Segurança

ONTAP Technical Reports

NetApp
January 23, 2026

Índice

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.

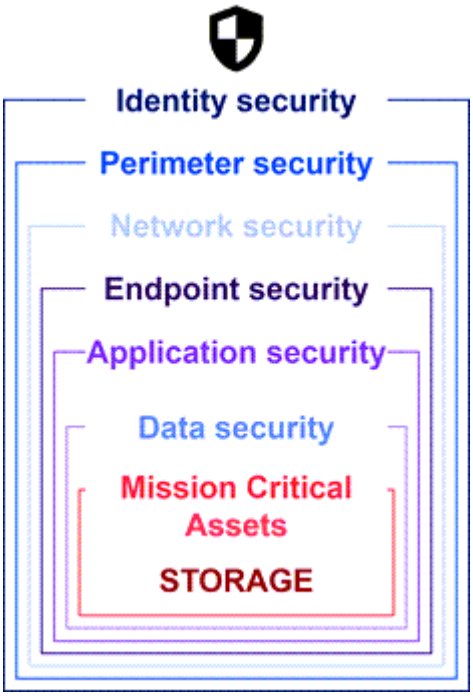
As organizações devem examinar toda a postura de segurança de perímetro, rede, identidade, aplicativo e onde os dados estão no nível de storage e proteger essas camadas. A adoção de uma abordagem centrada em dados à proteção cibernética na camada de storage é crucial no cenário de ameaças atual. Embora 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.

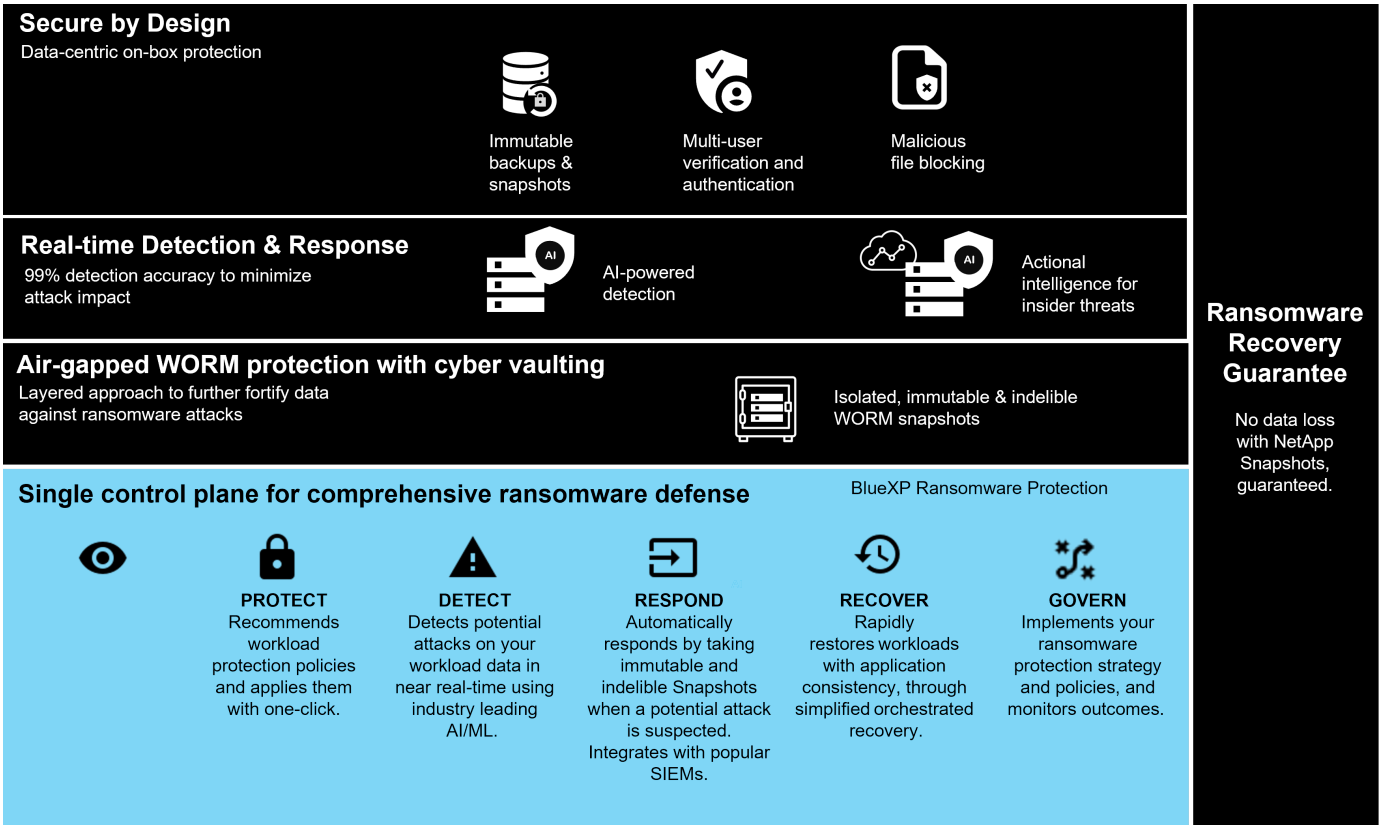
Proteção contra ransomware na camada de dados

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
- **Detecção 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.



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.

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.

O NetApp ONTAP atende ao requisito para a autenticação de CLI SSH baseada na Web "Autenticação multifator (MFA)" no Gerenciador de sistema.

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 detetar 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.

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 deteção 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 deteção 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 deteta criptografia de cabeçalho. A potência de IA e os sinais adicionais permitem que o ARP/AI forneça uma precisão de deteção 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 deteção, 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 deteção de ransomware em tempo real baseada em IA da NetApp atinge a classificação AAA"

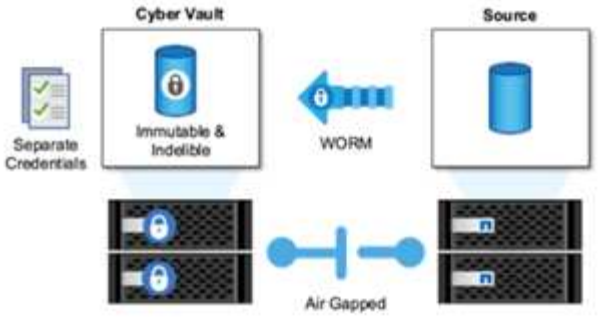
Proteção WORM com uso de cofres cibernéticos no ONTAP

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 indeléveis.

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, desconetar 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 on-line. 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.

Não só "Consultor digital da NetApp" pode ajudar "eliminar vulnerabilidades de segurança", mas também fornece insights e orientações específicos para a proteção contra ransomware. Um cartão de bem-estar dedicado mostra as ações necessárias e os riscos abordados, para que você possa ter certeza de que seus sistemas estão cumprindo essas recomendações de práticas recomendadas.

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.

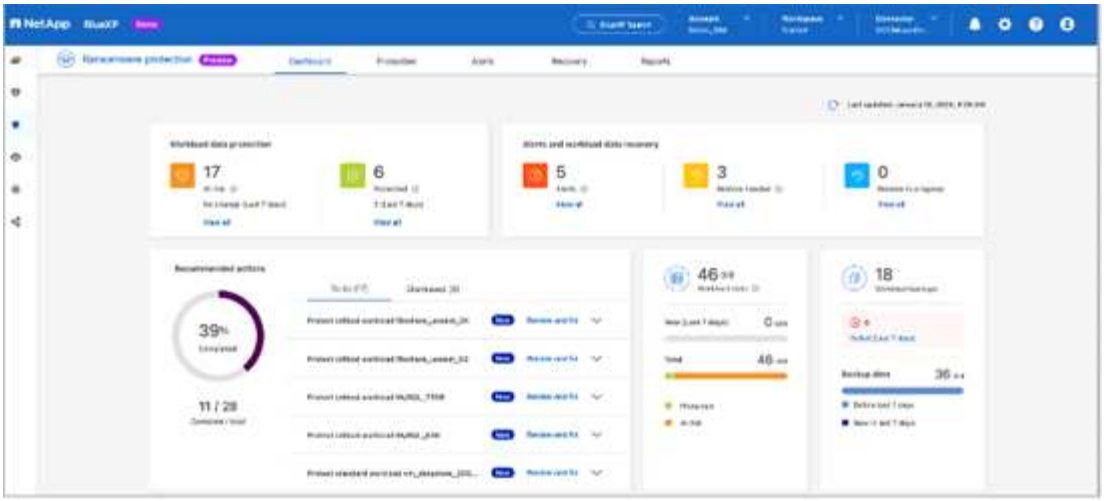
Para ver a proteção contra ransomware em ação, "Consultor digital"consulte .

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 que sua organização tem. As ameaças internas são a causa de 18% das violações de dados, de acordo com o 2022 "Relatório de investigações de violação de dados da Verizon". As organizações podem aumentar a vigilância com a implantação de controles de confiança zero líderes do setor relacionados aos 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.

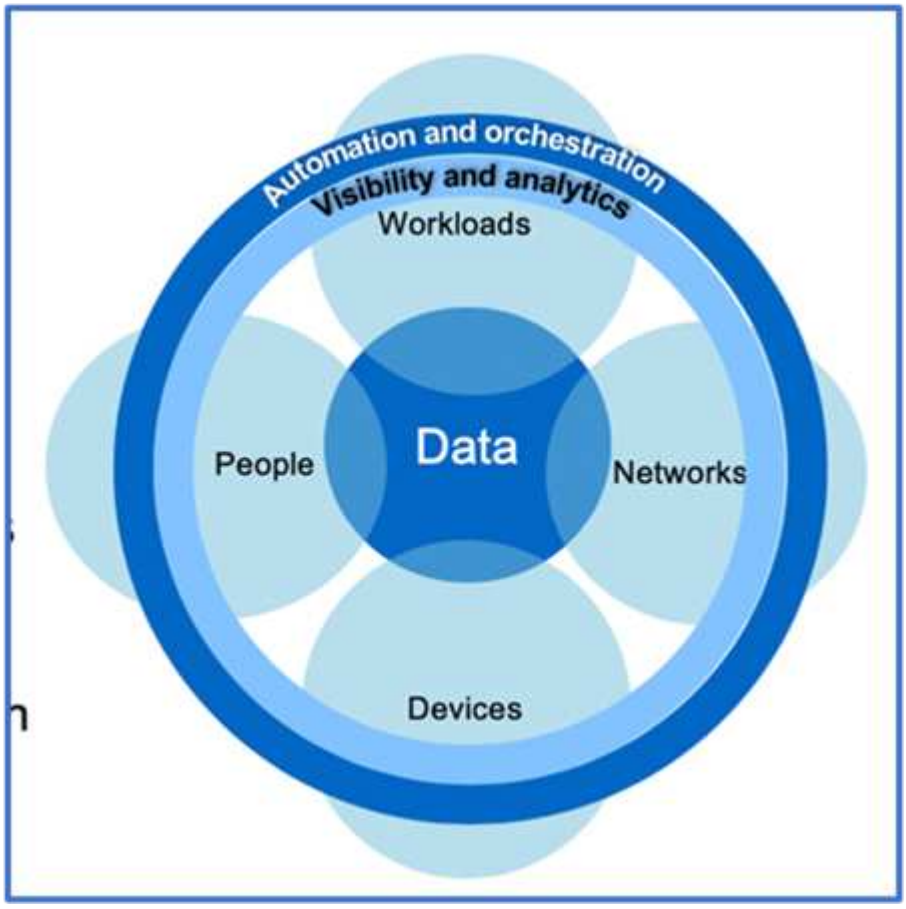
Recursos de segurança

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 próximos 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 sensíveis que não devem ser expostos fora de uma organização. A divulgação de dados tóxicos pode violar a conformidade regulatória e prejudicar a reputação de uma organização. Em termos de conformidade regulatória, os dados tóxicos incluem dados do titular do 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 o NetApp "NetApp Data Classification" (anteriormente conhecido como Cloud Data Sense), um kit de ferramentas baseado em IA para escanear, analisar e categorizar seus dados automaticamente.

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 indeléveis 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 de cluster, "Autenticação de vários fatores (MFA)" pode ser implantado para acesso à linha de comando ONTAP web administrative Access e Secure Shell (SSH). O MFA para acesso administrativo é um requisito para organizações do setor público dos EUA ou aquelas que precisam seguir o PCI-DSS. O MFA torna impossível para um invasor comprometer uma conta usando apenas um nome de usuário e senha. O MFA requer dois ou mais fatores independentes para autenticar. Um exemplo de autenticação de dois fatores é algo que um usuário possui, como uma chave privada, e algo que um usuário conhece, como uma senha. O acesso administrativo à Web ao ONTAP System Manager ou ao ActiveIQ Unified Manager é habilitado pela Security Assertion Markup Language (SAML) 2,0. O acesso à linha de comando SSH usa autenticação de dois fatores encadeada 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. Registo 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.

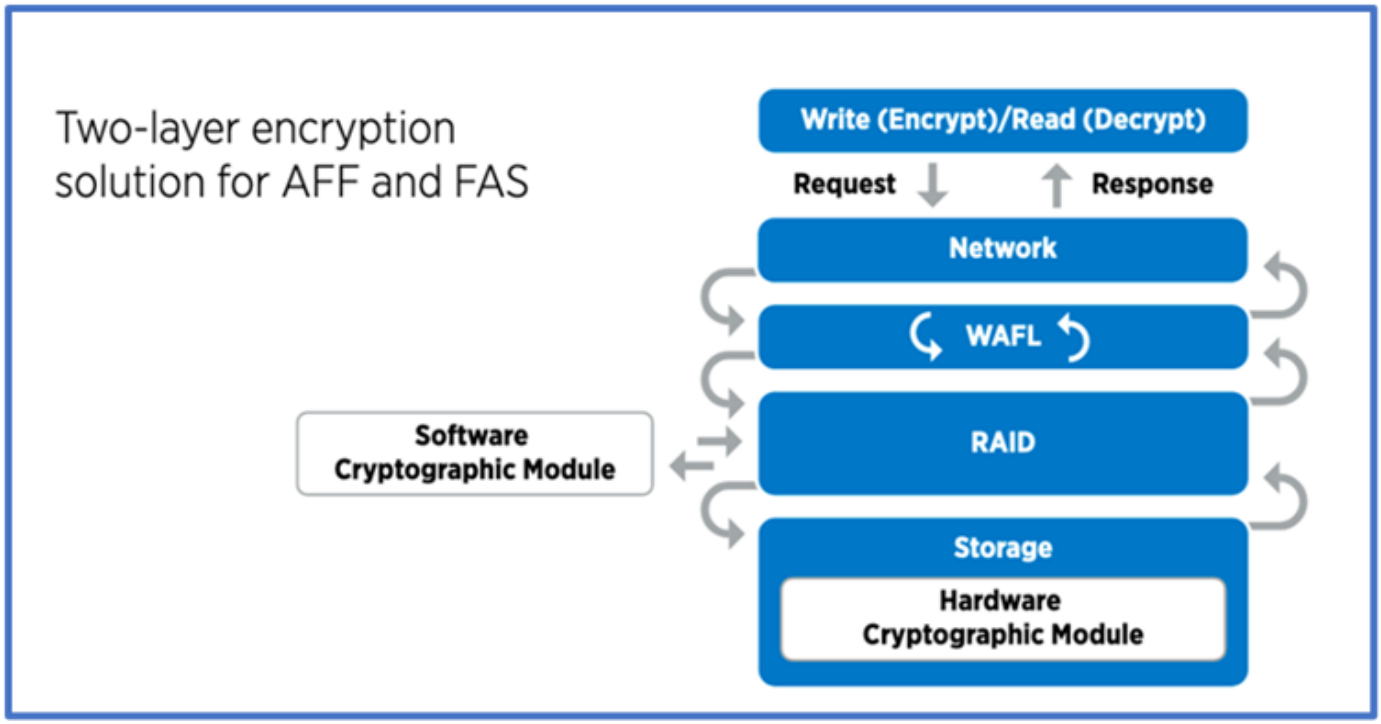
Uso de criptografia para dados em repouso e dados em trânsito

Criptografia de dados em repouso

Todos os dias, há novos requisitos para mitigar os riscos do sistema de storage e as lacunas de infraestrutura quando uma organização reutiliza unidades, retorna unidades com defeito ou atualiza "NetApp Storage Encryption (NSE) n.o 44; NetApp volume Encryption (NVE) n.o 44; e NetApp Aggregate Encryption" ajude você a criptografar todos os seus dados em repouso o tempo todo, seja tóxico ou não, sem afetar as operações diárias. "NSE" É uma solução de hardware ONTAP "dados em repouso"que utiliza unidades com autocriptografia validadas FIPS 140-2 nível 2. "NVE e NAE" São uma solução de software ONTAP "dados em repouso"que utiliza o "Módulo criptográfico NetApp validado FIPS 140-2 nível 1". Com NVE e NAE, os discos rígidos ou 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 em camadas que fornece redundância de criptografia e segurança adicional. Se uma camada for violada, a segunda camada ainda protege os dados. Esses recursos tornam o ONTAP bem posicionado para "criptografia pronta para quantum"o .

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.

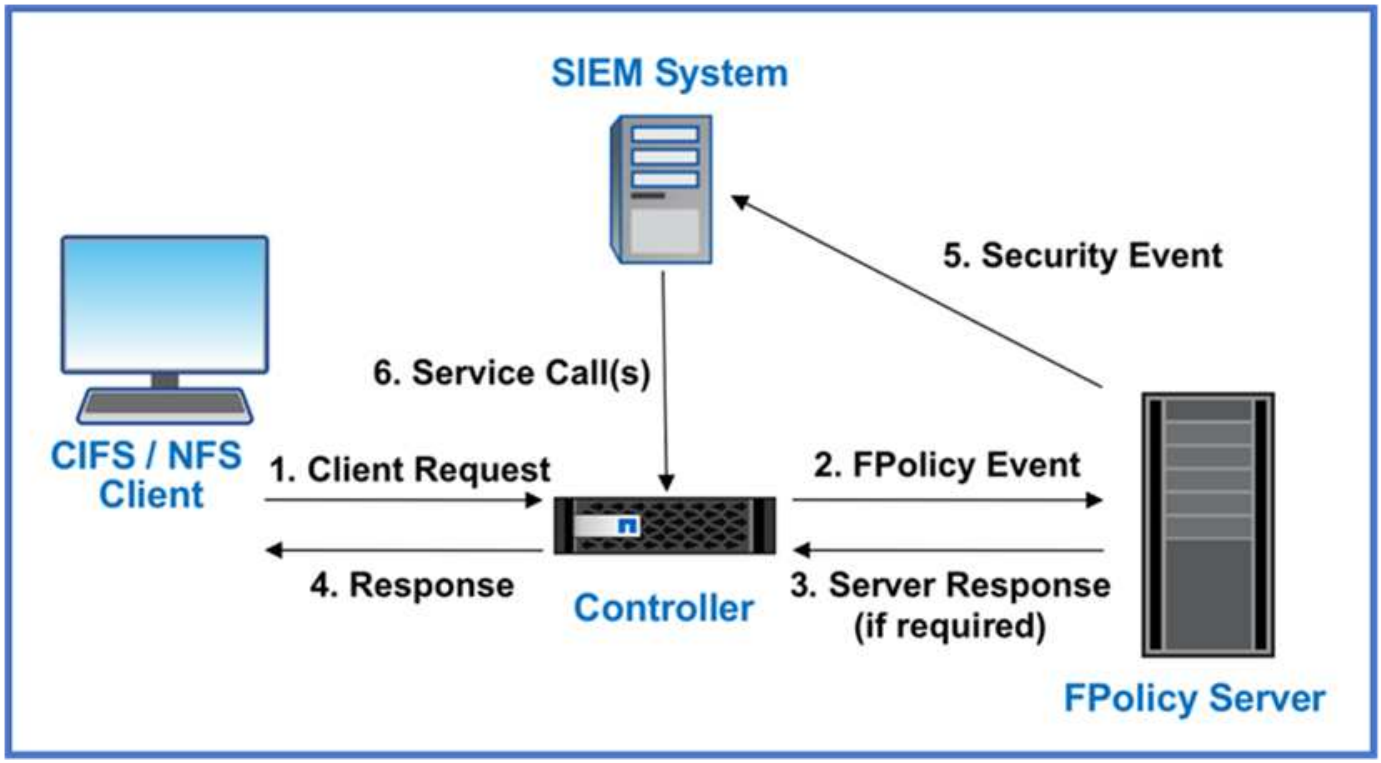
Criptografia de dados em trânsito

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 provisionamento de software de código aberto, gerenciamento de configurações e implantação de aplicações. Ele é executado em muitos sistemas Unix-like, e pode configurar tanto sistemas Unix-like como Microsoft Windows. Ele inclui sua própria linguagem declarativa para descrever

a configuração do sistema. Ansible foi escrito por Michael DeHaan e adquirido pela Red Hat em 2015. O Ansible está sem agente, conetando-se temporariamente remotamente por meio de SSH ou Gerenciamento remoto do Windows (permitindo a execução remota do PowerShell) para executar tarefas. O NetApp desenvolveu mais do que "150 módulos do Ansible para o software ONTAP"o , possibilitando ainda mais integração com a estrutura de automação do Ansible. Os módulos do Ansible para NetApp fornecem um conjunto de instruções para definir o estado desejado e reencaminhá-lo para o ambiente NetApp de destino. Os módulos são criados para dar suporte a tarefas como configuração de licenciamento, criação de agregados e máquinas virtuais de armazenamento, criação de volumes e restauração de instantâneos para citar alguns. Uma função do Ansible foi "Publicado no GitHub" específica do Guia de implantação de recursos unificados (UC) do NetApp DoD.

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.xatrs, 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 intercetar a solicitação de acesso do usuário e encaminhá-la para o PDP.

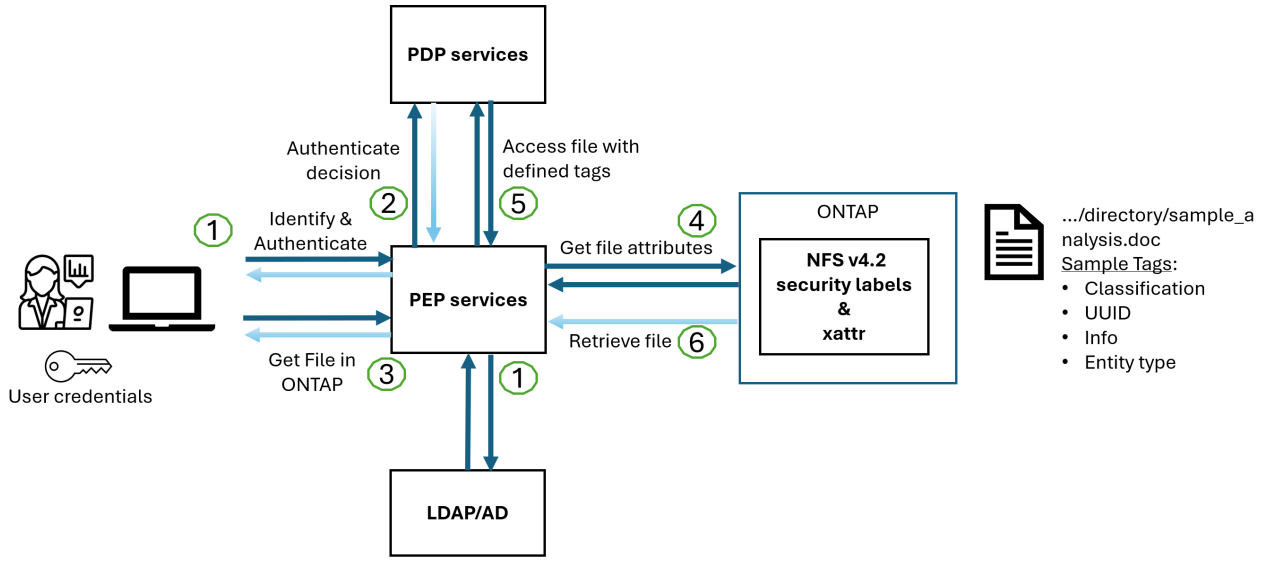
2. Em seguida, o PDP avalia essa solicitação em relação às políticas estabelecidas da ABAC.

   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 aspetos dos dados de arquivos, incluindo xatrs, sejam preservados e transferidos juntamente com o arquivo. Os xatrs 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 xatrs 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 xatrs 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 aspeto 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	{
	"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"
	}
	}

especificação	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

Chave	Valor

briefings	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizensaStatus	{
	"value": "US"
	}

folgas	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

CountryOfAffiliations	[
	{
	"value": "USA"
	}
	]

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	{
	"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"
	},

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"

Informações sobre direitos autorais

Informações sobre marcas comerciais