Sécurité

ONTAP Technical Reports

NetApp
January 23, 2026

Sommaire

Sécurité

Rapports techniques sur la sécurité ONTAP

ONTAP continue d'évoluer, et la sécurité fait partie intégrante de la solution. Les dernières versions d'ONTAP comprennent bon nombre de nouvelles fonctions de sécurité essentielles pour protéger les données de l'entreprise dans le cloud hybride, éviter les attaques par ransomware et se conformer aux pratiques recommandées par le secteur. Ces nouvelles fonctionnalités contribuent également à l'adoption d'un modèle « zéro confiance ».

Ces rapports techniques sont détaillés dans "Sécurité et chiffrement des données ONTAP"la documentation produit.

Cyber-coffre ONTAP

"Cyber-coffre ONTAP" Le cyber-coffre basé sur ONTAP de NetApp offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. En exploitant la « Air gapping » logique associée à des méthodologies de renforcement solides, ONTAP vous permet de créer des environnements de stockage isolés et sécurisés, résilients face aux cybermenaces en constante évolution. Avec ONTAP, vous pouvez assurer la confidentialité, l'intégrité et la disponibilité de vos données tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Attaques par ransomware

"Tr-4572 : la solution NetApp pour ransomware" Découvrez l'évolution des ransomwares et comment identifier les attaques, prévenir la propagation et restaurer les données aussi rapidement que possible grâce à la solution NetApp pour ransomware. Les conseils et solutions fournis dans ce document sont conçus pour aider les entreprises à disposer de solutions de cyberrésilience tout en respectant leurs objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

"Tr-4526 : stockage WORM conforme avec NetApp SnapLock"
De nombreuses entreprises ont recours au stockage des données WORM (Write Once, Read Many) pour respecter les exigences de conformité réglementaires, ou simplement pour ajouter une couche supplémentaire à leur stratégie de protection des données. Découvrez comment intégrer SnapLock, la solution WORM de ONTAP, dans des environnements qui nécessitent le stockage de données WORM.

Zéro confiance

"NetApp et le modèle « zéro confiance »" La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.

Authentification multifacteur

"Tr-4647 : guide d'implémentation et des bonnes pratiques pour l'authentification multifacteur dans ONTAP"
Découvrez la fonctionnalité d'authentification multifacteur d'ONTAP pour un accès administratif via System Manager, Active IQ Unified Manager et l'authentification CLI ONTAP Secure Shell (SSH).

"Tr-4717 : authentification ONTAP SSH avec une carte d'accès commune"
Découvrez comment configurer et tester des clients SSH tiers, en association avec le logiciel ActivClient, pour authentifier un administrateur de stockage ONTAP via la clé publique stockée sur une carte d'accès commun (CAC) lorsqu'elle est configurée dans ONTAP.

Colocation

"Tr-4160 : Colocation sécurisée dans ONTAP"
Découvrez comment implémenter la colocation sécurisée à l'aide des VM de stockage dans ONTAP, y compris les considérations de conception et les pratiques recommandées.

Normes

"Tr-4401 : PCI-DSS 4.0 et ONTAP"
Découvrez comment valider un système par rapport à la norme PCI DSS 4.0 et répondre aux exigences des contrôles que vous appliquez à un système NetApp ONTAP.

Contrôle d'accès basé sur les attributs

"Contrôle d'accès basé sur les attributs avec ONTAP" Apprenez à configurer les étiquettes de sécurité NFSv4.2 et les attributs étendus (xattrs) pour prendre en charge le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC), une stratégie d'autorisation qui définit des autorisations basées sur les attributs utilisateur, ressource et environnement.

Solution NetApp pour ransomware

Attaques par ransomware et portefeuille de solutions de protection de NetApp

Les ransomwares restent l'une des menaces les plus importantes qui ont entraîné des interruptions d'activité pour les entreprises en 2024. D'après le "Sophos : État des ransomware 2024", les attaques par ransomware ont affecté 72 % de leur public interrogé. Les attaques par ransomware ont évolué pour être plus sophistiquées et ciblées : les acteurs de menaces utilisent des techniques avancées, telles que l'intelligence artificielle, pour optimiser leur impact et leurs bénéfices.

Les entreprises doivent regarder l'ensemble de leur posture de sécurité du périmètre, du réseau, de l'identité, des applications et de l'emplacement des données au niveau du stockage, et sécuriser ces couches. L'adoption d'une approche axée sur les données en matière de cybersécurité au niveau de la couche de stockage est cruciale dans le paysage actuel des menaces. Bien qu'aucune solution ne puisse déjouer toutes les attaques, l'utilisation d'un portefeuille de solutions, notamment des partenariats et des tiers, offre une défense multicouche.

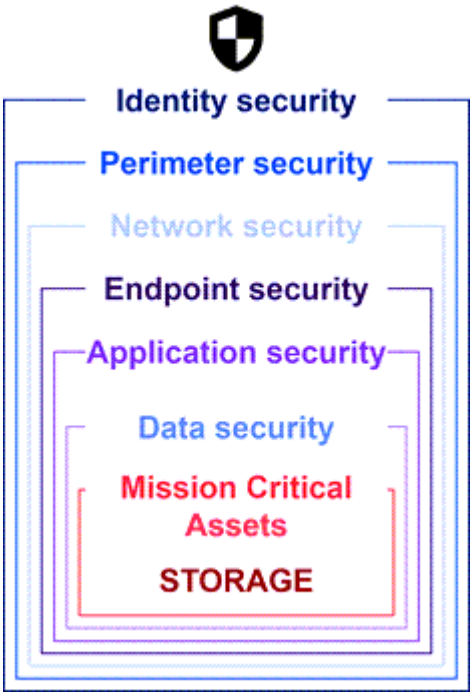
Le Gamme de produits NetApp fournit divers outils efficaces pour la visibilité, la détection et la résolution des problèmes, ce qui vous aide à détecter rapidement les ransomware, à prévenir la propagation et à restaurer rapidement, si nécessaire, pour éviter les interruptions coûteuses. Les solutions de défense à plusieurs

couches classiques restent répandues, tout comme les solutions tierces et partenaires pour la visibilité et la détection. Une solution efficace reste une partie essentielle de la réponse à toute menace. L'approche unique du secteur qui repose sur la technologie NetApp Snapshot immuable et la solution SnapLock Logical Air Gap est un atout concurrentiel dans le secteur et constitue la bonne pratique du secteur pour la résolution des problèmes par ransomware.

À partir de juillet 2024, le contenu du rapport technique *TR-4572: NetApp ransomware protection*, qui a été publié au format PDF, est disponible sur docs.netapp.com.

Les données sont la cible principale

Les cybercriminels ciblent de plus en plus directement les données, en reconnaissant leur valeur. Bien que la sécurité du périmètre, du réseau et des applications soit importante, il est possible de les contourner. La couche de stockage, qui se concentre sur la protection des données à la source, constitue une dernière ligne de défense critique. Les attaques par ransomware ont pour objectif d'accéder aux données de production et de les chiffrer ou de les rendre inaccessibles. Pour y parvenir, les attaquants doivent déjà avoir percé les défenses existantes déployées par les entreprises aujourd'hui, du périmètre à la sécurité des applications.



Malheureusement, de nombreuses entreprises ne tirent pas parti des fonctionnalités de sécurité au niveau de la couche de données. C'est là qu'intervient la gamme de solutions NetApp pour la protection contre les ransomwares, pour vous protéger dans votre dernier domaine de défense.

Le vrai coût des ransomwares

Le paiement d'une rançon en elle-même n'a pas le plus grand effet financier sur une entreprise. Bien que le paiement ne soit pas insignifiant, il reste insignifiant comparé au coût des temps d'indisponibilité liés à un incident d'ransomware.

Le paiement d'une rançon n'est qu'un élément du coût de la récupération lorsqu'il s'agit de faire face à des attaques par ransomware. En excluant toute rançon payée, les entreprises ont déclaré en 2024 un coût moyen de restauration suite à une attaque par ransomware de 2,7 millions de dollars, soit une augmentation de près de 1 million de dollars par rapport aux 1,2 million de dollars rapportés en 2023 "2024 Sophos State of ransomware". Les coûts peuvent être 10 fois plus élevés pour les entreprises qui dépendent fortement de la

disponibilité INFORMATIQUE, telles que l'e-commerce, les actions boursières et les soins de santé.

Les coûts de la cyberassurance continuent également d'augmenter, étant donné la très réelle probabilité d'une attaque par ransomware sur les entreprises assurées.

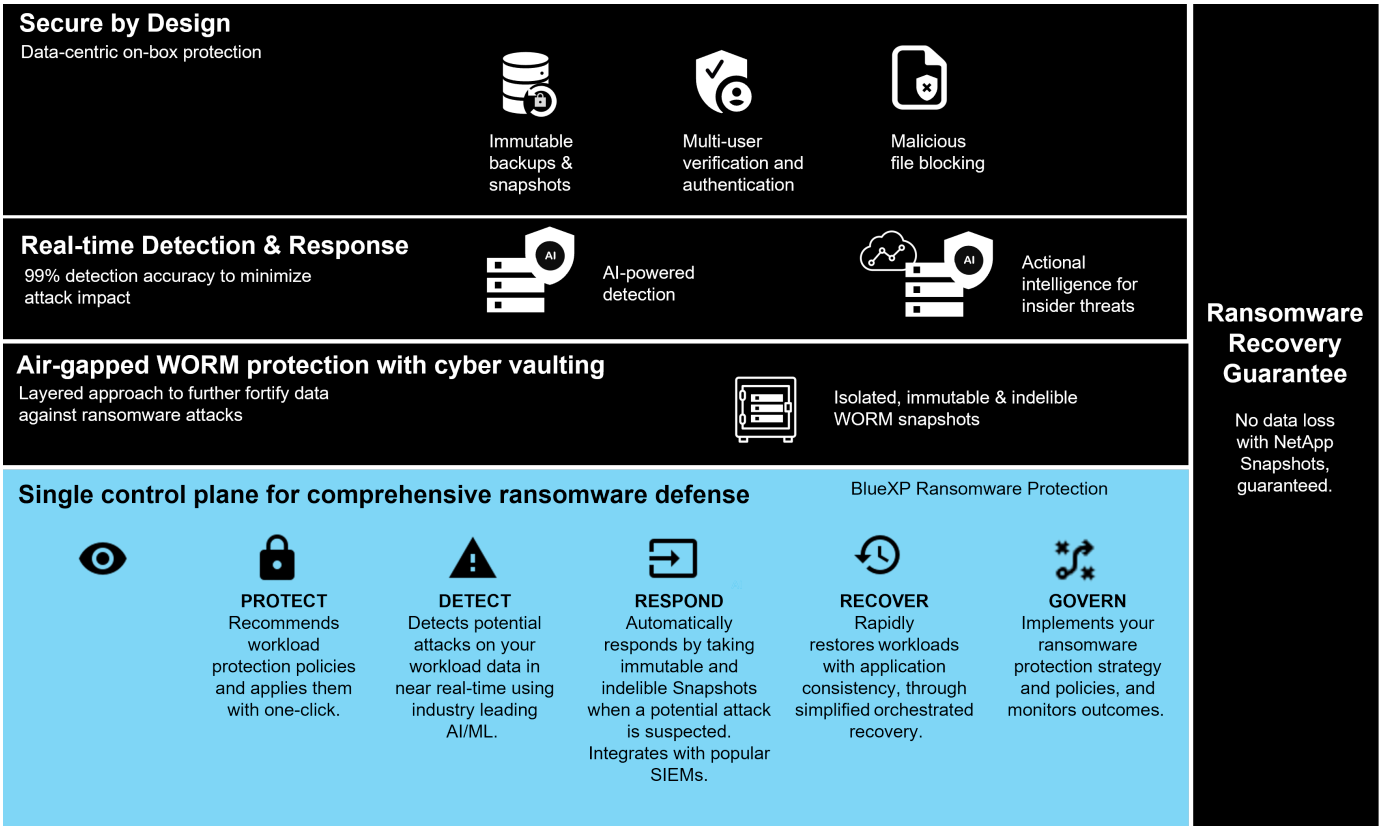
Protection contre les ransomware au niveau de la couche de données

NetApp comprend que la sécurité de votre entreprise est vaste et approfondie dans tout le périmètre, jusqu'à l'emplacement des données au niveau de la couche de stockage. Votre pile de sécurité est complexe et doit assurer la sécurité à tous les niveaux de votre pile technologique.

La protection en temps réel au niveau de la couche de données est encore plus importante et a des exigences uniques. Pour être efficace, les solutions de cette couche doivent offrir les attributs critiques suivants :

- **Sécurité par conception** pour minimiser les risques d'attaque réussie
- **Détection et réponse en temps réel** pour minimiser l'impact d'une attaque réussie
- **Protection WORM à air Gap** pour isoler les sauvegardes de données critiques
- **Un seul plan de contrôle** pour une défense complète contre les ransomware

NetApp peut vous offrir tout cela et bien plus encore.



Le portefeuille de solutions NetApp pour la protection contre les ransomwares

NetApp "protection intégrée contre les ransomware"propose une défense à facettes et robuste en temps réel pour vos données stratégiques. Au cœur de ces outils, des algorithmes avancés de détection optimisés par l'IA surveillent en continu les modèles de données, ce qui permet d'identifier rapidement les menaces de ransomware avec une précision de 99 %. En réagissant rapidement aux attaques, notre stockage peut créer rapidement des snapshots de données et sécuriser les copies, assurant ainsi une restauration rapide.

Pour renforcer encore davantage les données, la "cyber-archivage" capacité de NetApp isole les données avec un air Gap logique. En protégeant les données stratégiques, nous assurons une continuité rapide de l'activité.

NetApp"Protection contre les ransomwares NetApp" réduit les charges opérationnelles avec un plan de contrôle unique pour coordonner et exécuter intelligemment une défense contre les ransomwares centrée sur la charge de travail de bout en bout, afin que vous puissiez identifier et protéger les données de charge de travail critiques à risque en un seul clic, détecter et répondre avec précision et automatiquement pour limiter l'impact d'une attaque potentielle et récupérer les charges de travail en quelques minutes, et non en quelques jours, en protégeant vos précieuses données de charge de travail et en minimisant les perturbations coûteuses.

En tant que solution ONTAP intégrée native pour protéger les accès non autorisés à vos données, "Vérification multiadministrateur" bénéficiez de fonctionnalités robustes qui assurent l'exécution des opérations telles que la suppression de volumes, la création d'utilisateurs administratifs ou la suppression de snapshots uniquement après approbation d'un second administrateur désigné. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables. Vous pouvez configurer autant d'approbateurs administrateurs désignés que vous le souhaitez avant de supprimer un instantané.

> NetApp ONTAP répond à la condition requise pour "Authentification multifacteur (MFA)" l'authentification Web dans System Manager et l'authentification via l'interface de ligne de commandes SSH.

Avec la protection contre les ransomwares de NetApp, travaillez sereinement dans un environnement aux menaces qui ne cesse d'évoluer. Son approche globale ne se contente pas de vous défendre contre les variantes actuelles des ransomwares. Elle s'adapte également aux menaces émergentes, assurant ainsi la sécurité à long terme de votre infrastructure de données.

Découvrez les autres options de protection

- "Protection contre les ransomware via Digital Advisor"
- "Data Infrastructure Insights Stockage Charge de travail Sécurité"
- "FPolicy"
- "SnapLock et copies Snapshot inviolables"

Garantie de restauration contre les ransomwares

NetApp garantit la restauration des données Snapshot en cas d'attaque par ransomware. Notre garantie : si nous ne pouvons pas vous aider à restaurer vos données de snapshot, nous nous engageons à trouver la solution. La garantie est disponible pour tout achat de systèmes AFF A-Series, AFF C-Series, ASA et FAS.

En savoir plus >>

- "Description du service de garantie de récupération"
- "Blog sur la garantie de restauration contre les ransomwares".

Informations associées

- "Page des ressources du site de support NetApp"
- "Sécurité des produits NetApp"

SnapLock et copies Snapshot inviolables pour la protection contre les ransomwares

SnapLock, l'une des armes essentielles de l'arsenal de NetApp Snap, s'est avéré très efficace pour protéger les données contre les menaces de ransomware. En empêchant la suppression non autorisée des données, SnapLock fournit une couche de sécurité supplémentaire qui garantit l'intégrité et l'accessibilité des données critiques, même en cas d'attaques malveillantes.

Conformité SnapLock

SnapLock Compliance (SLC) assure une protection indélébile de vos données. SLC interdit la suppression de données même lorsqu'un administrateur tente de réinitialiser la baie. Contrairement à d'autres produits concurrents, SnapLock Compliance n'est pas vulnérable aux piratages d'ingénierie sociale par l'intermédiaire des équipes de support de ces produits. Les données protégées par des volumes SnapLock Compliance peuvent être récupérables jusqu'à leur date d'expiration.

Pour activer SnapLock, une "ONTAP One" licence est requise.

En savoir plus >>

- "Documentation SnapLock"

Des snapshots inviolables

Les copies Snapshot inviolables constituent un moyen pratique et rapide de protéger vos données contre les actes malveillants. Contrairement à SnapLock Compliance, TPS est généralement utilisé sur les systèmes principaux où l'utilisateur peut protéger les données pendant un temps déterminé et les laisser localement pour des restaurations rapides ou où les données n'ont pas besoin d'être répliquées hors du système principal. TPS utilise les technologies SnapLock pour empêcher la suppression du snapshot principal, même par un administrateur ONTAP, pendant la même période d'expiration de la rétention SnapLock. La suppression de Snapshot est impossible même si le volume n'est pas activé sur SnapLock, bien que les snapshots ne possèdent pas la même nature indélébile que les volumes SnapLock Compliance.

Pour rendre les snapshots inviolables, une "ONTAP One" licence est requise.

En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware".

Blocage des fichiers FPolicy

FPolicy empêche le stockage des fichiers indésirables sur votre appliance de stockage haute performance. FPolicy vous permet également de bloquer les extensions de fichiers ransomware connues. Un utilisateur dispose toujours des autorisations d'accès complètes au dossier de départ, mais FPolicy ne permet pas à un utilisateur de stocker les fichiers marqués par votre administrateur comme bloqués. Le cas échéant, il n'est pas important que ces fichiers soient des fichiers MP3 ou des extensions de fichiers ransomware connues.

Bloquez les fichiers malveillants avec le mode natif FPolicy

Le mode natif NetApp FPolicy (une évolution du nom, la stratégie de fichiers) est un framework de blocage

d'extension de fichiers qui vous permet de bloquer les extensions de fichiers indésirables dans votre environnement. Fait partie de ONTAP depuis plus de dix ans, il est incroyablement utile pour vous protéger contre les ransomware. Ce moteur « zéro confiance » est très utile, car vous bénéficiez de mesures de sécurité supplémentaires qui vont au-delà des autorisations de liste de contrôle d'accès (ACL).

Dans ONTAP System Manager et la NetApp Console, une liste de plus de 3 000 extensions de fichiers est disponible pour référence.

> Certaines extensions peuvent être légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus. Créez votre propre liste adaptée à votre environnement avant de configurer FPolicy natif.

Le mode natif FPolicy est inclus dans toutes les licences ONTAP.

En savoir plus >>

- "Blog : lutter contre les ransomware : troisième partie : ONTAP FPolicy, un autre outil puissant et natif (appelé gratuitement)"

Activez l'analyse du comportement des utilisateurs et des entités (UEBA) avec le mode externe FPolicy

Le mode externe FPolicy est un framework de notification et de contrôle de l'activité des fichiers qui offre une visibilité sur l'activité des fichiers et des utilisateurs. Ces notifications peuvent être utilisées par une solution externe pour effectuer des analyses basées sur l'IA afin de détecter les comportements malveillants.

Le mode externe FPolicy peut également être configuré pour attendre l'approbation du serveur FPolicy avant de permettre l'exécution d'activités spécifiques. Vous pouvez configurer plusieurs règles de ce type sur un cluster, ce qui vous apporte une grande flexibilité.

> Les serveurs FPolicy doivent répondre aux requêtes FPolicy s'ils sont configurés pour être approuvés. Sinon, les performances du système de stockage risquent d'être affectées.

Le mode externe FPolicy est inclus dans "Toutes les licences ONTAP".

En savoir plus >>

- "Blog : lutter contre les ransomware : quatrième partie — UBA et ONTAP avec le mode externe FPolicy."

Data Infrastructure Insights Stockage Charge de travail Sécurité

Storage Workload Security (SWS) est une fonctionnalité de NetApp Data Infrastructure Insights qui améliore considérablement la posture de sécurité, la récupérabilité et la responsabilité d'un environnement ONTAP . SWS adopte une approche centrée sur l'utilisateur, en suivant toutes les activités des fichiers de chaque utilisateur authentifié dans l'environnement. Il utilise des analyses avancées pour établir des modèles d'accès normaux et saisonniers pour chaque utilisateur. Ces modèles sont utilisés pour identifier rapidement les comportements suspects sans avoir besoin de signatures de ransomware.

Lorsque SWS détecte un ransomware potentiel ou une suppression de données, il peut prendre des mesures automatiques telles que :

- Prenez un instantané du volume affecté.

- Bloquez le compte utilisateur et l'adresse IP suspectés d'activité malveillante.
- Envoyez une alerte aux administrateurs.

Comme il peut prendre des mesures automatisées pour arrêter rapidement une menace interne et suivre chaque activité de fichier, SWS simplifie et accélère la restauration suite à un événement de ransomware. Grâce aux outils avancés d'audit et d'analyse intégrés, les utilisateurs peuvent immédiatement voir quels volumes et fichiers ont été affectés par une attaque, quel compte d'utilisateur l'attaque a été et quelle action malveillante a été exécutée. Les snapshots automatiques atténuent les dommages et accélèrent la restauration des fichiers.

Les alertes issues de la protection anti-ransomware autonome (ARP) de ONTAP sont également visibles dans SWS, fournissant une interface unique aux clients qui utilisent à la fois ARP et SWS pour se protéger contre les attaques par ransomware.

En savoir plus >>

- "Data Infrastructure Insights NetApp"

Détection et réponse basées sur l'IA intégrées à NetApp ONTAP

Comme les menaces de ransomware sont de plus en plus sophistiquées, vos mécanismes de défense aussi devraient-ils le faire. La protection anti-ransomware autonome (ARP) de NetApp est optimisée par l'IA avec la détection d'anomalies intelligente intégrée à ONTAP. Activez-la pour ajouter une couche de défense supplémentaire à votre cyberrésilience.

ARP et ARP/ai sont configurables via l'interface de gestion intégrée ONTAP, System Manager et activées par volume.

Protection autonome contre les ransomwares (ARP)

La protection anti-ransomware autonome (ARP), une autre solution ONTAP intégrée native depuis 9.10.1, examine l'activité des fichiers de workloads de volume de stockage NAS et l'entropie des données pour détecter automatiquement les ransomwares. ARP fournit aux administrateurs une détection en temps réel, des informations et un point de restauration des données pour une détection intégrée sans précédent des ransomwares.

Pour ONTAP 9.15.1 et les versions antérieures qui prennent en charge ARP, ARP démarre en mode d'apprentissage pour apprendre l'activité typique des données de charge de travail. Cela peut prendre sept jours pour la plupart des environnements. Une fois le mode d'apprentissage terminé, le protocole ARP passe automatiquement en mode actif et commence à rechercher les activités anormales des workloads qui

pourraient être des ransomware.

En cas d'activité anormale, un snapshot automatique est immédiatement pris, ce qui fournit un point de restauration aussi proche que possible du moment de l'attaque avec un minimum de données infectées. Simultanément, une alerte automatique (configurable) est générée et permet aux administrateurs de voir l'activité anormale des fichiers afin qu'ils puissent déterminer si l'activité est malveillante et prendre les mesures appropriées.

Si l'activité correspond à une charge de travail attendue, les administrateurs peuvent facilement la marquer comme un faux positif. ARP apprend ce changement comme une activité normale de la charge de travail et ne le signale plus comme une attaque potentielle à l'avenir.

Pour activer ARP, une "ONTAP One" licence est requise.

En savoir plus >>

- "Protection autonome contre les ransomwares"

Protection anti-ransomware autonome/IA (ARP/ai)

Présenté en tant que préversion technologique d'ONTAP 9.15.1, ARP/ai va encore plus loin avec la détection en temps réel intégrée des systèmes de stockage NAS. La nouvelle technologie de détection optimisée par l'IA est entraînée sur plus d'un million de fichiers et diverses attaques par ransomware connues. En plus des signaux utilisés dans ARP, ARP/ai détecte également le chiffrement des en-têtes. La puissance ai et les signaux supplémentaires permettent à ARP/ai d'offrir une précision de détection supérieure à 99 %. Ce résultat a été validé par se Labs, un laboratoire de test indépendant qui a donné à ARP/ai son meilleur classement AAA.

L'entraînement des modèles étant effectué en continu dans le cloud, l'ARP/l'IA ne requiert pas de mode d'apprentissage. Elle est active dès sa mise sous tension. La formation continue implique également que l'ARP/l'IA est toujours validée contre les nouveaux types d'attaques par ransomware dès qu'ils surviennent. ARP/ai est également fourni avec des fonctionnalités de mise à jour automatique qui fournissent de nouveaux paramètres à tous les clients pour maintenir la détection des ransomware à jour. Toutes les autres fonctionnalités de détection, d'aperçu et de point de restauration des données d'ARP sont conservées pour ARP/ai.

Pour activer ARP/ai, une "ONTAP One" licence est requise.

En savoir plus >>

- "Blog : la solution NetApp de détection des ransomwares en temps réel basée sur l'IA classe AAA"

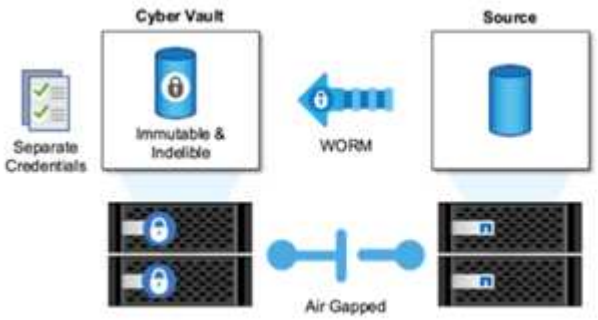
Protection WORM protégée par air avec archivage électronique dans ONTAP

L'approche de NetApp en matière de cyber-coffre est une architecture de référence dédiée pour un cyber-coffre à air Gap logique. Cette approche tire parti des technologies de renforcement de la sécurité et de conformité, telles que SnapLock, pour permettre des snapshots immuables et indélébiles.

Cyber-archivage avec SnapLock Compliance et un air Gap logique

La tendance est de plus en plus marquée aux pirates informatiques qui détruisent les copies de sauvegarde et, dans certains cas, même les chiffrent. C'est pourquoi beaucoup dans le secteur de la cybersécurité recommandent d'utiliser des sauvegardes « air Gap » dans le cadre d'une stratégie globale de cyberrésilience.

Le problème, c'est que les lacunes traditionnelles (bandes et supports hors ligne) peuvent considérablement augmenter le temps de restauration, augmentant ainsi les temps d'indisponibilité et les coûts globaux associés. Même une approche plus moderne de la solution de l'air Gap peut s'avérer problématique. Par exemple, si le coffre-fort de sauvegarde est temporairement ouvert pour recevoir de nouvelles copies de sauvegarde, puis déconnecte et ferme sa connexion réseau aux données primaires pour être à nouveau « à air Gap », un attaquant pourrait tirer parti de l'ouverture temporaire. Au cours de la connexion, un attaquant pourrait frapper pour compromettre ou détruire les données. Ce type de configuration ajoute également généralement une complexité indésirable. L'air Gap logique est un excellent substitut à un air Gap traditionnel ou moderne car il possède les mêmes principes de protection de sécurité tout en conservant la sauvegarde en ligne. Avec NetApp, simplifiez les opérations de « air gapping » sur bande ou sur disque grâce à des opérations de « air gapping » logiques, réalisables avec des snapshots et des NetApp SnapLock Compliance immuables.



NetApp a publié la fonctionnalité SnapLock il y a plus de 10 ans pour répondre aux exigences de conformité des données, telles que la loi HIPAA (Health Insurance Portability and Accountability Act), la loi Sarbanes-Oxley et d'autres règles relatives aux données réglementaires. Vous pouvez également archiver les snapshots primaires de façon sécurisée sur des volumes SnapLock de façon à ce que ces copies puissent être validées sur WORM, empêchant ainsi la suppression. Il existe deux versions de licence SnapLock : SnapLock Compliance et SnapLock Enterprise. Pour la protection contre les ransomwares, NetApp recommande SnapLock Compliance, car vous pouvez définir une période de conservation spécifique pendant laquelle les snapshots sont verrouillés et ne peuvent pas être supprimés, même par les administrateurs ONTAP ou par le support NetApp.

En savoir plus >>

- "Blog : présentation du cyber-coffre-fort ONTAP"

Des snapshots inviolables

Si l'utilisation de SnapLock Compliance comme air Gap logique offre une protection ultime pour empêcher les pirates de supprimer vos copies de sauvegarde, il est nécessaire de déplacer les snapshots à l'aide de SnapVault vers un volume secondaire compatible SnapLock. Par conséquent, de nombreux clients déploient cette configuration sur un système de stockage secondaire sur le réseau. Cela peut entraîner des temps de restauration plus longs qu'avec la restauration d'un Snapshot de volume primaire sur le système de stockage primaire.

À partir de ONTAP 9.12.1, les copies Snapshot inviolables assurent une protection proche du niveau SnapLock Compliance pour vos copies Snapshot sur le stockage primaire et dans les volumes primaires. Il n'est pas nécessaire d'archiver l'instantané à l'aide de SnapVault sur un volume secondaire SnapLocaché. Les snapshots inviolables utilisent la technologie SnapLock pour empêcher la suppression du snapshot principal, même par un administrateur ONTAP complet, pendant toute la durée de conservation SnapLock. Cela permet des délais de restauration plus rapides et la possibilité de sauvegarder un volume FlexClone à l'aide d'une copie Snapshot protégée et inviolable, ce que vous ne pouvez pas faire avec une copie Snapshot stockage SnapLock Compliance classique.

La principale différence entre les snapshots SnapLock Compliance et inviolables est que SnapLock Compliance n'autorise pas l'initialisation et la suppression de la baie ONTAP si des volumes SnapLock Compliance existent avec des snapshots voûtés qui n'ont pas encore atteint leur date d'expiration. Pour rendre les snapshots inviolables, une licence SnapLock Compliance est requise.

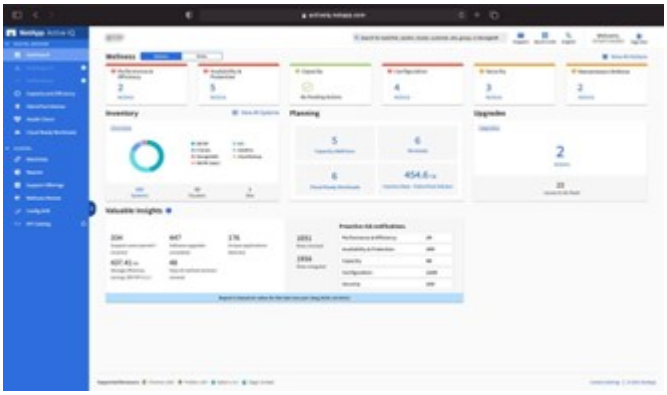
En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware"

Protection contre les ransomware via Digital Advisor

Digital Advisor optimisé par Active IQ simplifie la maintenance proactive et l'optimisation du stockage NetApp avec des informations exploitables pour une gestion des données optimale. S'appuyant sur les données de télémétrie de notre base installée très diversifiée, il utilise des techniques avancées d'IA et de ML pour identifier les opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage.

Non seulement peut "Conseiller digital NetApp" vous y aider "éliminez les failles de sécurité", mais il fournit également des informations et des recommandations spécifiques pour vous protéger contre les ransomwares. Une carte d'intégrité dédiée présente les actions nécessaires et les risques résolus. Vous êtes ainsi sûr que vos systèmes respectent ces recommandations en matière de bonnes pratiques.



Les risques et les actions suivis sur la page ransomware Defense Wellness incluent notamment les éléments suivants :

- Le nombre de copies Snapshot des volumes est faible, ce qui réduit la protection potentielle contre les ransomware.
- FPolicy n'est pas activé pour toutes les machines virtuelles de stockage (SVM) configurées pour les protocoles NAS.

Pour voir la protection contre les ransomware en action, voir "Conseiller digital".

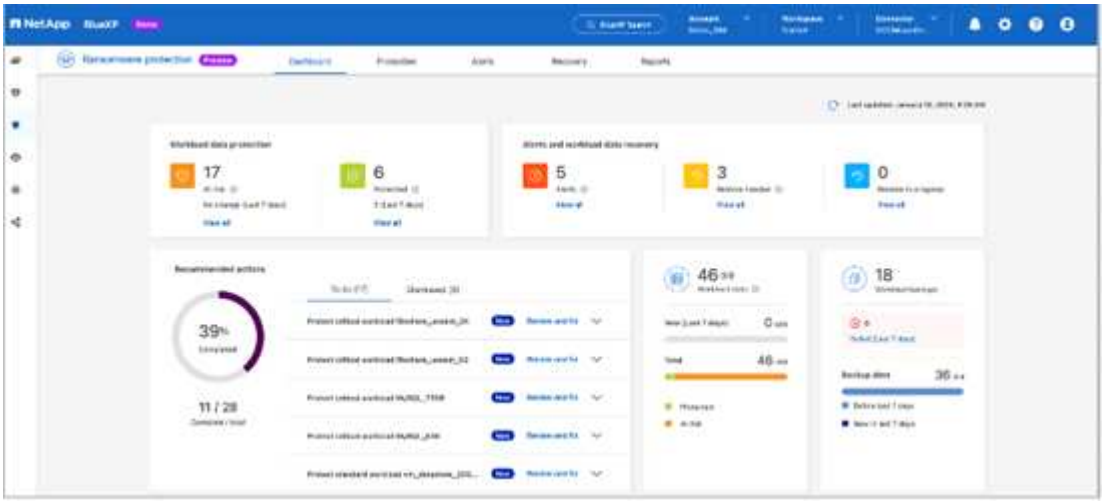
Résilience complète avec la protection contre les ransomwares NetApp

Il est important que la détection des ransomwares ait lieu le plus tôt possible afin de pouvoir empêcher leur propagation et éviter des temps d'arrêt coûteux. Une stratégie efficace de détection des ransomwares doit toutefois inclure plus d'une seule couche de protection. La protection contre les ransomwares de NetApp adopte une approche globale qui comprend des fonctionnalités en temps réel, intégrées, s'étendant aux

services de données à l'aide de la NetApp Console et une solution isolée et en couches pour le cyber-coffre-fort.

Protection contre les ransomwares NetApp

La NetApp Console est un plan de contrôle unique permettant d'orchestrer intelligemment une défense complète contre les ransomwares centrée sur la charge de travail. La protection contre les ransomwares NetApp rassemble les puissantes fonctionnalités de cyber-résilience d' ONTAP, telles que ARP, FPolicy et les snapshots inviolables, et les services de données NetApp , tels que NetApp Backup and Recovery. Il ajoute également des recommandations et des conseils avec des flux de travail automatisés pour fournir une défense de bout en bout via une interface utilisateur unique. Il fonctionne au niveau de la charge de travail pour garantir que les applications qui font fonctionner votre entreprise sont protégées et peuvent être récupérées le plus rapidement possible en cas d'attaque.



Avantages pour le client :

- La préparation assistée par ransomware réduit la surcharge opérationnelle et améliore l'efficacité
- La détection d'anomalies optimisée par l'IA et le ML améliore la précision et accélère la réponse pour maîtriser les risques
- La restauration guidée cohérente au niveau des applications vous permet de restaurer les workloads plus facilement et en quelques minutes

"Protection contre les ransomwares NetApp"rend ces fonctions NIST plus faciles à réaliser :

- Automatiquement **découvrir** et hiérarchiser les données dans le stockage NetApp **en mettant l'accent sur les principales charges de travail basées sur les applications**.
- **Protection en un clic** de la sauvegarde des données de la charge de travail la plus importante, immuable, configuration sécurisée, blocage des fichiers malveillants et domaine de sécurité différent.
- **Détectez avec précision** les ransomware au plus vite * en utilisant **la détection d'anomalies basée sur l'IA nouvelle génération.**
- Réponse automatisée et flux de travail et intégration avec les meilleures solutions * SIEM et XDR.*
- Restaurez rapidement les données à l'aide d'une récupération * orchestrée simplifiée* pour accélérer la continuité des applications.
- Mettez en œuvre votre **stratégie** et **politiques** de protection contre les ransomware et **surveillez les résultats**.

NetApp et le modèle « zéro confiance »

NetApp et le modèle « zéro confiance »

La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». NetApp ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.

À partir de juillet 2024, le contenu du rapport technique *TR-4829: NetApp and Zero Trust: Enabling a data-Centric Zero Model*, qui a été publié au format PDF, est disponible sur docs.netapp.com.

Les données constituent les ressources les plus importantes de votre entreprise. Selon le 2022 , les menaces internes sont la cause de 18 % des violations de données "Rapport d'enquête sur les violations de données Verizon". Les entreprises peuvent améliorer leur vigilance en déployant des contrôles « zéro confiance » de pointe sur les données à l'aide du logiciel de gestion des données NetApp ONTAP.

Qu'est-ce que le principe zéro confiance ?

Le modèle Zero Trust a été développé pour la première fois par John Kindervag, de Forrester Research. Le service informatique envisage la sécurité du réseau de l'intérieur vers l'extérieur plutôt que de l'extérieur vers l'intérieur. L'approche « zéro confiance » de l'intérieur identifie un micronoyau et un périmètre (MCAP). Le MCAP est une définition intérieure des données, des services, des applications et des ressources à protéger avec un ensemble complet de contrôles. Le concept de périmètre extérieur sécurisé est obsolète. Les entités fiables et autorisées à s'authentifier avec succès via le périmètre peuvent alors rendre l'organisation vulnérable aux attaques. Les initiés, par définition, sont déjà à l'intérieur du périmètre sécurisé. Les employés, prestataires et partenaires sont des initiés, et ils doivent être autorisés à opérer avec des contrôles appropriés pour remplir leurs rôles au sein de l'infrastructure de votre entreprise.

Zéro confiance a été mentionné comme une technologie qui offre une promesse au DoD en septembre 2019 "FY19-23 Stratégie de modernisation numérique du Département de la Défense des États-Unis". Le modèle « zéro confiance » est défini comme « Une stratégie de cybersécurité qui intègre la sécurité dans l'ensemble de l'architecture dans le but d'enrayer les fuites de données. Ce modèle de sécurité centré sur les données élimine l'idée de réseaux, périphériques, rôles ou processus fiables ou non approuvés, et passe à des niveaux de confiance basés sur plusieurs attributs qui activent des stratégies d'authentification et d'autorisation dans le concept d'accès le moins privilégié. Mettre en œuvre la confiance zéro exige de repenser la façon dont nous utilisons l'infrastructure existante pour mettre en œuvre la sécurité en simplifiant et en améliorant l'efficacité tout en assurant la continuité des opérations. »

En août 2020, le NIST a publié "Architecture Zero Trust Pub 800-207 spéciale" (ZTA). ZTA se concentre sur la protection des ressources, et non des segments de réseau, car l'emplacement du réseau n'est plus considéré comme le composant principal de la posture de sécurité de la ressource. Les ressources sont des données et de l'informatique. Les stratégies ZTA sont destinées aux architectes de réseaux d'entreprise. ZTA présente une nouvelle terminologie issue des concepts originaux de Forrester. Les mécanismes de protection appelés le point de décision de la politique (PDP) et le point d'application de la politique (PEP) sont analogues à une

passerelle de segmentation Forrester. ZTA présente quatre modèles de déploiement :

- Déploiement basé sur un agent ou une passerelle
- Déploiement basé sur l'enclave (un peu similaire au MCAP de Forrester)
- Déploiement sur portail de ressources
- Sandbox d'application de périphérique

Pour les besoins de cette documentation, nous utilisons les concepts et la terminologie de Forrester Research plutôt que le NIST ZTA.

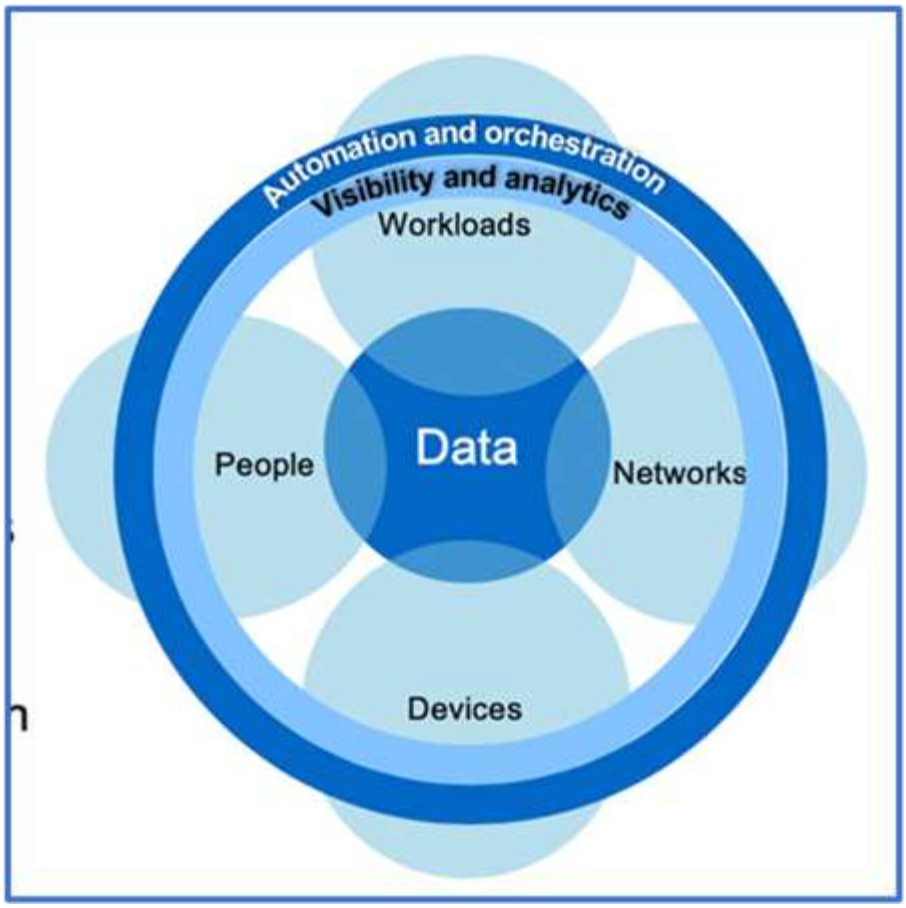
Ressources de sécurité

Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le "Portail de sécurité NetApp".

Concevez une approche « zéro confiance » centrée sur les données avec ONTAP

Un réseau « zéro confiance » est défini par une approche centrée sur les données dans laquelle les contrôles de sécurité doivent être aussi proches que possible des données. Les fonctionnalités de ONTAP, associées à l'écosystème de partenaires NetApp FPolicy, peuvent fournir les contrôles nécessaires au modèle « zéro confiance » centré sur les données.

ONTAP est le logiciel de gestion des données riche en fonctions de sécurité de NetApp, et le moteur « zéro confiance » FPolicy est une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire et basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP.



Concevez un MCAP « zéro confiance » centré sur les données

Pour concevoir un MCAP Zero Trust axé sur les données, procédez comme suit :

1. Identifiez l'emplacement de toutes les données de l'entreprise.
2. Classez vos données.
3. Supprimez en toute sécurité les données dont vous n'avez plus besoin.
4. Comprendre quels rôles doivent avoir accès aux classifications de données.
5. Appliquez le principe du privilège minimum pour appliquer les contrôles d'accès.
6. Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données.
7. Utilisez le chiffrement pour les données au repos et en transit.
8. Contrôlez et consignez tous les accès.
9. Alertez les accès suspects ou les comportements à adopter.

Identifiez l'emplacement de toutes les données de l'entreprise

La fonctionnalité FPolicy de ONTAP associée à l'écosystème de partenaires Alliance NetApp de FPolicy vous permet d'identifier l'emplacement des données de votre entreprise et les personnes qui y ont accès. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. Pour plus d'informations sur l'analyse comportementale des utilisateurs, reportez-vous à la section contrôle et journalisation de tous les accès. Si vous ne comprenez pas où se trouvent vos données et qui y a accès, l'analyse comportementale des utilisateurs peut fournir une base pour établir une classification et une politique à partir d'observations empiriques.

Classez vos données

Dans la terminologie du modèle Zero Trust, la classification des données implique l'identification des données toxiques. Les données toxiques sont des données sensibles qui ne sont pas destinées à être exposées en dehors d'une organisation. La divulgation de données toxiques pourrait violer la conformité réglementaire et nuire à la réputation d'une organisation. En termes de conformité réglementaire, les données toxiques incluent les données des titulaires de cartes pour le "Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS)" , données personnelles pour l'UE "Règlement général sur la protection des données (RGPD)" , ou des données de santé pour le "Loi américaine sur la transférabilité et la responsabilité en matière d'assurance maladie (HIPAA)" . Vous pouvez utiliser NetApp "NetApp Data Classification" (anciennement connu sous le nom de Cloud Data Sense), une boîte à outils basée sur l'IA, pour numériser, analyser et catégoriser automatiquement vos données.

Supprimez les données dont vous n'avez plus besoin en toute sécurité

Une fois les données de votre entreprise classifiées, vous pouvez découvrir que certaines de vos données ne sont plus nécessaires ou pertinentes pour le fonctionnement de votre entreprise. La conservation de données inutiles est une responsabilité et ces données doivent être supprimées. Pour obtenir un mécanisme avancé d'effacement cryptographique des données, consultez la description de la suppression sécurisée dans le chiffrement des données au repos.

Comprendre quels rôles doivent avoir accès aux classifications de données et appliquer le principe du privilège minimum pour appliquer les contrôles d'accès

Mapper l'accès aux données sensibles et appliquer le principe du privilège minimum implique de donner aux personnes de votre entreprise l'accès aux seules données requises pour accomplir leur travail. Ce processus implique le contrôle d'accès basé sur les rôles ("RBAC"), qui s'applique à l'accès aux données et à l'accès administratif.

Avec ONTAP, un SVM (Storage Virtual machine) peut être utilisé pour segmenter l'accès aux données de l'entreprise par les locataires au sein d'un cluster ONTAP. Le RBAC peut être appliqué à l'accès aux données ainsi qu'à l'accès administratif à la SVM. Le RBAC peut également être appliqué au niveau administratif du cluster.

En plus de RBAC, vous pouvez utiliser ONTAP "vérification multiadministrateur" (MAV) pour demander à un ou plusieurs administrateurs d'approuver des commandes telles que `volume delete` ou `volume snapshot delete`. Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.

ONTAP est un autre moyen de protéger les snapshots"verrouillage des copies snapshot". Le verrouillage des snapshots est une fonctionnalité SnapLock dans laquelle les snapshots sont rendus indélébiles manuellement ou automatiquement avec une période de conservation définie dans la règle Snapshot du volume. Le verrouillage des snapshots est également appelé verrouillage inviolable des snapshots. Le verrouillage des snapshots permet d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer des snapshots sur les systèmes ONTAP primaires et secondaires. Il est possible d'effectuer une restauration rapide des copies Snapshot verrouillées sur les systèmes primaires afin de restaurer les volumes corrompus par des ransomwares.

Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données

Outre le RBAC d'administration de cluster, "Authentification multifacteur (MFA)" peut être déployé pour l'accès administratif web ONTAP et l'accès à la ligne de commande SSH (Secure Shell). L'authentification multifacteur en matière d'accès administratif est obligatoire pour les organisations du secteur public américain ou celles qui doivent suivre la norme PCI-DSS. L'authentification multifacteur empêche un attaquant de compromettre un compte en utilisant uniquement un nom d'utilisateur et un mot de passe. L'authentification MFA nécessite au

moins deux facteurs indépendants. Un exemple d'authentification à deux facteurs est quelque chose qu'un utilisateur possède, comme une clé privée, et quelque chose qu'un utilisateur sait, comme un mot de passe. L'accès administratif Web à ONTAP System Manager ou à ActiveIQ Unified Manager est activé par le langage SAML (Security assertion Markup Language) 2.0. L'accès en ligne de commande SSH utilise une authentification à deux facteurs chaînée avec une clé publique et un mot de passe.

Vous pouvez contrôler l'accès des utilisateurs et des machines via des API dotées des fonctionnalités de gestion des identités et des accès de ONTAP :

- Utilisateur :
  - **Authentification et autorisation.** Grâce aux fonctionnalités de protocole NAS pour SMB et NFS.
  - **Vérification.** Syslog d'accès et d'événements. Une journalisation d'audit détaillée du protocole CIFS pour tester les règles d'authentification et d'autorisation. Audit précis et granulaire de l'accès NAS détaillé dans FPolicy au niveau des fichiers.
- Périphérique :
  - **Authentification.** Authentification basée sur certificat pour l'accès à l'API.
  - **Autorisation.** Contrôle d'accès basé sur des rôles (RBAC) par défaut ou personnalisé.
  - **Vérification.** Syslog de toutes les actions entreprises.

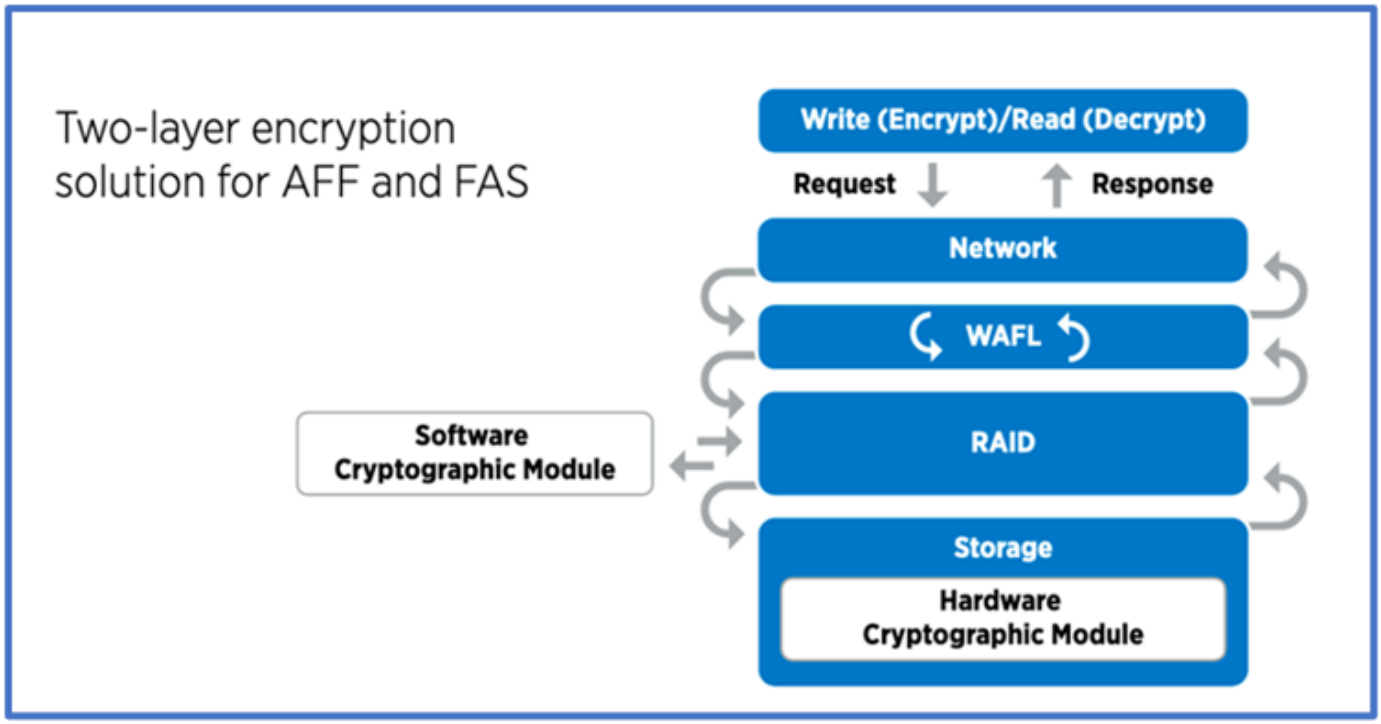
Utilisez le chiffrement pour les données au repos et en transit

Chiffrement des données au repos

Chaque jour, lorsqu'une entreprise réutilise des disques, renvoie des disques défectueux ou effectue des mises à niveau vers des disques de plus grande capacité, elle doit satisfaire de nouvelles exigences afin de réduire les risques liés aux systèmes de stockage et les écarts d'infrastructure. En tant qu'administrateurs et opérateurs de ressources de données, les ingénieurs du stockage doivent gérer et maintenir les données en toute sécurité tout au long de leur cycle de vie. "Chiffrement de stockage NetApp (NSE) ;#44 ; NetApp Volume Encryption (NVE) ;#44 ; et chiffrement d'agrégat NetApp" vous aider à chiffrer toutes vos données au repos en permanence, qu'elles soient toxiques ou non, et sans affecter les opérations quotidiennes. "NSE" Est une solution matérielle ONTAP "données au repos" qui utilise des disques auto-cryptés conformes à la norme FIPS 140-2 de niveau 2. "NVE et NAE" Sont une solution logicielle ONTAP "données au repos" qui utilise le "Module cryptographique NetApp conforme à la norme FIPS 140-2 de niveau 1". Avec NVE et NAE, vous pouvez utiliser des disques durs ou des disques SSD pour le chiffrement des données au repos. De plus, les disques NSE peuvent être utilisés pour fournir une solution de chiffrement à plusieurs couches native qui assure la redondance du chiffrement et une sécurité supplémentaire. Si l'une des couches est rompue, la seconde couche sécurise toujours les données. Ces fonctionnalités font de ONTAP une solution bien positionnée pour "chiffrement prêt pour le quantum".

NVE propose également une fonctionnalité appelée "suppression sécurisée" qui supprime de manière cryptographique les données toxiques des fuites de données lorsque les fichiers sensibles sont écrits sur un volume non classifié.

Soit le "Gestionnaire de clés intégré Onboard Key Manager (OKM)", qui est le gestionnaire de clés intégré dans ONTAP, soit un "approuvée" tiers "gestionnaires de clés externes" peut être utilisé avec NSE et NVE pour stocker des clés en toute sécurité.



Comme le montre la figure ci-dessus, le chiffrement matériel et logiciel peut être combiné. Cette fonctionnalité a permis à l' "Validation de ONTAP dans les solutions commerciales de la NSA pour le programme classifié" de stocker des données les plus secrètes.

Chiffrement des données à la volée

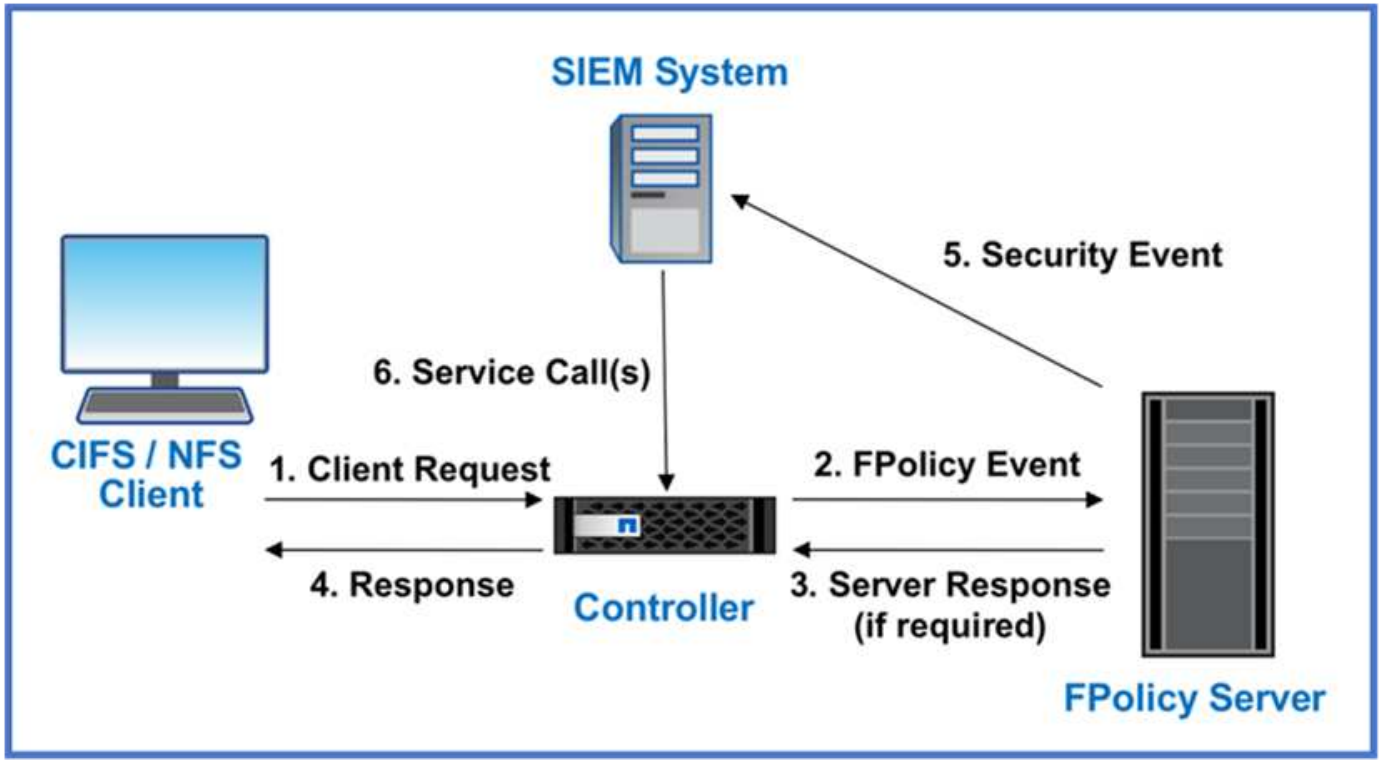
Le chiffrement des données à la volée ONTAP protège l'accès aux données utilisateur et l'accès au plan de contrôle. L'accès aux données utilisateur peut être chiffré par chiffrement SMB 3.0 pour l'accès aux partages Microsoft CIFS ou par krb5P pour NFS Kerberos 5. L'accès aux données utilisateur peut également être chiffré avec "IPSec" pour CIFS, NFS et iSCSI. L'accès au plan de contrôle est chiffré avec TLS (transport Layer Security). ONTAP fournit "FIPS"le mode de conformité pour l'accès au plan de contrôle, qui active les algorithmes approuvés FIPS et désactive les algorithmes non approuvés FIPS. La réplication des données est chiffrée avec "chiffrement des pairs de cluster". Cela assure le cryptage pour les technologies ONTAP SnapVault et SnapMirror.

Contrôlez et consignez tous les accès

Une fois les règles RBAC en place, vous devez déployer des fonctionnalités actives de surveillance, d'audit et d'alerte. Le moteur « zéro confiance » FPolicy de NetApp ONTAP, couplé au "Écosystème de partenaires NetApp FPolicy", fournit les contrôles nécessaires au modèle « zéro confiance » centré sur les données. NetApp ONTAP est un logiciel de gestion des données riche en fonctions de sécurité. Il "FPolicy" s'agit d'une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP. La fonctionnalité FPolicy de ONTAP, associée à l'écosystème de partenaires Alliance NetApp de FPolicy, vous permet d'identifier l'emplacement et l'accès aux données de votre entreprise. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. L'analyse comportementale des utilisateurs peut être utilisée pour alerter l'utilisateur en cas d'accès aux données suspect ou aberrant qui ne correspond pas au modèle normal et, si nécessaire, prendre des mesures pour refuser l'accès.

Les partenaires FPolicy vont au-delà de l'analyse comportementale des utilisateurs et s'orientent vers le machine learning (ML) et l'intelligence artificielle (IA) pour assurer la fidélité des événements et réduire le nombre de faux positifs, voire de faux positifs. Tous les événements doivent être consignés sur un serveur

syslog ou sur un système de gestion des informations et des événements de sécurité (SIEM) pouvant également utiliser le ML et l'IA.



NetApp "Sécurité de la charge de travail de stockage DII" utilise l'interface FPolicy et l'analyse du comportement des utilisateurs sur les systèmes de stockage ONTAP cloud et sur site pour vous fournir des alertes en temps réel sur le comportement malveillant des utilisateurs. Storage Workload Security protège les données de l'organisation contre toute utilisation abusive par des utilisateurs malveillants ou compromis grâce à l'apprentissage automatique avancé et à la détection des anomalies. Storage Workload Security peut identifier les attaques de ransomware ou d'autres comportements malveillants, invoquer des instantanés et mettre en quarantaine les utilisateurs malveillants. Storage Workload Security dispose également d'une capacité d'analyse médico-légale permettant de visualiser en détail les activités des utilisateurs et des entités. La sécurité des charges de travail de stockage fait partie de NetApp Data Infrastructure Insights.

Outre la sécurité des workloads de stockage, ONTAP dispose d'une fonctionnalité intégrée de détection des ransomwares appelée "Protection autonome contre les ransomwares" ARP. ARP utilise le machine learning pour déterminer si une activité anormale sur les fichiers indique qu'une attaque par ransomware est en cours, puis appelle une copie Snapshot et une alerte aux administrateurs. Storage Workload Security s'intègre à ONTAP pour recevoir des événements ARP et fournit une couche supplémentaire d'analytique et de réponses automatiques.

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence des commandes ONTAP", reportez-vous à la .

Contrôles d'orchestration et d'automatisation de la sécurité NetApp externes à ONTAP

L'automatisation vous permet d'effectuer un processus ou une procédure avec une assistance humaine minimale. L'automatisation permet aux entreprises d'étendre les déploiements « zéro confiance » bien au-delà des procédures manuelles pour se défendre contre les activités imcretes également automatisées.

Ansible est un outil open source de provisionnement logiciel, de gestion de la configuration et de déploiement des applications. Il fonctionne sur de nombreux systèmes Unix et peut configurer à la fois les systèmes Unix et Microsoft Windows. Il comprend son propre langage déclaratif pour décrire la configuration du système. Ansible a été écrit par Michael DeHaan et acquis par Red Hat en 2015. Ansible se connecte temporairement à distance sans agent via SSH ou Windows Remote Management (permettant l'exécution à distance de PowerShell). NetApp a développé plus de "150 modules Ansible pour le logiciel ONTAP", permettant une intégration supplémentaire avec la structure d'automatisation Ansible. Les modules Ansible pour NetApp fournissent un ensemble d'instructions sur la manière de définir l'état souhaité et de le relayer vers l'environnement NetApp cible. Les modules sont conçus pour prendre en charge des tâches telles que la configuration de licences, la création d'agrégats et de machines virtuelles de stockage, la création de volumes et la restauration de snapshots, pour n'en nommer que quelques-uns. Un rôle Ansible a été "Publié sur GitHub" spécifique au guide de déploiement des fonctionnalités unifiées du Ministère de la Défense NetApp.

En utilisant la bibliothèque de modules disponibles, les utilisateurs peuvent facilement développer des playbooks Ansible et les personnaliser en fonction de leurs propres applications et des besoins de l'entreprise pour automatiser des tâches courantes. Une fois qu'un PlayBook est écrit, vous pouvez l'exécuter pour exécuter la tâche spécifiée, ce qui permet de gagner du temps et d'améliorer la productivité. NetApp a créé et partagé des exemples de playbooks pouvant être utilisés directement ou personnalisés en fonction de vos besoins.

Data Infrastructure Insights est un outil de surveillance de l'infrastructure qui vous donne une visibilité sur l'ensemble de votre infrastructure. Avec Data Infrastructure Insights, vous pouvez surveiller, dépanner et optimiser toutes vos ressources, y compris vos instances de cloud public et vos centres de données privés. Data Infrastructure Insights peut réduire le temps moyen de résolution de 90 % et empêcher 80 % des problèmes de cloud d'affecter les utilisateurs finaux. Il peut également réduire les coûts d'infrastructure cloud de 33 % en moyenne et réduire votre exposition aux menaces internes en protégeant vos données grâce à des renseignements exploitables. La fonctionnalité de sécurité de la charge de travail de stockage de Data Infrastructure Insights permet l'analyse du comportement des utilisateurs avec l'IA et le ML pour alerter lorsque des comportements d'utilisateur aberrants se produisent en raison d'une menace interne. Pour ONTAP, Storage Workload Security utilise le moteur Zero Trust FPolicy.

Zero Trust et déploiements de cloud hybride

NetApp est l'autorité en matière de données pour le cloud hybride. NetApp propose une variété d'options pour étendre les systèmes de gestion de données sur site au cloud hybride avec Amazon Web Services (AWS), Microsoft Azure, Google Cloud et d'autres fournisseurs de cloud de premier plan. Les solutions cloud hybrides NetApp prennent en charge les mêmes contrôles de sécurité Zero Trust que ceux disponibles avec les systèmes ONTAP sur site et le stockage défini par logiciel ONTAP Select .

Vous pouvez facilement étendre la capacité des clouds publics sans contraintes CAPEX typiques en utilisant des services de fichiers cloud natifs de classe entreprise pour AWS (FSxN), Google Cloud (GCNV) et Azure NetApp Files pour Microsoft Azure. Idéals pour les charges de travail gourmandes en données telles que l'analyse et DevOps, ces services de données cloud combinent le stockage élastique à la demande en tant que service de NetApp avec la gestion des données ONTAP dans une offre entièrement gérée.

ONTAP permet le déplacement de données entre vos systèmes ONTAP sur site et l'environnement de stockage AWS, Google Cloud ou Azure avec le logiciel de réplication de données NetApp SnapMirror .

Contrôle d'accès basé sur les attributs

Contrôle d’accès basé sur les attributs avec ONTAP

À partir de la version 9.12.1, vous pouvez configurer ONTAP avec les étiquettes de sécurité NFSv4.2 et les attributs étendus (xattrs) pour prendre en charge le contrôle d’accès basé sur les rôles (RBAC) avec des attributs et le contrôle d’accès basé sur les attributs (ABAC).

ABAC est une stratégie d’autorisation qui définit les autorisations en fonction des attributs utilisateur, des attributs de ressource et des conditions environnementales. L’intégration de ONTAP avec les étiquettes de sécurité NFS v4.2 et les xattrs est conforme aux normes NIST pour les solutions ABAC, comme indiqué dans la publication spéciale NIST 800-162.

Vous pouvez utiliser les étiquettes de sécurité NFS v4.2 et les xattrs pour attribuer des attributs et des étiquettes définis par l’utilisateur de fichiers. ONTAP peut s’intégrer au logiciel de gestion des accès et des identités orienté ABAC pour appliquer des règles de contrôle d’accès granulaires aux fichiers et dossiers en fonction de ces attributs et étiquettes.

Informations associées

- "Approches de l’ABAC avec ONTAP"
- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d’implémentation"

Approches du contrôle d’accès basé sur les attributs (ABAC) dans ONTAP

ONTAP propose plusieurs approches pour assurer le contrôle d’accès basé sur des attributs (ABAC) au niveau des fichiers, notamment les étiquettes de sécurité NFS v4.2 et les attributs étendus (xattrs) à l’aide de NFS.

Étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, la fonctionnalité NFS v4.2 appelée NFS est prise en charge.

Les étiquettes de sécurité NFS v4.2 permettent de gérer l’accès granulaire aux fichiers et dossiers à l’aide d’étiquettes SELinux et de MAC (obligatoire Access Control). Ces étiquettes MAC sont stockées avec des fichiers et des dossiers et fonctionnent en conjonction avec les autorisations UNIX et les listes de contrôle d’accès NFS v4.x.

La prise en charge des étiquettes de sécurité NFS v4.2 signifie que ONTAP reconnaît et comprend désormais les paramètres d’étiquette SELinux du client NFS. Les étiquettes de sécurité NFS v4.2 sont couvertes par la norme RFC-7204.

Voici quelques cas d’utilisation des étiquettes de sécurité NFS v4.2 :

- Étiquetage MAC des images de machines virtuelles (VM)
- Classification de sécurité des données pour le secteur public (secret, secret et autres classifications)
- Conformité en matière de sécurité
- Linux sans disque

Activez les étiquettes de sécurité NFS v4.2

Vous pouvez activer ou désactiver les étiquettes de sécurité NFS v4.2 à l’aide de la commande suivante (privilège avancé requis) :

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

Pour en savoir plus, `vserver nfs modify` consultez le "Référence des commandes ONTAP".

Modes d'application pour les étiquettes de sécurité NFS v4.2

À partir de ONTAP 9.9.1, ONTAP prend en charge les modes d'application suivants :

- **Mode serveur limité** : ONTAP ne peut pas appliquer les étiquettes mais peut les stocker et les transmettre.

  La possibilité de modifier les étiquettes MAC revient au client de les appliquer.

- **Mode invité** : si le client n'est pas étiqueté NFS-Aware (v4.1 ou inférieur), les étiquettes MAC ne sont pas transmises.

  ONTAP ne prend actuellement pas en charge le mode complet (stockage et application des étiquettes MAC).

Exemples d'étiquettes de sécurité NFS v4.2

L'exemple de configuration suivant illustre les concepts d'utilisation de Red Hat Enterprise Linux version 9.3 (Plough).

L'utilisateur `jrsmith`, créé à partir des informations d'identification de John R. Smith, possède le compte Privileges suivant :

- Nom d'utilisateur = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Il existe deux rôles : le compte admin qui est un utilisateur privilégié et un utilisateur `jrsmith` comme décrit dans le tableau Privileges MLS suivant :

Utilisateurs	Rôle	Type	Niveaux
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

Dans cet exemple d'environnement, l'utilisateur `jrsmith` a accès aux fichiers aux niveaux de `s0 s3` . Nous pouvons améliorer les classifications de sécurité existantes, comme décrit ci-dessous, afin de nous assurer que les administrateurs n'ont pas accès aux données spécifiques aux utilisateurs.

- s0 = données utilisateur admin des privilèges
- s0 = données non classées
- s1 = confidentiel

- s2 = données secrètes
- s3 = données les plus secrètes

Exemple d'étiquettes de sécurité NFS v4.2 avec MCS

Outre la sécurité multi-niveaux (MLS), une autre fonctionnalité appelée sécurité multi-catégories (MCS) vous permet de définir des catégories telles que des projets.

Étiquette de sécurité NFS	Valeur
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Attributs étendus (xattrs)

À partir de ONTAP 9.12.1, ONTAP prend en charge xattrs. Xattrs permet d'associer des métadonnées à des fichiers et des répertoires au-delà de ce qui est fourni par le système, tels que les listes de contrôle d'accès (ACL) ou les attributs définis par l'utilisateur.

Pour implémenter xattrs, vous pouvez utiliser `setfattr` et `getfattr` les utilitaires de ligne de commande sous Linux. Ces outils fournissent un moyen puissant de gérer des métadonnées supplémentaires pour les fichiers et les répertoires. Elles doivent être utilisées avec précaution, car une utilisation inappropriée peut entraîner des comportements inattendus ou des problèmes de sécurité. Reportez-vous toujours aux `setfattr` pages de manuel et `getfattr` ou à toute autre documentation fiable pour obtenir des instructions d'utilisation détaillées.

Lorsque xattrs est activé sur un système de fichiers ONTAP, les utilisateurs peuvent définir, modifier et récupérer des attributs arbitraires sur les fichiers. Ces attributs peuvent être utilisés pour stocker des informations supplémentaires sur le fichier qui ne sont pas capturées par l'ensemble standard d'attributs de fichier, telles que les informations de contrôle d'accès.

Il existe plusieurs exigences et limites pour l'utilisation de xattrs dans ONTAP :

- Red Hat Enterprise Linux 8.4 ou version ultérieure
- Ubuntu 22.04 ou version ultérieure
- Chaque fichier peut avoir jusqu'à 128 xattrs
- Les clés xattr sont limitées à 255 octets
- La taille de la clé ou de la valeur combinée est de 1,729 octets par xattr
- Les répertoires et les fichiers peuvent avoir des xattrs
- Pour définir et récupérer les xattrs, `w` ou les bits de mode d'écriture doivent être activés pour l'utilisateur et le groupe

Les Xattrs sont utilisés dans l'espace de nom de l'utilisateur et n'ont aucune signification intrinsèque à ONTAP lui-même. Au lieu de cela, leurs applications pratiques sont déterminées et gérées exclusivement par l'application côté client qui interagit avec le système de fichiers.

Exemples de cas d'utilisation de xattr :

- Enregistrement du nom de l'application responsable de la création d'un fichier

- Conservation d'une référence à l'e-mail à partir duquel un fichier a été obtenu
- Établissement d'un cadre de catégorisation pour l'organisation des objets de fichier
- Étiquetage des fichiers avec l'URL de leur source de téléchargement d'origine

Commandes de gestion des xattrs

- `setfattr` définit un attribut étendu d'un fichier ou d'un répertoire :

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

  Exemple de commande :

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

- `getfattr` récupère la valeur d'un attribut étendu spécifique ou répertorie tous les attributs étendus d'un fichier ou d'un répertoire :

  Attribut spécifique :
  `getfattr -n <attribute_name> <file or directory name>`

  Tous les attributs :
  `getfattr <file or directory name>`

  Exemple de commande :

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

Exemples de paires de valeurs de clé xattr

Le tableau suivant présente deux exemples de paire de valeurs de clé xattr :

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

Autorisations utilisateur avec ACE pour xattrs

Une entrée de contrôle d'accès (ACE) est un composant d'une liste de contrôle d'accès qui définit les droits ou autorisations d'accès accordés à un utilisateur individuel ou à un groupe d'utilisateurs pour une ressource spécifique, comme un fichier ou un répertoire. Chaque ACE spécifie le type d'accès autorisé ou refusé et est associé à une entité de sécurité particulière (identité d'utilisateur ou de groupe).

Entrée de contrôle d'accès (ACE) requise pour les xattrs

- Retrieve xattr : autorisations requises pour qu'un utilisateur puisse lire les attributs étendus d'un fichier ou d'un répertoire. Le « R » signifie que l'autorisation de lecture est nécessaire.
- Set xattrs : les autorisations nécessaires pour modifier ou définir les attributs étendus. « A », « W » et « T » représentent différents exemples d'autorisations, telles que l'ajout, l'écriture et une autorisation spécifique liée aux xattrs.
- Fichiers : les utilisateurs doivent ajouter, écrire et éventuellement accorder une autorisation spéciale liée aux xattrs pour définir des attributs étendus.
- Répertoires : une autorisation spécifique « T » est requise pour définir des attributs étendus.

Type de fichier	Récupérer xattr	Définissez xattrs
Fichier	R	A,W,T
Répertoire	R	T

Intégration au logiciel ABAC Identity and Access Control

Pour exploiter pleinement les capacités d'ABAC, ONTAP peut s'intégrer à un logiciel de gestion des identités et des accès orienté ABAC.

Dans un système ABAC, le point d'application de la politique (PEP) et le point de décision de la politique (PDP) jouent des rôles cruciaux. Le PPE est responsable de l'application des politiques de contrôle d'accès, tandis que le PDP prend la décision d'accorder ou de refuser l'accès en fonction des politiques.

Dans la pratique, une entreprise utiliserait un mélange d'étiquettes de sécurité NFS et de xattrs. Ils sont utilisés pour représenter une variété de métadonnées, y compris la classification, la sécurité, l'application et le contenu, qui sont tous des éléments essentiels dans la prise de décisions ABAC. Xattrs, par exemple, peut être utilisé pour stocker les attributs de ressource que le PDP utilise pour son processus de prise de décision. Un attribut peut être défini pour représenter le niveau de classification d'un fichier (par exemple, « non classé », « confidentiel », « secret » ou « secret supérieur »). Le PDP pourrait alors utiliser cet attribut pour appliquer une stratégie qui limite les utilisateurs à accéder uniquement aux fichiers dont le niveau de classification est égal ou inférieur à leur niveau d'autorisation.

Ce contenu suppose que l'identité, l'authentification et les services d'accès du client incluent au moins une PPE et un PDP qui servent d'intermédiaires pour l'accès au système de fichiers.

Exemple de flux de processus pour ABAC

1. L'utilisateur présente les informations d'identification (par exemple, PKI, OAuth, SAML) pour accéder au système à PEP et obtient les résultats du PDP.

   Le rôle du PPE est d'intercepter la demande d'accès de l'utilisateur et de la transférer au PDP.

2. Le PDP évalue ensuite cette demande par rapport aux politiques établies de l'ABAC.

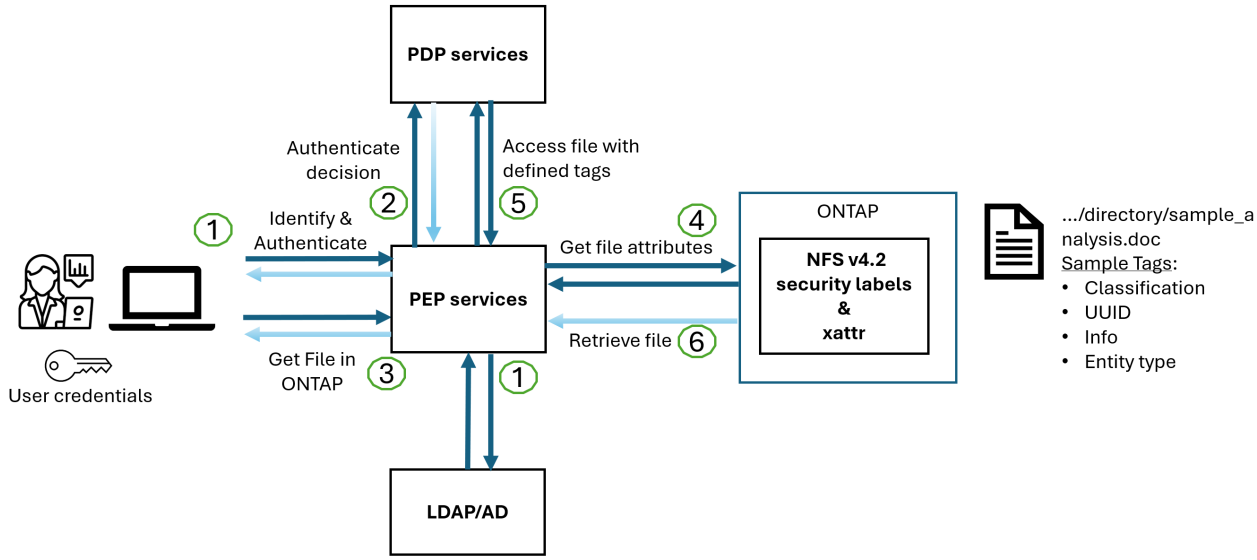
   Ces stratégies tiennent compte de divers attributs liés à l'utilisateur, à la ressource en question et à l'environnement environnant. En fonction de ces politiques, le PDP prend une décision d'accès d'autoriser ou de refuser, puis communique cette décision à la PPE.

   PDP fournit une politique à PEP pour qu'elle l'applique. Le PPE applique ensuite cette décision, en accordant ou en refusant la demande d'accès de l'utilisateur conformément à la décision du PDP.

3. Après une demande réussie, l'utilisateur demande un fichier stocké dans ONTAP (AFF, AFF-C, par exemple).

4. Si la demande réussit, PEP obtient des étiquettes de contrôle d'accès à grain fin à partir du document.
5. PEP demande la politique de l'utilisateur en fonction des certificats de cet utilisateur.
6. PEP prend une décision en fonction de la politique et des balises si l'utilisateur a accès au fichier et permet à l'utilisateur de le récupérer.

L'accès réel peut être effectué à l'aide de jetons.



Clonage ONTAP et SnapMirror

Les technologies de clonage et de SnapMirror de ONTAP sont conçues pour offrir des fonctionnalités de réplication et de clonage des données efficaces et fiables, garantissant que tous les aspects des données de fichiers, y compris les xattrs, sont conservés et transférés avec le fichier. Les xattrs sont essentiels car ils stockent des métadonnées supplémentaires associées à un fichier, telles que des étiquettes de sécurité, des informations de contrôle d'accès et des données définies par l'utilisateur, qui sont essentielles pour maintenir le contexte et l'intégrité du fichier.

Lorsqu'un volume est cloné à l'aide de la technologie FlexClone de ONTAP, une réplique inscriptible exacte du volume est créée. Ce processus de clonage est instantané et compact. Il inclut toutes les données de fichiers et métadonnées, garantissant ainsi la réplication complète des fichiers xattrs. De même, SnapMirror garantit la mise en miroir parfaite des données vers un système secondaire. Cela inclut les xattrs, qui sont essentiels pour que les applications qui s'appuient sur ces métadonnées fonctionnent correctement.

En incluant les xattrs dans les opérations de clonage et de réplication, NetApp ONTAP s'assure que l'ensemble du dataset, avec toutes ses caractéristiques, est disponible et cohérent sur l'ensemble des systèmes de stockage primaire et secondaire. Cette approche globale de la gestion des données est cruciale pour les entreprises qui ont besoin d'une protection cohérente des données, d'une restauration rapide et du respect des normes de conformité et réglementaires. Elle simplifie également la gestion des données entre différents environnements, sur site ou dans le cloud, garantissant ainsi aux utilisateurs que leurs données sont complètes et non modifiées au cours de ces processus.

Les étiquettes de sécurité NFS v4.2 présentent les restrictions définies dans le Étiquettes de sécurité NFS v4.2.

Audit des modifications apportées aux étiquettes

L'audit des modifications apportées aux étiquettes de sécurité xattrs ou NFS constitue un aspect essentiel de la gestion et de la sécurité du système de fichiers. Les outils d'audit standard du système de fichiers permettent de surveiller et de consigner toutes les modifications apportées à un système de fichiers, y compris les modifications apportées aux xattrs et aux étiquettes de sécurité.

Dans les environnements Linux, le `auditd` démon est généralement utilisé pour établir un audit pour les événements du système de fichiers. Il permet aux administrateurs de configurer des règles pour surveiller des appels système spécifiques liés aux modifications xattr, telles que `setxattr`, `lsetxattr` et pour définir des attributs et, `lremovexattr` et `fsetxattr` `fremovexattr` pour supprimer des attributs `removexattr`.

ONTAP FPolicy étend ces fonctionnalités en fournissant une structure robuste pour la surveillance et le contrôle en temps réel des opérations de fichiers. FPolicy peut être configuré pour prendre en charge divers événements xattr, offrant un contrôle granulaire des opérations sur fichiers et la possibilité d'appliquer des règles complètes de gestion des données.

Pour les utilisateurs utilisant xattrs, en particulier dans les environnements NFS v3 et NFS v4, seules certaines combinaisons d'opérations et de filtres de fichiers sont prises en charge pour la surveillance. La liste des combinaisons de filtres et d'opérations de fichiers prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFS v3 et NFS v4 est détaillée ci-dessous :

Opérations de fichiers prises en charge	Filtres pris en charge
`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`

Exemple de fragment de journal auditd pour une opération 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"
```

L'activation "ONTAP FPolicy" pour les utilisateurs travaillant avec xattrs fournit une couche de visibilité et de contrôle qui est essentielle au maintien de l'intégrité et de la sécurité du système de fichiers. Grâce aux fonctionnalités avancées de surveillance de FPolicy, les entreprises peuvent s'assurer que toutes les modifications apportées aux xattrs font l'objet d'un suivi, d'un audit et d'une mise en adéquation avec leurs normes de sécurité et de conformité. Cette approche proactive de la gestion du système de fichiers explique pourquoi l'activation de ONTAP FPolicy est fortement recommandée pour toute entreprise qui souhaite améliorer ses stratégies de gouvernance et de protection des données.

Exemples de contrôle de l'accès aux données

L'exemple d'entrée ci-dessous pour les données stockées dans le certificat PKI de John R. Smith montre comment l'approche de NetApp peut être appliquée à un fichier et fournit un contrôle d'accès précis.

Ces exemples sont fournis à titre d'exemple et il incombe au client de déterminer les métadonnées associées aux étiquettes de sécurité et aux fichiers xattrs NFS v4.2. Les détails sur la mise à jour et la conservation des étiquettes sont omis pour plus de simplicité.

Exemple de valeurs de certificat PKI

Clé	Valeur
EntitySecurityMark	t:s01 = non confidentiel

Info	{
	"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"
	}
	}

spécifications	« DOD »
uuid	b4111349-7875-4115-ad30-0928565f2e15

Clé	Valeur

AdminOrganisation	{
	"value": "DoD"
	}

réunions d'information	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

État de la citoyenneté	{
	"value": "US"
	}

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

Clé	Valeur

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

Identificateur numérique	{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

Démontez	{
	  "value": "DoD"
	}

DutyOrganisation	{
	  "value": "DoD"
	}

EntityType	{
	  "value": "GOV"
	}

Clé	Valeur

FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Ces droits ICP montrent les détails d'accès de John R. Smith, y compris l'accès par type de données et l'attribution.

Dans les cas où les métadonnées IC-TDF sont stockées séparément du fichier, NetApp préconise une couche supplémentaire de contrôle d'accès granulaire. Cela implique le stockage des informations de contrôle d'accès au niveau du répertoire et en association avec chaque fichier. Prenons l'exemple des balises suivantes liées à un fichier :

- Étiquettes de sécurité NFS v4.2 : utilisées pour prendre les décisions relatives à la sécurité
- Xattrs : fournir des renseignements supplémentaires pertinents au dossier et aux exigences du programme organisationnel

Les paires clé-valeur suivantes sont des exemples de métadonnées qui peuvent être stockées sous forme de xattrs et fournissent des informations détaillées sur le créateur du fichier et les classifications de sécurité associées. Ces métadonnées peuvent être exploitées par les applications client pour prendre des décisions éclairées en matière d'accès et organiser les fichiers en fonction des normes et des exigences de l'entreprise.

Exemple de paires clé-valeur xattr

Clé	Valeur
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Clé	Valeur

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"
	},

Clé	Valeur
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Informations associées

- "NFS dans NetApp ONTAP : guide des bonnes pratiques et d'implémentation"
- "Référence des commandes ONTAP"
- Demande de commentaires (RFC)
  - "RFC 7204 : exigences pour le protocole NFS étiqueté"
  - "RFC 2203 : spécification du protocole RPCSEC_GSS"
  - "RFC 3530 : protocole NFS (Network File System) version 4"