenticação especifica o método de autenticação usado para logins.

Método de autenticação	Descrição
<code>cert</code>	Autenticação de certificado SSL
<code>community</code>	Strings de comunidade SNMP
<code>domain</code>	Autenticação do ativo Directory
<code>nsswitch</code>	Autenticação LDAP ou NIS
<code>password</code>	Palavra-passe
<code>publickey</code>	Autenticação de chave pública
<code>usm</code>	Modelo de segurança do utilizador SNMP



O uso de NIS não é recomendado devido a falhas de segurança do protocolo.

A partir do ONTAP 9.3, a autenticação de dois fatores encadeada está disponível para contas SSH locais

admin usando publickey e password como os dois métodos de autenticação. Além do `-authentication-method` campo no `security login` comando, um novo campo chamado `-second-authentication-method` foi adicionado. `publickey` ou `password` pode ser especificado como `-authentication-method` ou `-second-authentication-method`. No entanto, durante a autenticação SSH, a ordem é sempre `publickey` com autenticação parcial, seguida pelo prompt de senha para autenticação completa.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

Começando com ONTAP 9.4, `nsswitch` pode ser usado como um segundo método de autenticação com `publickey`.

A partir do ONTAP 9.12.1, o FIDO2 também pode ser usado para autenticação SSH usando um dispositivo de autenticação de hardware YubiKey ou outros dispositivos compatíveis com o FIDO2.

Começando com ONTAP 9.13.1:

- `domain` as contas podem ser usadas como um segundo método de autenticação com `publickey`.
- Senha única baseada no tempo (totp) é uma senha temporária gerada por um algoritmo que usa a hora atual do dia como um de seus fatores de autenticação para o segundo método de autenticação.
- A revogação de chaves públicas é suportada com chaves públicas SSH, bem como certificados que serão verificados para expiração/revogação durante o SSH.

Para obter mais informações sobre autenticação multifator (MFA) para ONTAP System Manager, Active IQ Unified Manager e SSH, consulte ["TR-4647: Autenticação multifator no ONTAP 9"](#).

Contas administrativas padrão

A conta de administrador deve ser restrita porque a função de administrador tem acesso permitido usando todos os aplicativos. A conta `diag` permite o acesso ao shell do sistema e deve ser reservada apenas para o suporte técnico para executar tarefas de solução de problemas.

Existem duas contas administrativas padrão: `admin` e `diag`.

As contas órfãs são um grande vetor de segurança que muitas vezes leva a vulnerabilidades, incluindo a escalação de Privileges. Estas são contas desnecessárias e não utilizadas que permanecem no repositório de contas de usuário. São principalmente contas padrão que nunca foram usadas ou para as quais senhas nunca foram atualizadas ou alteradas. Para resolver esse problema, o ONTAP suporta a remoção e renomeação de contas.



Não é possível remover ou renomear contas incorporadas. Se um administrador remover a conta, após reinicializar, a conta incorporada será recriada. **NetApp recomenda** bloquear quaisquer contas incorporadas desnecessárias com o comando `lock`.

Embora contas órfãs representem um problema de segurança significativo, **NetApp recomenda fortemente**

testar o efeito da remoção de contas do repositório local.

Listar contas locais

Para listar as contas locais, execute o `security login show` comando.

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1

User/Group Name      Application  Authentication Method  Role Name  Acct Locked  Is-Nsswitch Group
-----
admin                console     password  admin      no        no
admin                http        password  admin      no        no
admin                ontapi      password  admin      no        no
admin                service-processor password  admin      no        no
admin                ssh         password  admin      no        no
autosupport          console     password  autosupport no        no
6 entries were displayed.
```

Definir a palavra-passe da conta de diagnóstico (diag)

Uma conta de diagnóstico nomeada `diag` é fornecida com o sistema de storage. Você pode usar a `diag` conta para executar tarefas de solução de problemas no `systemshell`. A `diag` conta é a única conta que pode ser usada para acessar o `systemshell` através do `diag` comando ``systemshell`` privilegiado .



O `systemshell` e a conta associada `diag` destinam-se a fins de diagnóstico de baixo nível. Seu acesso requer o nível de privilégio de diagnóstico e é reservado apenas para ser usado com orientação do suporte técnico para executar tarefas de solução de problemas. Nem a `diag` conta nem o `systemshell` destinam-se a fins administrativos gerais.

Antes de começar

Antes de aceder ao `systemshell`, tem de definir a `diag` palavra-passe da conta utilizando o `security login password` comando . Você deve usar princípios de senha fortes e alterar a `diag` senha em intervalos regulares.

Passos

1. Defina a `diag` senha do usuário da conta:

```
cluster1::> set -privilege diag
```

```
Warning: These diagnostic commands are for use by NetApp personnel only.  
Do you want to continue? \{y|n\}: y
```

```
cluster1::*> systemshell -node node-01  
      (system node systemshell)  
diag@node-01's password:
```

```
Warning: The system shell provides access to low-level  
diagnostic tools that can cause irreparable damage to  
the system if not used properly. Use this environment  
only when directed to do so by support personnel.
```

```
node-01%
```

Verificação multi-admin

A partir do ONTAP 9.11.1, você pode usar a verificação multiadministrador (MAV) para permitir que determinadas operações, como a exclusão de volumes ou snapshots, sejam executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração do MAV consiste no seguinte:

- ["Criando um ou mais grupos de aprovação de administrador"](#).
- ["Habilitando a funcionalidade de verificação de vários administradores"](#).
- ["Adicionar ou modificar regras"](#).

Após a configuração inicial, somente os administradores de um grupo de aprovação MAV (administradores MAV) podem modificar esses elementos.

Quando o MAV está ativado, a conclusão de cada operação protegida requer três passos:

1. Quando um usuário inicia a operação, um ["a solicitação é gerada"](#).
2. Antes de poder ser executado, o número necessário de ["Os administradores do MAV devem aprovar"](#).
3. Após a aprovação, o utilizador conclui a operação.

O MAV não se destina a ser usado com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada requer aprovação antes que a operação possa ser concluída. Se você quiser usar automação e MAV juntos, a NetApp recomenda que você use consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

Para obter informações mais detalhadas sobre o MAV, consulte o ["Documentação de verificação de vários administradores do ONTAP"](#).

Bloqueio instantâneo

O bloqueio de snapshot é um recurso do SnapLock no qual os snapshots são tornados indelévels manual ou automaticamente com um período de retenção na política de snapshot de volume. O objetivo do bloqueio de snapshot é impedir que administradores desonestos ou não confiáveis excluam snapshots no sistema ONTAP primário ou secundário.

O bloqueio instantâneo foi introduzido no ONTAP 9.12.1. O bloqueio de snapshot também é conhecido como bloqueio de snapshot à prova de violação. Embora exija a licença SnapLock e a inicialização do relógio de conformidade, o bloqueio de instantâneos não está relacionado ao SnapLock Compliance ou ao SnapLock Enterprise. Não há administrador de storage confiável, assim como o SnapLock Enterprise e ele não protege a infraestrutura de storage físico subjacente, como o SnapLock Compliance. Essa é uma melhoria em relação aos snapshots SnapVaulting para um sistema secundário. A recuperação rápida de snapshots bloqueados em sistemas primários pode ser obtida para restaurar volumes corrompidos por ransomware.

Para obter mais detalhes, consulte ["documentação de bloqueio de instantâneos"](#).

Configure o acesso à API baseado em certificado

Em vez de autenticação de ID de usuário e senha para acesso à API REST ou à API SDK de gerenciamento do NetApp ao ONTAP, a autenticação baseada em certificado deve ser usada.



Como alternativa à autenticação baseada em certificado para API REST, use ["Autenticação baseada em token OAuth 2.0"](#).)

Você pode gerar e instalar um certificado autoassinado no ONTAP conforme descrito nestas etapas.

Passos

1. Usando OpenSSL, gere um certificado executando o seguinte comando:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key  
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'test.key'
```

Este comando gera um certificado público nomeado `test.pem` e uma chave privada chamada `key.out`. O nome comum, CN, corresponde ao ID de usuário do ONTAP.

2. Instale o conteúdo do certificado público no formato pem (Privacy Enhanced mail) no ONTAP executando o seguinte comando e colando o conteúdo do certificado quando solicitado:

```
security certificate install -type client-ca -vserver cluster1
```

Please enter Certificate: Press <Enter> when done

3. Ative o ONTAP para permitir o acesso do cliente através de SSL e definir a ID do usuário para acesso à API.

```
security ssl modify -vserver cluster1 -client-enabled true  
security login create -user-or-group-name cert_user -application ontapi  
-authmethod cert -role admin -vserver cluster1
```

No exemplo a seguir, o ID de usuário `cert_user` agora está habilitado para usar o acesso à API autenticado por certificado. Um script Python simples do SDK para gerenciamento usando `cert_user` para exibir a versão do ONTAP aparece da seguinte forma:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

A saída do script exibe a versão do ONTAP.

```
./version.py
```

```
V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Para executar a autenticação baseada em certificado com a API REST do ONTAP, execute as seguintes etapas:

- a. No ONTAP, defina a ID do usuário para acesso http:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. No seu cliente Linux, execute o seguinte comando que produz a versão ONTAP como saída:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

Mais informações

- ["Autenticação baseada em certificado com o SDK de gerenciamento do NetApp para ONTAP"](#).

Autenticação baseada em token ONTAP OAuth 2,0 para API REST

Como alternativa à autenticação baseada em certificado, você pode usar a autenticação baseada em token OAuth 2,0 para API REST.

A partir do ONTAP 9.14,1, você tem a opção de controlar o acesso aos clusters do ONTAP usando a estrutura autorização aberta (OAuth 2,0). Você pode configurar esse recurso usando qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI do ONTAP, o Gerenciador do sistema e a API REST. No entanto, as decisões de autorização e controle de acesso do OAuth 2,0 só podem ser aplicadas quando um cliente acessa o ONTAP usando a API REST.

Os tokens OAuth 2,0 substituem senhas para autenticação de conta de usuário.

Para obter mais informações sobre como usar o OAuth 2,0, consulte ["Documentação do ONTAP sobre autenticação e autorização usando OAuth 2,0"](#).

Parâmetros de login e senha

Uma postura de segurança eficaz adere às políticas organizacionais estabelecidas, diretrizes e qualquer governança ou padrões que se apliquem à organização. Exemplos desses requisitos incluem vida útil do nome de usuário, requisitos de comprimento de senha, requisitos de caracteres e o armazenamento de tais contas. A solução ONTAP fornece recursos e funções para lidar com essas construções de segurança.

Novos recursos de conta local

Para oferecer suporte às políticas, diretrizes ou padrões de contas de usuário de uma organização, incluindo

governança, a seguinte funcionalidade é suportada no ONTAP:

- Configurando políticas de senha para impor um número mínimo de dígitos, caracteres minúsculos ou caracteres maiúsculos
- Exigindo um atraso após uma tentativa de login com falha
- Definir o limite inativo da conta
- A expirar uma conta de utilizador
- Exibindo uma mensagem de aviso de expiração de senha
- Notificação de um login inválido



As configurações configuráveis são gerenciadas usando o comando `security login role config modify`.

Suporte SHA-512

Para melhorar a segurança da senha, o ONTAP 9 suporta a função hash de senha SHA-2 e usa o padrão SHA-512 para hashing de senhas recém-criadas ou alteradas. Os operadores e administradores também podem expirar ou bloquear contas conforme necessário.

As contas de usuário pré-existentes do ONTAP 9 com senhas inalteradas continuam a usar a função hash MD5 após a atualização para o ONTAP 9.0 ou posterior. No entanto, a NetApp recomenda fortemente que essas contas de usuário migrem para a solução SHA-512 mais segura, fazendo com que os usuários alterem suas senhas.

A funcionalidade hash de senha permite executar as seguintes tarefas:

- Exibir contas de usuário que correspondem à função hash especificada:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name  application  authentication-method  hash-
function
-----
-----
cluster1 NewAdmin          console     password          sha512
cluster1 NewAdmin          ontapi      password          sha512
cluster1 NewAdmin          ssh         password          sha512
```

- As contas expiram que usam uma função hash especificada (por exemplo, MD5), que força os usuários a alterar suas senhas no próximo login:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Bloqueie contas com senhas que usam a função hash especificada.

```
cluster1::*> security login lock -vserver * -username * -hash-function md5
```

A função hash de senha é desconhecida para o usuário interno `autosupport` no SVM administrativo do cluster. Esta questão é cosmética. A função hash é desconhecida porque este usuário interno não tem uma senha configurada por padrão.

- Para exibir a função hash de senha para `autosupport` o usuário, execute os seguintes comandos:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: unknown
Second Authentication Method2: none
```

- Para definir a função hash de senha (padrão: SHA512), execute o seguinte comando:

```
::> security login password -username autosupport
```

Não importa para que a senha está definida.

```
security login show -user-or-group-name autosupport -instance
```

```
Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: sha512
Second Authentication Method2: none
```

Parâmetros da palavra-passe

A solução ONTAP suporta parâmetros de senha que atendem e suportam requisitos e diretrizes de políticas organizacionais.

A partir de 9.14.1, há uma complexidade maior e regras de bloqueio para senhas que se aplicam apenas a novas instalações do ONTAP.

Todas as senhas devem ser distintas do nome de usuário.

Atributo	Descrição	Padrão	Alcance
username-minlength	É necessário um comprimento mínimo do nome de utilizador	3	3-16
username-alphanum	Nome de utilizador alfanumérico	desativado	Ativado/desativado
passwd-minlength	É necessário um comprimento mínimo da palavra-passe	8	3-64
passwd-alphanum	Palavra-passe alfanumérica	ativado	Ativado/desativado
passwd-min-special-chars	Número mínimo de caracteres especiais necessários na senha	0	0-64
passwd-expiry-time	Tempo de expiração da senha (em dias)	Ilimitado, o que significa que as senhas nunca expiram	0-ilimitado 0 expiram agora

Atributo	Descrição	Padrão	Alcance
require-initial-passwd-update	Requer atualização inicial de senha no primeiro login	Desativado	Ativado/desativado Alterações permitidas através de console ou SSH
max-failed-login-attempts	Número máximo de tentativas falhadas	0, não bloqueie a conta	-
lockout-duration	Período máximo de bloqueio (em dias)	O padrão é 0, o que significa que a conta está bloqueada por um dia	-
disallowed-reuse	Não permitir as últimas palavras-passe N.	6	O mínimo é 6
change-delay	Atraso entre alterações de senha (em dias)	0	-
delay-after-failed-login	Atraso após cada tentativa de início de sessão falhada (em segundos)	4	-
passwd-min-lowercase-chars	Número mínimo de caracteres alfabéticos minúsculos necessário na senha	0, que não requer caracteres minúsculos	0-64
passwd-min-uppercase-chars	Número mínimo de caracteres alfabéticos maiúsculos necessário	0, que não requer caracteres maiúsculos	0-64
passwd-min-digits	Número mínimo de dígitos necessário na senha	0, que não requer dígitos	0-64
passwd-expiry-warn-time	Apresentar mensagem de aviso antes da expiração da palavra-passe (em dias)	Ilimitado, o que significa nunca avisar sobre a expiração da senha	0, o que significa avisar o usuário sobre a expiração da senha após cada login bem-sucedido
account-expiry-time	A conta expira em N dias	Ilimitado, o que significa que as contas nunca expiram	O tempo de expiração da conta deve ser maior que o limite inativo da conta
account-inactive-limit	Duração máxima de inatividade antes da expiração da conta (em dias)	Ilimitado, o que significa que as contas inativas nunca expiram	O limite inativo da conta deve ser inferior ao tempo de expiração da conta

Exemplo

```
cluster1::*> security login role config show -vserver cluster1 -role admin

Vserver: cluster1
Role Name: admin
Minimum Username Length Required: 3
Username Alpha-Numeric: disabled
Minimum Password Length Required: 8
Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
Password Expires In (Days): unlimited
Require Initial Password Update on First Login: disabled
Maximum Number of Failed Attempts: 0
Maximum Lockout Period (Days): 0
Disallow Last 'N' Passwords: 6
Delay Between Password Changes (Days): 0
Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

Métodos de administração do sistema

Estes são parâmetros importantes para fortalecer a administração do sistema ONTAP.

Acesso à linha de comando

Estabelecer acesso seguro aos sistemas é uma parte essencial da manutenção de uma solução segura. As opções de acesso de linha de comando mais comuns são SSH, Telnet e RSH. Destes, o SSH é a melhor prática mais segura e padrão do setor para acesso remoto à linha de comando. A NetApp recomenda fortemente o uso de SSH para acesso de linha de comando à solução ONTAP.

Configurações do SSH

O `security ssh show` comando mostra as configurações dos algoritmos de troca de chaves SSH, cifras e algoritmos MAC para o cluster e SVMs. O método de troca de chaves usa esses algoritmos e cifras para especificar como as chaves de sessão únicas são geradas para criptografia e autenticação e como a autenticação do servidor ocorre.

```
cluster1::> security ssh show
```

Vserver	Ciphers	Key Exchange Algorithms	MAC Algorithms
-----	-----	-----	-----
nsadhanaccluster-2			
	aes256-ctr,	diffie-helman-group-	hmac-sha2-256
	aes192-ctr,	exchange-sha256,	hmac-sha2-512
	aes128-ctr	ecdh-sha2-nistp384	
vs0	aes128-gcm	curve25519-sha256	hmac-sha1
vs1	aes256-ctr,	diffie-hellman-group-	hmac-sha1-96
	aes192-ctr,	exchange-sha256	hmac-sha2-256
	aes128-ctr,	ecdh-sha2-nistp384	hmac-sha2-256-
	3des-cbc,	ecdh-sha2-nistp512	etm
	aes128-gcm		hmac-sha2-512
3 entries were displayed.			

Banners de login

Os banners de login permitem que uma organização apresente quaisquer operadores, administradores e até mesmo errantes com termos e condições de uso aceitável, e eles indicam quem é permitido o acesso ao sistema. Esta abordagem é útil para estabelecer expectativa de acesso e uso do sistema. O `security login banner modify` comando modifica o banner de login. O banner de login é exibido imediatamente antes da etapa de autenticação durante o processo de login do dispositivo SSH e console. O texto do banner deve estar em aspas duplas (" "), como mostrado no exemplo a seguir.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

Parâmetros de banner de login

Parâmetro	Descrição
vserver	Use este parâmetro para especificar o SVM com o banner modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster. A mensagem no nível do cluster é usada como padrão para SVMs de dados que não têm uma mensagem definida.

Parâmetro	Descrição
message	Este parâmetro opcional pode ser usado para especificar uma mensagem de banner de login. Se o cluster tiver um conjunto de mensagens de banner de login, o banner de login do cluster também será usado por todos os SVMs de dados. A configuração de um banner de login do SVM substitui a exibição do banner de login do cluster. Para redefinir um banner de login SVM de dados para usar o banner de login do cluster, use este parâmetro com o valor "-". Se você usar esse parâmetro, o banner de login não poderá conter novas linhas (também conhecidas como extremidades de linhas [EOLS] ou quebras de linha). Para inserir uma mensagem de banner de login com novas linhas, não especifique nenhum parâmetro. Você é solicitado a inserir a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas. Carateres não ASCII devem usar Unicode UTF-8.
uri	`(ftp
http):(hostname	IPv4`
	Use este parâmetro para especificar o URI a partir do qual o banner de login é baixado. A mensagem não deve exceder 2048 bytes de comprimento. Carateres não ASCII devem ser fornecidos como Unicode UTF-8.

Mensagem do dia

O `security login motd modify` comando atualiza a mensagem do dia (MOTD).

Existem duas categorias de MOTD: O MOTD em nível de cluster e os dados SVM-nível MOTD. Um usuário que faz login no clustershell de um SVM de dados pode ver duas mensagens: O MOTD de nível de cluster seguido pelo MOTD de nível SVM para esse SVM.

O administrador do cluster pode ativar ou desativar o MOTD no nível do cluster em cada SVM individualmente, se necessário. Se o administrador do cluster desativar o MOTD no nível do cluster para um SVM, um usuário que faz login no SVM não verá a mensagem no nível do cluster. Apenas um administrador de cluster pode ativar ou desativar a mensagem de nível de cluster.

Parâmetro MOTD	Descrição
SVM	Use este parâmetro para especificar o SVM para o qual o MOTD é modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster.

Parâmetro MOTD	Descrição
mensagem	Este parâmetro opcional pode ser usado para especificar uma mensagem. Se você usar este parâmetro, o MOTD não pode conter novas linhas. Se você não especificar nenhum parâmetro além do <code>-vserver</code> parâmetro, será solicitado que você insira a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas. Carateres não ASCII devem ser fornecidos como Unicode UTF-8. A mensagem pode conter conteúdo gerado dinamicamente usando as seguintes sequências de escape: • <code>\</code> - Um único caráter de reação • <code>\b</code> - Sem saída (suportado apenas para compatibilidade com Linux) • <code>\C</code> - Nome do cluster • <code>\d</code> - Data atual como definido no nó de login • <code>\t</code> - Hora atual como definido no nó de login • <code>\I</code> - Endereço IP de LIF de entrada (imprime console para um <code>console login</code>) • <code>\l</code> - Nome do dispositivo de login (imprime console para um <code>console login</code>) • <code>\L</code> - Último login para o usuário em qualquer nó no cluster • <code>\m</code> - Arquitetura da máquina • <code>\n</code> - Nome do nó ou data SVM • <code>\N</code> - Nome do usuário que faz login • <code>\o</code> - O mesmo que <code>o</code>. Fornecido para compatibilidade com Linux. • <code>\O</code> - Nome de domínio DNS do nó. Observe que a saída depende da configuração da rede e pode estar vazia. • <code>\r</code> - Número de versão do software • <code>\s</code> - Nome do sistema operacional • <code>\u</code> - Número de sessões ativas de clustershell no nó local. Para o administrador do cluster: Todos os usuários do clustershell. Para os dados SVM admin: Apenas sessões ativas para esses dados SVM. • <code>\U</code> - Igual a <code>\u</code>, mas tem <code>user</code> ou <code>users</code> anexa • <code>\v</code> - String de versão de cluster eficaz • <code>\W</code> - Sessões ativas em todo o cluster para o usuário que faz (<code>`who`login</code>)

Para obter mais informações sobre como configurar a mensagem do dia no ONTAP, consulte ["Documentação do ONTAP na mensagem do dia"](#).

Tempo limite da sessão da CLI

O tempo limite padrão da sessão da CLI é de 30 minutos. O tempo limite é importante para evitar sessões obsoletas e piggybacking da sessão.

Use o `system timeout show` comando para exibir o tempo limite atual da sessão da CLI. Para definir o

valor de tempo limite, use o `system timeout modify -timeout <minutes>` comando.

Acesso à Web com o Gerenciador do sistema NetApp ONTAP

Se um administrador do ONTAP preferir usar uma interface gráfica em vez da CLI para acessar e gerenciar um cluster, use o Gerenciador do sistema do NetApp ONTAP. Ele é incluído com o ONTAP como um serviço da Web, habilitado por padrão e acessível usando um navegador. Aponte o navegador para o nome do host se estiver usando DNS ou o endereço IPv4 ou IPv6 através de `https://cluster-management-LIF` do .

Se o cluster usar um certificado digital autoassinado, o navegador pode exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) no cluster para autenticação do servidor.

A partir do ONTAP 9.3, a autenticação SAML (Security Assertion Markup Language) é uma opção para o Gerenciador de sistemas do ONTAP.

Autenticação SAML para o Gerenciador de sistemas do ONTAP

O SAML 2.0 é um padrão amplamente adotado do setor que permite que qualquer provedor de identidade (IDP) compatível com SAML de terceiros execute MFA usando mecanismos exclusivos para o IDP escolhido pela empresa e como fonte de logon único (SSO).

Há três funções definidas na especificação SAML: O principal, o IDP e o provedor de serviços. Na implementação do ONTAP, um dos principais é o administrador de cluster que obtém acesso ao ONTAP por meio do Gerenciador de sistemas do ONTAP ou do NetApp Active IQ Unified Manager. O IDP é um software IDP de terceiros. A partir do ONTAP 9.3, os Serviços Federados do Microsoft Active Directory (ADFS) e o IDP Shibboleth de código aberto são IDPs suportados. A partir do ONTAP 9.12.1, o Cisco DUO é um IDP suportado. O fornecedor de serviços é a funcionalidade SAML incorporada ao ONTAP usada pelo Gerenciador de sistemas do ONTAP ou pela aplicação Web do Active IQ Unified Manager.

Ao contrário do processo de configuração de dois fatores SSH, depois que a autenticação SAML é ativada, o ONTAP System Manager ou o ONTAP Service Processor Access requer que todos os administradores existentes se autenticuem através do IDP SAML. Não são necessárias alterações nas contas de utilizador do cluster. Quando a autenticação SAML está ativada, um novo método de autenticação de `saml` é adicionado aos usuários existentes com funções de administrador para `http` aplicativos e `ontapi` .

Depois que a autenticação SAML estiver ativada, novas contas adicionais que exigem acesso SAML IDP devem ser definidas no ONTAP com a função de administrador e o método de autenticação `saml` para `http` aplicativos e `ontapi`. Se a autenticação SAML estiver desativada em algum momento, essas novas contas exigirão que o `password` método de autenticação seja definido com a função de administrador `http` e `ontapi` os aplicativos e a adição `console` do aplicativo para autenticação ONTAP local ao Gerenciador do sistema do ONTAP.

Depois que o IDP SAML é ativado, o IDP executa a autenticação para o acesso do Gerenciador de sistema do ONTAP usando métodos disponíveis para o IDP, como LDAP (Lightweight Directory Access Protocol), AD (Active Directory), Kerberos, senha e assim por diante. Os métodos disponíveis são exclusivos do IDP. É importante que as contas configuradas no ONTAP tenham IDs de usuário mapeadas para os métodos de autenticação IDP.

Os IDPs que foram validados pelo NetApp são Microsoft ADFS, Cisco DUO e IDP de código aberto Shibboleth.

A partir do ONTAP 9.14.1, o Cisco DUO pode ser usado como um segundo fator de autenticação para SSH.

Para obter mais informações sobre MFA para ONTAP System Manager, Active IQ Unified Manager e SSH,

consulte ["TR-4647: Autenticação multifator no ONTAP 9"](#).

Insights do Gerenciador de sistemas da ONTAP

A partir do ONTAP 9.11.1, o Gerenciador de sistemas do ONTAP fornece insights para ajudar os administradores de cluster a otimizar suas tarefas diárias. Os insights de segurança são baseados nas recomendações deste relatório técnico.

Insight de segurança	Determinação
O Telnet está ativado	A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro.
O Remote Shell (RSH) está ativado	O NetApp recomenda SSH para acesso remoto seguro.
O AutoSupport está usando um protocolo inseguro	O AutoSupport não está configurado para ser enviado por xref.:/ontap-security-hardening/HTTPS.
O banner de login não está configurado no cluster ao nível do cluster	Aviso se o banner de login não estiver configurado para o cluster.
O SSH está usando cifras inseguras	Aviso se o SSH usa cifras inseguras.
Poucos servidores NTP estão configurados	Aviso se o número de servidores NTP configurados for inferior a três.
Usuário de administrador padrão não bloqueado	Quando não estiver usando nenhuma conta administrativa padrão (admin ou diag) para fazer login no System Manager e essas contas não estiverem bloqueadas, a recomendação é bloqueá-las.
Defesa contra ransomware: Os volumes não têm políticas de Snapshot	Nenhuma política de snapshot adequada é anexada a um ou mais volumes.
Defesa de ransomware: Desative a exclusão automática do Snapshot	A eliminação automática de instantâneos está definida para um ou mais volumes.
Os volumes não estão sendo monitorados para ataques de ransomware	A proteção autônoma contra ransomware é compatível com vários volumes, mas ainda não está configurada.
Os SVMs não estão configurados para proteção autônoma contra ransomware	A proteção autônoma contra ransomware é compatível com vários SVMs, mas ainda não está configurada.
FPolicy nativo não está configurado	O FPolicy não está definido para SVMs nas.
Ative o modo ativo de proteção autônoma contra ransomware	Vários volumes concluíram o modo de aprendizagem e você pode ativar o modo ativo
A conformidade com o FIPS 140-2 global está desativada	A conformidade com o FIPS 140-2 global não está ativada.
O cluster não está configurado para notificações	E-mails, webhooks ou traphosts SNMP não estão configurados para receber notificações.

Para obter mais informações sobre os insights do Gerenciador de sistemas do ONTAP, consulte ["Documentação do ONTAP System Manager Insights"](#).

Tempo limite da sessão do System Manager

Pode alterar o tempo limite de inatividade da sessão do Gestor do sistema. O tempo limite de inatividade padrão é de 30 minutos. Um tempo limite é importante para evitar sessões obsoletas e piggybacking da

sessão.



Se SAML estiver configurado, o tempo limite de inatividade será controlado pelas configurações no IDP.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Configurações da IU**,  selecione .
3. Na caixa **tempo limite de inatividade**, digite um valor de minutos entre 2 e 180 ou digite "0" para desativar o tempo limite.
4. Selecione **Guardar**.

Proteção autônoma contra ransomware da ONTAP

Para complementar a análise de comportamento do usuário para segurança de workloads de storage, a proteção autônoma contra ransomware do ONTAP analisa cargas de trabalho de volume e entropia para detectar ransomware, captura um snapshot e notifica o administrador quando um ataque é suspeito.

Além da detecção e prevenção de ransomware usando análise comportamental de usuário (UBA) externa do FPolicy com o NetApp Data Infrastructure Insights Storage Workload Security e o ecossistema de parceiros do NetApp FPolicy, o ONTAP 9.10.1 apresenta proteção autônoma contra ransomware. A proteção autônoma contra ransomware do ONTAP usa um recurso integrado de aprendizado de máquina (ML) que analisa a atividade da carga de trabalho em volume, além da entropia de dados, para detectar ransomware automaticamente. Ele monitora atividades diferentes do UBA para poder detectar ataques que o UBA não detecta.

Para obter informações mais detalhadas sobre essa capacidade, ["Soluções da NetApp para ransomware"](#) consulte ou ["Documentação autônoma de proteção de ransomware da ONTAP"](#).

Auditoria de sistema administrativo de storage

Garanta a integridade da auditoria de eventos transferindo eventos do ONTAP para um servidor syslog remoto. Esse servidor pode ser um sistema de gerenciamento de eventos de informações de segurança, como Splunk.

Envie syslog

As informações de log e auditoria são inestimáveis para uma organização do ponto de vista de suporte e disponibilidade. Além disso, as informações e detalhes contidos em logs (syslog) e relatórios de auditoria e saídas são geralmente de natureza sensível. Para manter a postura e os controles de segurança, é imperativo que as organizações gerenciem dados de log e auditoria de maneira segura.

O descarregamento de informações do syslog é necessário para limitar o escopo ou a pegada de uma violação a um único sistema ou solução. Portanto, a NetApp recomenda descarregar com segurança as informações do syslog para um local seguro de armazenamento ou retenção.

Crie um destino de encaminhamento de registros

Use o `cluster log-forwarding create` comando para criar destinos de encaminhamento de log para o

log remoto.

Parâmetros

Use os seguintes parâmetros para configurar o `cluster log-forwarding create` comando:

- *** Anfitrião de destino.*** Esse nome é o nome do host ou o endereço IPv4 ou IPv6 do servidor para o qual encaminhar os logs.

```
-destination <Remote InetAddress>
```

- **Porto de destino.** Esta é a porta na qual o servidor de destino escuta.

```
[-port <integer>]
```

- **Protocolo de encaminhamento de registros.** Este protocolo é utilizado para enviar mensagens para o destino.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted\}]
```

O protocolo de encaminhamento de registros pode utilizar um dos seguintes valores:

- `udp-unencrypted`. User Datagram Protocol sem segurança.
 - `tcp-unencrypted`. TCP sem segurança.
 - `tcp-encrypted`. TCP com Transport Layer Security (TLS).
- **Verifique a identidade do servidor de destino.** Quando esse parâmetro é definido como verdadeiro, a identidade do destino de encaminhamento de log é verificada validando seu certificado. O valor só pode ser definido como verdadeiro quando o `tcpencrypted` valor é selecionado no campo protocolo.

```
[-verify-server \{true|false\}]
```

- *** Syslog facilidade.*** Esse valor é o recurso syslog a ser usado para os logs encaminhados.

```
[-facility <Syslog Facility>]
```

- **Ignorar o teste de conectividade.** Normalmente, o `cluster log-forwarding create` comando verifica se o destino está acessível enviando um ping ICMP (Internet Control Message Protocol) e falha se não estiver acessível. Definir este valor para `true` ignorar a verificação de ping para que você possa configurar o destino quando ele não estiver acessível.

```
[-force [true]]
```



O NetApp recomenda usar o `cluster log-forwarding` comando para forçar a conexão a um `-tcp-encrypted` tipo.

Notificação de evento

Proteger as informações e os dados que saem de um sistema é vital para manter e gerenciar a postura de segurança do sistema. Os eventos gerados pela solução ONTAP fornecem uma riqueza de informações sobre o que a solução está encontrando, as informações processadas e muito mais. A vitalidade desses dados destaca a necessidade de gerenciá-los e migrá-los de forma segura.

O `event notification create` comando envia uma nova notificação de um conjunto de eventos definido por um filtro de eventos para um ou mais destinos de notificação. Os exemplos a seguir descrevem a configuração de notificação de eventos e o `event notification show` comando, que exibe os filtros e destinos de notificação de eventos configurados.

```
cluster1::> event notification create -filter-name filter1 -destinations
email_dest,syslog_dest,snmp-traphost
```

```
cluster1::> event notification show
```

ID	Filter Name	Destinations
----	-----	-----
1	filter1	email_dest, syslog_dest, snmp-traphost

Criptografia de storage no ONTAP

Para proteger dados confidenciais em caso de um disco que seja roubado, devolvido ou reutilizado, use a criptografia de storage NetApp baseada em hardware ou a criptografia de volume NetApp/NetApp agregada baseada em software. Ambos os mecanismos são validados pelo FIPS-140-2 e, ao usar mecanismos baseados em hardware com mecanismos baseados em software, a solução se qualifica para o Programa soluções comerciais para classificados (CSfC). Ele permite maior proteção de segurança para dados secretos e secretos em repouso nas camadas de hardware e software.

A criptografia de dados em repouso é importante para proteger dados confidenciais em caso de um disco que seja roubado, retornado ou reutilizado.

A ONTAP 9 tem três soluções de criptografia de dados em repouso compatíveis com FIPS (Federal Information Processing Standard) 140-2:

- O NetApp Storage Encryption (NSE) é uma solução de hardware que usa unidades com autcriptografia.
- O NetApp volume Encryption (NVE) é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele esteja habilitado com uma chave exclusiva para cada volume.
- O NetApp Aggregate Encryption (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.

O NSE, NVE e NAE podem usar o gerenciamento de chaves externas ou o OKM (Onboard Key Manager). O

uso de NSE, NVE e NAE não afeta os recursos de eficiência de storage da ONTAP. No entanto, os volumes NVE são excluídos da deduplicação agregada. Os volumes NAE participam e se beneficiam da deduplicação agregada.

O OKM fornece uma solução de criptografia autônoma para dados em repouso com NSE, NVE ou NAE.

NVE, NAE e OKM usam o ONTAP CryptoMod. O CryptoMod está listado na lista de módulos validados do CMVP FIPS 140-2. "[FIPS 140-2 Cert no. 4144](#)" Consulte .

Para iniciar a configuração OKM, use o `security key-manager onboard enable` comando. Para configurar gerenciadores de chaves KMIP (Key Management Interoperability Protocol) externos, use o `security key-manager external enable` comando. A partir do ONTAP 9.6, a alocação a vários clientes é suportada para gerentes de chaves externos. Use o `-vserver <vserver name>` parâmetro para habilitar o gerenciamento de chaves externas para uma SVM específica. Antes de 9,6, o `security key-manager setup` comando foi usado para configurar os gerenciadores OKM e de chaves externas. Para o gerenciamento de chaves integradas, essa configuração orienta o operador ou o administrador pela configuração da senha e parâmetros adicionais para configurar o OKM.

Uma parte da configuração é fornecida no exemplo a seguir:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

A partir do ONTAP 9.4, você pode usar a `-enable-cc-mode` opção `True` com `security key-manager setup` para exigir que os usuários inseram a senha após uma reinicialização. Para o ONTAP 9.6 e posterior, a

sintaxe de comando é `security key-manager onboard enable -cc-mode-enabled yes`.

A partir do ONTAP 9.4, você pode usar o `secure-purge` recurso com privilégios avançados para "esfregar" dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física. O seguinte comando limpa com segurança os arquivos excluídos no vol1 no SVM VS1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

A partir do ONTAP 9.7, NAE e NVE são ativados por padrão se a licença VE estiver em vigor, os gerenciadores de chaves externos ou OKM são configurados e NSE não é usado. Os volumes NAE são criados por padrão em agregados NAE e os volumes NVE são criados por padrão em agregados não-naE. Você pode substituir isso digitando o seguinte comando:

```
cluster1::*> options -option-name  
encryption.data_at_rest_encryption.disable_by_default true
```

A partir do ONTAP 9.6, você pode usar um escopo SVM para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para servir dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário. Para obter mais informações, consulte ["Habilite o gerenciamento de chaves externas no ONTAP 9.6 e posterior"](#) a documentação do ONTAP.

A partir do ONTAP 9.11.1, é possível configurar a conectividade a servidores de gerenciamento de chaves externas em cluster, designando servidores de chaves primárias e secundárias em um SVM. Para obter mais informações, consulte ["configurar servidores de chaves externas em cluster"](#) a documentação do ONTAP.

A partir do ONTAP 9.13.1, você pode configurar servidores de gerenciador de chaves externos no gerenciador de sistema. Para obter mais informações, consulte ["Gerenciar gerenciadores de chaves externos"](#) a documentação do ONTAP.

Criptografia de replicação de dados

Para complementar a criptografia de dados em repouso, você pode criptografar o tráfego de replicação de dados ONTAP entre clusters usando TLS com uma chave pré-compartilhada para SnapMirror, SnapVault ou FlexCache.

Ao replicar dados para recuperação de desastre, armazenamento em cache ou backup, você precisa proteger esses dados durante o transporte por cabo de um cluster ONTAP para outro. Isso evita ataques intermediários maliciosos contra dados confidenciais quando eles estão em trânsito.

A partir do ONTAP 9.6, a criptografia de peer de cluster fornece suporte à criptografia TLS 1.2 AES-256 GCM para recursos de replicação de dados do ONTAP, como SnapMirror, SnapVault e FlexCache. A criptografia é configurada por meio de uma chave pré-compartilhada (PSK) entre dois peers de cluster.

A partir do ONTAP 9.15.1, a criptografia de peer de cluster fornece suporte à criptografia TLS 1.3 AES-256 GCM para recursos de replicação de dados do ONTAP, como SnapMirror, SnapVault e FlexCache. A criptografia é configurada por meio de uma chave pré-compartilhada (PSK) entre dois peers de cluster.

Os clientes que utilizam tecnologias como NSE, NVE e NAE para proteger dados em repouso também podem usar criptografia de dados completamente atualizando para o ONTAP 9.6 ou posterior para usar peer de cluster criptografado.

O peer de cluster criptografa todos os dados entre os peers de cluster. Por exemplo, ao usar o SnapMirror, todas as informações de peering, bem como todos os relacionamentos SnapMirror entre o peer de cluster de origem e o cluster de destino, são criptografados. Você não pode enviar dados em texto não criptografado entre peers de cluster com a criptografia de peering de cluster ativada.

A partir do ONTAP 9.6, novos relacionamentos de peer de cluster têm criptografia habilitada por padrão. Para habilitar a criptografia em peer de cluster que foram criados antes do ONTAP 9.6, você deve atualizar o cluster de origem e o cluster de destino para a versão 9.6. Além disso, você deve usar o `cluster peer modify` comando para alterar tanto os peers de cluster de origem quanto de destino para usar a criptografia de peering de cluster.

Você pode converter um relacionamento de peer de cluster existente para usar criptografia de peer de cluster no ONTAP 9.6, conforme mostrado no exemplo a seguir:

On the destination cluster peer:

```
cluster2::> cluster peer modify cluster1 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter a passphrase.

On the source cluster peer:

```
cluster1::> cluster peer modify cluster2 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter the same passphrase you created in the previous step.

Criptografia de dados em trânsito IPsec

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec. O IPsec fornece uma alternativa à criptografia NFS ou SMB/CIFS e é a única opção de criptografia em voo para tráfego iSCSI.

Em algumas situações, pode haver um requisito para proteger todos os dados do cliente transportados por cabo (ou em trânsito) para o SVM do ONTAP. Isso impede a repetição e ataques maliciosos contra dados confidenciais em trânsito.

A partir do ONTAP 9.8, a Segurança de Protocolo de Internet (IPsec) oferece suporte de criptografia de ponta a ponta para todo o tráfego IP entre um cliente e um SVM do ONTAP. A criptografia de dados IPsec para todo o tráfego IP inclui protocolos NFS, iSCSI e SMB/CIFS. O IPsec fornece a única opção de criptografia em voo

para tráfego iSCSI.

Fornecer criptografia NFS por cabo é um dos principais casos de uso do IPsec. Antes do ONTAP 9,8, a criptografia por cabo NFS exigiu a configuração e configuração do Kerberos para usar o krb5p para criptografar dados NFS em trânsito. Isso nem sempre é simples ou fácil de realizar em todos os ambientes do cliente.

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec.

IPsec é um padrão IETF. O ONTAP usa IPsec no modo de transporte. Ele também aproveita o protocolo IKE (Internet Key Exchange) versão 2, que usa uma chave pré-compartilhada (PSK) para negociar material chave entre o cliente e o ONTAP com IPv4 ou IPv6. Por padrão, o IPsec usa criptografia de 256 bits AES-GCM do Suite-B. Suite-B AES-GMAC256 e AES-CBC256 com encriptação de 256 bits também são suportados.

Embora o recurso IPsec deva estar habilitado no cluster, ele se aplica a endereços IP SVM individuais por meio do uso de uma entrada SPD (Security Policy Database). A entrada SPD (diretiva) contém o endereço IP do cliente (sub-rede IP remota), o endereço IP SVM (sub-rede IP local), o conjunto de codificação de criptografia a ser usado e o segredo pré-compartilhado (PSK) necessário para autenticar via IKEv2 e estabelecer a conexão IPsec. Além da entrada de diretiva IPsec, o cliente deve ser configurado com as mesmas informações (IP local e remoto, PSK e conjunto de codificação) antes que o tráfego possa fluir pela conexão IPsec. A partir do ONTAP 9.10,1, o suporte à autenticação de certificado IPsec é adicionado. Isso remove os limites de diretiva IPsec e habilita o suporte do sistema operacional Windows para IPsec.

Se houver um firewall entre o cliente e o endereço IP SVM, ele deverá permitir que os protocolos ESP e UDP (portas 500 e 4500), tanto de entrada (entrada) quanto de saída (saída), para que a negociação IKEv2 seja bem-sucedida e, assim, permita o tráfego IPsec.

Para criptografia de tráfego de peering de cluster e NetApp SnapMirror, a criptografia de peering de cluster (CPE) ainda é recomendada por IPsec para garantir o trânsito seguro por cabo. O CPE tem melhor desempenho para essas cargas de trabalho do que o IPsec. Você não precisa de uma licença para IPsec e não há restrições de importação ou exportação.

Você pode ativar o IPsec no cluster e criar uma entrada SPD para um único cliente e um único endereço IP SVM, conforme mostrado no exemplo a seguir:

On the Destination Cluster Peer

```
cluster1::> security ipsec config modify -is-enabled true
```

```
cluster1::> security ipsec policy create -vserver vs1 -name test34 -local  
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
```

When prompted enter and confirm the pre shared secret (PSK).

Informações relacionadas

["Prepare-se para usar a segurança IP na rede ONTAP"](#)

Modo FIPS e gerenciamento TLS e SSL no ONTAP

O padrão FIPS 140-2 especifica requisitos de segurança para módulos criptográficos dentro de sistemas de segurança que protegem informações confidenciais em sistemas de computador e telecomunicações. O padrão FIPS 140-2 aplica-se *especificamente* ao módulo criptográfico, em vez do produto, arquitetura, dados ou ecossistema. O módulo criptográfico é o componente específico (hardware, software, firmware ou uma combinação dos três) que implementa funções de segurança aprovadas pelo NIST.

A ativação da conformidade com o FIPS 140-2 tem efeitos em outros sistemas e comunicações internas e externas ao ONTAP 9. A NetApp recomenda fortemente testar essas configurações em um sistema que não seja de produção com acesso ao console.

A partir do suporte a ONTAP 9.11,1 e TLS 1,3, é possível validar o FIPS 140-3.



A configuração FIPS se aplica ao ONTAP e ao Platform BMC.

Configuração do modo FIPS do NetApp ONTAP

O NetApp ONTAP tem uma configuração do modo FIPS que instancia um nível adicional de segurança ao plano de controle:

- A partir do ONTAP 9.11.1, quando o modo de conformidade com o FIPS 140-2 está ativado, os TLSv1, TLSv1,1 e SSLv3 são desativados e apenas os TLSv1,2 e TLSv1,3 permanecem ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
- Para versões do ONTAP anteriores a 9.11.1, quando o modo de conformidade com FIPS 140-2 estiver ativado, tanto o TLSv1 quanto o SSLv3 são desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.
- "[Módulo de segurança criptográfica NetApp \(NCSM\)](#)", Validado pelo FIPS 140-2 nível 1, fornece conformidade com software.



O NIST enviou um padrão FIPS-140-3 e o NCSM terá validações FIPS-140-2 e FIPS-140-3. Todas as validações do FIPS 140-2 serão transferidas para o status histórico em 21 de setembro de 2026, ou seja, cinco anos após o último dia para novos envios de certificados.

Ative o modo de conformidade FIPS-140-2 e FIPS-140-3

A partir do ONTAP 9, é possível habilitar o modo de conformidade FIPS-140-2 e FIPS-140-3 para interfaces do plano de controle em todo o cluster.

- "[Ativar FIPS](#)"
- "[Exibir status FIPS](#)"

Protocolos e capacitação FIPS

O `security config modify` comando permite modificar a configuração de segurança existente em todo o cluster. Se ativar o modo compatível com FIPS, o cluster selecionará automaticamente apenas protocolos TLS.

- Use o `-supported-protocols` parâmetro para incluir ou excluir protocolos TLS independentemente do modo FIPS. Por padrão, o modo FIPS é desativado e os protocolos TLSv1,3 (começando com ONTAP 9.11.1) e TLSv1,2 são ativados.
- As versões anteriores do ONTAP tinham os seguintes protocolos TLS ativados por padrão:
 - TLSv1,1 (desativado por padrão a partir do ONTAP 9.12.1)
 - TLSv1 (desativado por padrão a partir do ONTAP 9,8)
- Para compatibilidade com versões anteriores, o ONTAP suporta a adição de SSLv3 à lista de protocolos compatíveis quando o modo FIPS está desativado.

Capacitação FIPS e cifras

- Utilize o `-supported-cipher-suites` parâmetro para configurar apenas o AES (Advanced Encryption Standard) ou AES e 3DES.
- Você pode desativar cifras fracas, como RC4, especificando `!RC4`. Por padrão, a configuração de codificação suportada é `ALL:!LOW:!aNULL:!EXP:!eNULL`. Essa configuração significa que todos os conjuntos de criptografia suportados para os protocolos estão ativados, exceto aqueles que usam algoritmos de criptografia de 64 bits ou 56 bits sem autenticação, criptografia, sem exportação e pacotes de criptografia de baixa criptografia.
- Selecione um conjunto de codificações que esteja disponível com o protocolo selecionado correspondente. Uma configuração inválida pode fazer com que algumas funcionalidades não funcionem corretamente.
- Para obter a sintaxe correta da cadeia de caracteres de cifra, consulte "[página de cifras](#)" On OpenSSL (publicado pela fundação do software OpenSSL). A partir do ONTAP 9.9,1 e versões posteriores, não é mais necessário reiniciar todos os nós manualmente depois de modificar a configuração de segurança.

Proteção de segurança SSH e TLS

A administração SSH do ONTAP 9 requer um cliente OpenSSH 5,7 ou posterior. Os clientes SSH devem negociar com o algoritmo de chave pública ECDSA (Elliptic Curve Digital Signature Algorithm) para que a conexão seja bem-sucedida.

Para proteger a segurança TLS, ative apenas o TLS 1,2 e use conjuntos de codificação capazes de Perfect Forward Secrecy (PFS). O PFS é um método de troca de chaves que, quando usado em combinação com protocolos de criptografia como o TLS 1,2, ajuda a impedir que um invasor descriptografe todas as sessões de rede entre um cliente e um servidor.

Ative os conjuntos de codificação compatíveis com TLSv1,2 e PFS

Para ativar apenas conjuntos de encriptação compatíveis com TLS 1,2 e PFS, utilize o `security config modify` comando a partir do nível de privilégio avançado.



Antes de alterar a configuração da interface SSL, certifique-se de que o cliente suporta as cifras DHE e ECDHE ao se conectar ao ONTAP para manter a conectividade com o ONTAP.

Exemplo

```
cluster1::*> security config modify -interface SSL -supported-protocols  
TLSv1.2 -supported-cipher-suites  
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirme `y` para cada prompt. Para obter mais informações sobre PFS, consulte este ["NetApp blog"](#).

Informações relacionadas

["Publicação Federal Information Processing Standard \(FIPS\) 140"](#)

Crie um certificado digital assinado pela CA

Para muitas organizações, o certificado digital auto-assinado para o acesso à Web ONTAP não é compatível com suas políticas INFOSEC. Em sistemas de produção, é uma prática recomendada do NetApp instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL.

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da CA.

Passos

1. Para criar um certificado digital assinado pela CA da organização, faça o seguinte:
 - a. Gerar um CSR.
 - b. Siga o procedimento da sua organização para solicitar um certificado digital usando a CSR da CA da sua organização. Por exemplo, usando a interface da Web do Microsoft Active Directory Certificate Services, vá para <CA_server_name>/certsrv e solicite um certificado.
 - c. Instale o certificado digital no ONTAP.

Protocolo de estado do certificado online

O OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS, como LDAP ou TLS, recebam status de certificado digital quando o OCSP está ativado. O aplicativo recebe uma resposta assinada significando que o certificado solicitado é bom, revogado ou desconhecido.

O OCSP permite determinar o status atual de um certificado digital sem exigir listas de revogação de certificados (CRLs).

Por padrão, a verificação do status do certificado OCSP está desativada. Ele pode ser ativado com o comando `security config ocsp enable -app name`, onde o nome do aplicativo pode ser `autosupport`, `audit_log`, `fabricpool`, `ems`, `kmip`, `ldap_ad`, `ldap_nis_namemap`, `all` ou `.` O comando requer nível de privilégio avançado.

Gerenciamento do SSHv2

O `security ssh modify` comando substitui as configurações existentes dos

algoritmos de troca de chaves SSH, cifras ou algoritmos MAC para o cluster ou um SVM com as configurações especificadas.



A NetApp recomenda o seguinte:

- Use senhas para sessões de usuário.
- Use uma chave pública para acesso à máquina.

Cifras suportadas e trocas de chaves

Cifras	Troca de chaves
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-group-Exchange-SHA1 (SHA-1)
aes128-ctr	diffie-hellman-group14-SHA1 (SHA-1)
aes256-cbc	diffie-hellman-group1-SHA1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Criptografia simétrica AES e 3DES suportada

O ONTAP também suporta os seguintes tipos de criptografia simétrica AES e 3DES (também conhecidos como cifras):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm

- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm



A configuração de gerenciamento SSH se aplica ao ONTAP e à plataforma BMC.

NetApp AutoSupport

O recurso AutoSupport do ONTAP permite que você monitore proativamente a integridade do sistema e envie mensagens e detalhes automaticamente para o suporte técnico da NetApp, para a equipe de suporte interna da organização ou para um parceiro de suporte. Por padrão, as mensagens AutoSupport para o suporte técnico do NetApp são ativadas quando o sistema de armazenamento é configurado pela primeira vez. Além disso, o AutoSupport começa a enviar mensagens para o suporte técnico da NetApp 24 horas depois de ativado. Este período de 24 horas é configurável. Para aproveitar a comunicação com a equipe de suporte interno de uma organização, a configuração do host de e-mail deve ser concluída.

Somente o administrador do cluster pode executar o gerenciamento de AutoSupport (configuração). O administrador do SVM não tem acesso ao AutoSupport. O recurso AutoSupport pode ser desativado. No entanto, a NetApp recomenda habilitá-la porque o AutoSupport ajuda a acelerar a identificação e a resolução de problemas caso ocorra algum problema no sistema de storage. Por padrão, o sistema coleta informações do AutoSupport e as armazena localmente, mesmo que você desative o AutoSupport.

Para obter mais detalhes sobre mensagens AutoSupport, incluindo o que está contido nas várias mensagens e onde diferentes tipos de mensagens são enviadas, consulte "[Consultor digital da NetApp](#)"a documentação.

As mensagens do AutoSupport contêm dados confidenciais, incluindo, entre outros, os seguintes itens:

- Ficheiros de registo
- Dados sensíveis ao contexto relativos a subsistemas específicos
- Dados de configuração e status
- Dados de performance

O AutoSupport suporta HTTPS e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.

Além disso, você deve utilizar o `system node autosupport modify` comando para especificar os destinos dos dados do AutoSupport (por exemplo, suporte técnico da NetApp, operações internas de uma organização ou parceiros). Esse comando também permite especificar quais detalhes específicos do AutoSupport enviar (por exemplo, dados de desempenho, arquivos de log, etc.).

Para desativar completamente o AutoSupport, use o `system node autosupport modify -state disable` comando.

Protocolo de hora de rede

Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com pelo menos três servidores NTP externos.

Podem ocorrer problemas quando o tempo do cluster é impreciso. Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com servidores NTP externos.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Você pode associar um máximo de 10 servidores NTP externos usando o `cluster time-service ntp server create` comando. Para redundância e qualidade do serviço de tempo, você deve associar pelo menos três servidores NTP externos ao cluster.

Para obter detalhes sobre a configuração do NTP no ONTAP, "[Gerenciamento do tempo do cluster \(somente administradores de cluster\)](#)" consulte .

Contas locais do sistema de arquivos nas (grupo de trabalho CIFS)

A autenticação de cliente de grupo de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Use o `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

A partir do ONTAP 9, você pode configurar um servidor CIFS em um grupo de trabalho com clientes CIFS que se autenticam no servidor usando usuários e grupos definidos localmente. A autenticação de cliente de grupo de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Para configurar o servidor CIFS, use o `vserver cifs create` comando. Depois que o servidor CIFS é criado, você pode associá-lo a um domínio CIFS ou associá-lo a um grupo de trabalho. Para ingressar em um grupo de trabalho, use o `-workgroup` parâmetro. Aqui está um exemplo de configuração:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSEVER1  
-workgroup Sales
```



Um servidor CIFS no modo de grupo de trabalho suporta apenas a autenticação do Windows NT LAN Manager (NTLM) e não suporta autenticação Kerberos.

A NetApp recomenda a utilização da função de autenticação NTLM com grupos de trabalho CIFS para manter a postura de segurança da sua organização. Para validar a postura de segurança do CIFS, o NetApp recomenda o uso do `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações de IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

Auditoria do sistema de arquivos nas

Os sistemas de arquivos nas ocupam um espaço maior no cenário de ameaças atuais.

As funções de auditoria são essenciais para oferecer suporte à visibilidade.

A segurança exige validação. ONTAP oferece mais eventos e detalhes de auditoria em toda a solução. Como os sistemas de arquivos NAS ocupam um espaço cada vez maior no cenário de ameaças atual, as funções de auditoria são essenciais para garantir visibilidade. Devido à capacidade de auditoria aprimorada no ONTAP, os detalhes de auditoria do CIFS são mais abundantes do que nunca. Detalhes importantes, incluindo os seguintes, são registrados com os eventos criados:

- Acesso a arquivos, pastas e compartilhamentos
- Arquivos criados, modificados ou excluídos
- Acesso de leitura de ficheiros bem-sucedido
- Tentativas falhadas de ler ou gravar ficheiros
- Alterações de permissão de pasta

Crie uma configuração de auditoria

É necessário habilitar a auditoria CIFS para gerar eventos de auditoria. Use o `vserver audit create` comando para criar uma configuração de auditoria. Por padrão, o log de auditoria usa um método de rotação baseado no tamanho. Você pode usar uma opção de rotação baseada no tempo, se especificado no campo Rotation Parameters (parâmetros de rotação). Os detalhes adicionais da configuração de rotação de auditoria de log incluem o cronograma de rotação, os limites de rotação, os dias de rotação da semana e o tamanho da rotação. O texto a seguir fornece um exemplo de configuração que descreve uma configuração de auditoria usando uma rotação mensal baseada em tempo agendada para todos os dias da semana às 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Eventos de auditoria CIFS

Os eventos de auditoria CIFS são os seguintes:

- **Compartilhamento de arquivos:** Gera um evento de auditoria quando um compartilhamento de rede CIFS é adicionado, modificado ou excluído usando os comandos relacionados `vserver cifs share`.
- **Alteração da política de auditoria:** Gera um evento de auditoria quando a política de auditoria é desativada, ativada ou modificada usando os comandos relacionados `vserver audit`.
- **Conta de usuário:** Gera um evento de auditoria quando um usuário local CIFS ou UNIX é criado ou excluído; uma conta de usuário local é ativada, desativada ou modificada; ou uma senha é redefinida ou alterada. Este evento usa o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-user`.
- **Security group:** Gera um evento de auditoria quando um grupo de segurança local CIFS ou UNIX é criado ou excluído usando o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-group`.
- **Alteração da política de autorização:** Gera um evento de auditoria quando os direitos são concedidos ou revogados para um usuário CIFS ou um grupo CIFS usando o `vserver cifs users-and-groups privilege` comando.



Esta funcionalidade é baseada na função de auditoria do sistema, que permite que um administrador analise o que o sistema está permitindo e executando a partir da perspectiva de um usuário de dados.

Efeito de APIS REST na auditoria nas

O ONTAP inclui a capacidade de contas de administrador acessarem e manipularem arquivos SMB/CIFS ou NFS usando APIs REST. Embora as APIs REST só possam ser executadas por administradores do ONTAP, os comandos da API REST ignoram o log de auditoria nas do sistema. Além disso, as permissões de arquivo também podem ser ignoradas pelos administradores do ONTAP ao usar APIs REST. No entanto, as ações do administrador com APIs REST em arquivos são capturadas no log do histórico de comandos do sistema.

Criar função de API REST sem acesso

É possível impedir que os administradores do ONTAP usem APIs REST para acesso a arquivos ao criar uma função de API REST que não tenha acesso a volumes do ONTAP por meio DE REST. Para provisionar essa função, execute as etapas a seguir.



A API REST `/api/storage/volumes` é usada para mais do que apenas acesso a arquivos. Ela é usada pelo System Manager e outras interfaces gráficas para criar, visualizar e modificar volumes.

Passos

1. Crie uma nova função REST que não tenha acesso a volumes de storage, além de ter todos os outros acessos à API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Atribua a conta de administrador à nova função API REST que você criou na etapa anterior.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```



Se você quiser impedir que a conta de administrador de cluster do ONTAP integrada use APIs REST para acesso a arquivos, primeiro será necessário ["crie uma nova conta de administrador e desative ou exclua a conta interna"](#).

Configure e ative a assinatura e a vedação CIFS SMB

Você pode configurar e ativar a assinatura SMB que protege a segurança do Data Fabric. Isso garante que o tráfego entre sistemas de storage e clientes não seja comprometido com replay ou ataques man-in-the-middle. A assinatura SMB protege verificando se as mensagens SMB têm assinaturas válidas.

Sobre esta tarefa

Um vetor de ameaça comum para sistemas de arquivos e arquiteturas está no protocolo SMB. Para lidar com esse vetor, a solução ONTAP 9 usa assinatura e vedação padrão do setor SMB. A assinatura de SMB protege a segurança do Data Fabric ao garantir que o tráfego entre sistemas de storage e clientes não seja comprometido com replays ou ataques diretos. Ele faz isso verificando se as mensagens SMB têm assinaturas válidas.

Embora a assinatura SMB esteja desativada por padrão no interesse do desempenho, a NetApp recomenda fortemente que você a ative. Além disso, a solução ONTAP oferece suporte à criptografia SMB, que também é conhecida como vedação. Esta abordagem permite o transporte seguro de dados numa base de partilha por partilha. Por predefinição, a encriptação SMB está desativada. No entanto, a NetApp recomenda que você ative a criptografia SMB.

Agora, a assinatura e a vedação LDAP são suportadas no SMB 2,0 e posterior. A assinatura (proteção contra adulteração) e a vedação (criptografia) permitem a comunicação segura entre SVMs e servidores do ativo Directory. A criptografia AES acelerada (Intel AES NI) agora é suportada no SMB 3,0 e posterior. O Intel AES NI melhora o algoritmo AES e acelera a criptografia de dados com famílias de processadores suportadas.

Passos

1. Para configurar e ativar a assinatura SMB, use o `vserver cifs security modify` comando e verifique se o `-is-signing-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Para configurar e ativar a selagem e a criptografia SMB, use o `vserver cifs security modify` comando e verifique se o `-is-smb-encryption-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----  -----
vs1      true
```

Proteção do NFS

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente para um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente. Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na

ordem em que aparecem na política de exportação.

O controle de acesso é fundamental para manter uma postura segura. Portanto, o ONTAP usa o recurso de política de exportação para limitar o acesso de volume NFS a clientes que correspondem a parâmetros específicos. As políticas de exportação contêm uma ou mais regras de exportação que processam cada solicitação de acesso de cliente. Uma política de exportação está associada a cada volume para configurar o acesso do cliente ao volume. O resultado deste processo determina se o cliente é concedido ou negado (com uma mensagem de permissão negada) o acesso ao volume. Este processo também determina que nível de acesso é fornecido ao volume.



Uma política de exportação com regras de exportação deve existir em um SVM para que os clientes acessem os dados. Um SVM pode conter várias políticas de exportação.

A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

As regras de exportação determinam as permissões de acesso do cliente aplicando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação (por exemplo, NFSv4 ou SMB)
- Um identificador de cliente (por exemplo, nome de host ou endereço IP)
- O tipo de segurança usado pelo cliente para autenticar (por exemplo, Kerberos v5, NTLM ou AUTH_SYS)

Se uma regra especificar vários critérios e o cliente não corresponder a um ou mais deles, a regra não se aplica.

Um exemplo de política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

O tipo de segurança determina o nível de acesso que um cliente recebe. Os três níveis de acesso são somente leitura, leitura-gravação e superusuário (para clientes com ID de usuário 0). Como o nível de acesso determinado pelo tipo de segurança é avaliado nesta ordem, você deve observar as regras listadas:

Regras para parâmetros de nível de acesso em regras de exportação

Para que um cliente obtenha os seguintes níveis de acesso	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente
Apenas de leitura normal do utilizador	Somente leitura (<code>-rorule</code>)
Leitura-escrita normal do utilizador	Somente leitura (<code>-rorule</code>) e leitura-gravação (<code>-rwrule</code>)
Somente leitura do superusuário	Apenas leitura (<code>-rorule</code>) e <code>-superuser</code>

Para que um cliente obtenha os seguintes níveis de acesso	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente
Leitura-gravação do superusuário	Somente leitura (<code>-rorule</code>) e leitura-gravação (<code>-rwrule</code>) e. <code>-superuser</code>

Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- Qualquer
- Nenhum
- Nunca

Esses tipos de segurança não são válidos para uso com o `-superuser` parâmetro:

- krb5
- ntlm
- sistema

Regras para resultados de parâmetros de acesso

Se o tipo de segurança do cliente ...	Então ...
Corresponde a um tipo de segurança especificado no parâmetro de acesso.	O cliente recebe acesso para esse nível com seu próprio ID de usuário.
Não corresponde a um tipo de segurança especificado, mas o parâmetro Access inclui a opção <code>none</code> .	O cliente recebe acesso para esse nível e recebe o usuário anônimo com o ID de usuário especificado pelo <code>-anon</code> parâmetro.
Não corresponde a um tipo de segurança especificado e o parâmetro Access não inclui a opção <code>none</code> .	O cliente não recebe nenhum acesso para esse nível.  Esta restrição não se aplica ao <code>-superuser</code> parâmetro porque este parâmetro sempre inclui nenhum, mesmo quando não especificado.

Kerberos 5 e Krb5p

A partir do ONTAP 9, a autenticação Kerberos 5 com serviço de privacidade (krb5p) é suportada. O modo de autenticação krbp5 é seguro e protege contra adulteração e espionagem de dados usando checksums para criptografar todo o tráfego entre cliente e servidor. A solução ONTAP suporta criptografia AES de 128 bits e 256 bits para Kerberos. O serviço de privacidade inclui verificar a integridade dos dados recebidos, autenticar usuários e criptografar dados antes da transmissão.

A opção krb5p está mais presente no recurso de política de exportação, onde é definida como uma opção de criptografia. O método de autenticação krb5p.1X pode ser usado como um parâmetro de autenticação, como mostrado no exemplo a seguir:

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip  
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3  
-access- type read
```

Ative a assinatura e a vedação do protocolo Lightweight Directory Access

Assinatura e selagem são suportados para habilitar a segurança da sessão em consultas a um servidor LDAP. Essa abordagem fornece uma alternativa à segurança de sessão LDAP-over-TLS.

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. As configurações de segurança de sessão em um SVM correspondem às disponíveis no servidor LDAP. Por padrão, a assinatura e a vedação LDAP são desativadas.

Passos

1. Para ativar esta função, execute o `vserver cifs security modify` comando com o `session-security-for-ad-ldap` parâmetro.

Opções para funções de segurança LDAP:

- **Nenhum:** Padrão, sem assinatura ou vedação
- **Sign:** Assine o tráfego LDAP
- **Seal:** Assine e criptografe o tráfego LDAP



Os parâmetros de sinal e selo são cumulativos, o que significa que, se a opção de sinal for usada, o resultado será LDAP com assinatura. No entanto, se a opção de vedação for usada, o resultado será sinal e selo. Além disso, se um parâmetro não for especificado para esse comando, o padrão será nenhum.

O seguinte é um exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock  
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Crie e use um FPolicy do NetApp

Você pode criar e usar um FPolicy, um componente de infraestrutura da solução ONTAP, que permite que aplicativos parceiros monitorem e definam permissões de acesso a arquivos. Uma das aplicações mais avançadas é a Segurança de workload de storage, uma aplicação SaaS da NetApp que oferece visibilidade e controle centralizados de todos os acessos a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atingidas.

O controle de acesso é um conceito chave de segurança. A visibilidade e a capacidade de responder a acesso aos arquivos e operações de arquivos são essenciais para manter sua postura de segurança. Para

fornecer visibilidade e controle de acesso para arquivos, a solução ONTAP usa o recurso NetApp FPolicy.

As políticas de arquivo podem ser definidas com base no tipo de arquivo. O FPolicy determina como o sistema de armazenamento processa solicitações de sistemas clientes individuais para operações como criar, abrir, renomear e excluir. A partir do ONTAP 9, a estrutura de notificação de acesso a arquivos FPolicy é aprimorada com controles de filtragem e resiliência contra interrupções de rede curtas.

Passos

1. Para aproveitar o recurso FPolicy, primeiro você deve criar a política FPolicy com o `vserver fpolicy policy create` comando.



Além disso, use o `-events` parâmetro se você usar o FPolicy para visibilidade e a coleção de eventos. A granularidade adicional fornecida pelo ONTAP permite filtrar e acessar o nível de controle do nome de usuário. Para controlar o Privileges e o acesso com nomes de usuário, especifique o `-privilege-user-name` parâmetro.

O texto a seguir fornece um exemplo de criação de FPolicy:

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,vle1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Depois de criar a política FPolicy, você deve ativá-la com o `vserver fpolicy enable` comando. Este comando também define a prioridade ou a sequência da entrada FPolicy.



A sequência FPolicy é importante porque, se várias políticas se inscreveram no mesmo evento de acesso ao arquivo, a sequência dita a ordem em que o acesso é concedido ou negado.

O texto a seguir fornece uma configuração de exemplo para ativar a política FPolicy e validar a configuração com o `vserver fpolicy show` comando:

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                Policy Name                Sequence  Status
Engine
-----
vs1.example.com        vs1_pol
vs2.example.com        vs2_pol
external
2 entries were displayed.
```

Melhorias de FPolicy

O ONTAP 9 inclui os aprimoramentos de FPolicy descritos nas seções a seguir.

Controles de filtragem

Novos filtros estão disponíveis para `SetAttr` e para remover notificações sobre atividades de diretório.

Resiliência assíncrona

Se um servidor FPolicy que opera no modo assíncrono sofrer uma interrupção na rede, as notificações FPolicy geradas durante a interrupção serão armazenadas no nó de storage. Quando o servidor FPolicy volta online, ele é alertado das notificações armazenadas e pode buscá-las a partir do nó de armazenamento. O período de tempo em que as notificações podem ser armazenadas durante uma interrupção é configurável até 10 minutos.

Caraterísticas de segurança das funções de LIF no ONTAP

Um LIF é um endereço IP ou nome de porta mundial (WWPN) com caraterísticas associadas, como uma função, uma porta inicial, um nó inicial, uma lista de portas para failover e uma política de firewall. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede. É fundamental entender as caraterísticas de segurança de cada função de LIF.

Funções do LIF

As funções de LIF podem ser as seguintes:

- **Data LIF:** Um LIF associado a um SVM e usado para comunicação com clientes.
- **Cluster LIF:** Um LIF usado para transportar tráfego entre nós em um cluster.
- **LIF de gerenciamento de nós:** Um LIF que fornece um endereço IP dedicado para gerenciar um nó específico em um cluster.
- **Cluster Management LIF:** Um LIF que fornece uma única interface de gerenciamento para todo o cluster.
- **Intercluster LIF:** Um LIF usado para comunicação entre clusters, backup e replicação.

Caraterísticas de segurança de cada função de LIF

	Data LIF	LIF do cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Requer sub-rede IP privada?	Não	Sim	Não	Não	Não
Requer rede segura?	Não	Sim	Não	Não	Sim
Política de firewall predefinida	Muito restritivo	Completamente aberto	Média	Média	Muito restritivo
O firewall é personalizável?	Sim	Não	Sim	Sim	Sim



- Como o LIF do cluster está completamente aberto sem política de firewall configurável, ele deve estar em uma sub-rede IP privada em uma rede segura isolada.
- As funções de LIF nunca devem ser expostas à Internet.

Para saber mais sobre como garantir a segurança dos LIFs, consulte ["Configurar políticas de firewall para LIFs"](#). Esta página também fornece detalhes sobre as políticas de serviço do LIF a partir do ONTAP 9.10.1.

Para saber mais sobre como criar uma nova política de serviço, consulte o `network interface service-policy create` comando no ["Referência de comandos."](#)

Segurança de protocolo e porta

Além de executar operações e funções de segurança on-box, o endurecimento de uma solução também deve incluir mecanismos de segurança off-box. Aproveitar dispositivos de infraestrutura adicionais, como firewalls, sistemas de prevenção de intrusão (IPSs) e outros dispositivos de segurança, para filtrar e limitar o acesso ao ONTAP é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esta informação é um componente chave para filtrar e limitar o acesso ao ambiente e aos seus recursos.

Protocolos e portas comumente usados

Serviço	Porta/protocolo	Descrição
SSH	22/TCP	Login SSH
telnet	23/TCP	Início de sessão remoto
Domain	53/TCP	Servidor de nomes de domínio
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Chamada de procedimento remoto
NTP	123/UDP	Protocolo de hora de rede
msrpc	135/TCP	Chamada de procedimento remoto da Microsoft
Netbios-name	137/TCP 137/UDP	Serviço de nomes NetBIOS
netbios-ssn	139/TCP	Sessão de serviço NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Link seguro:http
microsoft-ds	445/TCP	Serviços de diretório Microsoft
IPsec	500/UDP	Segurança do protocolo da Internet
mount	635/UDP	Montagem em NFS
named	953/UDP	Daemon de nomes

Serviço	Porta/protocolo	Descrição
NFS	2049/UDP 2049/TCP	Daemon do servidor NFS
nrv	2050/TCP	Protocolo de volume remoto NetApp
iscsi	3260/TCP	Porta de destino iSCSI
Lockd	4045/TCP 4045/UDP	Daemon de bloqueio NFS
NFS	4046/TCP	Protocolo de montagem NFS
acp-proto	4046/UDP	Protocolo de contabilidade
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Segurança do protocolo da Internet
acp	5125/UDP 5133/UDP 5144/TCP	Porta de controle alternativa para disco
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS: Protocolo binário de escuta
TELNET	8023/TCP	Telnet com escopo de nó
HTTPS	8443/TCP	Ferramenta GUI 7MTT através do xref:./ontap-security-hardening/HTTPS
RSH	8514/TCP	RSH do nó-escopo
KMIP	9877/TCP	Porta de cliente KMIP (somente host local interno)
ndmp	10000/TCP	NDMP
cifs testemunha do porto	40001/TCP	Porta de testemunhas CIFS
TLS	50000/TCP	Segurança da camada de transporte
Iscsi	65200/TCP	Porta iSCSI
SSH	65502/TCP	Shell seguro
vsun	65503/TCP	vsun

Portas internas do NetApp

Porta/protocolo	Descrição
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp

Porta/protocolo	Descrição
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp
931	RPC de cluster NetApp
932	RPC de cluster NetApp
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp

Porta/protocolo	Descrição
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp
7824	RPC de cluster NetApp

Relatórios técnicos do ONTAP nas

NetApp soluções NAS simplificam o gerenciamento de dados e ajudam você a acompanhar o crescimento enquanto otimizam os custos.

ONTAP S3

["TR-4814: S3 nas melhores práticas da ONTAP"](#) Saiba mais sobre as práticas recomendadas para usar o Amazon Simple Storage Service (S3) com o software ONTAP, além de recursos e configurações para usar o ONTAP como um armazenamento de objetos com aplicativos S3 nativos ou como um destino de disposição em camadas para o FabricPool.

Relatórios técnicos do ONTAP SMB

NetApp soluções NAS simplificam o gerenciamento de dados e ajudam você a acompanhar o crescimento enquanto otimizam os custos.

SMB

["TR-4740: SMB 3,0 multicanal"](#) A Microsoft introduziu o Multichannel no protocolo SMB 3,0 com o objetivo de melhorar o protocolo SMB3, abordando as limitações de desempenho e confiabilidade do SMB1 e do SMB2. Saiba mais sobre o recurso multicanal no ONTAP, incluindo seus recursos, práticas recomendadas e resultados de teste de desempenho.

Multiprotocolo

["TR-4887: Visão geral e melhores práticas de nas multiprotocolo na ONTAP"](#) Saiba como o acesso nas multiprotocolo funciona no ONTAP e as práticas recomendadas para ambientes multiprotocolo.

Sistemas de armazenamento

AFX

NetApp AFX visão geral: saiba mais sobre NetApp AFX

NetApp AFX ainda é ONTAP — é simplesmente uma maneira diferente de aproveitar os benefícios do ONTAP. NetApp AFX oferece arquitetura desagregada para cargas de trabalho NAS e de objetos, mantendo o software ONTAP completo que você já conhece e adora.

Uma Evolução da Inovação: NetApp ONTAP

NetApp ONTAP foi criado em 1992 como uma nova maneira de fornecer cargas de trabalho NFS para vários clientes, enquanto revolucionava o desempenho, a resiliência, as cópias em pontos no tempo e muito mais. Originalmente, ele suportava apenas NFSv2, mas, à medida que a demanda por versões mais recentes do NFS, outros protocolos de dados e mais recursos de proteção de dados crescia, NetApp ONTAP precisou evoluir.

A seguir está uma linha do tempo abreviada de algumas das principais evoluções do ONTAP que ocorreram nos últimos 30 anos.

A evolução do NetApp ONTAP

Década	Características
1990s	NFSv2, NFSv3, CIFS, Snapshots, sistema de arquivos WAFL, AutoSupport, SnapMirror
2000s	SnapVault, SnapLock, NFSv4, protocolos de bloco, FlexVols, FlexClone, GX/com escalabilidade horizontal, deduplicação, clones de arquivos
2010s	Clustered ONTAP, eficiências de storage inline, NFSv4.1/pNFS, NVMe, RAID-TEC, FlexGroup volumes, criptografia de volume, AFF, Cloud Volumes ONTAP, QoS, FabricPool, Azure NetApp Files (ANF), Google Cloud NetApp Volumes (GCNV), All SAN Array (ASA)
2020s	SnapMirror Business Continuity, FlexCache, ONTAP S3, IPsec, Proteção Autônoma contra Ransomware, SnapMirror dentro e fora de ANF e GCNV, Amazon FSxN, ASAr2, NetApp AFX você está aqui

NetApp ONTAP personalidades

Durante anos, ONTAP funcionou como uma plataforma unificada, combinando arquivos, blocos e objetos em um único sistema. Isso posicionou ONTAP como o canivete suíço do datacenter – uma plataforma capaz de fazer tudo o que você pedisse.

No entanto, à medida que as aplicações evoluíram e os requisitos dos datacenters mudaram com uma série de transformações na indústria de TI, a demanda por plataformas que pudessem realizar tarefas específicas

aumentou. Como resultado, existem agora algumas maneiras diferentes de consumir ONTAP.

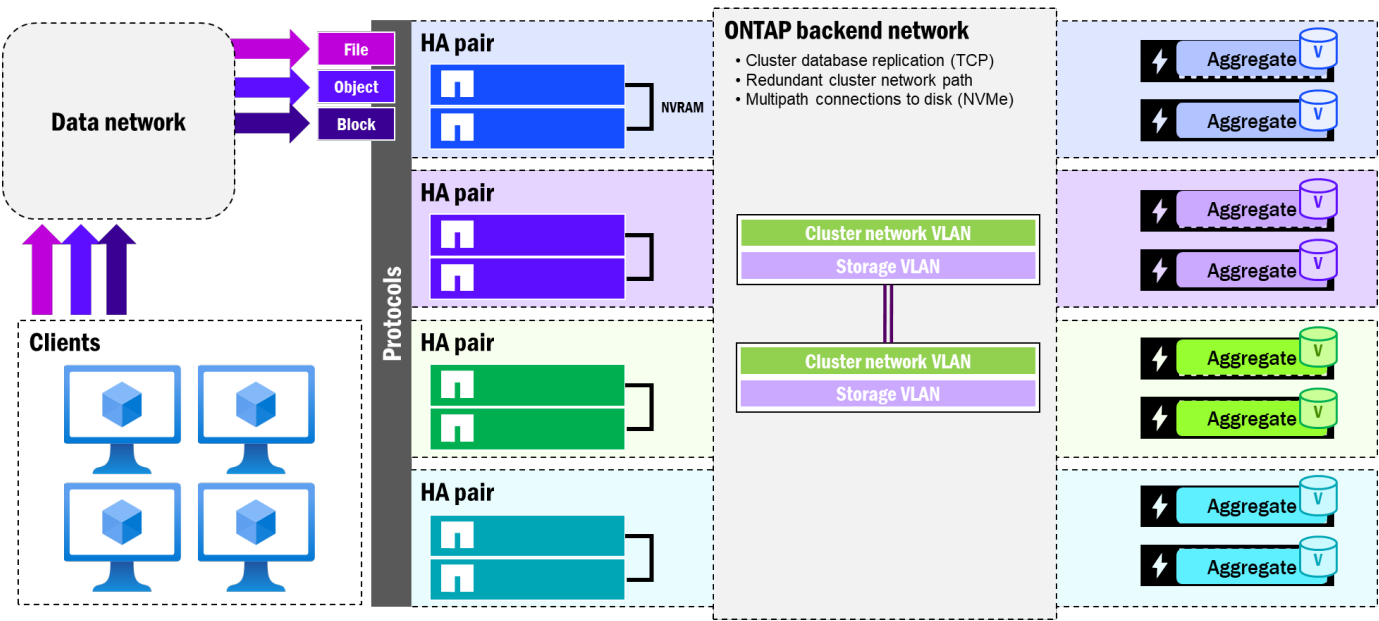
NetApp ONTAP personalidades

Personalidade do ONTAP	Descrição
ONTAP unificado	O mesmo ONTAP que você sempre conheceu, ainda está sendo ativamente desenvolvido e aprimorado.
Todos os arrays SAN	ONTAP que suporta apenas iSCSI, FCP e NVMe sobre FC/TCP e fornece funcionalidade de controlador ativo-ativo, bem como conceitos desagregados em ASAr2.
ONTAP residente em nuvem	ONTAP executado na nuvem; seja em sistemas físicos localizados em um data center na nuvem ou em instâncias virtualizadas do ONTAP.
ONTAP/AFX desagregado	ONTAP utiliza arquitetura desagregada para cargas de trabalho de NAS e objetos de alto desempenho.

Visão geral da arquitetura unificada do ONTAP

O diagrama a seguir mostra a arquitetura geral unificada do ONTAP, com uma descrição de como tudo se encaixa abaixo dele.

Arquitetura geral do ONTAP



Alguns aspectos-chave da arquitetura ONTAP:

- Suporte a arquivos, objetos e blocos
- Os protocolos são fornecidos por meio de uma rede de dados de cliente front-end
- Vários nós independentes podem ser agrupados em cluster
- Cada nó pode fornecer endereços IP flutuantes independentes para casos de uso de dados e gerenciamento

- Os nós em cluster se conectam a um switch de backend fornecido pela NetApp por meio de uma VLAN de cluster
- Os nós são apresentados como par de HA para proporcionar resiliência em caso de falhas de hardware ou de energia
- Os pares de HA possuem placas NVRAM conectadas diretamente que replicam para proteger as gravações
- A cada nó é atribuído pelo menos um agregado e ele detém um subconjunto do número total de discos
- Em situações de failover, os discos de um nó são reatribuídos ao parceiro de HA (e somente ao parceiro de HA)
- Os gabinetes de discos geralmente são conectados diretamente aos nós por meio de cabeamento multipath, mas sistemas de ponta introduzem o conceito de redes de storage no mesmo switch de cluster de backend
- Volumes (FlexVols e FlexGroup volumes) fornecem os pontos de entrada para o storage para acesso aos dados

O que é NetApp AFX?

Um ponto importante a ter em mente é que NetApp AFX ainda é ONTAP.

É simplesmente uma maneira diferente de aproveitar os benefícios do ONTAP. A mesma imagem que você instalaria para seus sistemas Unified ONTAP ou All SAN Array é a mesma imagem usada com NetApp AFX. A base de código é idêntica, mas a forma como os sistemas são inicializados determina qual caminho de código é seguido, como o storage de backend é apresentado e quais recursos e protocolos são suportados.

NetApp AFX oferece arquitetura desagregada para cargas de trabalho NAS e de objetos, mantendo o software ONTAP completo que você já conhece e aprecia. ONTAP desagregado refere-se a uma arquitetura de storage onde cada nó controlador NetApp enxerga a mesma capacidade por meio de switches de rede redundantes e uma rede de alta velocidade e baixa latência. Essa abordagem permite que os nós controladores e a capacidade de storage sejam dimensionados independentemente uns dos outros para atender melhor às necessidades de diversas cargas de trabalho de alto desempenho. Em outras palavras, quando você precisar de desempenho adicional, basta adicionar nós controladores. Se precisar de capacidade adicional, adicione gabinetes. Isso oferece aos administradores de storage a flexibilidade de apresentar uma solução de storage econômica para seus usuários finais.

Como nenhum nó controlador possui discos de forma independente, também não existem agregados físicos com suas próprias restrições de capacidade e desempenho. Em vez disso, a capacidade é apresentada como um modelo compartilhado com o qual todos os nós podem interagir, e ONTAP pode gerenciar automaticamente.

ONTAP desagregado

Compute nodes



High Speed, Low Latency Network

Capacity

Termos e conceitos-chave

A seguir, estão os termos diretamente relacionados ao AFX. Para terminologia específica do ONTAP, consulte a documentação do produto.

["Documentação do produto ONTAP"](#).

ONTAP desagregado

Refere-se à nova arquitetura baseada em ONTAP que oferece a capacidade de escalar computação e capacidade independentemente uma da outra. O termo "Disaggregated ONTAP" não é um nome de produto, mas sim uma forma de diferenciar entre ONTAP unificada e as arquiteturas NetApp AFX.

NetApp AFX

NetApp AFX é o nome oficial do produto para a arquitetura ONTAP desagregada e foi anunciado no NetApp Insight 2025.

Nós de computação

Em NetApp AFX, um nó de computação refere-se ao nó controlador de storage (e os termos são frequentemente usados de forma intercambiável na documentação). Esses nós não possuem disco integrado e são projetados para serem totalmente modulares, permitindo a escalabilidade independente que a arquitetura ONTAP desagregada proporciona.

Zona de disponibilidade de armazenamento

Uma Zona de Disponibilidade de Armazenamento (SAZ, na sigla em inglês) é o único conjunto de capacidade em um NetApp AFX cluster, onde todos os discos são compartilhados entre todos os nós. A SAZ possibilita funcionalidades como capacidade compartilhada, desempenho aprimorado, deduplicação global e muito mais.

O que há de novo no NetApp AFX

Esta seção contém as atualizações mais recentes para NetApp AFX e será atualizada a cada nova versão. Consulte esta página periodicamente para obter novas informações, mas também verifique as notas de lançamento da versão.

Quais são as novidades na versão mais recente do NetApp ONTAP para AFX?

Última versão:

ONTAP 9.19.1RC1 (a partir de maio de 2026)

Novos recursos no NetApp AFX:

- Desduplicação global
- Eficiência de storage dinâmica
- Leitura antecipada avançada
- Suporte para 32 nós
- Suporte para 32PB
- 512 volumes constituintes por FlexGroup volume

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1.0	Junho de 2026	Lançamento inicial

Como a arquitetura AFX da NetApp difere do ONTAP unificado

NetApp AFX introduz diferenças arquitetônicas significativas em relação ao ONTAP unificado na forma como o storage é apresentado, como os nós interagem com os discos e como a capacidade é gerenciada.

Anteriormente, apresentamos uma visão geral de como a arquitetura unificada do ONTAP fornece storage de arquivos, objetos e blocos por meio de pares HA diretamente conectados, que possuem seus próprios conjuntos de discos e apresentam capacidade física por meio de agregados de discos. Nesta seção, discutiremos com mais detalhes algumas das principais diferenças entre as arquiteturas unificadas do ONTAP e NetApp AFX.

Como saber se um sistema está executando NetApp AFX

A principal maneira de verificar se o seu sistema está executando NetApp AFX é executar o seguinte comando:

```
AFX::> node show -fields personality
node                personality
-----
afx-01              AFX
afx-02              AFX
```

Outra pista é a nova Storage Availability Zone, mas esse também é um conceito disponível para NetApp All-SAN Arrays (ASA). Você pode ver sua capacidade via esse comando.

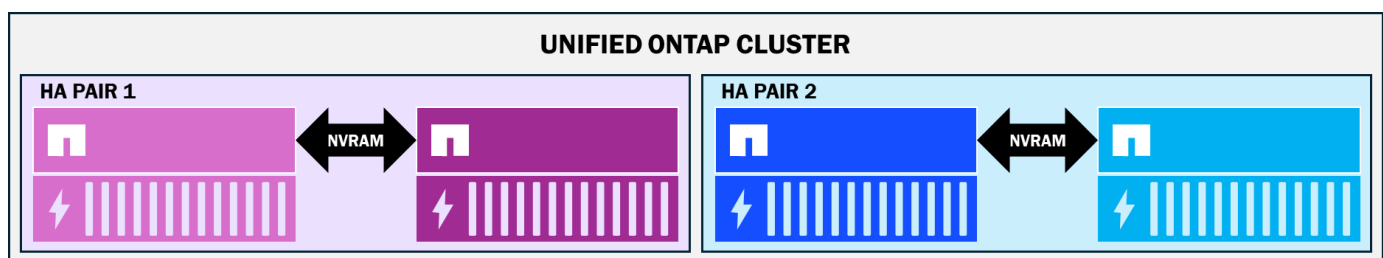
```
AFX::> storage availability-zone show

Availability Zone Name: storage_availability_zone_0
Availability Zone UUID: 545cb59f-32e9-11f1-a2f5-
d039eabdd925

Total Size: 69.59TB
Physical Used: 837.1GB
Physical Used Percent: 1%
Available: 68.77TB
Metadata Used: 837.1GB
Log and Recovery Metadata: 834.6GB
Delayed Frees: 2.50GB
Physical User Data Without Snapshot Copies: 17.24MB
Logical User Data Without Snapshot Copies: 17.24MB
Efficiency Ratio Without Snapshot Copies: 1.00:1
Space Full Threshold Percent: 98%
Space Nearly Full Threshold Percent: 95%
```

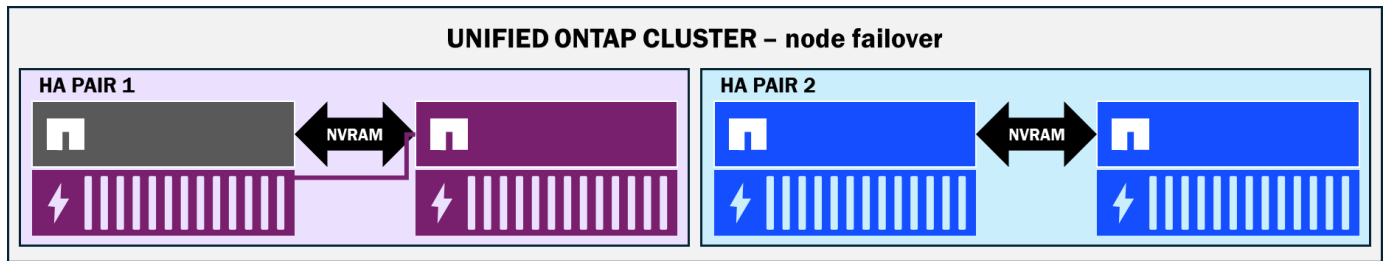
Relações nó-disco

Na arquitetura unificada do ONTAP, as operações de leitura e gravação são direcionadas para um subconjunto específico de discos. Portanto, mesmo que você tenha 24 gavetas de discos em um cluster de 24 nós (uma gaveta por nó), em qualquer momento cada nó só poderá acessar diretamente uma gaveta de discos, o que limita a capacidade e o desempenho disponíveis no cluster.



Além disso, como NVRAM está diretamente conectada entre pares de HA, os nós precisam estar fisicamente próximos uns dos outros e são mais fortemente acoplados como destinos de failover. Por exemplo, quando um nó realiza failover para seu nó parceiro, os únicos discos aos quais ele tem acesso físico são os discos no domínio do par de HA.

Cluster ONTAP unificado durante failover de HA

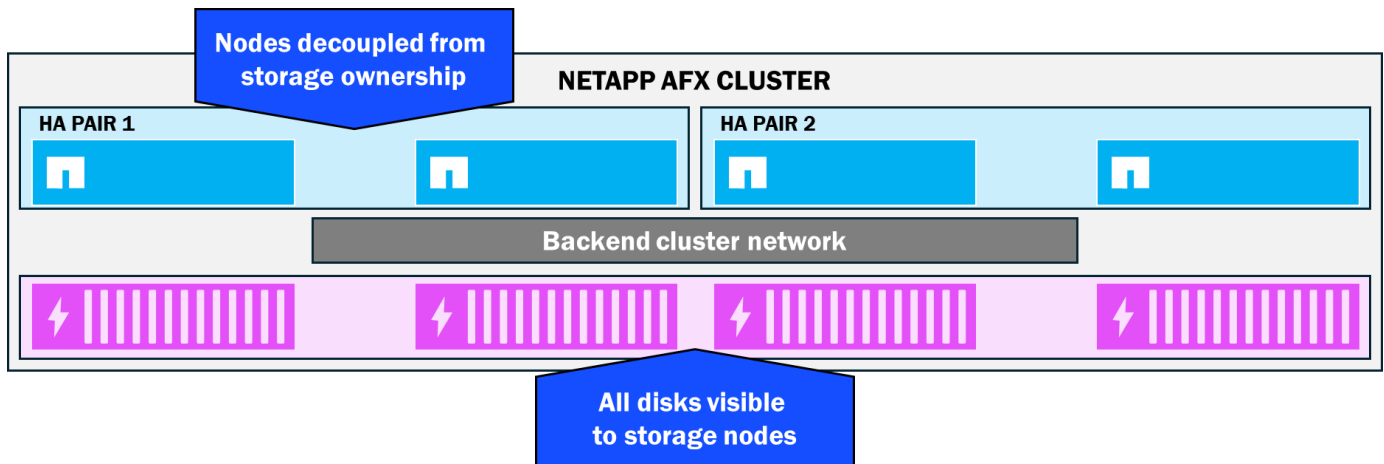


No NetApp AFX, há algumas mudanças importantes na forma como os discos são apresentados aos nós de computação.

Todos os discos são visíveis para todos os nós de armazenamento—sem propriedade de disco

No NetApp AFX, todos os nós e gabinetes estão conectados ao mesmo switch de backend, o que permite ao ONTAP estender o domínio de visibilidade geral dos discos para toda a pilha. Como resultado, nenhum nó possui discos específicos. Em vez disso, todos os discos participam de um único pool de capacidade chamado Storage Availability Zone, o que proporciona gerenciamento de capacidade mais simples e maior potencial de desempenho (mais discos disponíveis significam mais desempenho disponível).

NetApp AFX Zona de disponibilidade de armazenamento

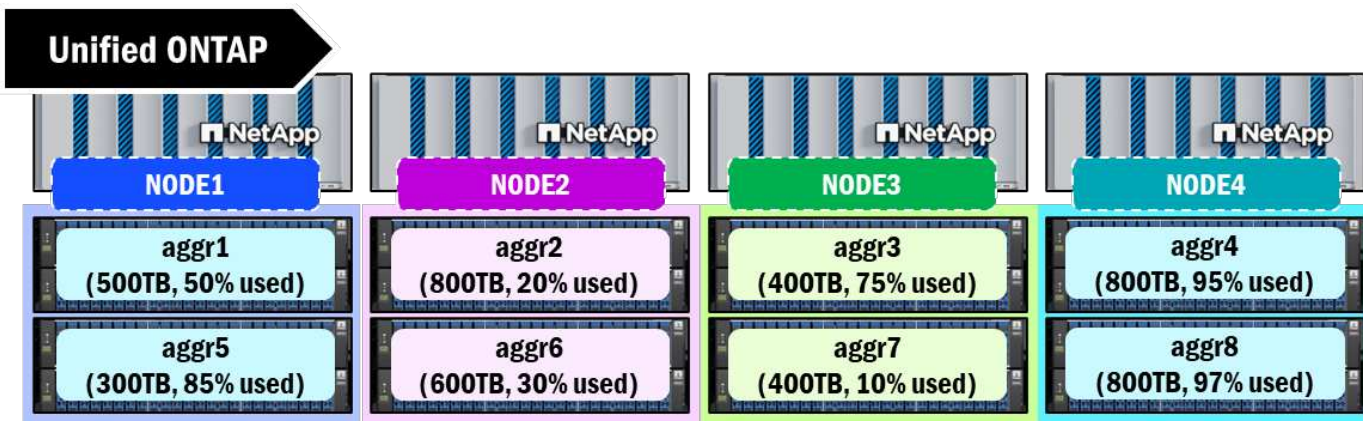


Chega de agregados físicos

O Unified ONTAP agrupa discos em grupos RAID e os combina em uma estrutura de capacidade conhecida como agregado. Esse agregado representa a forma como a capacidade física é apresentada ao storage e define o limite de espaço disponível para a criação de volumes que disponibilizam dados aos usuários finais. Cada nó deve ter pelo menos um agregado atribuído, e esses agregados têm um limite atual de 800TB. Uma vez atingido esse limite, não há mais espaço disponível para gravações adicionais.

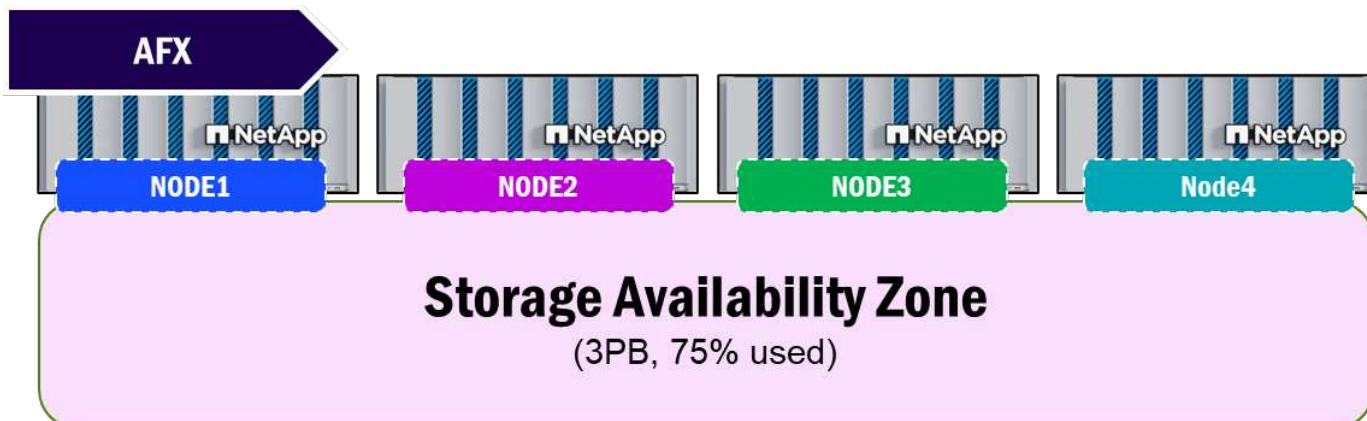
Os agregados físicos também podem apresentar alguns desafios de gerenciamento de capacidade, já que os administradores de storage às vezes precisam reorganizar manualmente os volumes para manter o equilíbrio da capacidade entre os nós do cluster. Esses desafios também podem ser ampliados ao utilizar uma arquitetura de volume com escalabilidade horizontal (como um volume FlexGroup). Os agregados também podem variar em tamanho, quantidade de discos, tipos de disco etc., o que também pode criar algumas diferenças de desempenho ao percorrer os nós.

Agregados no ONTAP unificado



NetApp AFX pega o conceito de um agregado físico e o virtualiza, tornando-o gerenciado pelo ONTAP, e então migra o gerenciamento de capacidade de uma metodologia por nó para uma por cluster através da nova Storage Availability Zone. Esse pool único de capacidade proporciona uma abordagem "o que você vê é o que você obtém" para o gerenciamento de espaço.

NetApp AFX Zona de disponibilidade de armazenamento



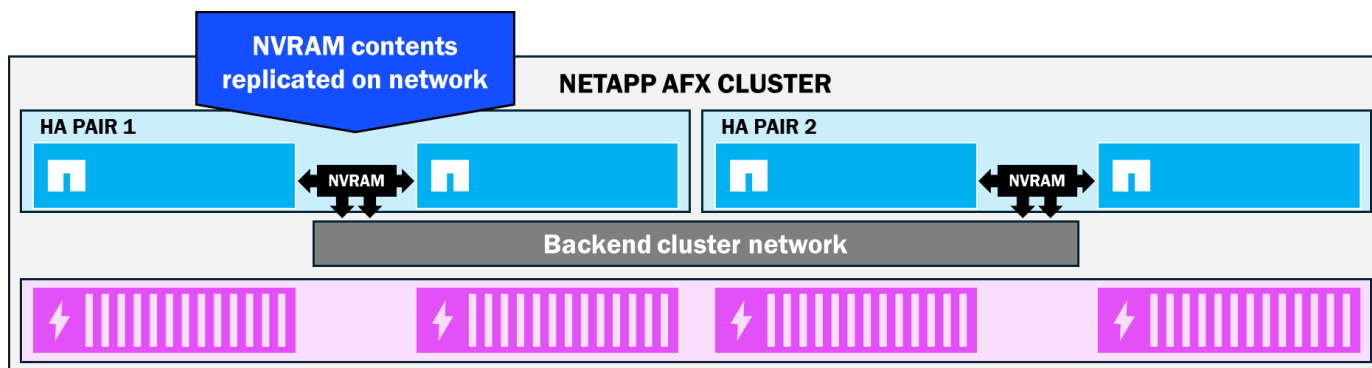
NVRAM passou de conexão direta para replicação comutada

ONTAP utiliza NVRAM como uma camada de proteção para proteger as gravações recebidas em um cluster. Cada nó em um cluster ONTAP possui uma placa NVRAM com bateria. Quando uma gravação é enviada para um volume a partir de um cliente, ela é armazenada primeiro na NVRAM. O conteúdo da NVRAM é então gravado em disco quando a NVRAM está cheia ou quando um timer de 10s expira (o que ocorrer primeiro). Isso é conhecido como ponto de consistência.

O conteúdo do NVRAM também é constantemente replicado entre pares de HA, o que ajuda ainda mais a proteger a consistência de dados, pois, em caso de falha de um nó, o conteúdo do NVRAM será preservado no nó sobrevivente e gravado em disco.

Em clusters ONTAP unificados, as placas NVRAM entre pares de HA são conectadas diretamente umas às outras. NetApp AFX move a replicação da NVRAM para a rede de backend do cluster. Como resultado, os nós parceiros de HA não têm um requisito de distância tão rígido para os nós. Em vez disso, os pares de HA podem ser separados até a distância máxima do ethernet.

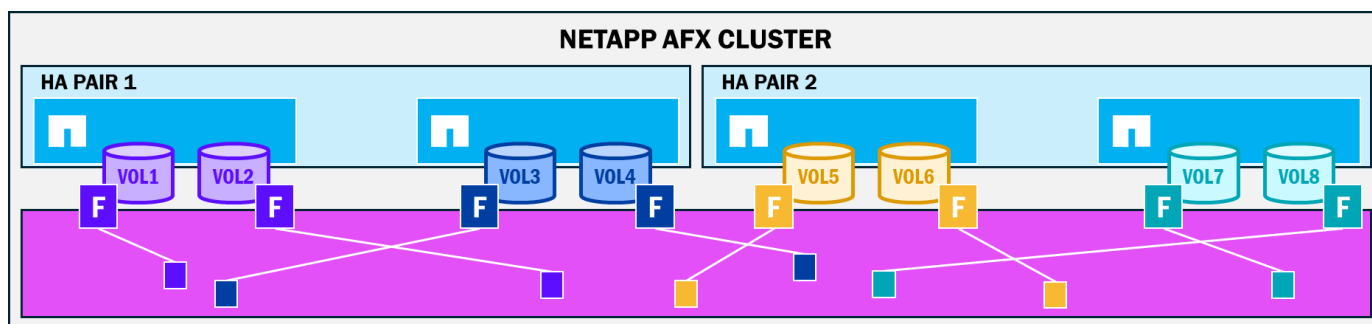
Replicação de NVRAM NetApp AFX



Dados gravados em qualquer (e todos) os discos na zona de disponibilidade

NetApp AFX elimina o conceito de propriedade de disco e migra a estrutura física agregada para uma abordagem virtualizada gerenciada pelo ONTAP, onde toda a capacidade adquirida para o cluster fica disponível para os nós conectados ao cluster. Com o AFX, todos os nós têm a capacidade de gravar em qualquer e todos os discos na Storage Availability Zone, independentemente da relação de propriedade nó:volume. Os nós ainda mantêm o conceito de propriedade de volume, já que as gravações ainda passam pela NVRAM, mas esses dados podem ser armazenados em qualquer lugar na capacidade disponível. Isso significa que um número maior de discos pode participar de uma única carga de trabalho, o que proporciona benefícios de desempenho.

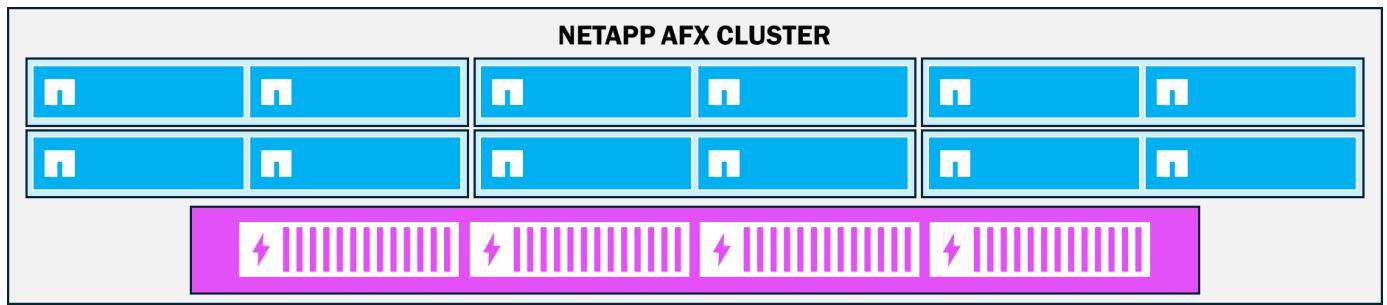
Como os dados chegam a uma Storage Availability Zone



Escala independente de capacidade e nós de computação

Com os recursos de hardware desacoplados na arquitetura NetApp AFX, os nós não precisam mais ser adicionados lado a lado com os discos associados. Quando um cluster está com poucos recursos relacionados ao desempenho, como RAM, CPU ou throughput de rede, apenas os nós de storage precisam ser adicionados ao cluster e podem aproveitar a Storage Availability Zone existente. Por outro lado, se a necessidade for de capacidade, apenas os shelves precisarão ser adicionados à configuração. Essa flexibilidade garante que você compre apenas os recursos de que vai precisar, evitando o superprovisionamento.

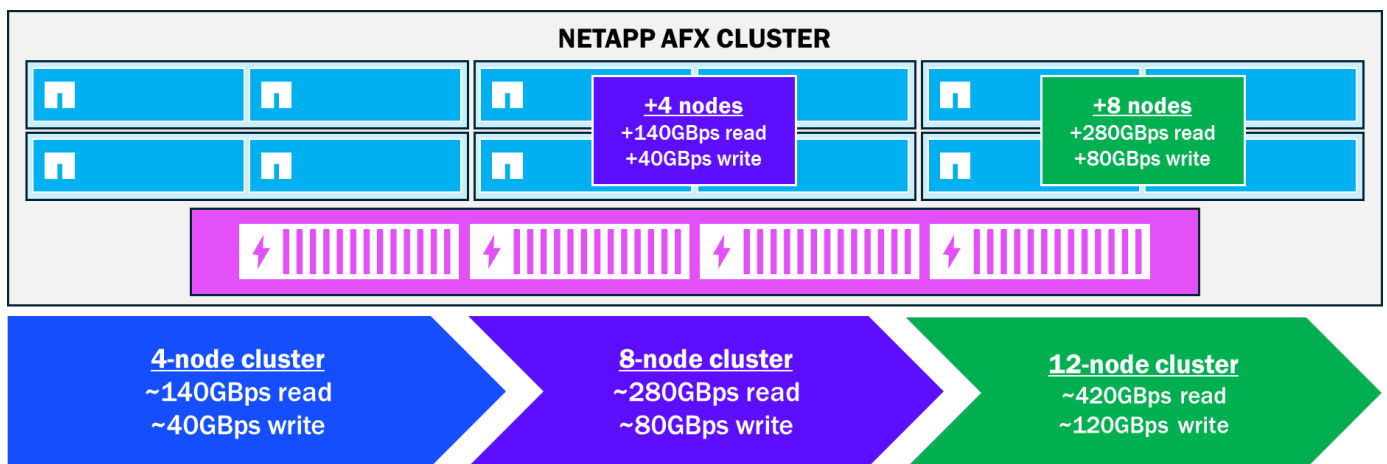
NetApp AFX – Escala independente



Escalabilidade linear do desempenho do nó

À medida que nós são adicionados a um cluster AFX, mais CPU, RAM e recursos de rede são introduzidos na carga de trabalho. Conforme esses recursos são incorporados ao ambiente, os aumentos de desempenho são lineares. O gráfico abaixo mostra como esse desempenho aumentaria com a adição de nós.

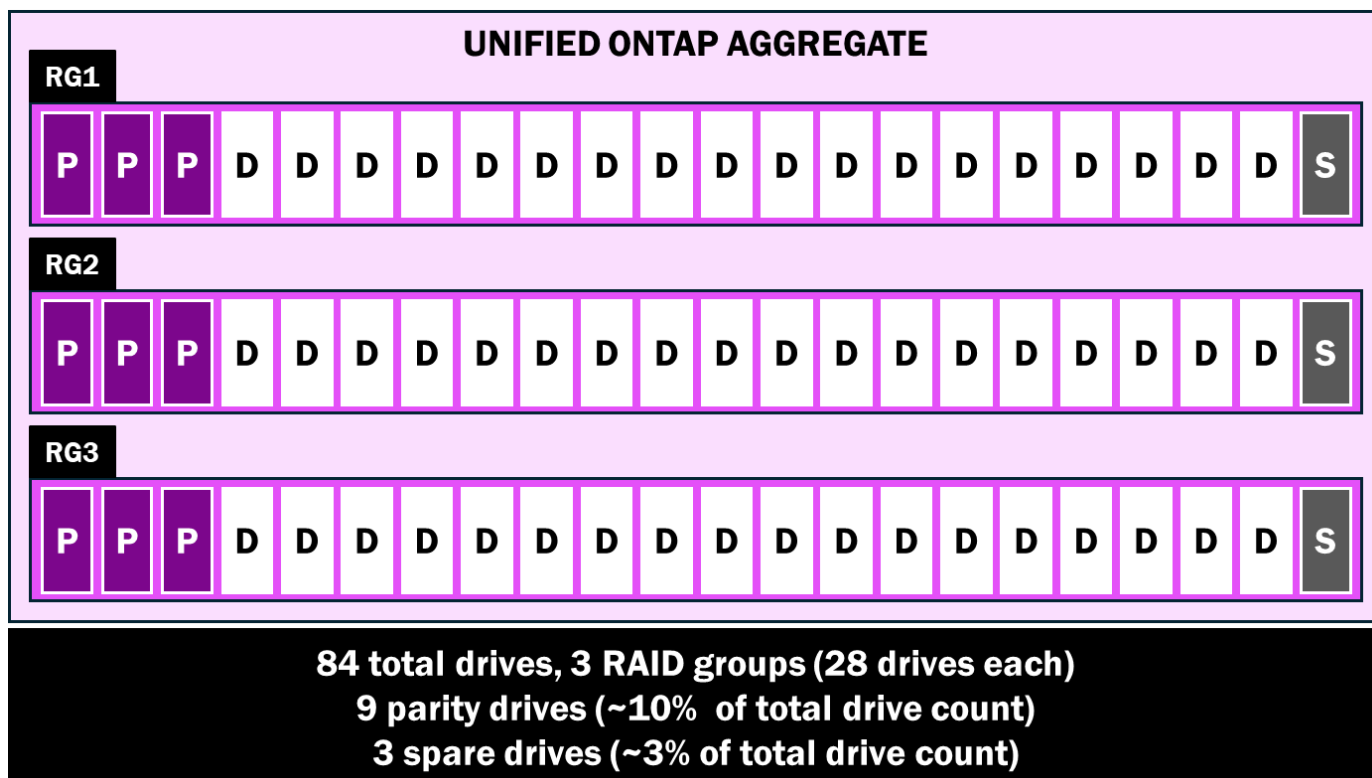
O desempenho linear aumenta com a adição de nós NetApp AFX



Grupos RAID maiores, menos discos de paridade

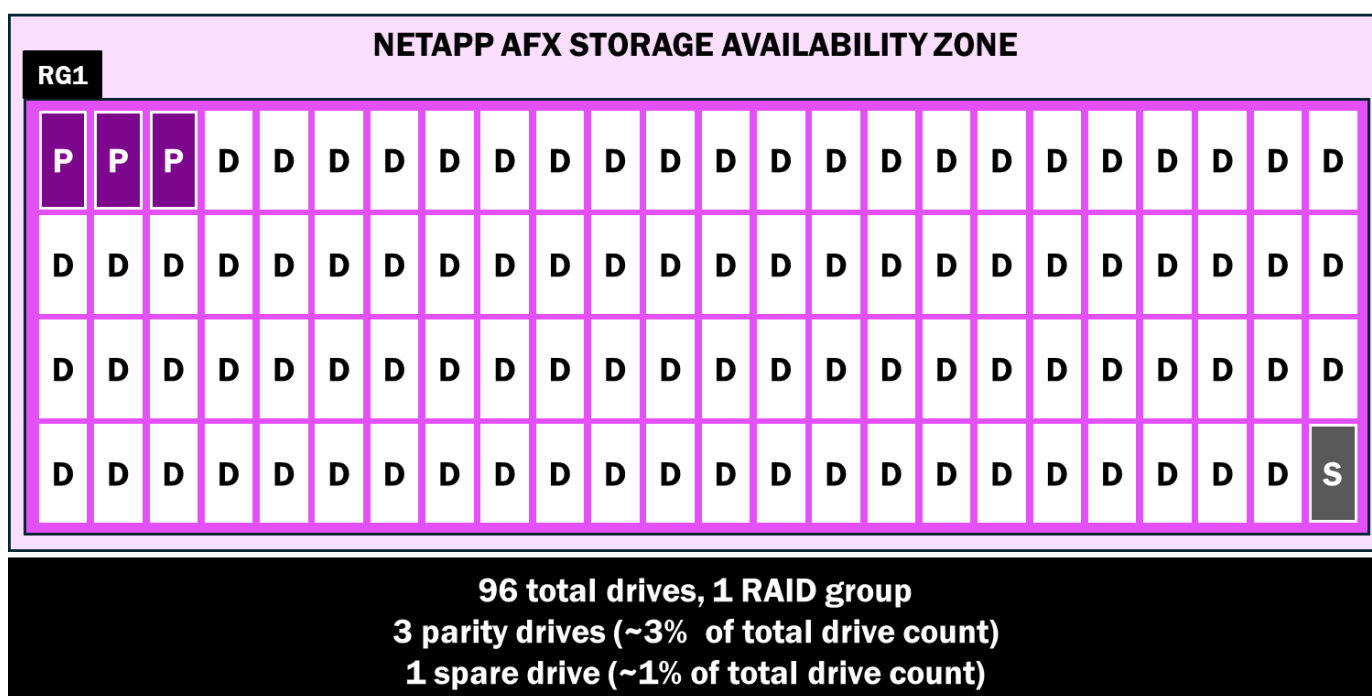
ONTAP oferece uma combinação de proteção de dados e desempenho para discos por meio de grupos RAID – especificamente RAID-TEC, que oferece proteção de paridade tripla em caso de falhas de disco. RAID-TEC pode sobreviver a até três falhas simultâneas de unidades em um grupo RAID. No ONTAP unificado, os grupos RAID têm um número máximo de 28 discos, onde 3 discos são usados para paridade e 1 disco é reservado como reserva. Como resultado, 24 dos 28 discos são usados para operações de dados/faixas RAID.

Grupos RAID ONTAP unificados



NetApp AFX ainda utiliza RAID-TEC, mas aumenta o tamanho do grupo RAID para 96 discos, exigindo apenas 3 discos de paridade e 1 sobressalente. Grupos RAID maiores proporcionam melhor desempenho geral, enquanto a exposição à falha de disco é minimizada por uma combinação de baixas taxas de falha para SSD, operações distribuídas de forma mais uniforme por um conjunto maior de discos, bem como melhorias na reconstrução de discos de dados a partir da paridade no NetApp AFX.

NetApp AFX Storage Availability Zone grupo RAID



A tabela a seguir estima a quantidade de capacidade bruta utilizável para 84 discos em ONTAP unificado e

NetApp AFX com tamanhos de unidade variáveis.

Comparação aproximada da capacidade bruta, 84 unidades – Unified ONTAP e NetApp AFX

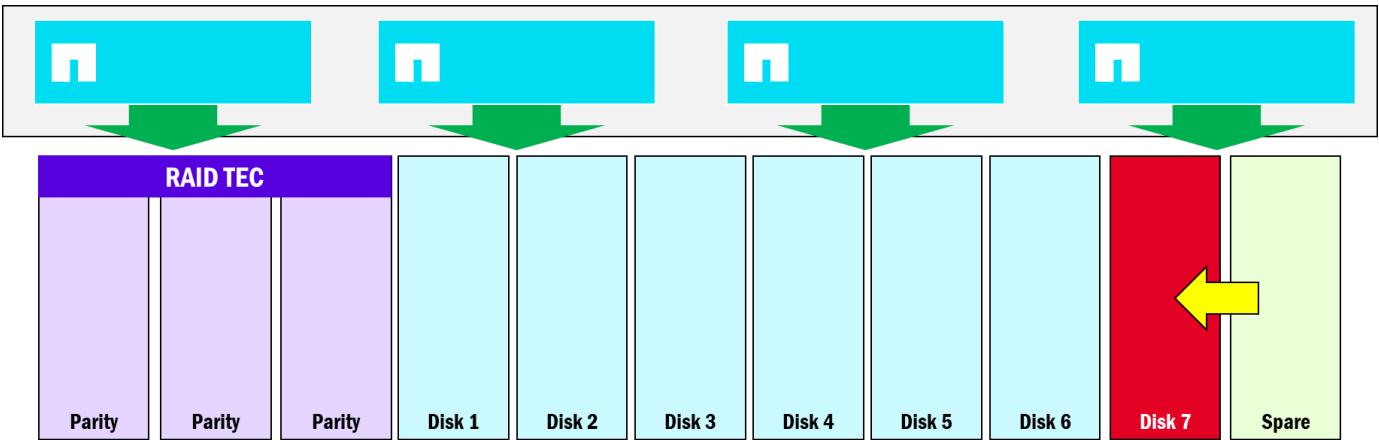
Tamanho da unidade	Capacidade bruta (unificada)	Capacidade bruta (AFX)
7,6 TB	~547,2TB	~608TB (+60,8TB)
15,3 TB	~1101,6TB	~1224TB (+122,4TB)
30,6 TB	~2203,2TB	~2448TB (+244,7TB)
60,1 TB	~4327,2TB	~4808TB (+480,8TB)

Tempos de reconstrução de falha de disco mais rápidos

No ONTAP unificado, cada nó possui um subconjunto de discos na pilha de storage. Isso significa que esse nó só grava nesses discos, mas também que a reconstrução dos discos é feita por um único nó em caso de falha de disco.

NetApp AFX dispensa a necessidade de propriedade de disco. Como resultado, todas as unidades podem ser gravadas a partir de um único nó, se necessário. Isso também significa que, quando uma unidade precisa ser reconstruída a partir da paridade, todos os nós do cluster participam, permitindo que as reconstruções ocorram mais rapidamente do que se um único nó tivesse que fazê-las sozinho.

Reconstrução de disco no NetApp AFX

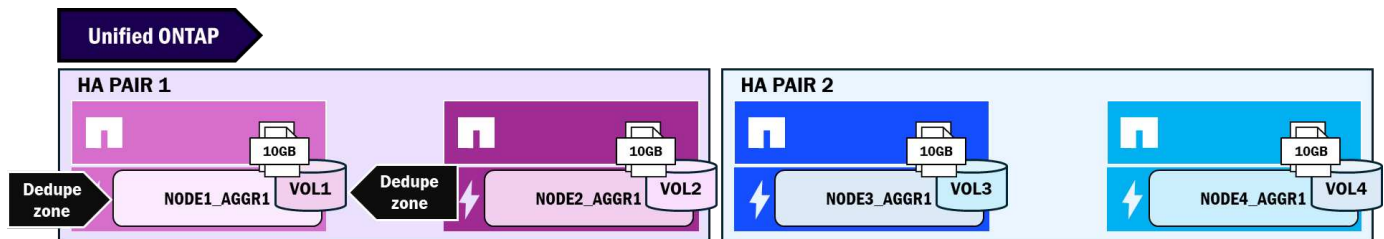


Domínios de deduplicação

A deduplicação permite que um sistema de storage encontre blocos duplicados em seu sistema de arquivos e, em seguida, crie ponteiros para um único bloco para reduzir a quantidade total de capacidade utilizada. No ONTAP unificado, a deduplicação segue um limite específico para os blocos que podem ser reduzidos. Esses limites dependem do tipo de deduplicação em uso. Em geral:

- Deduplicação baseada em volume → Limite de volume
- Desduplicação entre volumes → Limite de agregado

Domínios de deduplicação ONTAP unificados



A tabela abaixo mostra o comportamento da capacidade para dados duplicados em diferentes cenários no ONTAP unificado. À medida que as cópias de arquivos abrangem nós e agregados (e, portanto, domínios de deduplicação), a economia de espaço é reduzida.

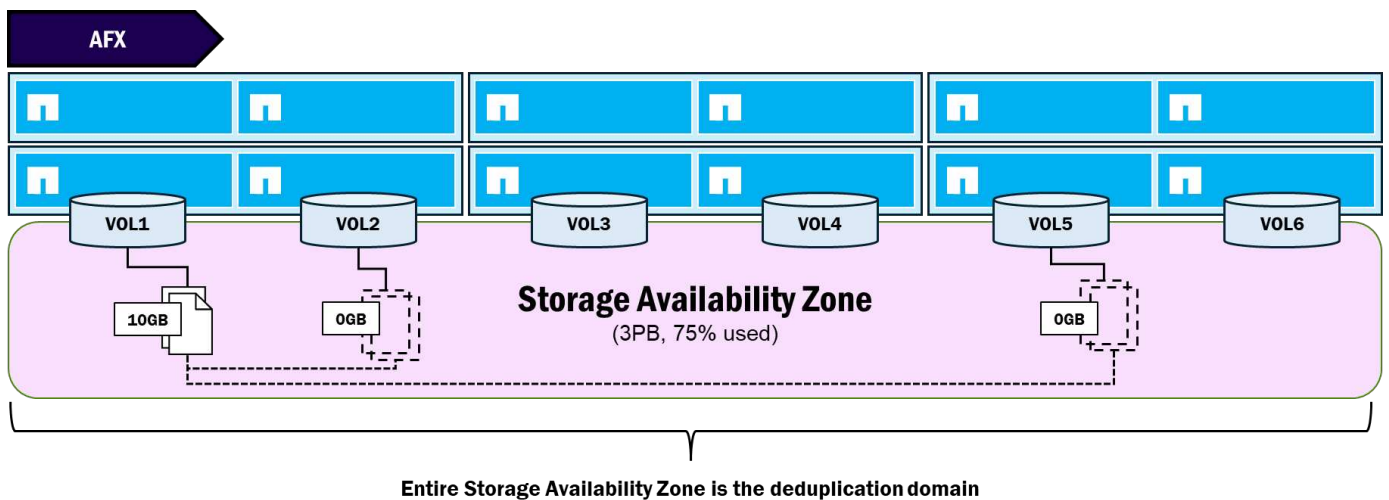
Comportamentos de deduplicação em diferentes cenários para arquivos idênticos de 10GB – ONTAP

Cenário	Espaço utilizado
Quatro cópias do mesmo arquivo de 10 GB, no mesmo volume (desduplicação de volume)	10 GB
Quatro cópias do mesmo arquivo de 10GB, em volumes diferentes, com o mesmo agregado (desduplicação entre volumes ativada)	10 GB
Quatro cópias do mesmo arquivo de 10GB, 4 volumes diferentes, 4 agregados diferentes (desduplicação entre volumes ativada)	40 GB

Como o NetApp AFX remove agregados físicos e move o gerenciamento de capacidade para a nova Storage Availability Zone, os limites do domínio de deduplicação também mudam. No AFX, o domínio de deduplicação está no nível do volume (como o ONTAP unificado) e no nó (em vez do agregado) antes da versão 9.19.1.

A partir do ONTAP 9.19.1, o AFX oferece suporte a um domínio de deduplicação global no nível da Storage Availability Zone, de modo que todos os blocos duplicados no cluster storage pool sejam tratados da mesma forma.

NetApp AFX – Domínio de deduplicação global (ONTAP 9.19.1)



A tabela abaixo mostra o comportamento da capacidade para dados duplicados em diferentes cenários no NetApp AFX.

Comportamentos de deduplicação em diferentes cenários para arquivos idênticos de 10 GB – NetApp AFX

Cenário	Espaço utilizado
Quatro cópias do mesmo arquivo de 10 GB, no mesmo volume (deduplicação de volume)	10GB (9.18.1) 10GB (9.19.1)
Quatro cópias do mesmo arquivo de 10GB, em volumes diferentes, no mesmo nó (deduplicação entre volumes ativada)	10GB (9.18.1) 10GB (9.19.1)
Quatro cópias do mesmo arquivo de 10GB, em 4 volumes diferentes, em 4 nós diferentes (deduplicação entre volumes ativada)	40GB (9.18.1) 10GB (9.19.1)

Funcionalidades que foram removidas/não são suportadas

NetApp AFX foi projetado para cargas de trabalho de NAS e objetos de alto desempenho – particularmente (mas não exclusivamente) aquelas na área de treinamento e inferência de IA. Com o design do NetApp AFX, algumas decisões foram tomadas para desativar alguns dos recursos no ONTAP.

- Devido ao foco em NAS de alto desempenho e objetos, as cargas de trabalho em bloco foram removidas da solução NetApp AFX. Não há suporte para os protocolos de dados FCP, iSCSI ou NVMe e não há planos para adicionar protocolos em bloco.
- Desagregado é sinônimo de desagregado, o que significa que os agregados (pelo menos como conceito de administração de storage físico) foram removidos. A remoção do agregado físico não só simplifica o gerenciamento de capacidade no ONTAP, mas também fornece o mecanismo para permitir um único pool de capacidade.
- A remoção dos agregados implica na remoção também de seus recursos específicos. O Metrocluster, por exemplo, utiliza espelhamento em nível de agregado para seus recursos de failover de site. Portanto, o Metrocluster também foi removido do NetApp AFX. A funcionalidade de failover de site será fornecida pelo novo recurso SnapMirror Active-Sync para NAS, oferecido no ONTAP 9.19.1GA.
- O recurso de hierarquização de dados frios chamado FabricPool também não está disponível para o NetApp AFX no momento, pois também é específico para agregados.
- As movimentações de volume baseadas em cópias também não são mais necessárias no NetApp AFX, devido à nova arquitetura de capacidade. Para obter mais informações, consulte [Movimentações de volume sem cópia](#).
- A remoção de funcionalidades também implica em algumas alterações na CLI/GUI/API REST, portanto, quaisquer comandos ou chamadas de API para funcionalidades que não sejam mais suportadas também serão removidos.
- O ZAPI está atualmente indisponível para NetApp AFX.
- Descarregamento de cópia NFS para virtualização (FlexGroup volumes com Distribuição Granular de Dados somente)

Alterações no gerenciamento do ONTAP

Em geral, o gerenciamento do NetApp AFX não altera os mecanismos usados para gerenciar um cluster. Os administradores ainda podem usar a CLI, a GUI e as APIs REST para acessar e configurar um cluster. Mas o NetApp AFX apresentou uma oportunidade para aprimorar alguns aspectos de como as operações de gerenciamento de storage são realizadas.

Gerenciamento de capacidade mais simples

A NetApp AFX Storage Availability Zone reduz os pontos de extremidade de gerenciamento, passando de uma abordagem baseada em nós e agregados para um único pool de capacidade disponível para todo o cluster. À medida que os volumes crescem e diminuem, ONTAP automaticamente aloca e devolve capacidade para a Storage Availability Zone.

Por isso, os administradores de armazenamento não precisam mais se preocupar em localizar e gerenciar espaço livre em até 24 nós e potencialmente centenas de agregados. Em vez disso, há apenas um local onde a capacidade é gerenciada e visualizada.

Por exemplo, na CLI do ONTAP unificado, se você quisesse ver informações sobre a capacidade física total de um cluster, usaria “aggregate show-space”, que exibiria todas as entradas de agregados. No NetApp AFX, você tem “cluster space show”, que mostrará apenas a única Storage Availability Zone.

Comparação lado a lado dos comandos CLI de capacidade no ONTAP unificado e NetApp AFX

```
unified::> aggr show-space
```

Unified ONTAP

Feature	Used	Used%
Volume Footprints	250.2TB	50%
Aggregate Metadata	31.06MB	0%
Snapshot Reserve	8.41GB	5%
Total Used	1.2TB	95%
.....		
Total Physical Used	225.2TB	50%
Total Provisioned Space	450.2TB	90%

8 entries were displayed.

```
AFX::> cluster space show
```

AFX

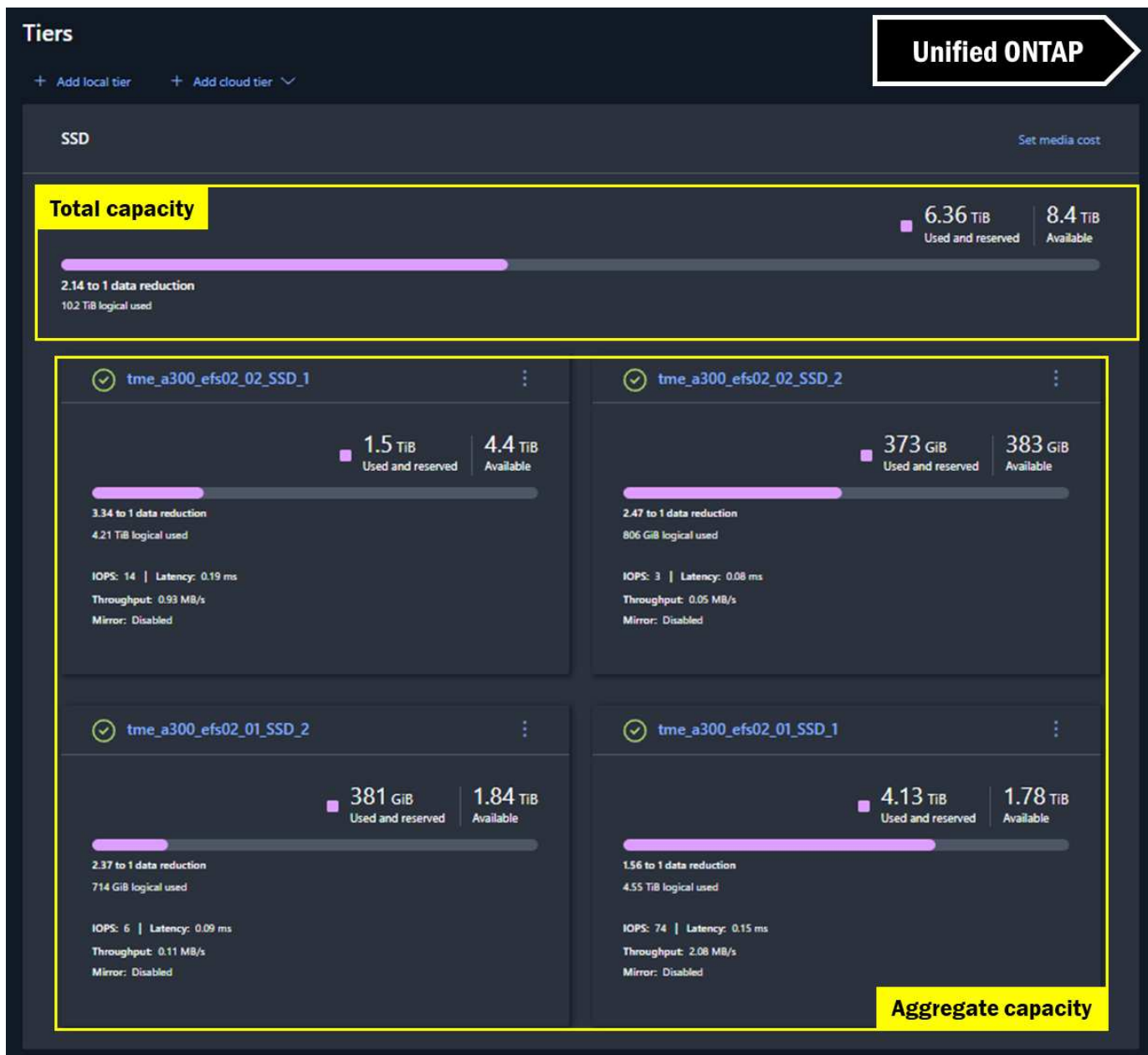
Availability Zone Name: storage

Total Size: 3PB
Physical Used: 2PB
Physical Used Percent: 75%
Available: 1PB
Metadata Used: 1.71TB
Log and Recovery Metadata: 1.71TB
Delayed Frees: 1.22GB
Physical User Data Without Snapshot Copies: 3.33MB
Logical User Data Without Snapshot Copies: 3.33MB
Efficiency Ratio Without Snapshot Copies: 1.00:1
Space Full Threshold Percent: 98%
Space Nearly Full Threshold Percent: 95%

1 entry was displayed.

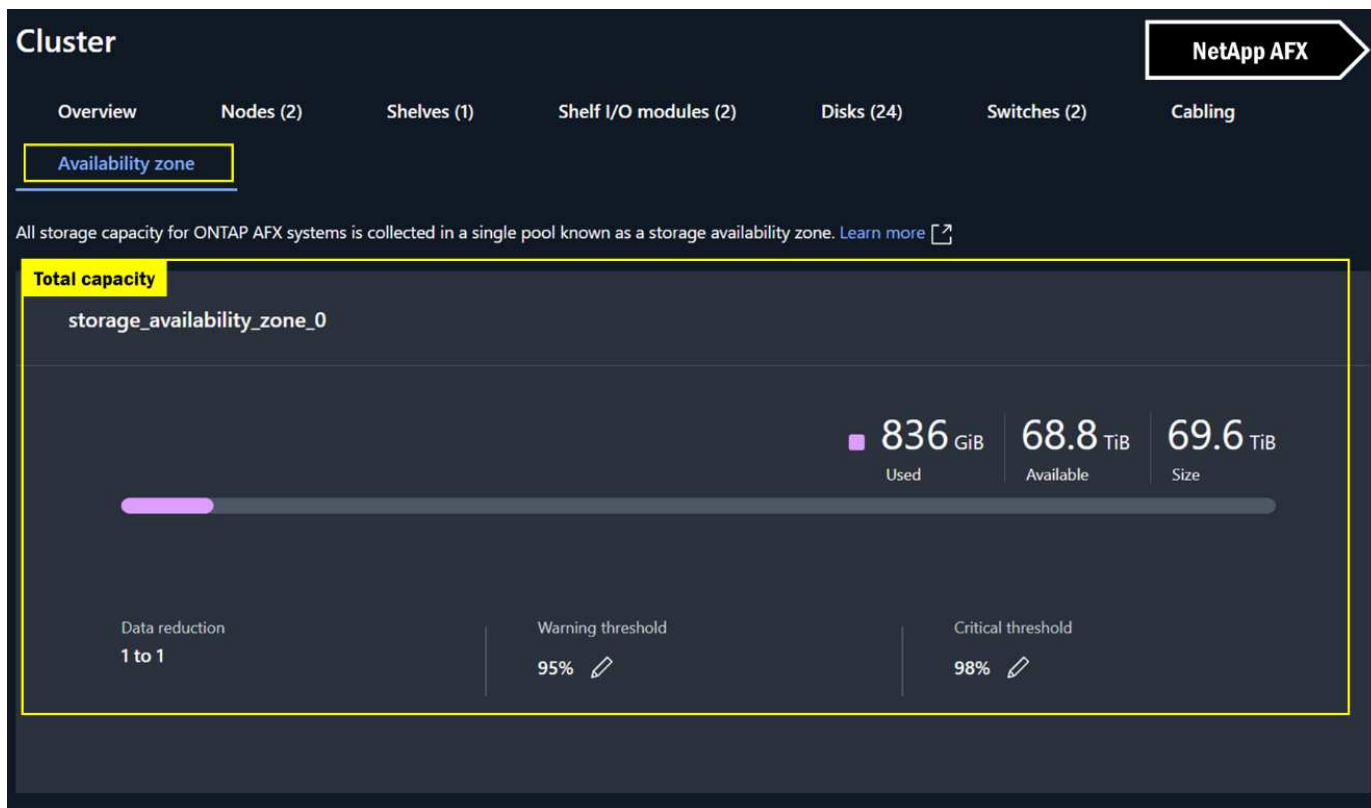
Na interface gráfica do usuário (GUI) do Unified ONTAP System Manager, os tiers são usados para mostrar a capacidade. De fato, a GUI tenta mostrar a capacidade holística do cluster somando os totais, mas ainda exibirá o uso geral por agregado.

System Manager visualizações de capacidade – Unified ONTAP



No NetApp AFX System Manager, a visualização do espaço do cluster é praticamente a mesma, mas como não há agregados, não há cálculos adicionais a serem feitos. A capacidade que você vê é a capacidade que você obtém.

System Manager visualizações de capacidade – NetApp AFX

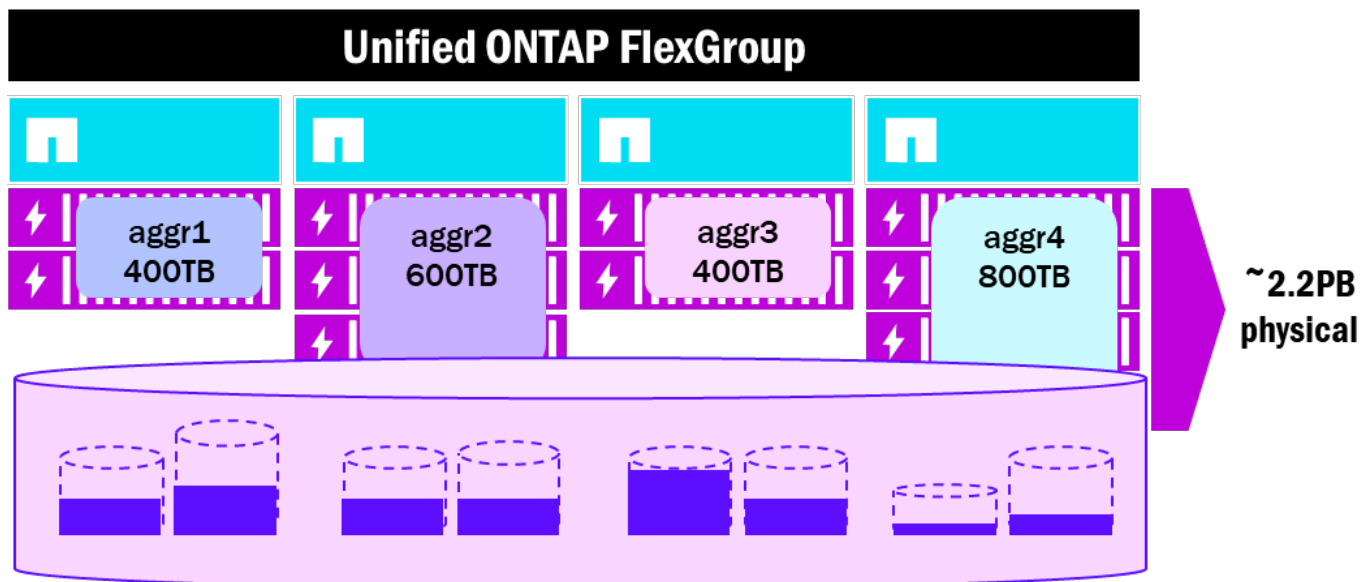


FlexGroup melhorias no gerenciamento de volumes

Um volume FlexGroup consiste em múltiplos volumes FlexVol constituintes subjacentes criados em vários nós e agregados no cluster e apresentados como um único namespace grande para clientes NAS. Volumes FlexGroup oferecem benefícios de desempenho, escalabilidade, balanceamento de carga e quantidade de arquivos para cargas de trabalho de alto desempenho. No entanto, como são coordenados entre nós e agregados, ocasionalmente encontram algumas limitações físicas quando a capacidade começa a se esgotar, já que os sistemas de arquivos independentes fornecidos pelos agregados também têm uso e limites de capacidade independentes. Por exemplo, se um agregado com volumes constituintes FlexGroup começar a se encher antes de outros agregados no cluster, então todo o próprio FlexGroup poderá estar sujeito a problemas de capacidade ou desempenho.

Como resultado, os administradores de armazenamento podem acabar se preocupando demais com a infraestrutura subjacente de FlexGroup e se concentrando menos na manutenção de outros aspectos do ambiente.

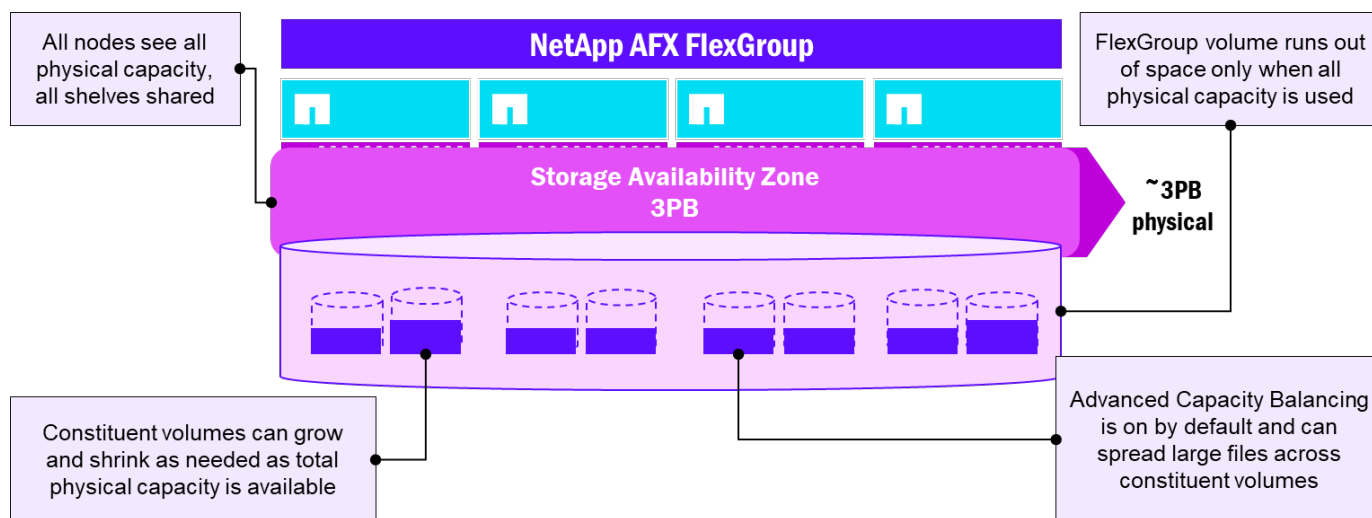
FlexGroup layout de volume - agregados ONTAP unificados



NetApp AFX apresenta capacidade em uma única Storage Availability Zone, o que reflete mais fielmente a forma como os volumes FlexGroup foram projetados para funcionar. Em vez de múltiplos volumes constituintes em diversos agregados distintos de tamanhos potencialmente variados, todos os volumes residem no mesmo pool de capacidade, o que simplifica consideravelmente a sobrecarga no gerenciamento do uso de um volume FlexGroup.

Além disso, o AFX habilita o Balanceamento de Capacidade Avançado por padrão para FlexGroup volumes, o que ajuda a distribuir melhor os arquivos maiores no volume. Agora, os constituintes do volume FlexGroup deixam de ser um conceito de gerenciamento e passam a funcionar silenciosamente em segundo plano.

Layout de volume FlexGroup - NetApp AFX



Tarefas automatizadas de administração de storage

Com a Storage Availability Zone no NetApp AFX, toda a capacidade é compartilhada entre todos os nós. Embora os nós ainda possuam volumes, ONTAP gerencia automaticamente o uso da capacidade de cada nó, emprestando e liberando capacidade com base no que cada nó precisa em determinado momento. Isso significa que os administradores de storage não precisam mais se preocupar com a melhor forma de equilibrar o espaço utilizável.

Além disso, o gerenciamento de grupo RAID é automatizado pelo ONTAP, onde discos recém-adicionados

serão adicionados a grupos RAID existentes ou novos sem intervenção do administrador. ONTAP também gerencia a movimentação de volumes entre nós sem a necessidade de copiar dados.

Movimentações de volume sem cópia

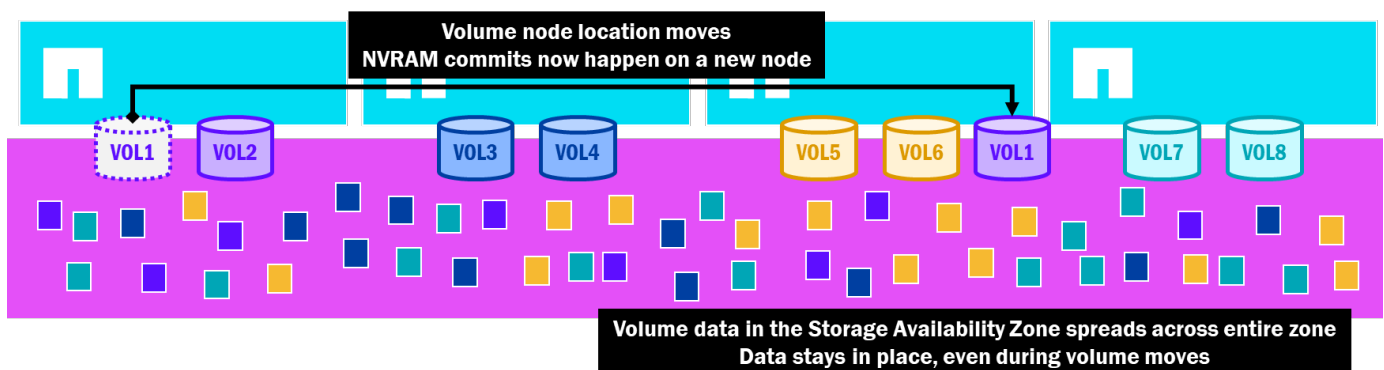
O Unified ONTAP oferece uma maneira de mover volumes entre nós ou agregados sem interrupções, permitindo o gerenciamento do desempenho e do uso da capacidade em todo o cluster.

Quando uma movimentação de volume é iniciada, ocorre o seguinte:

- Um novo volume vazio é criado no agregado de destino
- Metadados do volume (como informações de eficiência de storage, identificadores de arquivos, etc.) são replicados para o novo volume de destino
- Os dados do volume são replicados para o volume de destino através da rede do cluster de back-end via tecnologia SnapMirror—o agregado de destino precisa ter espaço livre disponível para a movimentação, caso contrário, a tarefa de movimentação falhará
- A replicação de volume ocorre novamente para garantir que ambos os volumes estejam consistentes com quaisquer alterações de dados
- É iniciado um processo de transição para desativar o volume de origem e promover o volume de destino como o novo volume de origem para os clientes
- A E/S do cliente sofre uma breve pausa durante a transição, mas não são necessárias remontagens

No NetApp AFX, a Storage Availability Zone apresenta toda a capacidade para todos os nós, e todos os nós podem gravar em qualquer disco desse pool. Uma vez que os dados são colocados, eles permanecem onde foram alocados – mesmo se o volume for movido. Isso significa que nenhuma cópia de dados é necessária. O processo de movimentação de volume é idêntico ao ONTAP unificado, exceto pela necessidade de replicar dados via SnapMirror. Nenhuma capacidade extra é necessária.

Movimentação de volumes com zero cópia no NetApp AFX



A mobilidade de volumes leves permite que o AFX automatize muitas das tarefas administrativas sem restrições de desempenho ou capacidade, e essas movimentações de volume são usadas em alguns novos recursos oferecidos pelo NetApp AFX, conforme descrito nos tópicos abaixo.

Comportamento de failover de HA

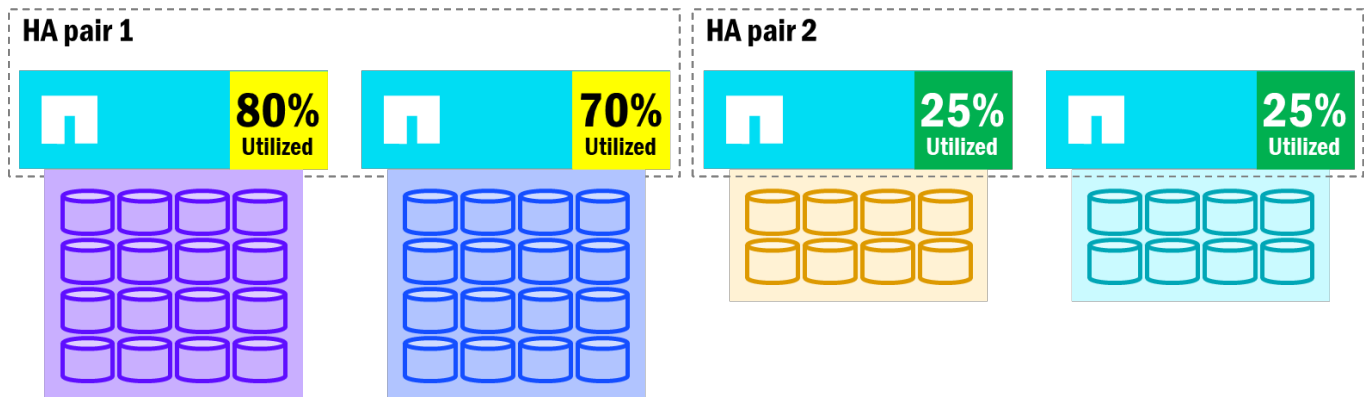
No ONTAP unificado, os nós possuem discos e agregados, onde os dados são servidos por meio de volumes. As gravações são realizadas usando a NVRAM local de um nó para descarregar os dados nos discos que o nó possui. Quando um nó é reiniciado ou falha, o ONTAP aciona a transferência dos recursos do nó com falha, transferindo a propriedade dos discos e agregados para o nó parceiro. As interfaces de rede também são transferidas para portas no espaço IP e, como o conteúdo da NVRAM está sendo constantemente

replicado entre o par de HA, o nó irá descarregar o conteúdo da NVRAM para confirmar as gravações do nó com falha nos discos. Depois disso, o nó sobrevivente passa a possuir os agregados e volumes do nó com falha até que o giveback do nó ocorra. Isso significa que todo o tráfego para esses volumes – bem como para os volumes já pertencentes ao nó sobrevivente – será processado em um único nó até que o problema de failover seja resolvido.

Como parte da implantação inicial do cluster ONTAP unificado, recomenda-se planejar com antecedência para failovers a fim de evitar que um único nó sobrecarregue seu parceiro. Isso por si só representa um desafio, pois é difícil prever quais volumes podem ser vilões de desempenho, mas recursos como movimentação de volume sem interrupção e políticas de qualidade do serviço de volumes podem ajudar na mitigação.

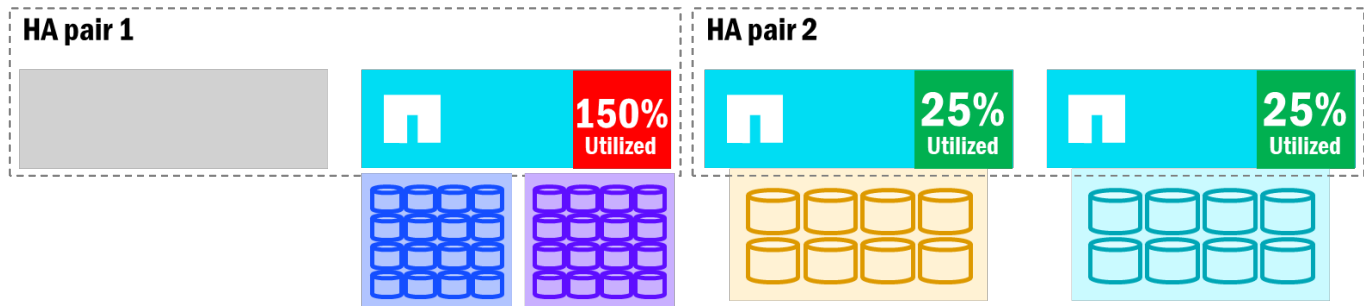
As imagens abaixo mostram como clusters ONTAP unificados podem apresentar desequilíbrio de desempenho entre os nós, bem como como um failover pode causar degradação de desempenho em alguns casos.

Unified ONTAP – possíveis desequilíbrios na utilização dos nós



Quando os nós de um par de HA ficam desequilibrados em contagem de volume e utilização de desempenho, as falhas de nós impactam o desempenho geral, já que o nó sobrevivente passa a ser o proprietário de todos os volumes do nó com falha. Enquanto isso, outros nós no cluster podem ter espaço para assumir trabalho adicional.

Unified ONTAP – Impacto do failover na utilização dos nós



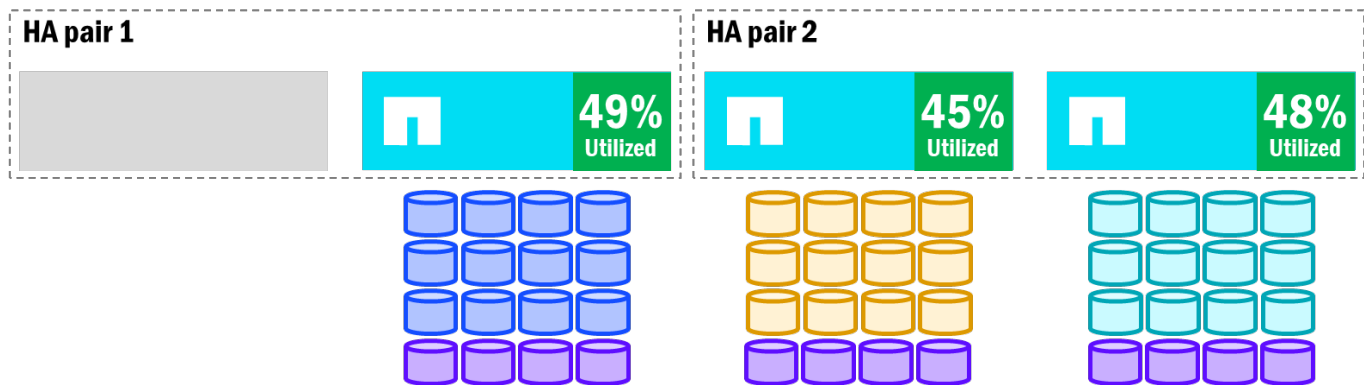
No exemplo acima, quando um parceiro de par de HA precisa assumir trabalho adicional, ele pode ficar sobrecarregado e afetar o desempenho de todos os volumes nesse nó. A movimentação de volumes pode ajudar a aliviar a situação, mas requer cópias entre os nós (o que exige espaço livre), e o tempo necessário para isso pode exceder o tempo necessário para que os nós retornem ao estado original. Além disso, se você realocar um volume, ele não retornará ao nó original. Em vez disso, ele permanecerá no nó para o qual foi movido.

Com o NetApp AFX, as falhas de nós assumem alguns comportamentos diferentes.

- Como os nós não possuem discos e não existem agregados físicos, uma falha de nó não exigirá a transferência desses recursos. Em vez disso, apenas as interfaces de rede e a propriedade dos volumes são transferidas para outros nós.
- As confirmações de NVRAM ainda ocorrem, mas através da rede de HA em vez de uma conexão direta.
- Após a primeira transferência de volumes para o nó parceiro, o AFX redistribuirá os volumes entre os demais nós sobreviventes do cluster. Isso é possível graças à movimentação de volumes sem cópia.
- Quando o nó for recuperado, os volumes retornarão ao nó original.

NetApp AFX já mantém o equilíbrio de desempenho entre os nós do cluster para manter uma utilização relativamente uniforme, portanto, quando ocorre um failover e os volumes são reequilibrados, a utilização dos nós deve ser aproximadamente a mesma em todo o cluster.

NetApp AFX - Reequilíbrio de volume após falha



Adições e remoções de nós

Tanto o ONTAP unificado quanto o NetApp AFX permitem a adição e remoção de nós do cluster. No entanto, devido a algumas diferenças arquitetônicas, o processo de adição e remoção de nós difere um pouco.

Adição/remoção de nós no ONTAP unificado

Já aprendemos que unified ONTAP possui uma relação direta de propriedade entre nó e disco e que todos os nós devem ter alguns discos e pelo menos um agregado associado a eles. Com isso em mente, o seguinte se aplica a adições e remoções.

- A adição de nós no ONTAP unificado não requer etapas adicionais, mas para garantir desempenho equilibrado em todos os nós (incluindo os novos), os volumes precisam ser movidos para os novos nós. Isso exige uma análise prévia dos volumes existentes e suas cargas de trabalho, decisões sobre quais volumes mover e, em seguida, a movimentação propriamente dita dos volumes, o que, novamente, requer uma cópia desses dados na rede do cluster de backend.
- A remoção de nós no ONTAP unificado exigiria a evacuação manual dos volumes existentes no nó, o que significa que você deve identificar quais nós podem hospedar quais volumes para manter um desempenho uniforme e deve ter capacidade livre suficiente para fornecer um local para esses volumes serem movidos. Se a capacidade livre for um desafio, movimentos adicionais de volumes podem ser necessários para redistribuir as cargas de trabalho no cluster. A remoção de nós também envolve a remoção de par de HA, portanto o trabalho envolvido é dobrado. Como os nós possuem discos, uma reinicialização completa dos discos também seria necessária para esses nós. Cada uma dessas coisas adiciona tempo e esforço ao que deveria ser uma tarefa relativamente simples.

Adição/remoção de nós no NetApp AFX

Também descobrimos que o NetApp AFX não aproveita a propriedade padrão de nó para disco e não usa agregados físicos para apresentar capacidade ao cluster. Por causa disso, a adição e remoção de nós se comportam de maneira um pouco diferente.

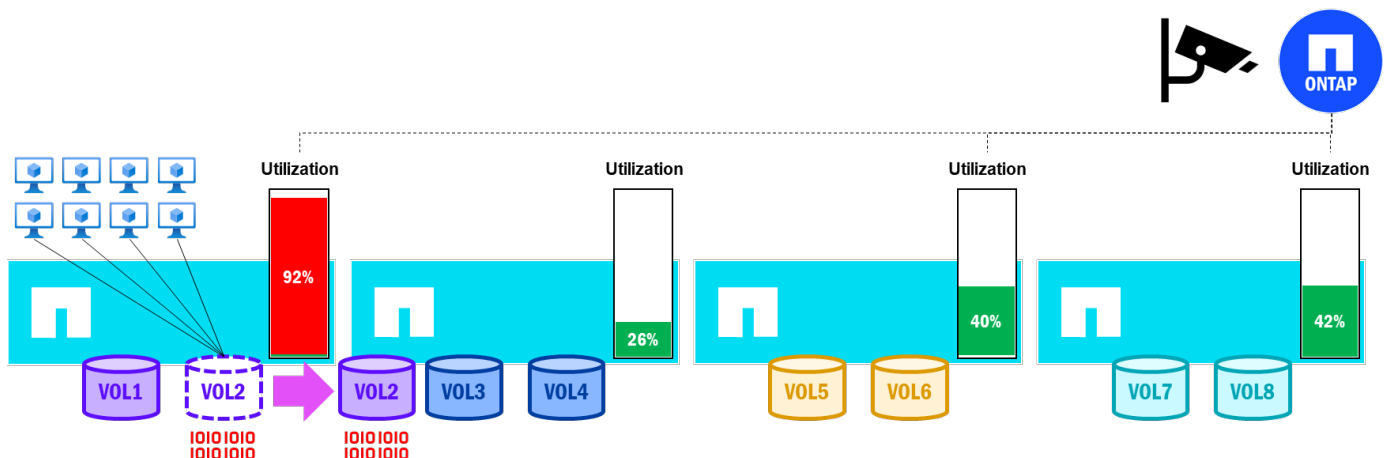
- A adição de nós no NetApp AFX não exigirá a mesma análise prévia de volume, nem exigirá intervenção administrativa para garantir que cada nó tenha um equilíbrio uniforme de volumes. Em vez disso, ONTAP equilibra automaticamente a quantidade de volumes entre os nós recém-adicionados para manter perfis de desempenho relativamente uniformes. ONTAP moverá automaticamente os volumes entre os nós sem copiar nada, reduzindo o tempo, a capacidade e o esforço necessários para adicionar nós a um cluster.
- A remoção de nós no NetApp AFX também não exige muita intervenção manual, se é que exige alguma. Quando um nó é marcado para remoção, ONTAP move automaticamente os volumes entre os nós (novamente, sem copiar) para evacuar os nós que estão sendo removidos. E como não há discos pertencentes aos nós, não é necessário reinicializar os discos após a remoção dos nós. Isso torna os nós no AFX modulares por natureza e fáceis de escalar para cima ou para baixo.

Movimentos de volume orientados para o desempenho

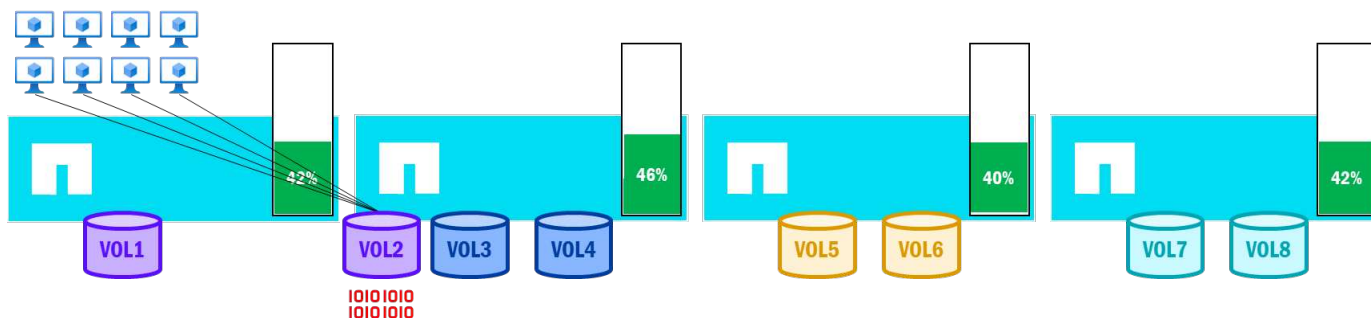
NetApp A funcionalidade de movimentação de volumes sem cópia do AFX permite o rebalanceamento de volumes conforme necessário, sem copiar dados, o que possibilita operações rápidas e sem a necessidade de capacidade adicional. Isso significa que a movimentação de volumes pode se tornar uma parte mais importante do balanceamento de carga automatizado disponível para clusters ONTAP. Agora que mover um volume não custa praticamente nada, o ONTAP pode aproveitar essa valiosa ferramenta para incorporar recursos como o balanceamento de carga de volumes orientado ao desempenho.

No NetApp AFX com ONTAP 9.18.1 e versões posteriores, a utilização de nó, par de HA e volume é monitorada constantemente, enquanto os dados de desempenho são coletados e analisados. Se a utilização de um nó ficar fora dos limites definidos, então o ONTAP selecionará automaticamente um volume para mover para um nó menos utilizado, buscando manter o desempenho equilibrado em todo o cluster.

Movimentos de volume orientados pelo desempenho no NetApp AFX – alta utilização desencadeia um movimento de volume



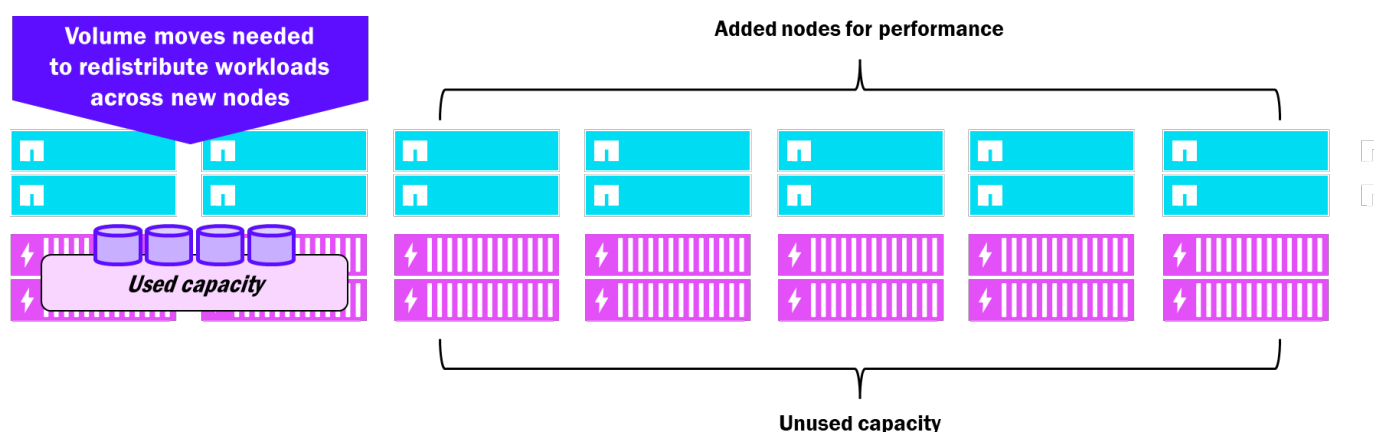
Movimentação de volume orientada por desempenho no NetApp AFX – Utilização equilibrada dos nós após a movimentação de volume



Escala e expansão do cluster

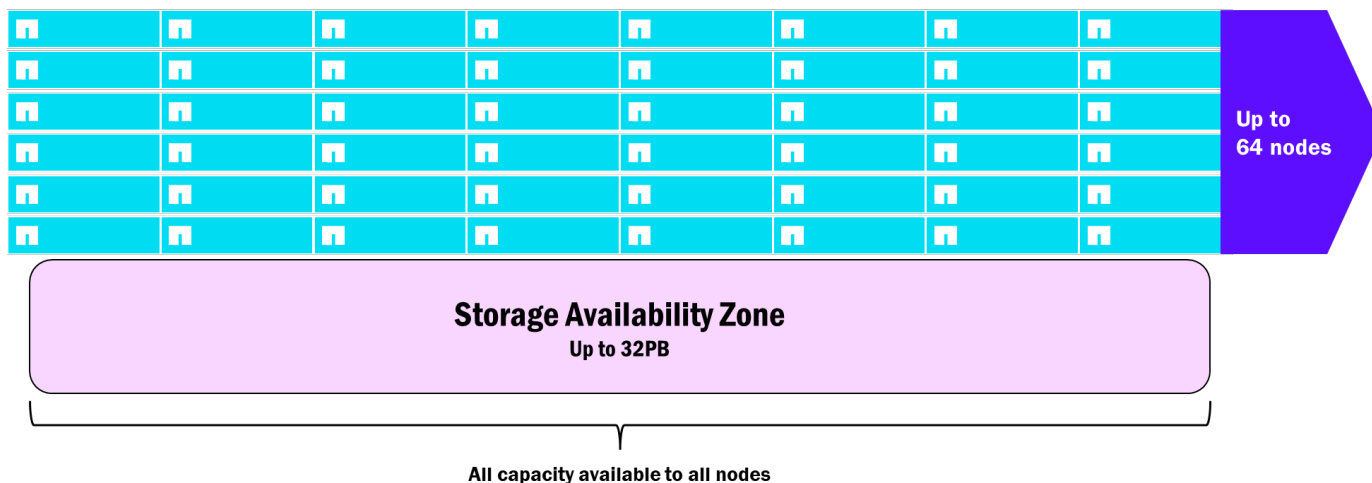
Os clusters Unified ONTAP suportam até 24 nós, e cada nó adicionado também deve ser adicionado com discos (tanto para funcionalidades do sistema quanto para serviços de dados). É possível adicionar gavetas de discos ao cluster, mas elas sempre ficam conectadas a um único par de HA e pertencem apenas a um único nó, mesmo que o cluster tenha 24 nós. Isso significa que a capacidade é adicionada ao cluster mesmo quando apenas o desempenho é necessário, e esse aumento de desempenho fica restrito principalmente a um conjunto específico de discos pertencentes aos novos nós. Como resultado, você pode acabar com capacidade extra que não necessariamente precisa.

Unified ONTAP – considerações adicionais de escala



NetApp AFX suporta clusters em maior escala. A partir da versão 9.19.1, os clusters AFX podem atingir até 32 nós em um único cluster. E como todos os nós podem ver e acessar todos os discos, eles podem compartilhar o desempenho e a capacidade (até 32PB a partir do ONTAP 9.19.1) dessas unidades, de forma que nunca haja recursos ociosos. A movimentação de volumes não requer cópias, portanto ONTAP consegue mover automaticamente os volumes para os nós recém-adicionados para garantir uma utilização uniforme dos nós, enquanto a capacidade é distribuída uniformemente por meio da Storage Availability Zone.

NetApp AFX – considerações adicionais de escala



Alterações no volume raiz

No NetApp ONTAP, cada nó recebe um volume raiz, que é usado para arquivos e funções específicos do sistema, como arquivos de log, imagens de boot, arquivos de core, bancos de dados de cluster e muito mais.

No ONTAP unificado, esses volumes raiz residiam em agregados raiz físicos. Para reduzir a quantidade de capacidade utilizada pelos agregados raiz, eles eram criados em partições de unidades de dados por meio do Advanced Disk Partitioning (ADP).

NetApp AFX remove agregados físicos da equação e, como resultado, elimina a necessidade de agregados raiz e do uso do ADP. Os volumes raiz ainda são um conceito, mas agora residem em áreas virtualizadas do pool de capacidade e não exigem configuração adicional. Além disso, a funcionalidade do volume raiz foi alterada. As imagens de inicialização e os bancos de dados de cluster replicados foram movidos da pilha de storage para uma mídia de inicialização integrada em cada nó AFX. Agora, se o acesso à pilha de storage for perdido, os nós ainda podem inicializar e manter a elegibilidade para o cluster, o que simplifica a solução de problemas.

Mídia de inicialização integrada

NetApp AFX nodes utilizam mídia de inicialização integrada, que é um dispositivo M.2 conectado via NVMe com aproximadamente 3,8 TB de capacidade. Esses dispositivos de inicialização contêm arquivos de imagem de inicialização e bancos de dados replicados que são separados dos gabinetes de armazenamento, o que proporciona redundância extra em caso de problemas de acesso ao disco. Se a mídia de inicialização falhar, o nó será assumido pelo seu parceiro de HA e a mídia de inicialização poderá ser substituída. Após a substituição, uma nova imagem ONTAP será carregada no dispositivo por um administrador de storage e o ONTAP reconstruirá automaticamente o banco de dados do cluster para restaurar a funcionalidade completa.

Desempenho

NetApp AFX foi desenvolvido com foco em desempenho e escalabilidade, sendo especificamente voltado para cargas de trabalho que exigem alta taxa de transferência de leitura e gravação e que podem fornecer escalabilidade simples e linear.

Desempenho por nó

Cada nó de storage NetApp AFX fornece uma quantidade específica de throughput para leituras e gravações. À medida que nós são adicionados ao cluster, eles aumentam linearmente esse desempenho, conforme abordado na seção "Escalamento linear do desempenho do nó" deste documento.

Atualmente, os tipos de nós são "[AFX 1K](#)" e fornecem taxas de transferência para leitura e gravação aproximadamente nos valores abaixo. À medida que novos hardwares forem disponibilizados para NetApp AFX, esses limites poderão ser alterados. NOTA: O desempenho máximo foi alcançado utilizando vários clientes lendo e gravando vários arquivos, conforme mostrado na seção "[Resultados do benchmark](#)" abaixo.

Estimativas de desempenho por nó

Tipo de nó	Desempenho máximo de leitura	Desempenho de gravação máximo
AFX 1K	~35GB/s	~10GB/s



Para obter as estimativas de desempenho mais recentes, consulte sua equipe de vendas NetApp.

Desempenho por prateleira

Cada prateleira contém módulos de prateleira de alto desempenho com 16 portas Ethernet de 100 GB que utilizam a comunicação RoCEv2 para interação de storage de alta largura de banda com os nós de computação no cluster. Como qualquer recurso físico, essas prateleiras têm máximos que podem ser alcançados – principalmente porque NetApp AFX pode apresentar vários nós apontando para o mesmo conjunto de discos. A tabela a seguir mostra o desempenho máximo estimado de leitura e gravação para uma única prateleira para unidades TLC e QLC. Para obter mais informações sobre as diferenças entre TLC e QLC, consulte "[TLC vs. QLC](#)".

Estimativas de desempenho por prateleira

Tipo de módulo de prateleira	Desempenho máximo de leitura	Desempenho de gravação máximo
NSM 140	140GB/s (TLC e QLC)	70GB/s TLC 35GB/s QLC



Para obter as estimativas de desempenho mais recentes, consulte sua equipe de vendas NetApp.

Densidade de performance

Desacoplar os nós de storage dos shelves na arquitetura ONTAP desagregada permite que mais nós direcionem o tráfego para menos shelves, o que ajuda a reduzir a área total do datacenter necessária para obter o máximo desempenho com apenas a capacidade de que você precisa.

Esse conceito de "densidade de desempenho" permite que os administradores de storage aproveitem ao máximo o hardware disponível, sem precisar superdimensionar o ambiente de storage.

Por exemplo, em um cluster ONTAP unificado, como cada nó possui seu próprio conjunto de discos, o desempenho é direcionado apenas aos discos pertencentes ao nó e, como apenas um nó pode acessar um conjunto de discos, ele não pode necessariamente saturar os discos disponíveis e atingir seu desempenho máximo.

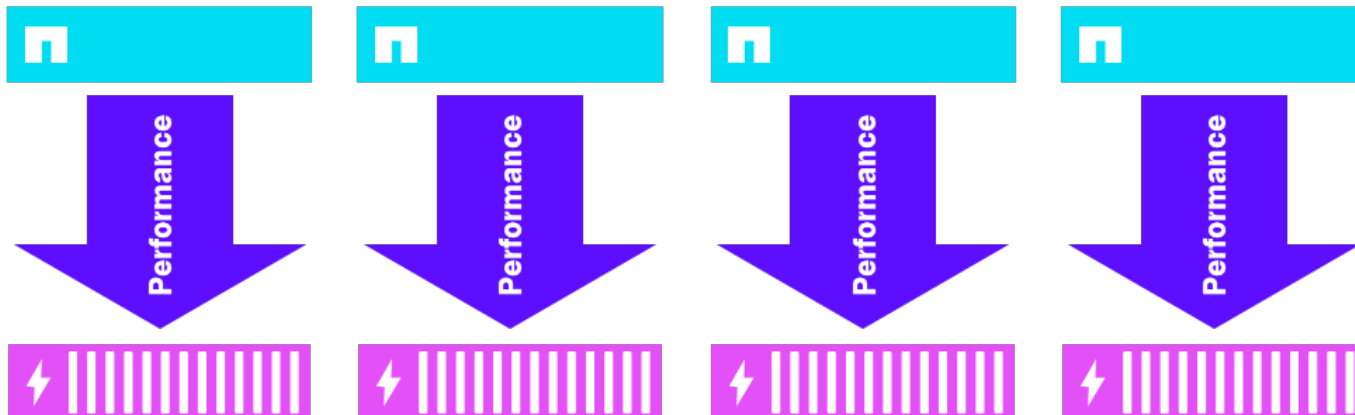
Unified ONTAP – Como o desempenho é distribuído

Unified ONTAP – A90

4 nodes, 4 shelves, 80GB/s read, 17.2GB/s write*

Per node

~20GB/s reads
~4.3GB/s writes



*internal benchmarks using elbench

NetApp AFX agrupa todos os discos em uma única Storage Availability Zone, permitindo que todos os nós utilizem todos os discos. E como os discos e os nós são independentes, você não precisará de tantas shelves para obter o mesmo desempenho. Isso condensa o desempenho e maximiza o potencial máximo de desempenho da shelf.

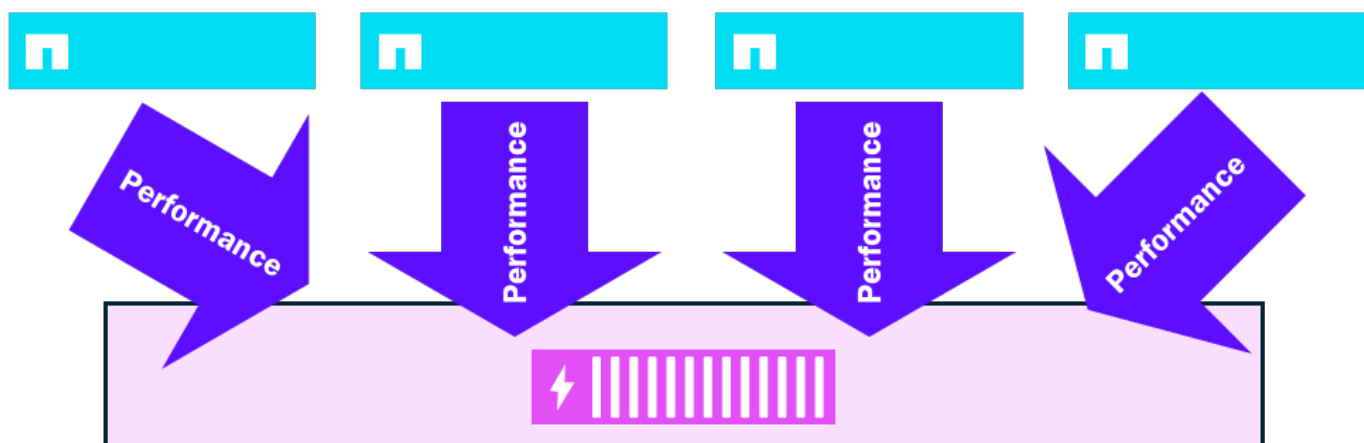
NetApp AFX – densidade de desempenho

NetApp AFX

4 nodes, 1 shelf, 140GB/s read, 40GB/s write*

Per node

~35GB/s reads
~10GB/s writes



*internal benchmarks using elbench

Relações nó-prateleira

Os nós Unified ONTAP exigem pelo menos um conjunto de discos por nó e podem ter várias gavetas conectadas a um único nó. Consequentemente, podem ocorrer gargalos de desempenho no nó individual, que pode não ser capaz de saturar seus próprios discos.

NetApp AFX apresenta todos os gabinetes de discos a todos os nós. Cada gabinete contém módulos com 16 x 100GB interfaces compatíveis com RoCE para aumentar a quantidade total de desempenho permitida por gabinete. Devido a isso, você pode saturar um único gabinete com vários nós que estarão lendo e gravando no mesmo conjunto de discos.

A partir do ONTAP 9.19.1, a proporção de saturação nó:prateleira é de aproximadamente 4:1.

Resultados de benchmark

A seção a seguir aborda os resultados de benchmark usando um cluster AFX NetApp com os seguintes parâmetros de configuração.

- 4 nós, 4 interfaces de dados
- 2 prateleiras (discos de 7,6TB)
- ONTAP 9.19.1
- NFSv4.2 (pNFS, trunking de sessão)
- Volume FlexGroup
- "EIBencho" benchmark
- Gravações: `elbencho --hosts=x.x.x.[y-z] -d -w -b 1M -t 80 --iodepth 1 --direct -s 600g /fio_vol1/`
- Leituras: `elbencho --hosts=x.x.x.[y-z] -r -b 256k -t 80 --lat --iodepth 2 --direct -s 600g --infloop /fio_vol1/`
- 4 servidores Cisco C240 M8, 2 portas * placas CX-7 de 200GbE, 80 threads
- Opções de montagem NFS: `rw,vers=4.2,rsz=1048576,wsz=1048576,tru=on,cache=on,proto=tcp`

A configuração acima atingiu um valor muito próximo do máximo de leituras disponível para o cluster de 4 nós (~134GB/s) e ficou exatamente no limite máximo de gravações permitidas por nó (40GB/s).

NetApp AFX – EIBencho desempenho de leitura, 4 nós



NetApp AFX – EIBencho desempenho de gravação, 4 nós



Leitura antecipada agressiva

Em fluxos de trabalho de streaming de mídia, um filme 4K é frequentemente dividido em dezenas de milhares de arquivos, cada um com tamanho típico entre 50 MB e 250 MB. Cada arquivo representa um quadro, e o aplicativo lê um quadro inteiro em uma única solicitação. Para manter um fluxo contínuo e sem interrupções, sem buffering visível, essas leituras de quadros devem ser concluídas sem perdas.

ONTAP oferece uma opção em nível de volume (`-aggressive-readahead-mode` para otimizar essas cargas de trabalho. A partir do ONTAP 9.19.1, um novo `cross_file_sequential_read` modo para leitura antecipada agressiva foi introduzido no AFX para acelerar cargas de trabalho com padrões de E/S previsíveis em tipos de arquivo semelhantes (por exemplo, renderização e streaming de mídia).

A função `cross_file_sequential_read` prevê o próximo arquivo a ser lido com base em seu nome e inicia a leitura antecipada desses arquivos antes que o cliente emita a chamada de leitura. A lógica de previsão pressupõe que todos os arquivos em um diretório seguem um padrão de nomenclatura com um sufixo numérico crescente (por exemplo, `arquivo1`, `arquivo2`, `arquivo3`). Todos os arquivos no diretório devem seguir esse padrão, usando numeração decimal ou hexadecimal. Os nomes de arquivo podem ter até 255 caracteres. A lógica é independente da extensão e gera o próximo conjunto de nomes de arquivo no diretório atual com base apenas no nome do arquivo atual. Se um nome de arquivo gerado anteriormente usando numeração em base 10 não existir no diretório, os nomes são regenerados usando numeração hexadecimal. Se nenhum dos nomes de arquivo gerados existir, nenhuma pré-busca é emitida para esse conjunto. A pré-busca é retomada quando a próxima leitura do cliente é emitida.

Com essas opções ativadas, "teste de quadro" benchmarks de desempenho conseguiram ler 30.000 quadros 4K a 30 quadros por segundo com 30 clientes (NFSv3 e SMB3) e 34 clientes (NFSv4.1), sem nenhuma perda de quadro.

Embora a leitura sequencial entre arquivos seja projetada principalmente para cargas de trabalho de mídia,

outras cargas de trabalho com grande volume de leitura e padrões de acesso e nomes de arquivos previsíveis - como treinamento e inferência de IA - também podem se beneficiar.

Considerações e ressalvas

- Cache de buffer compartilhado – A leitura antecipada agressiva usa o mesmo buffer cache que outros volumes no nó. Habilitá-lo pode afetar o desempenho de leitura de outros volumes nesse nó.
- Desempenho do armazenamento subjacente – Se os arquivos não puderem ser lidos com rapidez suficiente (por exemplo, em sistemas FAS baseados em HDD), os dados em cache podem ser removidos antes que a leitura do cliente ocorra, anulando os benefícios da leitura antecipada.
- Requisitos de padrão de acesso – Se o padrão de leitura da carga de trabalho não for sequencial, ou se os arquivos em um diretório não estiverem nomeados em ordem sequencial crescente, o modo de leitura antecipada agressiva `cross_file_sequential_read` não proporcionará benefícios significativos.

Melhorias de desempenho do NFSv4.x

A versão de NFS 3 tem sido um padrão de excelência para aplicações NFS por décadas – desde 1995, quando foi oficialmente lançada. Sua combinação de desempenho e resiliência tornou difícil considerar a migração para versões mais recentes de NFS, e com razão.

No entanto, o NFSv3 não está isento de limitações. A ausência de estado no protocolo, embora excelente para o desempenho e para minimizar interrupções em caso de failover de storage, não é tão boa para consistência de dados e gerenciamento de bloqueios. Um servidor NFS não mantém um registro dos estados de bloqueio, então, se ocorrer uma falha, o servidor NFS pode ou não liberar os bloqueios, e o cliente NFS pode não saber se um arquivo está bloqueado ou não.

Security for NFSv3 is also a bit lacking. The protocol requires multiple open firewall ports to function properly and numeric IDs are sent in plaintext over the wire. Furthermore, NFS does not have robust ACL support, and does not include native file and folder auditing. As a result of these limitations, NFSv4 was created in 2003 via [link:https://datatracker.ietf.org/doc/html/rfc3530](https://datatracker.ietf.org/doc/html/rfc3530)[RFC-3530^] (obsoleted in 2015 by [link:https://datatracker.ietf.org/doc/html/rfc7530](https://datatracker.ietf.org/doc/html/rfc7530)[RFC-7530^]). Embora o NFSv4.x exista há mais de 20 anos, ainda não houve ampla adoção por alguns motivos.

- Complexidade do gerenciamento de identidades: muitos ambientes não possuem uma infraestrutura de serviço de nomes implementada para aproveitar adequadamente os requisitos de string de nome e de segurança Kerberos no NFSv4.x.
- Necessidade de clientes NFS mais recentes: essa preocupação é menos urgente nos ambientes NFS modernos de hoje, à medida que nos distanciamos da data de lançamento inicial do NFSv4. Quase todos os sistemas operacionais atualmente em uso incluem clientes NFS com suporte completo ao NFSv4, mas ainda existem sistemas legados que podem não ter os pacotes NFSv4.x necessários. De fato, alguns aplicativos ainda exigem o uso de versões mais antigas do NFS.
- Mentalidade de "em time que está ganhando não se mexe": as organizações de TI corporativas são notoriamente conservadoras na adoção de novas tecnologias – mesmo aquelas que existem há mais de 20 anos. E se a versão de NFS está funcionando bem, por que mudar?
- Preocupações com o desempenho: o desempenho de um protocolo com estado como o NFSv4.x ficou atrás do NFSv3 sem estado durante grande parte dos últimos 20 anos. No passado, o impacto no

desempenho muitas vezes superava os benefícios do NFSv4.x.

Melhorias no NFSv4.x no ONTAP 9.18.1 usando AFX

Algumas mudanças arquitetônicas no ONTAP proporcionaram um aumento de desempenho muito necessário ao NFS em geral e contribuíram significativamente para a melhoria do desempenho do NFSv4.x de forma geral.

A seguir está um resumo de alto nível de algumas dessas mudanças.

Aprimoramento de leitura sequencial: NFSv4.1 30% melhor que NFSv3

ONTAP 9.18.1 introduz suporte para multipath IO com NFSv4.1. Em vez de processar leituras do sistema de arquivos WAFL, o MPIO transfere as operações de leitura para um domínio de rede para serem atendidas de maneira segura para multipath. Essa abordagem reduz as trocas de contexto, proporcionando maior paralelismo geral no tráfego de leitura sequencial, além de reduzir a sobrecarga do gerenciamento de buffers ao ignorar WAFL.

Aprimoramento de leitura aleatória para FlexGroup volumes: NFSv4.1 dentro de 7% do NFSv3

FlexGroup volumes são volumes que combinam vários volumes constituintes subjacentes e os apresentam como um único namespace unificado. No AFX, volumes FlexGroup têm o Balanceamento Avançado de Capacidade habilitado por padrão, o que grava arquivos maiores que 10GB em vários volumes constituintes como arquivos multipartes. Devido à localização remota dessas partes de arquivo, as leituras aleatórias tradicionalmente apresentavam uma pequena desvantagem de desempenho com NFSv4.x (cerca de 18% a menos que NFSv3). ONTAP 9.18.1 introduz suporte para IO em cache para leituras multipartes com NFSv4.x para ajudar a resolver isso. NOTA: Esta alteração não se aplica a volumes FlexVol.

Gravações sequenciais: melhoria de +10% em relação às versões anteriores

Uma melhoria na forma como replicamos os dados NVLOG usados para a funcionalidade de failover de alta disponibilidade aumentou o desempenho geral de gravação sequencial para NetApp AFX systems.

Operações de metadados: desempenho dentro de 15% do NFSv3 para benchmarks de EDA

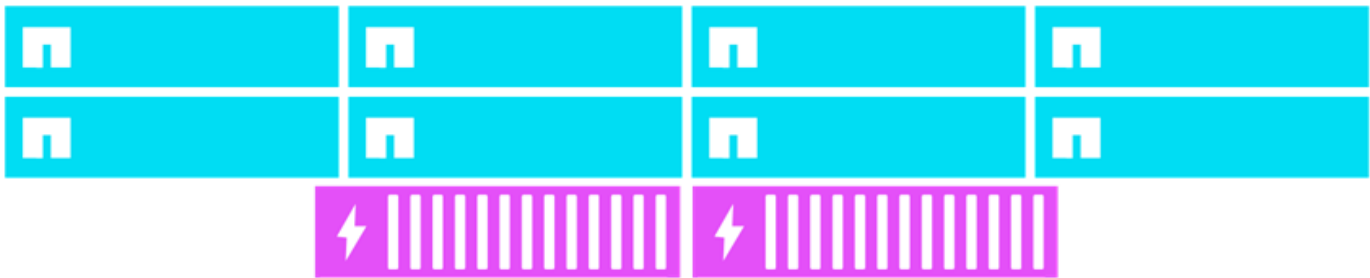
O NFSv4.1 tradicionalmente serializa todas as operações de OPEN e CLOSE, com um nó de cluster processando-as uma de cada vez antes que possam ser enviadas da rede para WAFL. ONTAP 9.18.1 introduz Concurrent Open Close (COC), que elimina a serialização de rede ao alterar a forma como as condições de corrida são resolvidas, removendo assim os gargalos de OPEN/CLOSE observados em versões anteriores.

Todas essas mudanças – juntamente com as alterações de arquitetura introduzidas no AFX – possibilitaram a melhoria do desempenho geral do NFSv4.1 no ONTAP 9.18.1.

Resultados de IO sequencial

Uma das áreas em que foram observadas melhorias modestas de desempenho foi na E/S sequencial (ou seja, E/S previsível e emitida consecutivamente). Em testes de desempenho padrão usando fio, o AFX executando ONTAP 9.18.1 apresentou uma melhoria de quase 30% no desempenho de leitura sequencial e de 10% no desempenho de gravação sequencial.

NetApp AFX – desempenho de E/S sequencial NFSv4.1 no ONTAP 9.18.1



	AFX 9.17.1	AFX 9.18.1
Seq. reads	220GB/s	283GB/s
Seq. writes	70.6GB/s	77.7GB/s

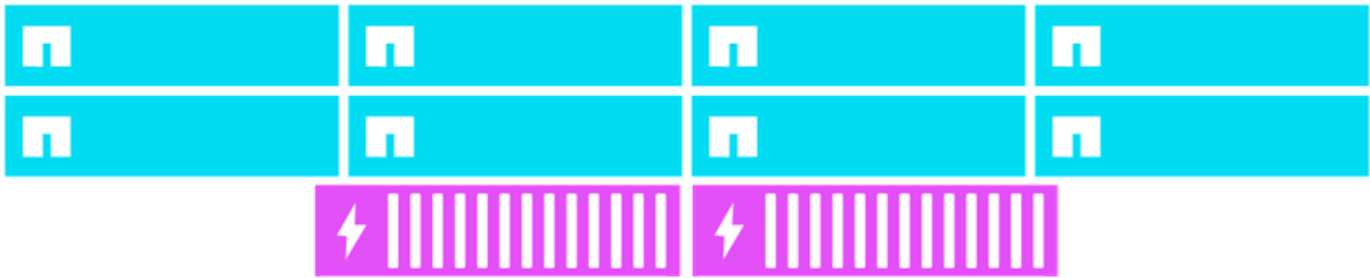
Resultados de carga de trabalho com grande volume de metadados

Ainda mais impressionantes são as melhorias em um dos principais pontos fracos de desempenho do NFSv4.x – metadados. Trata-se de operações de IO aleatórias, geralmente na faixa de 4K, usadas para gerenciar proprietários e atributos de arquivos, criar e listar arquivos, e assim por diante. Devido à natureza stateful do NFSv4.x, esses tipos de operações tendem a consumir mais CPU e latência, o que, por sua vez, reduz o desempenho geral possível.

Com as alterações no AFX ONTAP 9.18.1, o desempenho do NFSv4.x para esses tipos de cargas de trabalho melhorou substancialmente e reduziu a diferença em relação ao desempenho do NFSv3 (em até 15%).

Nossas equipes de engenharia de desempenho compararam o desempenho de benchmarks padrão de IA para imagens, EDA e compilação de software e constataram ganhos significativos em relação à versão anterior do ONTAP.

NetApp AFX – desempenho de E/S de metadados NFSv4.1 no ONTAP 9.18.1



	9.17.1	9.18.1	Delta
AI Image processing	209 KIOPS	239 KIOPS	+16%
Software dev	600 KIOPS	950 KIOPS	+58%
EDA	480 KIOPS	881 KIOPS	+84%

Ferramentas de gerenciamento

Embora existam algumas diferenças arquitetônicas consideráveis na forma como o armazenamento é apresentado no NetApp AFX, o conjunto de recursos e a maneira como ONTAP é gerenciado permanecem praticamente inalterados. Isso é totalmente intencional. ONTAP é ONTAP e, sempre que possível, a curva de aprendizado deve ser mínima ou inexistente. E, neste caso, NetApp AFX ainda está executando ONTAP.

Gerenciamento – CLI

No NetApp AFX, a CLI é quase idêntica à oferecida pela CLI unificada do ONTAP. Os comandos ainda são executados, em sua maioria, no nível do cluster, enquanto ainda existem comandos em nível de nó que podem ser emitidos. Ainda existem diretórios de comandos de nível superior e subcomandos, assim como a conclusão de comandos por tabulação. Além disso, todos os mesmos atalhos da CLI funcionam (por exemplo, filtrar conteúdo usando `-fields`).

As únicas diferenças reais na NetApp AFX CLI dizem respeito ao que foi adicionado e ao que foi removido (conforme abordado na seção "" deste documento). Se um recurso (como agregados ou Metrocluster) foi removido, o comando CLI correspondente não estará mais disponível.

Além disso, sempre que novos recursos e funcionalidades forem adicionados ao NetApp AFX, novos comandos também estarão disponíveis. Por exemplo, o novo ["NetApp AI Data Engine \(AIDE\)"](#) add-on interage diretamente com um NetApp AFX cluster por meio da rede de backend do cluster. Como resultado, os `dcn` e `data-engine` diretórios de comandos são adicionados à NetApp AFX CLI.

A seguir, são apresentados os diretórios de comandos de nível superior disponíveis com privilégios de administrador em um NetApp AFX cluster. Os comandos adicionados recentemente estão em negrito.

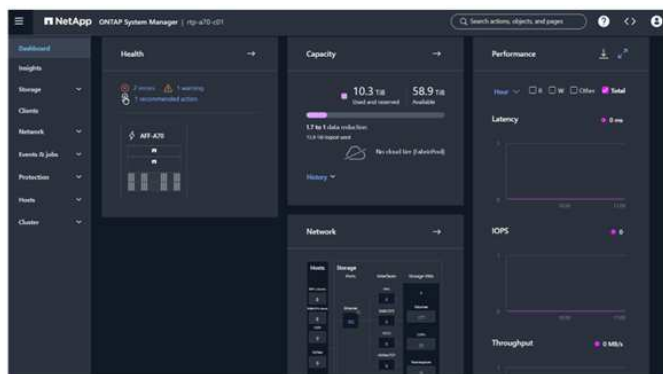
AFX::>

cluster	data-engine	dcn	event	exit
history	job	man	metrocluster	network
qos	redo	rows	run	security
set	snaplock	snapmirror	statistics	statistics-v1
storage	system	top	up	volume
vserver				

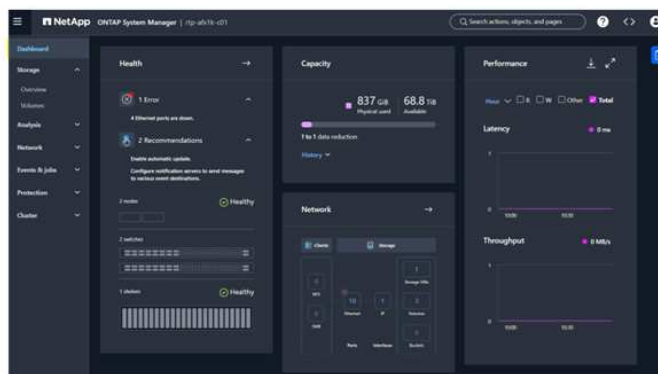
Gerenciamento – GUI

System Manager ainda é a interface GUI para interagir com NetApp AFX clusters para gerenciamento de recursos e, ao fazer login pela primeira vez, você provavelmente não perceberá à primeira vista que não está mais conectado a um sistema ONTAP unificado.

Comparação lado a lado das páginas iniciais unificadas do ONTAP e do NetApp AFX System Manager



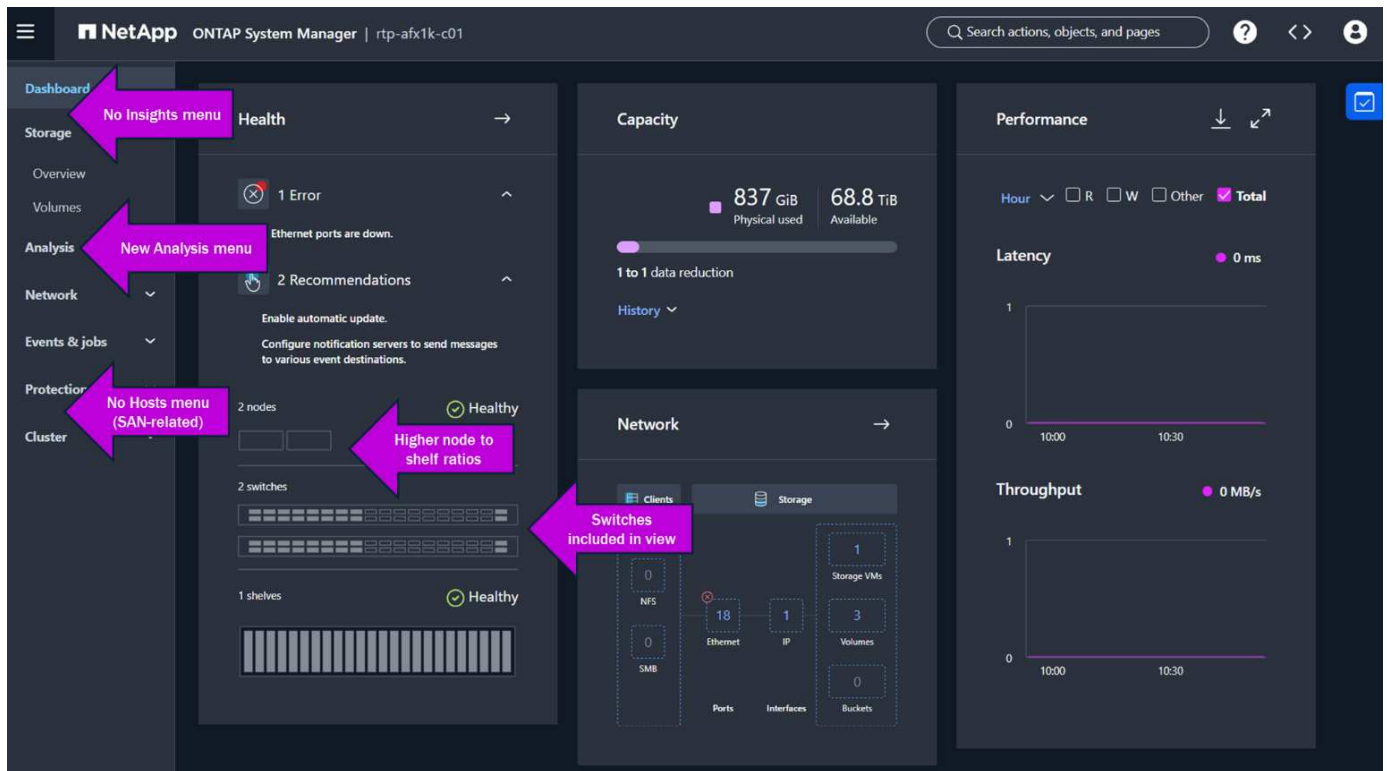
System Manager Dashboard view
Unified ONTAP



System Manager Dashboard view
NetApp AFX

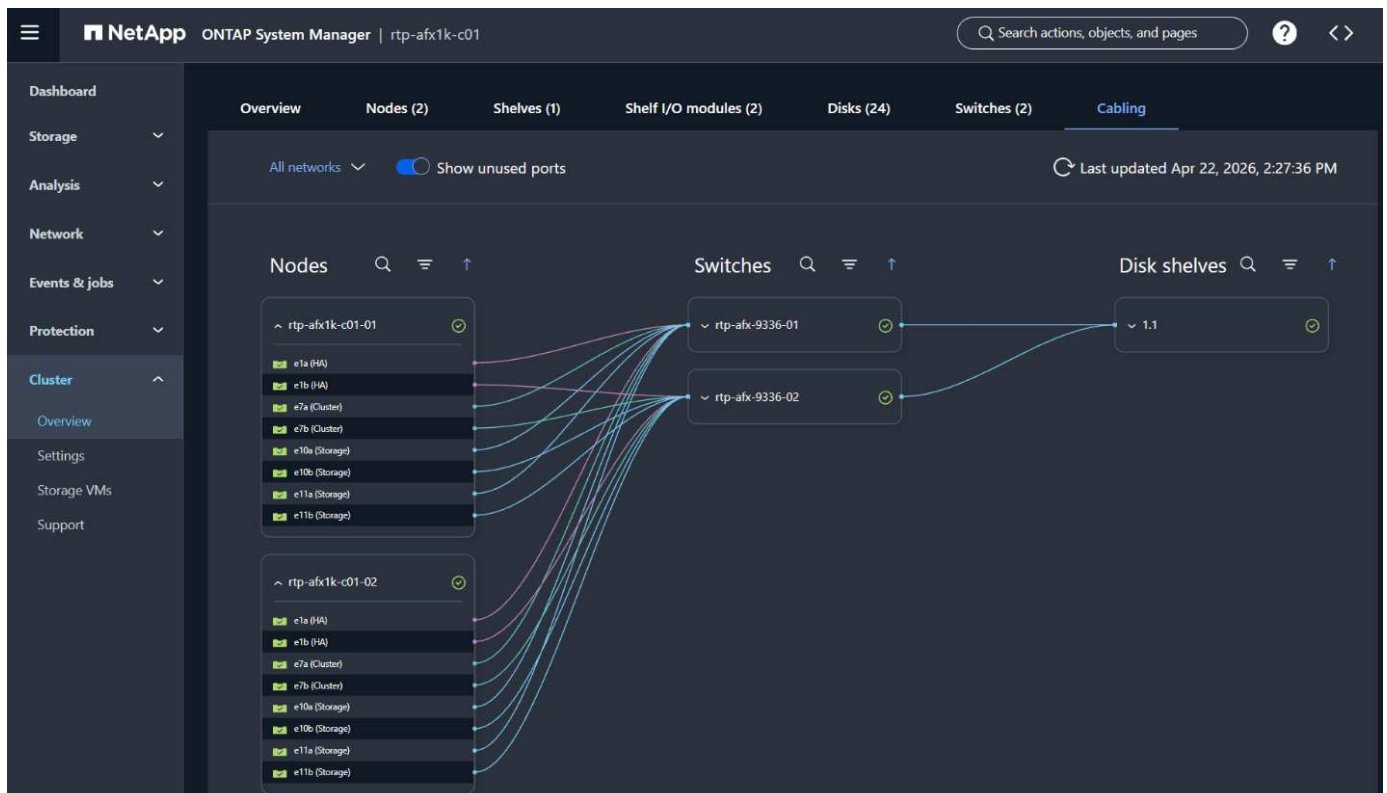
Como você pode ver acima, não há muitas diferenças óbvias no System Manager para unified ONTAP e NetApp AFX. Existem, no entanto, alguns indícios.

Como o NetApp AFX difere no System Manager



Ao explorar os menus e painéis, quase tudo permanece igual. Os volumes ainda mostram a capacidade usada e total. As interfaces de rede ainda mostram as portas e os endereços IP. Você ainda pode configurar políticas de proteção para SnapMirror. As visualizações de hardware ainda estão disponíveis. Mas NetApp AFX também aprimora um pouco as visualizações, oferecendo uma nova visualização de cabeamento, onde você pode detalhar e ver onde todos os cabos estão conectados em toda a pilha de storage.

NetApp visão da cablagem AFX



APIs REST

NetApp AFX também se esforça para manter a maioria das chamadas da API REST do ONTAP, o que significa que, se você criou um conjunto de ferramentas de automação baseadas na API REST, elas ainda poderão ser usadas na maioria dos casos. As principais exceções incluem agregados, Metrocluster, SAN e alguns contadores de desempenho. A documentação completa da API REST pode ser encontrada no System Manager do cluster NetApp AFX, acessando https://clus_mgmt_ip/docs/api.

Ferramentas de gerenciamento ONTAP off-box

NetApp AFX oferece algum suporte para ferramentas de gerenciamento off-box do ONTAP, tais como:

- NetApp System Manager
- NetApp Console
- Grafana Harvest (25.11.0 e posterior)
- NetApp Trident (25.10 e posterior)

NetApp AFX não oferece suporte atualmente a:

- NetApp ActiveIQ Unified Manager

Rede, segurança e operações

NetApp AFX oferece suporte à mesma pilha de rede, recursos de segurança, tecnologias de proteção de dados, operações não disruptivas e tipos de volume que o ONTAP unificado, com alguns ajustes exclusivos para a arquitetura desagregada.

Rede

A pilha de rede em NetApp AFX é idêntica à ONTAP unificada.

- Os LIFs de dados ainda são usados para apresentar endereços de rede a serviços internos e externos.
- Cada nó possui seu próprio conjunto de portas físicas e virtuais.
- VLANs, ifgroups e BGP ainda são suportados.
- As LIFs ainda podem realizar failover entre nós físicos e portas no cluster.
- Os espaços IP/domínios de broadcast permanecem configurados da mesma forma.
- Cada SVM pode ter sua própria rede de dados dedicada.
- As redes de gerenciamento podem ser segmentadas das redes de dados.
- As redes de dados dos clientes não sofrem alterações fora da nova adição do suporte a redes de 400 GB.
- Os switches do cluster de backend ainda são configurados por meio de um arquivo de "configuração padrão" fornecido por NetApp.

Algumas diferenças importantes entre as redes incluem:

- As portas de rede do cluster de backend agora suportam apenas conexões de 100GB com os switches do cluster.
- Como os switches do cluster são compatíveis com 400GB, as conexões dos nós de backend utilizam 4 x 100GB cabos breakout para reduzir o número de portas usadas nos switches.

- NVRAM agora é espelhada entre pares HA na rede do cluster de back-end por meio de uma nova configuração de VLAN HA nos switches.
- Uma nova rede DCN é adicionada por padrão para o AI Data Engine. Esses endereços IP são gerados automaticamente e podem ser alterados conforme necessário.

Segurança

NetApp AFX executa ONTAP, o que significa que utiliza a mesma segurança que ONTAP. Todos os criptomódulos são idênticos, o que significa que as certificações de segurança serão idênticas após a conclusão dos processos de certificação. NetApp AFX também aproveita o mesmo suporte para cifras de segurança que o ONTAP unificado.

Além disso, NetApp AFX oferece suporte a muitos dos recursos de segurança fornecidos pelo ONTAP unificado, incluindo (mas não se limitando a):

- Proteção autônoma contra ransomware
- Multilocação segura
- Criptografia em repouso (criptografia de volume) e em trânsito (TLS 1.3)
- Unidades de criptografia automática (SEDs)
- NFS e autenticação Kerberos SMB e criptografia
- Verificação multi-admin
- SnapLock

Para obter informações sobre as certificações que o unified ONTAP recebeu (bem como outras informações sobre reforço de segurança), consulte:

- ["Segurança de produtos NetApp"](#)
- ["Visão geral do fortalecimento da segurança do ONTAP"](#)

Snapshots e proteção de dados

NetApp AFX utiliza as mesmas tecnologias de snapshot e replicação que o ONTAP unificado, sem grandes alterações na forma como esses recursos funcionam. Na verdade, o AFX pode replicar de e para sistemas ONTAP unificados com o mesmo ["regras e configurações"](#) que você já conhece.

A única exceção no AFX para replicação diz respeito a volumes FlexGroup replicando para um sistema ONTAP unificado. Nesse caso, o sistema ONTAP unificado de destino deve estar executando ONTAP 9.16.1 ou posterior para fornecer suporte ao Advanced Capacity Balancing.

Operações não disruptivas

ONTAP oferece operações não disruptivas, como movimentação de volumes, atualizações, manutenção de clusters, failover de armazenamento e muito mais. NetApp AFX oferece as mesmas operações não disruptivas, com alguns ajustes.

- As mudanças de volume continuam sem causar interrupções, mas não exigem mais uma cópia.
- As falhas de armazenamento continuam sendo não disruptivas, mas após a falha inicial, os volumes são reequilibrados em todos os nós sobreviventes do cluster.
- As migrações LIF são idênticas.

- A manutenção e as atualizações de hardware são idênticas.

Tipos de volume

O Unified ONTAP suporta diversos tipos de volumes, tais como:

- FlexVols
- Volumes FlexGroup
- FlexCache
- FlexClone
- Buckets de objetos

NetApp AFX oferece suporte completo para cada um desses tipos de volume, bem como interoperabilidade total para volumes FlexCache com sistemas ONTAP unificados.

Para obter mais informações sobre como os volumes FlexGroup se beneficiam da arquitetura AFX, consulte ["FlexGroup melhorias no gerenciamento de volumes"](#).

Detalhes do hardware

A seção a seguir aborda detalhes sobre o hardware do cluster NetApp AFX. Para obter as informações mais recentes sobre o hardware NetApp AFX, consulte ["https://hww.netapp.com"](https://hww.netapp.com).

Hardware compatível

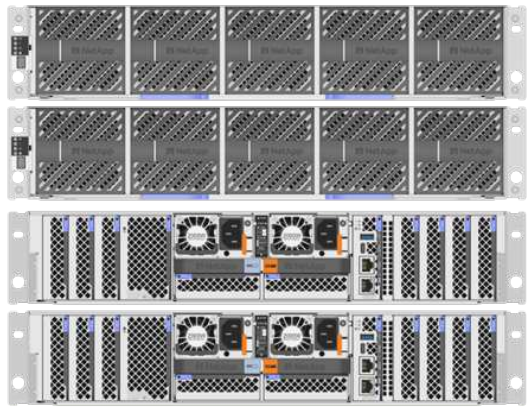
Para obter as informações mais recentes sobre o hardware compatível com NetApp AFX, consulte ["https://hww.netapp.com"](https://hww.netapp.com).

Nós

NetApp Os nós AFX são baseados no modelo AFF A1K de nós fornecido para clusters ONTAP unificados. Esses nós não possuem disco integrado para armazenamento e são projetados para serem modulares, permitindo a fácil adição e remoção de nós de acordo com os requisitos de desempenho. Cada nó ocupa 2U de espaço em rack e seu desempenho aumenta linearmente à medida que são adicionados a um cluster AFX.

NetApp detalhes do nó AFX 1K

AFX 1K



Processor/Memory (per HA pair)

- CPU: 208 cores, 52 cores per CPU, 4x1.7 Ghz
- RAM: 2048GB
- NVRAM: 128GB
- On-board NVMe 3.8TB boot device

I/O cards

- HA/cluster/storage (100GB only; 4x100GB breakout)
- Up to 400GB client data network
- 18x IO expansion per HA pair

Slots de hardware

NetApp AFX 1K nós utilizam as seguintes atribuições de slots.

- O slot 1 é dedicado à replicação de HA
- O slot 7 é dedicado à replicação do cluster
- Os slots 10 e 11 são dedicados à comunicação das prateleiras de storage

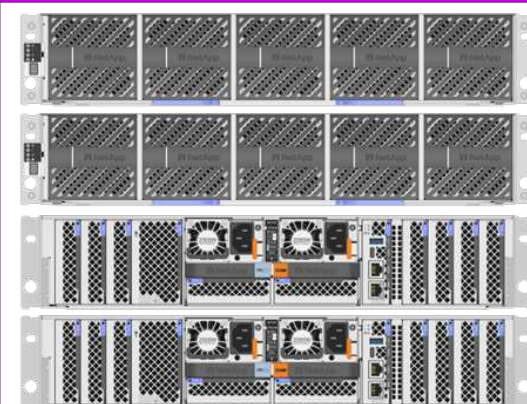
Prateleiras

NetApp AFX shelves utilizam os mesmos gabinetes que os sistemas AFF. A principal diferença nos shelves AFX está no módulo utilizado. Os módulos NSM140 oferecem recursos de desempenho aprimorados e ajudam a viabilizar o ONTAP desagregado. Algumas considerações importantes:

- Somente prateleiras totalmente abastecidas são suportadas.
- As prateleiras são detectadas automaticamente pelo NetApp AFX quando conectadas.
- Atualmente não há suporte para remoção de prateleiras.

NetApp detalhes do gabinete de prateleira AFX

AFX shelf enclosure



Enclosure

- 2U chassis
- 24 NVMe drives

NSM modules

- 2x NSM140 modules
- 16x 100GB ports (4x100GB breakout)
- RoCE connected
- Only switch connected
- Faster processor, more memory

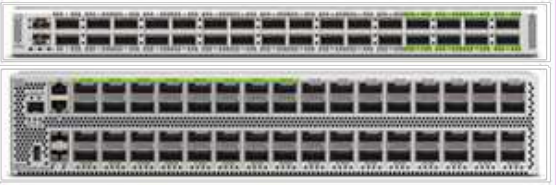
Switches

NetApp AFX ainda utiliza switches de cluster de backend para comunicação intracluster, como replicação de banco de dados de cluster, operações remotas de dados, operações de storage e espelhamento de NVRAM. Funcionalmente, as únicas diferenças entre o ONTAP unificado e os switches de cluster NetApp AFX são:

- Suporte a 400GbE
- Nova VLAN de HA
- Para obter mais informações, consulte o "[Cisco datasheet](#)".

NetApp switches de cluster AFX

AFX storage switch



The image shows two Cisco storage switches. The top switch is a Cisco 9332, a 1U model with 32 ports. The bottom switch is a Cisco 9364, a 2U model with 64 ports. Both switches feature 400-Gigabit QSFP-DD ports and 4 x 100GB breakout support.

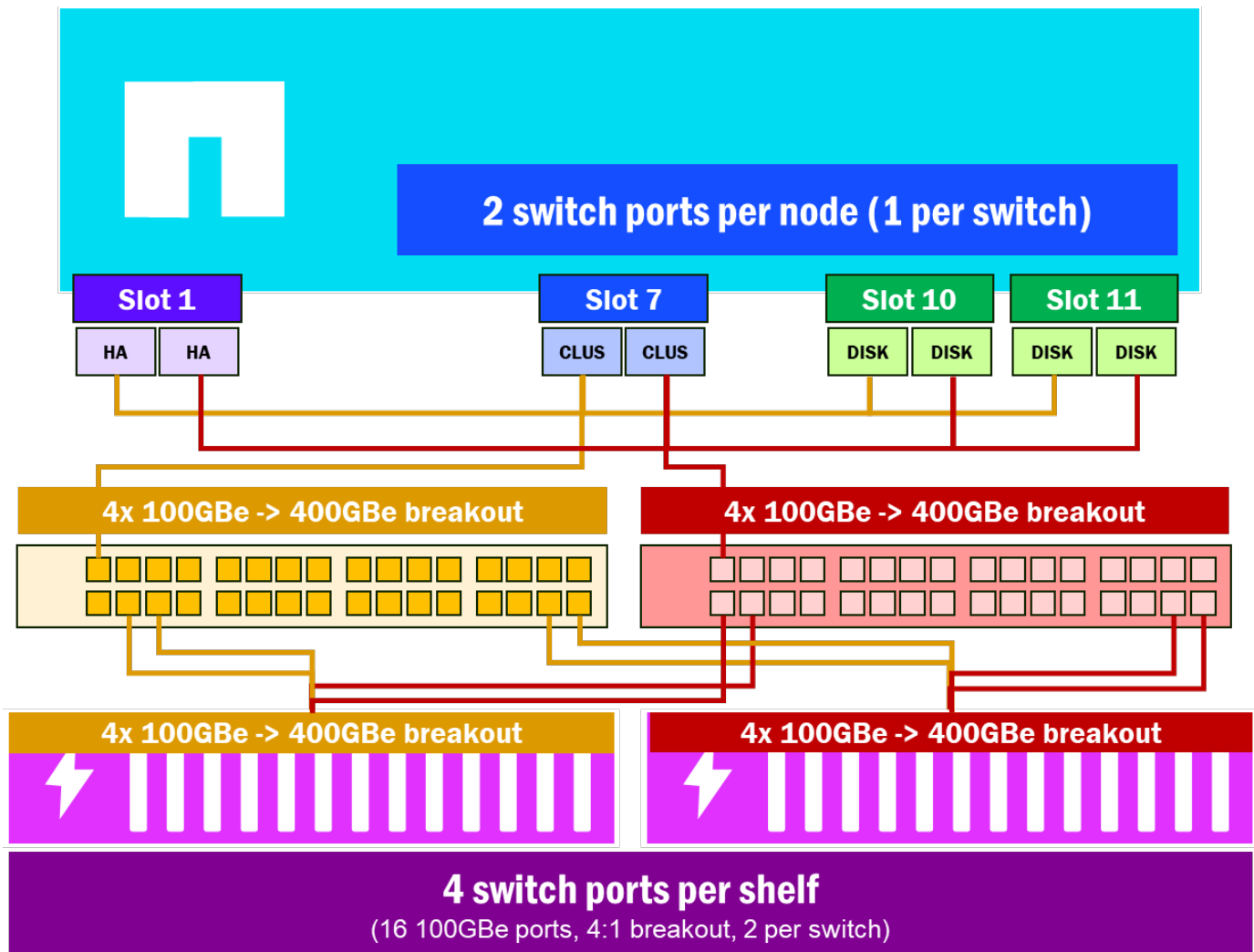
Switch details

- Cisco 9332 (32 ports, 1U) or 9364 (64 ports, 2U)
- 400-Gigabit QSFP-DD ports (32 or 64)
- 4 x 100GB breakout support
- MACsec encryption support
- 120MB memory buffer
- 32GB system memory
- 6 CPU cores

Conectividade do switch de cluster

NetApp AFX utiliza amplamente switches de cluster de backend para muitos de seus principais conceitos arquitetônicos. Por exemplo, interfaces de cluster, adaptadores de storage, gavetas de storage e placas NVRAM se conectam aos switches de cluster. Atualmente, todas essas interfaces suportam apenas comunicação de 100GB, enquanto os switches suportam 400GB. Como resultado, as interfaces de 100GB se conectam às interfaces de 400GB no switch por meio de 4 cabos breakout de 100GB. Essa abordagem reduz o número de portas utilizadas nos switches. Por exemplo, 16 portas de módulos de gaveta de storage de 100GB utilizarão apenas 4 portas nos switches, enquanto as 8 portas totais nos nós utilizam 2 portas de switch.

NetApp cabeamento para switches AFX



Tipos e tamanhos de discos

NetApp AFX atualmente suporta apenas SSDs NVMe conectados nos seguintes tamanhos:

- 7,6 TB
- 15,3 TB
- 30,1 TB
- 60,6 TB

TLC vs. QLC

NetApp AFX pode aproveitar ambos os tipos de flash, TLC e QLC. Os drives de 7,6 TB e 15,3 TB são modelos TLC, enquanto os drives maiores que 30,1 TB serão QLC. Independentemente do tipo de mídia, os padrões de desempenho da certificação NVIDIA SuperPod podem ser atendidos.

Todos os discos usados com NetApp AFX são discos com classificação de desempenho, e tanto QLC quanto TLC terão desempenho quase idêntico em tráfego de leitura. QLC fica um pouco atrás no desempenho de gravação em comparação com TLC e pode apresentar um desgaste ligeiramente maior com cargas de trabalho de gravação intensiva.

Para obter números de desempenho, consulte ["Desempenho por prateleira"](#).

Ao escolher o tipo de unidade a ser utilizada, considere quais cargas de trabalho o armazenamento irá hospedar e as compensações envolvidas entre desempenho e densidade de capacidade.

Máximos e limites

A seção a seguir aborda os valores máximos e mínimos de um cluster NetApp AFX em comparação com unified ONTAP.

Para os limites mais recentes, consulte "[Hardware Universe](#)".

NetApp AFX valores máximos e mínimos

Limite	ONTAP unificado	NetApp AFX
Contagem de volumes (cluster)	• 30.000 (dependendo da plataforma)	• 30.000
Tamanho agregado	• 800 TB	• N/A
Contagem de nós	• 24	• 8 (9.17.1) • 32 (9.19.1RC1)
Capacidade total	• Dependente do nó e da unidade. Consulte "hwu.netapp.com/br/" para obter detalhes.	• 2PB (9.17.1) • 3PB (9.18.1RC1) • 16PB (versão 9.18.1GA) • 20PB (9.19.1RC0) • 32PB (9.19.1RC1)
Contagem de prateleiras suportadas	• 8 por par de HA • 192 por cluster	• 12 por cluster (9.18.1GA) • 17 por cluster (9.19.1RC0) • 25 por cluster (9.19.1RC1) (sem limitação de par de HA)
Número total de unidades suportadas	• 240 por par de HA • 2880 (24 nós)	• 288 por cluster (com base nos limites de contagem por prateleira; sem limitação de par de HA) • 408 por cluster (9.19.1RC0) • 600 por cluster (9.19.1RC1)
Tamanho do volume	• 300TB (FlexVol) • 60PB (FlexGroup)	• 300TB (FlexVol) • 60PB (FlexGroup)*
Número máximo de arquivos por volume	• 2 bilhões (FlexVol) • 400 bilhões (FlexGroup)	• 2 bilhões (FlexVol) • 400 bilhões (FlexGroup)

Limite	ONTAP unificado	NetApp AFX
Número máximo de arquivos por diretório (valor padrão de maxdirsiz 320MB)	• ~4 milhões (FlexVol) • ~2 milhões (FlexGroup)	• ~4 milhões (FlexVol) • ~2 milhões (FlexGroup)
SnapMirror transferências simultâneas	• 250	• 250
Número de qtrees	• 4096	• 4096
Número máximo de conexões TCP por nó	• 100.000	• 100.000
Número máximo de bloqueios por nó	• 3 milhões	• 3 milhões
Número máximo de interfaces de dados (cluster)	• 4096	• 4096
Número máximo de componentes – FlexGroup	• 200	• 200 • 512 em 9.19.1 RC1
Número máximo de LIFs intercluster	• 8	• 8
Número máximo de espaços IP	• 512	• 512
Número máximo de FlexCache por origem	• 100	• 100
Número máximo de FlexCache (nó)	• 400	• 400

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- ["Hardware Universe"](#)
- ["Página do produto AFX"](#)
- ["Construindo a empresa impulsionada por IA: por que a infraestrutura é importante"](#)
- ["Blog: decidindo entre NFSv3 e NFSv4.X"](#)
- ["Ficha técnica AFX"](#)

Relatórios técnicos da ONTAP SnapCenter

O SnapCenter fornece uma plataforma unificada para proteção de dados consistente com aplicações e gerenciamento de clones. O SnapCenter simplifica o gerenciamento do ciclo de vida de backup, restauração e clone com workflows integrados na aplicação. Com gerenciamento de dados baseado em storage, o SnapCenter aumenta a performance e a disponibilidade e reduz o tempo de desenvolvimento e teste.



Esses relatórios técnicos expandem a "[SnapCenter](#)" documentação do produto.

SnapCenter para Oracle

["TR-4700: Plug-in SnapCenter para práticas recomendadas de banco de dados Oracle"](#) O NetApp SnapCenter é uma plataforma unificada e dimensionável para proteção de dados consistente com Oracle que automatiza operações complexas com controle e supervisão centralizados. Saiba mais sobre as práticas recomendadas para a implantação de bancos de dados Oracle com o SnapCenter.

["TR-4964: Backup, restauração e clonagem de banco de dados Oracle com os Serviços SnapCenter"](#) Saiba como configurar os Serviços SnapCenter para fazer backup, restaurar e clonar bancos de dados Oracle implantados no Amazon FSX para armazenamento ONTAP e instâncias de computação EC2. Embora seja muito mais fácil de configurar e usar, os Serviços SnapCenter fornecem as principais funcionalidades disponíveis através da interface SnapCenter.

SnapCenter para Microsoft SQL Server

["TR-4714: Práticas recomendadas para Microsoft SQL Server usando NetApp SnapCenter"](#) Saiba como implantar com sucesso o Microsoft SQL Server no armazenamento NetApp usando o SnapCenter para proteção de dados.

SnapCenter para Microsoft Exchange Server

["TR-4681: Práticas recomendadas para Microsoft Exchange Server usando NetApp SnapCenter"](#) Saiba como implantar com sucesso o Microsoft Exchange Server no armazenamento NetApp usando o SnapCenter para proteção de dados.

SnapCenter para SAP HANA

["TR-4614: Backup e recuperação do SAP HANA com o SnapCenter"](#) SnapCenter é uma plataforma unificada e escalável para proteção de dados consistente com aplicações para SAP HANA e outros bancos de dados. SnapCenter oferece controle e supervisão centralizados, ao mesmo tempo que delega aos usuários a capacidade de gerenciar tarefas de backup, restauração e clonagem específicas de cada aplicação. Com SnapCenter, administradores de banco de dados e armazenamento aprendem a usar uma única ferramenta para gerenciar operações de backup, restauração e clonagem para uma variedade de aplicações e bancos de dados.

["TR-4926: SAP HANA no Amazon FSX for NetApp ONTAP - Backup e recuperação com o SnapCenter"](#) Saiba mais sobre as práticas recomendadas para proteção de dados SAP HANA no Amazon FSX for NetApp ONTAP e SnapCenter. Os tópicos incluem conceitos do SnapCenter, recomendações de configuração e workflows de operação, incluindo configuração, operações de backup e operações de restauração e

recuperação.

["TR-4667: Automatizando operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"](#) A clonagem de storage da SnapCenter e a opção de definir com flexibilidade as operações de pré-clonagem e pós-clonagem. Isso permite que os administradores de base do SAP acelerem e automatizem operações de cópia, clone ou atualização do sistema SAP. Saiba agora a opção de escolher qualquer backup instantâneo do SnapCenter em qualquer armazenamento primário ou secundário permite que você solucione seus casos de uso mais importantes, incluindo corrupção lógica, teste de recuperação de desastres ou atualização de um sistema SAP QA.

["TR-4719: Backup e recuperação da replicação do sistema SAP HANA com o SnapCenter"](#) Saiba como a tecnologia SnapCenter e o plug-in SAP HANA podem ser usados para backup e recuperação em um ambiente de replicação do sistema SAP HANA.

["TR-4667: Automatizando as operações de clonagem e cópia do sistema SAP HANA com o SnapCenter"](#) A capacidade de criar NetApp backups de Snapshot consistentes com aplicações na camada de storage é a base para as operações de cópia do sistema e clone de sistema. Os backups Snapshot baseados em storage são criados com o plug-in NetApp SnapCenter para SAP HANA e as interfaces fornecidas pelo banco de dados SAP HANA. O SnapCenter Registra os backups de Snapshot no catálogo de backup do SAP HANA para que os backups possam ser usados para restauração e recuperação, bem como para operações de clonagem.

Guia de endurecimento SnapCenter

["TR-4957: Guia de proteção de segurança para NetApp SnapCenter"](#) Saiba como configurar o SnapCenter para ajudar as organizações a cumprir os objetivos de segurança prescritos para a confidencialidade, integridade e disponibilidade do sistema de informações.

Relatórios técnicos de disposição em camadas do ONTAP

Com a solução de disposição em camadas de dados da FabricPool, a experiência de usuário geral da empresa em sistemas flash melhora e evita a dor da rearquitetura de aplicações para eficiência de storage. O FabricPool reduz o espaço físico do storage e os custos associados ao ambiente de um sistema. Os dados ativos permanecem em SSDs de alta performance. Os dados inativos são dispostos em camadas em storage de objetos de baixo custo, preservando a eficiência do storage.



Esses relatórios técnicos expandem a ["ONTAP FabricPool"](#) documentação do produto.

["TR-4598: Melhores práticas da FabricPool"](#) Saiba mais sobre os recursos, requisitos, implementação e práticas recomendadas para o FabricPool.

["TR-4826: Guia de recomendação NetApp FabricPool com StorageGRID"](#) Saiba mais sobre as práticas recomendadas para implantar e dimensionar o StorageGRID como um nível de capacidade para o ONTAP Component FabricPool. Este documento também abrange os principais recursos, requisitos, implementação e práticas recomendadas ao usar o StorageGRID.

["TR-4695: Disposição em camadas de storage de banco de dados com NetApp FabricPool"](#) Saiba mais sobre os benefícios e opções de configuração do FabricPool com vários bancos de dados, incluindo o Oracle Relational Database Management System (RDBMS).

Relatórios técnicos de virtualização da ONTAP

As soluções de virtualização da NetApp ajudam a fornecer o máximo valor de seus servidores. Com uma infraestrutura de servidor virtual responsiva baseada em sistemas flash ONTAP inovadores e de alto desempenho, você ganha a capacidade de acessar seus dados muito mais rapidamente. Sua infraestrutura virtual granular é dimensionada sem interrupção para vários petabytes de dados, fornecendo a performance necessária para o acesso compartilhado a vários workloads. O ONTAP ajuda a simplificar e reduzir a complexidade da implantação da infraestrutura de servidores virtuais com parcerias importantes, orientações de implantação, integração de aplicativos e design superior. O ONTAP fornece muitas práticas e soluções recomendadas para um ambiente de virtualização robusto, tanto no local quanto na nuvem.

Esses relatórios técnicos expandem a "[Ferramentas do ONTAP para VMware vSphere](#)" documentação do produto.

["TR-4597: VMware vSphere for ONTAP"](#) O ONTAP é uma solução de storage líder para ambientes VMware vSphere há quase duas décadas e continua adicionando recursos inovadores para simplificar o gerenciamento e reduzir custos. Este documento apresenta a solução ONTAP para vSphere, incluindo as informações mais recentes do produto e as práticas recomendadas, para simplificar a implantação, reduzir riscos e simplificar o gerenciamento.

["TR-4400: VMware vSphere Virtual volumes \(vVols\) com NetApp ONTAP"](#) O ONTAP é uma solução de storage líder para ambientes VMware vSphere há mais de duas décadas e continua adicionando recursos inovadores para simplificar o gerenciamento e reduzir custos. Este documento abrange os recursos do ONTAP para volumes virtuais do VMware vSphere (vVols), incluindo as informações mais recentes do produto e casos de uso, juntamente com práticas recomendadas e outras informações para simplificar a implantação e reduzir erros.

["TR-4900: Gerente de recuperação de site da VMware com NetApp ONTAP"](#) A ONTAP é uma solução de storage líder para ambientes VMware vSphere desde sua introdução ao data center moderno em 2002 e continua adicionando recursos inovadores para simplificar o gerenciamento e reduzir custos. Este documento apresenta a solução ONTAP para o VMware Site Recovery Manager (SRM), o software de recuperação de desastres (DR) líder do setor da VMware, incluindo as informações mais recentes do produto e práticas recomendadas para simplificar a implantação, reduzir riscos e simplificar o gerenciamento contínuo.

["Introdução à automação para ONTAP e vSphere"](#) A automação tem sido parte integrante do gerenciamento de ambientes VMware desde os primeiros dias do VMware ESX. A capacidade de implantar infraestrutura como código e estender práticas para operações de nuvem privada ajuda a aliviar as preocupações relacionadas a escalabilidade, flexibilidade, autoprovisionamento e eficiência. Este documento apresenta a solução ONTAP para automatizar o ambiente ONTAP e VMware vSphere.

["WP-7353: Ferramentas ONTAP para VMware vSphere - Segurança do produto"](#) Este documento descreve as técnicas e a tecnologia usadas para proteger as ferramentas do ONTAP para VMware vSphere 9.X contra ameaças existentes e emergentes em ambientes de produtos.

["WP-7355: Plug-in SnapCenter VMware vSphere - Segurança do produto"](#) Este documento descreve as técnicas e a tecnologia usadas para proteger o plug-in do NetApp SnapCenter para VMware vSphere 4.X contra ameaças existentes e emergentes em ambientes de produtos.

["TR-4568: Diretrizes de implantação do NetApp e práticas recomendadas de armazenamento para o Windows Server"](#) O Microsoft Windows Server é um sistema operacional de classe empresarial que abrange rede,

segurança, virtualização, nuvem, infraestrutura de desktop virtual, proteção de acesso, proteção de informações, serviços da Web, infraestrutura de plataforma de aplicativos e muito mais. Este documento se concentra no Microsoft Windows, com ênfase particularmente pesada na tecnologia de virtualização Hyper-V, incluindo as informações mais recentes sobre o produto e práticas recomendadas, para simplificar a implantação, reduzir riscos e simplificar o gerenciamento.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais de terceiros e licenças usadas no software NetApp.

ONTAP

["Aviso para ONTAP 9.16,1"](#) ["Aviso para ONTAP 9.16,0"](#) ["Aviso para ONTAP 9.15,1"](#) ["Aviso para ONTAP 9.15,0"](#) ["Aviso para ONTAP 9.14,1"](#) ["Aviso para ONTAP 9.14,0"](#) ["Aviso para ONTAP 9.13,1"](#) ["Aviso para ONTAP 9.12,1"](#) ["Aviso para ONTAP 9.12,0"](#) ["Aviso para ONTAP 9.11,1"](#) ["Aviso para ONTAP 9.10,1"](#) ["Aviso para ONTAP 9.10,0"](#) ["Aviso para ONTAP 9.9,1"](#) ["Aviso para ONTAP 9.8"](#) ["Aviso para ONTAP 9.7"](#) ["Aviso para ONTAP 9.6"](#) ["Aviso para ONTAP 9.5"](#) ["Aviso para ONTAP 9.4"](#) ["Aviso para ONTAP 9.3"](#) ["Aviso para ONTAP 9.2"](#) ["Aviso para ONTAP 9.1"](#)

ONTAP Mediador para configurações MetroCluster IP

["9.9.1 Aviso para o Mediador ONTAP para configurações MetroCluster IP"](#) ["9,8 Aviso para o Mediador ONTAP para configurações MetroCluster IP"](#) ["9,7 Aviso para o Mediador ONTAP para configurações MetroCluster IP"](#)

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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 DOCUMENTOS, 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.