Protection autonome contre les ransomwares

ONTAP 9

NetApp
February 13, 2026

Sommaire

Protection autonome contre les ransomwares

Découvrez la protection anti-ransomware autonome de ONTAP

À partir d' ONTAP 9.10.1, les administrateurs ONTAP peuvent activer la protection autonome contre les ransomwares (ARP) pour analyser la charge de travail dans les environnements NAS (NFS et SMB) afin de détecter et d'alerter proactivement toute activité anormale pouvant indiquer une attaque de ransomware. À partir d' ONTAP 9.17.1, ARP prend également en charge les volumes de périphériques de blocs, y compris les volumes SAN contenant des LUN ou des espaces de noms NVMe, ou les volumes NAS contenant des disques virtuels provenant d'hyperviseurs tels que VMware.

ARP est directement intégré à ONTAP, assurant un contrôle et une coordination intégrés avec les autres fonctionnalités d'ONTAP. ARP fonctionne en temps réel, traitant les données au fur et à mesure de leur écriture ou de leur lecture dans le système de fichiers, et détectant et répondant rapidement aux attaques potentielles de ransomware.

ARP crée des instantanés verrouillés à intervalles réguliers, en plus des instantanés planifiés, pour une protection accrue. Il gère intelligemment la durée de conservation des instantanés. Si aucune activité inhabituelle n'est détectée, les instantanés sont rapidement recyclés. Toutefois, si une attaque est détectée, un instantané créé avant le début de l'attaque est conservé pendant une période prolongée. Pour plus d'informations, notamment sur les modifications apportées par la version ONTAP , consultez Instantanés ARP.

Licences et activation

Vous avez besoin d'une licence pour utiliser ARP. Décidez d'activer ARP par défaut sur les nouveaux volumes ou de l'activer manuellement par volume.

Options de licence pour ARP

La prise en charge d'ARP est incluse."Licence ONTAP One" . Si vous ne disposez pas de la licence ONTAP One, d'autres licences sont disponibles pour l'utilisation d'ARP qui diffèrent selon votre version d' ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.11.1 et versions ultérieures	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (Gestion des clés multi-locataires)

- Si vous effectuez une mise à niveau d' ONTAP 9.10.1 vers ONTAP 9.11.1 ou une version ultérieure et qu'ARP est déjà configuré sur votre système, vous n'avez pas besoin d'installer le nouveau `Anti-ransomware` licence. Pour les nouvelles configurations ARP, la nouvelle licence est requise.
- Si vous revenez d' ONTAP 9.11.1 ou version ultérieure à ONTAP 9.10.1 et que vous avez activé ARP avec la licence Anti_ransomware, vous verrez un message d'avertissement et devrez peut-être reconfigurer ARP. "Découvrez le rétablissement ARP" .

Options d'activation pour ARP

ARP offre des options d'activation flexibles au niveau du cluster, de la SVM et du volume, vous permettant de configurer une activation automatique par défaut pour les nouveaux volumes ou d'activer ARP manuellement sur les volumes existants selon vos besoins.

Activation automatique par défaut sur les nouveaux volumes

À partir d'ONTAP 9.18.1, ARP est activé par défaut automatiquement sur tous les nouveaux volumes pour les systèmes AFF séries A et AFF séries C, ASA et ASA r2. Cette activation automatique par défaut d'ARP ne s'applique pas à "volumes ou configurations non pris en charge".

L'activation par défaut d'ARP sur les nouveaux volumes prend effet après un délai de grâce de 12 heures suivant une mise à niveau ou immédiatement pour une nouvelle installation d'ONTAP 9.18.1, à condition qu'une licence ARP soit installée dans les deux cas. Vous devez activer ARP manuellement sur les volumes existants.

Pendant le délai de grâce, vous pouvez "désactivez l'activation par défaut pour les nouveaux volumes au niveau du cluster à l'aide de System Manager ou de l'interface de ligne de commande ONTAP". Si vous ne vous y opposez pas, ARP est automatiquement activé pour tous les nouveaux volumes créés après la fin du délai de grâce. Si vos besoins changent après le délai de grâce, vous avez également la flexibilité d'activer ou de désactiver l'activation par défaut à tout moment.

Activation manuelle par défaut sur les nouveaux volumes

Si vous avez désactivé l'activation automatique par défaut d'ARP au niveau du cluster, vous pouvez également choisir de "Activer manuellement ARP par défaut sur tous les nouveaux volumes" au niveau de la SVM. Pour ONTAP 9.17.1 et versions antérieures, c'est la seule façon de configurer ARP pour qu'il soit activé par défaut sur les nouveaux volumes.

Activation d'ARP sur tous les volumes existants ou sur certains volumes spécifiques

À partir de la version 9.18.1, vous pouvez activer manuellement ARP sur tous les volumes existants au niveau du cluster (sélectionnez **Cluster > Sécurité** et ⋮ dans la section **Anti-ransomware**, puis sélectionnez **Activer sur tous les volumes existants**).

Si vous préférez limiter l'activation d'ARP à un volume spécifique, vous pouvez "Activer ARP sur une base par volume".

Stratégie ONTAP de protection contre les ransomwares

Une protection efficace contre les ransomwares nécessite de nombreuses couches de protection fonctionnant ensemble.

Alors que ONTAP inclut des fonctionnalités telles que FPolicy, les instantanés, SnapLock et Active IQ Digital Advisor (également connu sous le nom de Digital Advisor) pour aider à se protéger contre les ransomwares, ARP fournit une couche de défense supplémentaire.

Pour en savoir plus sur les autres fonctionnalités du portefeuille NetApp qui protègent contre les ransomwares, consultez :

- "Ransomware et le portefeuille de solutions de protection de NetApp"
- "Renforcement du coffre-fort cybernétique ONTAP avec PowerShell"

Ce que le protocole ARP détecte

ONTAP ARP est conçu pour protéger contre les attaques par déni de service (DDoS), où l'attaquant retient les données jusqu'au paiement d'une rançon. ARP offre une détection des rançongiciels en temps réel basée sur les éléments suivants :

- Identification des données entrantes sous forme de texte chiffré ou brut.
- Une analytique qui détecte :
  - **Entropie** : (Utilisé dans NAS et SAN) Une évaluation du caractère aléatoire des données dans un fichier
  - **Types d'extensions de fichiers** : (utilisé uniquement dans NAS) Une extension de fichier qui n'est pas conforme aux types d'extension attendus
  - **IOPS de fichier** : (utilisé dans les NAS uniquement à partir d' ONTAP 9.11.1) Une augmentation de l'activité anormale du volume avec chiffrement des données

ARP détecte la propagation de la plupart des attaques de ransomware après le chiffrement d'un petit nombre de fichiers, répond automatiquement pour protéger les données et vous avertit qu'une attaque suspectée est en cours.

Aucun système de détection de ransomware ne peut garantir une sécurité totale. ARP fournit une couche de défense supplémentaire si le logiciel antivirus ne parvient pas à détecter une intrusion.

En savoir plus sur les modes ARP

Une fois ARP activé pour un volume, il entre dans une période d'apprentissage pour établir une ligne de base. ARP analyse les mesures du système pour développer un profil d'alerte avant de passer au mode de détection active. En mode actif, ARP surveille les activités anormales, prend des mesures de protection et génère des alertes s'il détecte un comportement anormal.

Pour ARP, les comportements du mode d'apprentissage et du mode actif diffèrent selon la version ONTAP , le type de volume et le protocole (NAS ou SAN).

Environnements NAS et types de modes

Le tableau suivant résume les différences entre ONTAP 9.10.1 et les versions ultérieures pour les environnements NAS.

Dans les versions utilisant l'ancien modèle ARP, une période d'apprentissage est recommandée avant le début de la surveillance active. Pour les environnements NAS qui prennent en chargeARP/IA , il n'y a pas de période d'apprentissage et la surveillance active commence immédiatement.

Mode	Description	Types et versions de volumes
Apprentissage	Pour certaines versions d' ONTAP et certains types de volumes, ARP est automatiquement configuré en mode d'apprentissage lorsque vous activez ARP. En mode d'apprentissage, le système ONTAP développe un profil d'alerte basé sur les domaines d'analyse suivants : entropie, types d'extensions de fichiers et IOPS de fichiers. Il est recommandé de laisser ARP en mode d'apprentissage pendant 30 jours. À partir d' ONTAP 9.13.1, ARP détermine automatiquement l'intervalle d'apprentissage optimal et automatise le basculement, qui peut intervenir avant 30 jours. Pour les versions antérieures à ONTAP 9.13.1, vous pouvez effectuer le basculement manuellement. À partir d' ONTAP 9.16.1 pour les volumes FlexVol , seul le mode actif existe et le mode d'apprentissage passe automatiquement en mode actif pour tous les volumes FlexVol mis à niveau vers cette version ou une version ultérieure. Pour ONTAP 9.16.1 à 9.17.1, les volumes FlexGroup ne sont pas encore pris en charge par ARP/AI et continuent d'exécuter l'ancien modèle ARP. C'est pourquoi une période d'apprentissage est toujours recommandée pour ces versions avec les volumes FlexGroup . À partir d' ONTAP 9.18.1, seul le mode actif existe pour les volumes FlexVol et FlexGroup . Tous les volumes mis à niveau passent automatiquement en mode actif. "En savoir plus sur le passage du mode apprentissage au mode actif" . La commande `security anti-ransomware volume workload-behavior show` affiche les extensions de fichier qui ont été détectées dans le volume. Si vous exécutez cette commande très tôt en mode d'apprentissage et qu'elle affiche une représentation précise des types de fichiers, vous ne devez pas utiliser ces données comme base pour passer en mode actif, car ONTAP collecte toujours d'autres metrics. Pour en savoir plus, `security anti-ransomware volume workload-behavior show` consultez le "Référence de commande ONTAP".	• Volumes FlexVol avec ONTAP 9.10.1 à 9.15.1 • Volumes FlexGroup avec ONTAP 9.13.1 à ONTAP 9.17.1
Actif	En mode actif, si une extension de fichier est signalée comme anormale, vous devez évaluer l'alerte. Vous pouvez agir sur l'alerte pour protéger vos données ou la marquer comme faux positif. Marquer une alerte comme faux positif met à jour le profil d'alerte. Par exemple, si l'alerte est déclenchée par une nouvelle extension de fichier et que vous la marquez comme faux positif, vous ne recevrez pas d'alerte la prochaine fois que l'extension de fichier sera détectée.	Toutes les versions ONTAP prises en charge et les volumes FlexVol et FlexGroup

Environnements SAN et types de modes

Les environnements SAN utilisent des périodes d'évaluation (similaires aux modes d'apprentissage des environnements NAS) avant de passer automatiquement à la détection active. Le tableau suivant récapitule les modes d'évaluation et actif.

Mode	Description	Types et versions de volumes
Évaluation	Une période d'évaluation de deux à quatre semaines est effectuée pour déterminer le comportement de chiffrement de base, tandis que ARP/AI assure une protection active immédiate des volumes SAN pendant la période d'évaluation. La détection et les alertes peuvent survenir pendant l'établissement des seuils de référence. Vous pouvez déterminer si la période d'évaluation est terminée en exécutant le `security anti-ransomware volume show` commande et vérification `Block device detection status` . "En savoir plus sur les volumes SAN et la période d'évaluation de l'entropie" .	• Volumes FlexVol avec ONTAP 9.17.1 et versions ultérieures
Actif	Après la période d'évaluation, vous pouvez déterminer si la protection ARP SAN est active en exécutant le `security anti-ransomware volume show` commande et vérification `Block device detection status` . Un statut de `Active_suitable_workload` Indique que la quantité d'entropie évaluée peut être surveillée avec succès. L'ARP ajuste automatiquement le seuil adaptatif en fonction des données examinées lors de l'évaluation.	• Volumes FlexVol avec ONTAP 9.17.1 et versions ultérieures

Évaluation des menaces et instantanés ARP

ARP évalue la probabilité d'une menace en fonction des données entrantes comparées aux analyses apprises. Lorsque ARP détecte une anomalie, une mesure est attribuée. ARP peut attribuer un snapshot au moment de la détection ou à intervalles réguliers.

seuils ARP

- **Faible** : première détection d'une anomalie dans le volume (par exemple, une nouvelle extension de fichier est observée dans le volume). Ce niveau de détection n'est disponible que dans les versions antérieures à ONTAP 9.16.1 qui n'ont pas ARP/ai.
  - À partir d' ONTAP 9.11.1, vous pouvez "personnaliser les paramètres de détection pour ARP" .
  - Dans ONTAP 9.10.1, le seuil de remontée à modéré est de 100 fichiers ou plus.
- **Modéré** : Une entropie élevée est détectée ou plusieurs fichiers portant la même extension inédite sont observés. Il s'agit du niveau de détection de base dans ONTAP 9.16.1 et versions ultérieures avec ARP/AI.

La menace devient modérée après ONTAP a généré un rapport d'analyse déterminant si l'anomalie correspond à un profil de rançongiciel. Lorsque la probabilité d'attaque est modérée, ONTAP génère une notification EMS vous invitant à évaluer la menace. ONTAP n'envoie pas d'alertes sur les menaces faibles ; cependant, à partir d'ONTAP 9.14.1, vous pouvez "modifier les paramètres d'alerte par défaut". voir "Réagir à une activité anormale" .

Vous pouvez afficher des informations sur les menaces modérées dans la section **Events** de System Manager

ou à l'aide de `security anti-ransomware volume show` la commande. Les événements à faible menace peuvent également être affichés à l'aide de `security anti-ransomware volume show` la commande dans les versions antérieures à ONTAP 9.16.1 qui n'ont pas ARP/ai. Pour en savoir plus, `security anti-ransomware volume show` consultez le "Référence de commande ONTAP".

Instantanés ARP

ARP crée un instantané lorsque les premiers signes d'une attaque sont détectés. Une analyse détaillée est ensuite effectuée pour confirmer ou infirmer l'attaque potentielle. Étant donné que les instantanés ARP sont créés de manière proactive avant même qu'une attaque ne soit entièrement confirmée, ils peuvent également être générés à intervalles réguliers pour certaines applications légitimes. La présence de ces instantanés ne doit pas être considérée comme une anomalie. Si une attaque est confirmée, la probabilité d'attaque est augmentée à `Moderate` et une notification d'attaque est générée.

À partir d' ONTAP 9.17.1, des instantanés ARP sont générés à intervalles réguliers pour les volumes NAS et SAN ainsi qu'en réponse aux anomalies détectées. ONTAP ajoute un nom au snapshot ARP pour le rendre facilement identifiable.

À partir d' ONTAP 9.11.1, vous pouvez modifier les paramètres de rétention. Pour plus d'informations, consultez la section "Modifier les options pour les instantanés" .

Le tableau suivant résume les différences entre les instantanés ARP par version.

Fonction	ONTAP 9.17.1 et versions ultérieures	ONTAP 9.16.1 et versions antérieures
Déclencheur de création	• Les instantanés sont créés à des intervalles fixes de 4 heures, quel que soit un déclencheur spécifique • Confirmation d'une attaque Un instantané « périodique » ou « d'attaque » est créé en fonction du type de déclencheur.	• Une entropie élevée est détectée • Une nouvelle extension de fichier est détectée (9.15.1 et versions antérieures) • Une augmentation des opérations sur les fichiers est détectée (9.15.1 et versions antérieures) L'intervalle de création d'instantané est basé sur le type de déclencheur.
Convention de nom préfixé	« Sauvegarde périodique anti-ransomware » « Sauvegarde anti-attaque anti-ransomware »	« Sauvegarde anti-ransomware »
Comportement de suppression	L'instantané ARP est verrouillé et ne peut pas être supprimé par l'administrateur	L'instantané ARP est verrouillé et ne peut pas être supprimé par l'administrateur
Nombre maximal d'instantanés	"Limite configurable de six instantanés"	"Limite configurable de six instantanés"

Fonction	ONTAP 9.17.1 et versions ultérieures	ONTAP 9.16.1 et versions antérieures
Période de conservation	Les instantanés sont normalement conservés pendant 12 heures. • Volumes NAS : si une attaque est confirmée par l'analyse des fichiers, les instantanés créés avant l'attaque sont conservés jusqu'à ce que l'administrateur marque l'attaque comme vraie ou comme un faux positif (suspect clair). • Volume SAN ou banques de données de machines virtuelles : si une attaque est confirmée par une analyse d'entropie de bloc, les instantanés créés avant l'attaque sont conservés pendant 10 jours (configurable).	• Déterminé en fonction des conditions de déclenchement (non fixe) • Les instantanés créés avant l'attaque sont conservés jusqu'à ce que l'administrateur marque l'attaque comme vraie ou comme un faux positif (suspect clair).
Action clairement suspecte	Les administrateurs peuvent effectuer une action de suspicion claire qui définit la conservation en fonction de la confirmation : • 24 heures pour la rétention des faux positifs • 7 jours pour une rétention de vrais positifs	Les administrateurs peuvent effectuer une action de suspicion claire qui définit la conservation en fonction de la confirmation : • 24 heures pour la rétention des faux positifs • 7 jours pour une rétention de vrais positifs Ce comportement de conservation préventive n'existe pas avant ONTAP 9.16.1
Délai d'expiration	Un délai d'expiration est défini pour tous les instantanés	Aucune

Comment récupérer des données dans ONTAP après une attaque par ransomware

ARP s'appuie sur la technologie éprouvée de protection des données et de reprise après sinistre ONTAP pour répondre aux attaques de ransomware. ARP crée des instantanés verrouillés lorsque les premiers signes d'une attaque sont détectés. Vous devrez d'abord confirmer si l'attaque est réelle ou un faux positif. Si l'attaque est confirmée, le volume peut être restauré à l'aide du snapshot ARP.

Les instantanés verrouillés ne peuvent pas être supprimés par des moyens normaux. Cependant, si vous décidez ultérieurement de marquer l'attaque comme un faux positif, ONTAP supprime la copie verrouillée.

Vous pouvez récupérer les fichiers affectés à partir de certains instantanés au lieu de restaurer l'intégralité du volume.

Consultez les rubriques suivantes pour plus d'informations sur la réponse à une attaque et la récupération des données :

- "Réagir à une activité anormale"
- "Récupérer des données à partir d'instantanés ARP"
- "Récupérer à partir des instantanés ONTAP"

- "Restauration intelligente par ransomware"

Protection de vérification multiadministrateur pour ARP

Depuis la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour la configuration ARP (Autonomous ransomware protection). Pour plus d'informations, voir "Activez la vérification multiadministrateur".

Protection anti-ransomware autonome avec l'intelligence artificielle (ARP/IA)

À partir d' ONTAP 9.16.1, ARP améliore la cyber-résilience en adoptant un modèle d'apprentissage automatique pour l'analyse anti-ransomware, qui détecte les formes de ransomware en constante évolution avec une précision de 99 % dans les environnements NAS. Le modèle d'apprentissage automatique d'ARP est pré-entraîné sur un vaste ensemble de fichiers, avant et après une simulation d'attaque de ransomware. Cette formation, gourmande en ressources, est réalisée en dehors ONTAP à l'aide d'ensembles de données de recherche forensique open source. Les données clients ne sont pas utilisées tout au long du processus de modélisation et aucun problème de confidentialité n'est soulevé. Le modèle pré-entraîné issu de cette formation est inclus avec ONTAP. Ce modèle n'est ni accessible ni modifiable via l'interface de ligne de ONTAP (CLI) ou l'API ONTAP .

Transition immédiate vers une protection active pour ARP/IA

Avec ARP/IA, il n'y a paspériode d'apprentissage . ARP/AI est actif immédiatement après l'installation ou la mise à niveau pour les types de volumes pris en charge suivants :

- Volumes NAS FlexVol avec ONTAP 9.16.1 et versions ultérieures
- Volumes NAS FlexGroup avec ONTAP 9.18.1 et versions ultérieures
- Les volumes SAN avec ONTAP 9.17.1 et versions ultérieures (actifs immédiatement, même pendant le"période d'évaluation")

Pour les volumes existants et nouveaux dont la fonctionnalité ARP est déjà activée, la protection ARP/AI sera automatiquement active après la mise à niveau de votre cluster vers une version ONTAP prenant en charge ARP/AI.

Mises à jour automatiques ARP/ai

Pour maintenir une protection à jour contre les dernières menaces de ransomware, ARP/AI propose des mises à jour automatiques fréquentes, en dehors des cadences habituelles de mise à niveau et de publication ONTAP . Si vous avez "mises à jour automatiques activées" Vous pourrez alors recevoir automatiquement les mises à jour de sécurité d'ARP/AI après avoir sélectionné les mises à jour automatiques des fichiers de sécurité. Vous pouvez également choisir "effectuer ces mises à jour manuellement" et contrôler quand les mises à jour se produisent.

Depuis ONTAP 9.16.1, les mises à jour de sécurité pour ARP/ai sont disponibles via System Manager en plus des mises à jour du système et du micrologiciel.

"En savoir plus sur les mises à jour ARP/ai"

Différences entre les modèles ARP/AI et ARP en un coup d'œil

Fonction	ARP	ARP/IA
Versions ONTAP	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 et versions ultérieures ; 9.15.1 (tech preview)

Fonction	ARP	ARP/IA
Méthode de détection	Analyse l'activité des fichiers, l'entropie des données et les types d'extension de fichiers	Modèle d'IA/apprentissage automatique entraîné sur de vastes ensembles de données forensiques ; analyse l'entropie et le comportement des fichiers
Période d'apprentissage	Nécessite un mode d'apprentissage de 30 jours pour les volumes NAS FlexVol (basculement automatique disponible dans la version 9.13.1 et ultérieures)	Aucune période d'apprentissage ; active immédiatement dès l'activation
Prise en charge des types de volumes	• FlexVol: 9.10.1 et versions ultérieures • FlexGroup: 9.13.1 et versions ultérieures • SAN: Non pris en charge	• FlexVol: 9.16.1 et versions ultérieures • FlexGroup: 9.18.1 et versions ultérieures • SAN : 9.17.1 et versions ultérieures (avec période d'évaluation)
Création d'instantanés	Déclenché par une entropie élevée, de nouvelles extensions de fichiers ou des pics d'opérations sur les fichiers	Créés à intervalles fixes de 4 heures et lors de la confirmation de l'attaque
Conservation des instantanés	Conservé jusqu'à ce que l'administrateur efface l'activité suspecte	Délai par défaut de 12 heures ; prolongé en fonction de la confirmation de l'attaque (24 heures pour un faux positif, 7 jours pour un positif confirmé)
Mises à jour	Logique de détection statique (mise à jour uniquement avec les mises à niveau ONTAP)	Mises à jour de sécurité automatiques indépendantes des versions d'ONTAP
Déploiement	Activation manuelle par volume ou paramètre par défaut au niveau SVM	Activation manuelle par volume ou paramètre par défaut au niveau de la SVM ; activation par défaut sur tous les nouveaux volumes au niveau du cluster pour les systèmes pris en charge en 9.18.1 et versions ultérieures
Période d'évaluation	Sans objet	Nécessaire pour les volumes SAN (2 à 4 semaines) afin d'établir les seuils de chiffrement de base

Informations associées

- "Référence de commande ONTAP"

Cas d’utilisation et considérations de la protection anti-ransomware autonome de ONTAP

La protection autonome contre les ransomwares (ARP) est disponible pour les charges de travail NAS à partir d' ONTAP 9.10.1 et SAN à partir d' ONTAP 9.17.1. Avant de déployer ARP, vous devez connaître les utilisations recommandées et les configurations prises en charge, ainsi que les implications en termes de performances.

Configurations prises en charge et non prises en charge

Lorsque vous décidez d’utiliser ARP, il est important de vous assurer que la charge de travail de votre volume est adaptée à ARP et qu’elle répond aux configurations système requises.

Charges de travail adaptées

ARP est adapté à ces types de charges de travail :

- Bases de données sur stockage NFS ou SAN
- Répertoires locaux Windows ou Linux

  Dans les environnements sans ARP/AI, les utilisateurs peuvent créer des fichiers dont les extensions ne sont pas détectées lors de la période d’apprentissage. De ce fait, le risque de faux positifs est plus élevé dans cette charge de travail.

- Images et vidéos

  Par exemple, les dossiers médicaux et les données EDA

Charges de travail non adaptées

ARP n’est pas adapté à ces types de charges de travail :

- Charges de travail avec une fréquence élevée d’opérations de création ou de suppression de fichiers (des centaines de milliers de fichiers en quelques secondes ; par exemple, charges de travail de test/développement).
- La détection des menaces par ARP repose sur sa capacité à reconnaître une augmentation inhabituelle des opérations de création, de renommage ou de suppression de fichiers. Si l’application elle-même est à l’origine de l’activité du fichier, elle ne peut être distinguée efficacement d’une activité de rançongiciel.
- Charges de travail où l’application ou l’hôte crypte les données.

  ARP distingue les données entrantes chiffrées ou non chiffrées. Si l’application chiffre les données elle-même, son efficacité est réduite. Cependant, ARP peut toujours fonctionner en fonction de l’activité du fichier (suppression, écrasement, création, ou renommage avec une nouvelle extension) et du type de fichier.

Configurations compatibles

ARP est disponible pour les volumes NAS NFS et SMB FlexVol à partir d' ONTAP 9.10.1. À partir de la version 9.17.1, ARP est disponible pour les volumes SAN FlexVol pour iSCSI, FC et NVMe avec stockage SAN.

Le protocole ARP est pris en charge pour les configurations MetroCluster à partir de ONTAP 9.10.1.

La prise en charge d'autres configurations et types de volumes est disponible dans les versions ONTAP suivantes :

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protégés avec réplication asynchrone SnapMirror	✓	✓	✓	✓	✓	✓	✓		
SVM protégé avec réplication asynchrone SnapMirror (reprise d'activité SVM)	✓	✓	✓	✓	✓	✓	✓		
Mobilité des données des SVM (`vserver migrate`)	✓	✓	✓	✓	✓	✓	✓		
Volumes FlexGroup [1]	✓	✓	✓	✓	✓	✓			
Vérification multi-administrateurs	✓	✓	✓	✓	✓				
ARP/ai avec mises à jour automatiques	✓	✓							

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Activation par défaut ARP/AI[2]	✓								

[1] ONTAP 9.16.1 et 9.17.1 ne fournissent pas de prise en charge ARP/AI pour les volumes FlexGroup . Après une mise à niveau vers ces versions, les volumes FlexGroup activés pour ARP continuent de fonctionner avec le même modèle ARP utilisé avant ARP/AI. À partir d' ONTAP 9.18.1, les volumes FlexGroup utilisent le modèle ARP/AI.

[2] À partir d'ONTAP 9.18.1, le comportement d'activation par défaut d'ARP/AI est disponible pour les systèmes AFF A-series et AFF C-series, ASA et ASA r2. Ce comportement active automatiquement ARP/AI sur tous les nouveaux volumes après un délai de grâce de 12 heures suivant une mise à niveau ou immédiatement pour les nouvelles installations d'ONTAP 9.18.1. Vous devrez activer ARP manuellement sur "volumes existants".

Interopérabilité SnapMirror et ARP

À partir d' ONTAP 9.12.1, ARP est pris en charge sur les volumes de destination asynchrones SnapMirror . Le protocole ARP n'est *pas* pris en charge avec SnapMirror synchrone ou SnapMirror synchrone actif.

Si un volume source SnapMirror est compatible ARP, le volume de destination SnapMirror acquiert automatiquement l'état de configuration ARP (tel que `dry-run` ou `enabled`), données d'entraînement ARP et instantané du volume source créé par ARP. Aucune activation explicite n'est requise.

Bien que le volume de destination soit constitué d'instantanés en lecture seule (RO), aucun traitement ARP n'est appliqué à ses données. Cependant, lorsque le volume de destination SnapMirror est converti en lecture-écriture (RW), ARP est automatiquement activé sur le volume de destination converti en RW. Le volume de destination ne nécessite aucune procédure d'apprentissage supplémentaire, outre celles déjà enregistrées sur le volume source.

Dans ONTAP 9.10.1 et 9.11.1, SnapMirror ne transfère pas l'état de configuration ARP, les données d'apprentissage et les snapshots des volumes source vers les volumes de destination. Par conséquent, lors de la conversion du volume de destination SnapMirror en RW, ARP doit être explicitement activé en mode d'apprentissage sur ce volume après la conversion.

ARP et machines virtuelles

ARP est pris en charge avec les machines virtuelles (VM) sur VMware. La détection ARP se comporte différemment selon qu'il s'agit de modifications internes ou externes à la VM. ARP n'est pas recommandé pour les charges de travail impliquant un grand nombre de fichiers hautement compressés (tels que 7z et ZIP) ou chiffrés (tels que des fichiers PDF, DOC ou ZIP protégés par mot de passe) au sein de la VM.

Modifications en dehors de la VM

ARP peut détecter les modifications d'extension de fichier sur un volume NFS en dehors de la machine virtuelle si une nouvelle extension entre dans le volume dans un état chiffré ou si une extension de fichier change.

Modifications au sein de la machine virtuelle

Si une attaque par rançongiciel modifie des fichiers à l'intérieur de la machine virtuelle sans effectuer de modifications à l'extérieur, ARP détecte la menace si l'entropie par défaut de la machine virtuelle est faible (par exemple, fichiers .txt, .docx ou .mp4). Pour ONTAP 9.16.1 et les versions antérieures, ARP crée un instantané

de protection dans ce scénario, mais ne génère pas d'alerte de menace, car les extensions de fichier externes à la machine virtuelle n'ont pas été altérées. À compter de la prise en charge SAN dans ONTAP 9.17.1, ARP génère également une alerte de menace s'il détecte une anomalie d'entropie à l'intérieur de la machine virtuelle.

Si, par défaut, les fichiers sont à entropie élevée (par exemple, des fichiers .gzip ou protégés par mot de passe), les capacités de détection d'ARP sont limitées. Dans ce cas, ARP peut néanmoins prendre des instantanés proactifs ; cependant, aucune alerte ne sera déclenchée si les extensions de fichier n'ont pas été altérées de manière externe.

Pour SAN, ARP analyse les statistiques d'entropie au niveau du volume et déclenche des détections lorsqu'une anomalie d'entropie est détectée.

> La détection des attaques se produisant au sein d'une VM est disponible uniquement pour les volumes FlexVol et n'est pas disponible si la banque de données de la VM est configurée sur un volume FlexGroup dans ONTAP 9.18.1 et versions ultérieures.

Configurations non prises en charge

ARP n'est pas pris en charge dans les environnements ONTAP S3.

ARP ne prend pas en charge les configurations de volume suivantes :

- Volumes FlexGroup (dans ONTAP 9.10.1 à 9.12.1).

  > À partir d' ONTAP 9.13.1 jusqu'à ONTAP 9.17.1, les volumes FlexGroup sont pris en charge mais sont limités au modèle ARP utilisé avant ARP/AI. Les volumes FlexGroup sont pris en charge avec ARP/AI à partir d' ONTAP 9.18.1.

- Volumes FlexCache (ARP est pris en charge sur les volumes FlexVol d'origine, mais pas sur les volumes de cache)
- Les volumes hors ligne
- Volumes SnapLock
- Synchronisation active SnapMirror
- SnapMirror synchrone
- SnapMirror asynchrone (dans ONTAP 9.10.1 et 9.11.1). SnapMirror asynchrone est pris en charge à partir d' ONTAP 9.12.1. [snapmirror] .
- Volumes restreints
- Volumes root des VM de stockage
- Volumes des machines virtuelles de stockage arrêtées

Considérations relatives aux performances ARP et à la fréquence

L'impact d'ARP sur les performances système est minime, mesuré en termes de débit et d'IOPS de pointe. L'impact de la fonctionnalité ARP dépend de la charge de travail du volume concerné. Pour les charges de travail courantes, les limites de configuration suivantes sont recommandées :

Caractéristiques de la charge de travail	Limite de volume recommandée par nœud	Dégradation des performances lorsque la limite de volume par nœud est dépassée [1]
Lecture intensive ou les données peuvent être compressées	150	4 % des IOPS maximales
Écriture intensive et les données ne peuvent pas être compressées	60	• NAS : 10 % des IOPS maximum pour ONTAP 9.15.1 et versions antérieures • NAS : 5 % du maximum d'IOPS pour ONTAP 9.16.1 et versions ultérieures • SAN : 5 % des IOPS maximum pour ONTAP 9.17.1 et versions ultérieures

[1] Les performances du système ne sont pas dégradées au-delà de ces pourcentages, quel que soit le nombre de volumes ajoutés au-delà des limites recommandées.

Étant donné que les analyses ARP s'exécutent dans une séquence prioritaire, les analyses s'exécutent sur chaque volume moins fréquemment à mesure que le nombre de volumes protégés augmente.

L'activation par défaut du protocole ARP sur un grand nombre de nouveaux volumes peut accroître l'utilisation des ressources système. Lors de l'activation d'ARP sur des volumes, tenez compte des besoins en espace des processus concurrents comme les snapshots.

Limites de volume pour ARP par plateforme

À partir de ONTAP 9.18.1, ARP prend en charge des limites de volume accrues en fonction du type de plateforme et du nombre de cœurs.

Type de plateforme	Nombre maximal de volumes compatibles ARP par nœud
Entrée de gamme (systèmes avec jusqu'à 20 cœurs de processeur)	250
Moyen (systèmes avec jusqu'à 64 cœurs CPU)	500
Haut de gamme (systèmes avec plus de 64 cœurs CPU)	1000

Le nombre de cœurs s'applique à chaque nœud individuel d'une paire haute disponibilité à 2 nœuds.

Vérification multiadministrateur avec volumes protégés par ARP

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) pour une sécurité supplémentaire avec ARP. MAV s'assure qu'au moins deux administrateurs authentifiés sont requis pour désactiver ARP, mettre en pause ARP ou marquer une attaque suspecte comme faux positif sur un volume protégé. Découvrez comment "Activez MAV pour les volumes protégés par ARP".

Vous devez définir des administrateurs pour un groupe MAV et créer des règles MAV pour les `security anti-ransomware volume disable` commandes , `security anti-ransomware volume pause` et `security anti-ransomware volume attack clear-suspect` ARP que vous souhaitez protéger. Chaque administrateur du groupe MAV doit approuver chaque nouvelle demande de règle et "Ajoutez à nouveau la règle MAV" dans les paramètres MAV.

Pour en savoir plus sur `security anti-ransomware volume disable`, `security anti-ransomware volume pause` et `security anti-ransomware volume attack clear-suspect` dans le "Référence de commande ONTAP".

Depuis ONTAP 9.14.1, ARP propose des alertes pour la création d'un snapshot ARP et l'observation d'une nouvelle extension de fichier. Les alertes pour ces événements sont désactivées par défaut. Elles peuvent être définies au niveau du volume ou de la SVM. Vous pouvez activer les alertes via `security anti-ransomware vserver event-log modify` ou au niveau du volume avec `security anti-ransomware volume event-log modify` .

Pour en savoir plus sur `security anti-ransomware vserver event-log modify` et `security anti-ransomware volume event-log modify` dans le "Référence de commande ONTAP".

Étapes suivantes

- "Activation de la protection autonome contre les ransomwares"
- "Activez MAV pour les volumes protégés par ARP"

Activer ARP

Activer la protection autonome contre les ransomwares ONTAP sur un volume

Depuis la version ONTAP 9.10.1, vous pouvez activer la protection anti-ransomware autonome (ARP) sur un volume existant ou créer un volume et activer ARP dès le début.

Description de la tâche

Pour activer ARP, suivez la procédure correspondant à votre environnement aprèsvous vous assurez que votre environnement répond à certaines exigences :

- NAS avec volumes FlexVol
- NAS avec volumes FlexGroup
- Volumes SAN

Après l'activation d'ARP, celui-ci peut entrer dans une période de transition en fonction de votre environnement et de votre version ONTAP :

Type de volume	Version ONTAP	Comportement après activation
NAS FlexGroup	ONTAP 9.18.1 et versions ultérieures	ARP/AI est immédiatement actif, sans période d'apprentissage.
	ONTAP 9.13.1 à 9.17.1	ARP démarre en mode apprentissage pendant 30 jours

Type de volume	Version ONTAP	Comportement après activation
NAS FlexVol	ONTAP 9.16.1 et versions ultérieures	ARP/AI est immédiatement actif, sans période d'apprentissage.
	ONTAP 9.10.1 à 9.15.1	ARP démarre en mode apprentissage pendant 30 jours
Volumes SAN	ONTAP 9.17.1 et versions ultérieures	Le système ARP/AI est immédiatement actif, lançant une période d'évaluation pour établir un seuil d'alerte approprié avant de passer d'un seuil initial conservateur.

Avant de commencer

Avant d'activer ARP, assurez-vous que votre environnement dispose des éléments suivants :

exigences spécifiques au NAS

- Une machine virtuelle de stockage (SVM) avec le protocole NFS ou SMB (ou les deux) activé.
- Charge de travail NAS avec clients configurés.
- Un actif"chemin de jonction" pour le volume.

exigences spécifiques au SAN

- Une machine virtuelle de stockage (SVM) avec le protocole iSCSI, FC ou NVMe activé.
- Charge de travail SAN avec clients configurés.

Exigences générales

- Le"licence correcte" pour votre version ONTAP .
- (Recommandé) Vérification multi-administrateur (MAV) activée (ONTAP 9.13.1 et versions ultérieures). Voir"Activez la vérification multiadministrateur" .

Activer ARP sur les volumes NAS FlexVol

Vous pouvez activer ARP sur les volumes NAS FlexVol à l'aide de System Manager ou de l'interface de ligne de commande ONTAP . Le processus diffère selon votre version ONTAP .

ONTAP 9.16.1 et versions ultérieures

À partir d' ONTAP 9.16.1, ARP/AI est actif immédiatement sans période d'apprentissage requise.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume à protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé.
3. Vérifiez l'état ARP du volume dans la boîte **Anti-ransomware**.

   Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Activer ARP sur un volume existant :

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

Créer un nouveau volume avec ARP activé :

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

Vérifier l'état ARP :

```
security anti-ransomware volume show
```

Pour en savoir plus, `security anti-ransomware volume show` consultez le "Référence de commande ONTAP".

ONTAP 9.10.1 à 9.15.1

Pour ONTAP 9.10.1 à 9.15.1, vous devez activer ARP initialement dans"mode d'apprentissage" (ou état de « répétition à blanc »). Le système analyse la charge de travail afin de caractériser le comportement normal. Démarrer en mode actif peut entraîner un nombre excessif de faux positifs.

Il est recommandé de laisser ARP s'exécuter en mode d'apprentissage pendant au moins 30 jours. À partir d' ONTAP 9.13.1, ARP détermine automatiquement l'intervalle optimal de la période d'apprentissage et automatise le basculement, qui peut intervenir avant 30 jours.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume à protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé.

3. Sélectionnez **Activé en mode d'apprentissage** dans la case **Anti-ransomware**.

> Tu peux"Désactiver l'apprentissage automatique des transitions de modes actifs sur la machine virtuelle de stockage associée" si vous souhaitez contrôler manuellement la transition du mode d'apprentissage au mode actif.

> Dans les volumes existants, les modes d'apprentissage et actif s'appliquent uniquement aux données nouvellement écrites, et non aux données existantes du volume. Les données existantes ne sont pas analysées et analysées, car les caractéristiques du trafic de données normal antérieur sont présumées basées sur les nouvelles données une fois que le volume est activé pour ARP.

4. Vérifiez l'état ARP du volume dans la boîte **Anti-ransomware**.

   Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Activer ARP sur un volume existant :

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

Pour en savoir plus, `security anti-ransomware volume dry-run` consultez le "Référence de commande ONTAP".

Créer un nouveau volume avec ARP activé :

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

Désactiver la commutation automatique (facultatif) :

Si vous avez effectué une mise à niveau vers ONTAP 9.13.1 via ONTAP 9.15.1 et que vous souhaitez contrôler manuellement le passage du mode d'apprentissage au mode actif pour tous les volumes associés, vous pouvez le faire à partir du SVM :

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

Vérifier l'état ARP :

```
security anti-ransomware volume show
```

Activer ARP sur les volumes NAS FlexGroup

Vous pouvez activer ARP sur les volumes NAS FlexGroup à l'aide de System Manager ou de l'interface de ligne de commande ONTAP . Le processus diffère selon votre version ONTAP .

ONTAP 9.18.1 et versions ultérieures

À partir d' ONTAP 9.18.1, ARP/AI est immédiatement actif pour les volumes FlexGroup sans période d'apprentissage requise.

System Manager

1. Sélectionnez **Stockage > Volumes**, puis sélectionnez le volume FlexGroup que vous souhaitez protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé.
3. Vérifiez l'état ARP du volume dans la boîte **Anti-ransomware**.

   Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Activer ARP sur un volume FlexGroup existant :

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

Créez un nouveau volume FlexGroup avec ARP activé :

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

Vérifier l'état ARP :

```
security anti-ransomware volume show
```

ONTAP 9.13.1 à 9.17.1

Pour ONTAP 9.13.1 à 9.17.1, les volumes FlexGroup commencent dans"mode d'apprentissage" . Le système analyse la charge de travail afin de caractériser le comportement normal.

Il est recommandé de laisser ARP s'exécuter en mode d'apprentissage pendant au moins 30 jours. ARP détermine automatiquement l'intervalle optimal de période d'apprentissage et automatise le basculement, qui peut se produire avant 30 jours.

System Manager

1. Sélectionnez **Stockage > Volumes**, puis sélectionnez le volume FlexGroup que vous souhaitez protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé.
3. Sélectionnez **Activé en mode d'apprentissage** dans la case **Anti-ransomware**.

Tu peux"désactiver l'apprentissage automatique des transitions vers les modes actifs" si vous souhaitez contrôler manuellement la transition du mode d'apprentissage au mode actif.

4. Vérifiez l'état ARP du volume dans la boîte **Anti-ransomware**.

CLI

Activer ARP sur un volume FlexGroup existant :

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

Créez un nouveau volume FlexGroup avec ARP activé :

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

Désactiver la commutation automatique (facultatif) :

Si vous souhaitez contrôler manuellement le passage du mode d'apprentissage au mode actif :

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

Vérifier l'état ARP :

```
security anti-ransomware volume show
```

Activer ARP sur les volumes SAN

À partir d' ONTAP 9.17.1, vous pouvez activer ARP sur les volumes SAN. La fonctionnalité ARP/AI est automatiquement activée et commence immédiatement à surveiller et à protéger activement les volumes SAN pendant la"période d'évaluation" tout en déterminant simultanément si les charges de travail sont adaptées à ARP et en définissant un seuil de chiffrement optimal pour la détection.

Vous pouvez activer ARP sur les volumes SAN à l'aide de System Manager ou de l'interface de ligne de commande ONTAP .

System Manager

Étapes

1. Sélectionnez **Stockage > Volumes**, puis sélectionnez le volume SAN que vous souhaitez protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé.
3. ARP/AI entre automatiquement en période d'évaluation.
4. Vérifiez l'état ARP et le statut d'évaluation dans la boîte **Anti-ransomware**.

   Pour afficher l'état ARP de tous les volumes : dans le volet **volumes**, sélectionnez **Afficher/Masquer**, puis assurez-vous que l'état **anti-ransomware** est vérifié.

CLI

Activer ARP sur un volume SAN existant :

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

Créer un nouveau volume SAN avec ARP activé :

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

Vérifiez l'état et le statut d'évaluation de l'ARP :

```
security anti-ransomware volume show
```

Vérifiez le `Block device detection status` terrain pour suivre l'avancement de la période d'évaluation.

Pour en savoir plus, `security anti-ransomware volume show` consultez le "Référence de commande ONTAP".

Informations associées

- "Passer en mode actif après une période d'apprentissage"

Activez la protection anti-ransomware autonome de ONTAP par défaut sur les nouveaux volumes

À partir d'ONTAP 9.10.1, vous pouvez configurer les machines virtuelles de stockage (SVM) afin que les nouveaux volumes soient activés par défaut avec Autonomous Ransomware Protection (ARP). Vous pouvez modifier ce paramètre à l'aide de System Manager ou avec l'interface de ligne de commande ONTAP.

À partir de ONTAP 9.18.1, ARP est activé par défaut sur tous les nouveaux volumes au niveau du cluster pour "systèmes pris en charge" après un délai de grâce de 12 heures suivant une mise à niveau ou une nouvelle installation du cluster. Si vous désactivez l'activation automatique par défaut de ARP au niveau du cluster, vous pouvez toujours choisir d'activer ARP manuellement par défaut sur tous les nouveaux volumes au niveau de la SVM.

Pour ONTAP 9.17.1 et versions antérieures, la configuration au niveau de la SVM est le seul moyen d'activer ARP par défaut sur les nouveaux volumes.

Description de la tâche

Par défaut, les nouveaux volumes sont créés avec la fonctionnalité ARP désactivée. Vous devrez activer la fonctionnalité ARP et la configurer pour qu'elle soit activée par défaut sur les nouveaux volumes créés dans la SVM.

Les volumes existants sans ARP activé ne modifieront pas automatiquement leur statut d'activation ARP lorsque vous modifierez la valeur par défaut du SVM. Les modifications des paramètres SVM décrites dans cette procédure n'affectent que les nouveaux volumes. Apprenez comment"Activez ARP pour les volumes existants" .

Après l'activation d'ARP, celui-ci peut entrer dans une période de transition en fonction de votre environnement et de votre version ONTAP :

Type de volume	Version ONTAP	Comportement après activation
NAS FlexGroup	ONTAP 9.18.1 et versions ultérieures	ARP/AI est immédiatement actif, sans période d'apprentissage.
	ONTAP 9.13.1 à 9.17.1	ARP démarre en mode apprentissage pendant 30 jours
NAS FlexVol	ONTAP 9.16.1 et versions ultérieures	ARP/AI est immédiatement actif, sans période d'apprentissage.
	ONTAP 9.10.1 à 9.15.1	ARP démarre en mode apprentissage pendant 30 jours
Volumes SAN	ONTAP 9.17.1 et versions ultérieures	Le système ARP/AI est immédiatement actif, lançant une période d'évaluation pour établir un seuil d'alerte approprié avant de passer d'un seuil initial conservateur.

Avant de commencer

Avant d'activer ARP, assurez-vous que votre environnement dispose des éléments suivants :

exigences spécifiques au NAS

- Une machine virtuelle de stockage (SVM) avec le protocole NFS ou SMB (ou les deux) activé.
- Un actif"chemin de jonction" pour le volume.

exigences spécifiques au SAN

- Une machine virtuelle de stockage (SVM) avec le protocole iSCSI, FC ou NVMe activé.

Exigences générales

- Le"licence correcte" pour votre version ONTAP .
- (Recommandé) Vérification multi-administrateur (MAV) activée (ONTAP 9.13.1+). Voir"Activez la

vérification multiadministrateur" .

Étapes

Vous pouvez utiliser System Manager ou l’interface de ligne de commandes de ONTAP pour activer le protocole ARP par défaut sur les nouveaux volumes.

System Manager

1. Sélectionnez **Stockage** ou **Cluster** (selon votre environnement), sélectionnez **VM de stockage**, puis sélectionnez la VM de stockage qui contiendra les volumes que vous souhaitez protéger avec ARP.
2. Accédez à l'onglet **Paramètres**. Sous **Sécurité**, localisez la vignette **Anti-ransomware**, puis sélectionnez .
3. Cochez la case pour activer l'anti-ransomware (ARP). Cochez la case supplémentaire pour activer ARP sur tous les volumes éligibles de la machine virtuelle de stockage.
4. Pour les versions ONTAP avec une période d'apprentissage recommandée, sélectionnez **Passer automatiquement du mode d'apprentissage au mode actif après un apprentissage suffisant**. Cela permet à ARP de déterminer l'intervalle d'apprentissage optimal et d'automatiser le passage au mode actif.

CLI

Modifier une SVM existante pour activer ARP par défaut dans les nouveaux volumes

Sélectionner `dry-run` si votre version d'ARP nécessite unpériode d'apprentissage . Sinon, sélectionnez `enabled` .

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

Créez une nouvelle SVM avec ARP activé par défaut pour les nouveaux volumes

Sélectionner `dry-run` si votre version d'ARP nécessite unpériode d'apprentissage . Sinon, sélectionnez `enabled` .

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

Modifier le SVM existant pour désactiver la transition automatique de l'apprentissage au mode actif

Si vous avez effectué une mise à niveau vers ONTAP 9.13.1 via ONTAP 9.15.1 et que l'état par défaut est `dry-run` (mode d'apprentissage), l'apprentissage adaptatif est activé afin que le changement vers `enabled` Le passage en mode actif se fait automatiquement. Vous pouvez désactiver cette commutation automatique afin de contrôler manuellement le passage du mode d'apprentissage au mode actif pour tous les volumes associés :

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

Vérifier l'état ARP

```
security anti-ransomware volume show
```

Informations associées

- "Passer en mode actif après une période d'apprentissage"
- "Affichage du volume de sécurité anti-ransomware"

Désactiver l'activation par défaut de la protection autonome contre les ransomwares ONTAP

À partir d'ONTAP 9.18.1, la protection autonome contre les ransomwares (ARP) est automatiquement activée par défaut sur tous les nouveaux volumes pour AFF A-series et AFF C-series, ASA et ASA r2 après une période de préchauffage de 12 heures suivant une mise à niveau ou une nouvelle installation, à condition qu'une licence ARP soit installée. Vous pouvez désactiver cette activation par défaut pendant ou après le délai de grâce de 12 heures à l'aide de System Manager ou de l'interface de ligne de commande ONTAP.

Les volumes existants doivent être "activé manuellement" pour ARP.

Description de la tâche

Le paramètre que vous choisissez pour cette procédure peut être modifié ultérieurement. Après le délai de grâce, vous avez toujours la flexibilité d'activer ou de désactiver l'activation par défaut à tout moment :

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour gérer les options d'activation par défaut d'ARP.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Effectuez l'une des opérations suivantes :
   - Désactiver pendant le délai de grâce :
     i. Dans la section **Anti-ransomware**, un message vous indiquera le nombre d'heures restantes avant l'activation d'ARP. Sélectionnez **Ne pas activer**.
     ii. Sélectionnez **Désactiver** dans la boîte de dialogue suivante pour confirmer que l'activation ARP par défaut est désactivée pour les nouveaux volumes.
   - Désactiver après délai de grâce :
     i. Dans la section **Anti-ransomware**, sélectionnez .
     ii. Cochez la case, puis cliquez sur **Enregistrer** pour désactiver l'activation ARP par défaut pour les nouveaux volumes.

CLI

1. Vérifiez l'état d'activation par défaut :

```
security anti-ransomware auto-enable show
```

2. Désactiver l'activation par défaut pour les nouveaux volumes :

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false
```

Informations associées

- "Activez la protection autonome contre les ransomwares ONTAP sur un volume individuel"

Passez en mode actif dans ONTAP ARP après une période d'apprentissage

Pour les environnements NAS, basculez manuellement ou automatiquement un volume compatible ARP du mode d'apprentissage au mode actif. Vous devrez changer de mode si vous utilisez ARP avec ONTAP 9.15.1 et versions antérieures ou si ARP est exécuté sur des volumes FlexGroup avec ONTAP 9.17.1 et versions antérieures.

Une fois qu'ARP a terminé son apprentissage pendant au moins 30 jours, vous pouvez basculer manuellement en mode actif. À partir d' ONTAP 9.13.1, ARP détermine automatiquement l'intervalle optimal de la période d'apprentissage et automatise le basculement, qui peut intervenir avant 30 jours.

Si vous utilisez ARP avec la protection ARP/AI, ARP s'active automatiquement. Aucune période d'apprentissage n'est requise.

Dans les volumes existants, les modes d'apprentissage et actif s'appliquent uniquement aux données nouvellement écrites, et non aux données existantes du volume. Les données existantes ne sont pas analysées et analysées, car les caractéristiques du trafic de données normal antérieur sont présumées basées sur les nouvelles données une fois que le volume est activé pour ARP.

Passer manuellement en mode actif après la période d'apprentissage

Pour ONTAP 9.10.1 à 9.15.1 (ONTAP 9.17.1 et versions antérieures avec volumes FlexGroup), vous pouvez passer manuellement du mode d'apprentissage ARP au mode actif à l'aide de System Manager ou de l'interface de ligne de commande ONTAP une fois la période d'apprentissage terminée.

Description de la tâche

La transition manuelle vers le mode actif après une période d'apprentissage décrite dans cette procédure est spécifique aux environnements NAS.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour passer du mode d'apprentissage au mode actif.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume prêt pour le mode actif.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **passer en mode actif** dans la zone anti-ransomware.
3. Vous pouvez vérifier l'état ARP du volume dans la zone **anti-ransomware**.

CLI

1. Modifiez le volume protégé pour passer en mode actif si ce n'est pas déjà fait automatiquement :

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   Vous pouvez également passer en mode actif à l'aide de la commande modifier le volume :

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. Vérifiez l'état ARP du volume.

   ```
   security anti-ransomware volume show
   ```

Passage automatique du mode d'apprentissage au mode actif

Depuis ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté aux analyses ARP et le passage du mode apprentissage au mode actif s'effectue automatiquement. La décision autonome d'ARP de passer automatiquement du mode apprentissage au mode actif repose sur les paramètres de configuration des options suivantes :

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Si la commutation automatique est activée, le volume passera automatiquement en mode actif après un maximum de 30 jours, même si toutes les conditions ne sont pas remplies. Cette limite de 30 jours est fixe et non modifiable.

Pour plus d'informations sur les options de configuration ARP, y compris les valeurs par défaut, reportez-vous au "Référence de commande ONTAP".

Informations associées

- "sécurité anti-ransomware volume"

En savoir plus sur la période d'évaluation d' ONTAP ARP pour les volumes SAN

À partir d' ONTAP 9.17.1, ARP nécessite une période d'évaluation pour déterminer si les niveaux d'entropie des charges de travail des volumes SAN sont adaptés à la protection contre les ransomwares. Une fois ARP activé sur un volume SAN, ARP/AI surveille et protège activement le volume pendant la période d'évaluation tout en déterminant simultanément un seuil de chiffrement optimal. La détection et les alertes peuvent survenir pendant la période d'évaluation en utilisant un seuil conservateur pendant l'établissement des seuils de référence. ARP distingue les charges de travail adaptées des charges de travail inappropriées dans le volume SAN évalué et, si les charges de travail sont jugées adaptées à la protection, définit automatiquement un seuil de chiffrement en fonction des statistiques de la période d'évaluation.

Comprendre l'évaluation de l'entropie

Le système collecte des statistiques de chiffrement en continu toutes les 10 minutes. Au cours de l'évaluation, des instantanés périodiques ARP sont également créés en continu toutes les quatre heures. Si le pourcentage de chiffrement dans un intervalle dépasse le seuil de chiffrement optimal identifié pour ce volume, une alerte est déclenchée, un `Anti_ransomware_attack_backup` un instantané est créé et le temps de conservation des instantanés est augmenté sur tous les instantanés ARP périodiques.

Confirmer que la période d'évaluation est active

Vous pouvez confirmer que l'analyse est active en exécutant la commande suivante et en confirmant un état de `evaluation_period`. Si un volume n'est pas éligible à l'évaluation, le statut d'évaluation ne sera pas

affiché.

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

Exemple de réponse :

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

Collecte des données de la période d'évaluation du moniteur

Vous pouvez surveiller la détection du chiffrement en temps réel en exécutant la commande suivante. Cette commande renvoie un histogramme indiquant la quantité de données dans chaque plage de pourcentage de chiffrement. L'histogramme est mis à jour toutes les 10 minutes.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

Exemple de réponse :

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

Charges de travail adaptées et seuils adaptatifs

L'évaluation se termine par l'un des résultats suivants :

- **La charge de travail est compatible avec ARP**. ARP définit automatiquement le seuil adaptatif à plus de 10 % du pourcentage de chiffrement maximal observé pendant la période d'évaluation. ARP continue également la collecte de statistiques et crée des instantanés ARP périodiques.
- **La charge de travail n'est pas adaptée à ARP**. ARP définit automatiquement le seuil adaptatif sur le pourcentage de chiffrement maximal observé pendant la période d'évaluation. ARP continue également de collecter des statistiques et de créer des instantanés ARP périodiques, mais le système recommande finalement de désactiver ARP sur le volume.

Déterminer les résultats de l'évaluation

Une fois la période d'évaluation terminée, ARP définit automatiquement le seuil adaptatif en fonction des résultats de l'évaluation.

Vous pouvez déterminer les résultats de l'évaluation en exécutant la commande suivante. L'adéquation du volume est indiquée dans le `Block device detection status` champ:

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

Exemple de réponse :

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

Vous pouvez également afficher le seuil de valeur adopté à la suite de l'évaluation :

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

Exemple de réponse :

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

Mettez en pause la protection anti-ransomware autonome de ONTAP pour exclure les événements de workloads de l'analyse

Si vous attendez des événements inhabituels des charges de travail, vous pouvez suspendre et reprendre temporairement l'analyse ARP (autonome ransomware protection) à tout moment.

À partir de ONTAP 9.13.1, vous pouvez activer la vérification multiadministrateur (MAV) de sorte que deux administrateurs d'utilisateurs authentifiés ou plus soient requis pour interrompre le protocole ARP.

"En savoir plus sur le MAV".

Description de la tâche

Pendant une pause ARP, ONTAP n'enregistre pas les événements ni les actions liés aux nouvelles écritures ; toutefois, l'analyse des journaux antérieurs se poursuit en arrière-plan.

> N'utilisez pas la fonction de désactivation ARP pour interrompre l'analyse. Ceci désactive ARP sur le volume et toutes les informations existantes concernant le comportement de la charge de travail apprise sont perdues. Cela nécessiterait un redémarrage de la période d'apprentissage.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour interrompre le protocole ARP.

System Manager

1. Sélectionnez **stockage > volumes**, puis sélectionnez le volume sur lequel vous souhaitez mettre en pause ARP.
2. Dans l'onglet **Sécurité** de la vue d'ensemble des volumes, sélectionnez **Suspendre l'anti-ransomware** dans la case **Anti-ransomware**.

> À partir d' ONTAP 9.13.1, si vous utilisez MAV pour protéger les paramètres ARP, l'opération de pause vous invite à obtenir l'approbation d'un ou plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" associé au groupe d'approbation MAV, sinon l'opération échouera.

3. Pour reprendre la surveillance, sélectionnez **Reprendre l'anti-ransomware**.

CLI

1. Suspendre ARP sur un volume :

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. Pour reprendre le traitement, utilisez `resume` commande :

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

Pour en savoir plus, `security anti-ransomware volume` consultez le "Référence de commande ONTAP".

3. Si vous utilisez MAV (disponible avec ARP à partir d' ONTAP 9.13.1) pour protéger les paramètres ARP, l'opération de pause vous invite à obtenir l'approbation d'un ou plusieurs administrateurs supplémentaires. L'approbation de tous les administrateurs associés au groupe d'approbation MAV est indispensable, faute de quoi l'opération échouera.

   Si vous utilisez MAV et qu'une opération de pause attendue nécessite des approbations supplémentaires, chaque approbateur de groupe MAV effectue les opérations suivantes :

   a. Afficher la demande :

```
security multi-admin-verify request show
```

   b. Approuver la demande :

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

   La réponse du dernier approbateur de groupe indique que le volume a été modifié et que l'état du

protocole ARP est mis en pause.

Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez rejeter une demande d'opération de pause :

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
Pour en savoir plus, `security multi-admin-verify request` consultez le "Référence de commande ONTAP".

Gérez les paramètres de détection des attaques par protection anti-ransomware autonome de ONTAP

À partir de la version ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des ransomwares sur un volume spécifique lorsque la protection anti-ransomware autonome est activée et signaler une augmentation connue sous le nom d'activité de fichier normale. Le réglage des paramètres de détection permet d'améliorer la précision des rapports en fonction de votre charge de travail de volume spécifique.

Fonctionnement de la détection des attaques

Lorsque la protection autonome contre les ransomwares (ARP) est en mode d'apprentissage ou d'évaluation, elle développe des valeurs de référence pour les comportements des volumes. Celles-ci incluent l'entropie, les extensions de fichiers et, à partir d' ONTAP 9.11.1, les IOPS. Ces valeurs de référence servent à évaluer les menaces de ransomware. Pour plus d'informations sur ces critères, consultez la page "Ce que le protocole ARP détecte" .

Certains volumes et charges de travail nécessitent des paramètres de détection différents. Par exemple, un volume compatible ARP peut héberger de nombreux types d'extensions de fichiers ; dans ce cas, vous pouvez modifier le seuil de nombre d'extensions de fichiers jamais vues auparavant à un nombre supérieur à la valeur par défaut de 20 ou désactiver les avertissements basés sur des extensions de fichiers jamais vues auparavant. À partir d' ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des attaques afin qu'ils correspondent mieux à vos charges de travail spécifiques.

À partir de ONTAP 9.14.1, vous pouvez configurer des alertes lorsque ARP observe une nouvelle extension de fichier et lorsque ARP crée un snapshot. Pour plus d'informations, voir [modify-alerts].

Détection d'attaques dans les environnements NAS

Dans ONTAP 9.10.1, ARP émet un avertissement s'il détecte les deux conditions suivantes :

- Plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans le volume
- Données d'entropie élevées

À partir de ONTAP 9.11.1, ARP émet un avertissement de menace si *seule* une condition est remplie. Par exemple, si plus de 20 fichiers avec des extensions de fichier qui n'ont pas été observées précédemment dans

le volume sont observés dans une période de 24 heures, ARP catégorise ceci comme une menace *indépendamment* de l'entropie observée. Les valeurs de 24 heures et 20 fichiers sont des valeurs par défaut, qui peuvent être modifiées.

> Pour réduire le nombre élevé de fausses alertes positives, accédez à Stockage > Volumes > Sécurité > Configurer les caractéristiques de la charge de travail et désactivez l'option Surveiller les nouveaux types de fichiers. Ce paramètre est désactivé par défaut dans ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1 et versions ultérieures.

Détection des attaques dans les environnements SAN

À partir d' ONTAP 9.17.1, ARP émet un avertissement s'il détecte des taux de chiffrement élevés dépassant un seuil appris automatiquement. Ce seuil est établi après une "période d'évaluation" mais peut être modifié.

Modifier les paramètres de détection d'attaque

En fonction du comportement attendu du volume compatible ARP, vous pourriez souhaiter modifier les paramètres de détection des attaques.

Étapes

1. Afficher les paramètres de détection d'attaque existants :

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                          Vserver Name : vs1
                                           Volume Name : vol1
          Block Device Auto Learned Encryption Threshold : 10
           Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                Is Detection Based on File Create Rate? : true
                Is Detection Based on File Rename Rate? : true
                Is Detection Based on File Delete Rate? : true
          Is Detection Relaxing Popular File Extensions? : true
               High Entropy Data Surge Notify Percentage : 100
                File Create Rate Surge Notify Percentage : 100
                File Rename Rate Surge Notify Percentage : 100
                File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 5
       Never Seen before File Extensions Duration in Hour : 48
```

2. Tous les champs affichés sont modifiables avec des valeurs booléennes ou entières. Pour modifier un champ, utilisez le bouton `security anti-ransomware volume attack-detection-parameters modify` commande.

   Pour en savoir plus, `security anti-ransomware volume attack-detection-parameters`

`modify` consultez le "Référence de commande ONTAP".

Signaler les surtensions connues

ARP continue de modifier les valeurs de base pour les paramètres de détection, même lorsqu'il est actif. Si vous connaissez des surtensions dans votre activité de volume, des surtensions ou des surtensions qui sont caractéristiques d'une nouvelle normale, vous devez les signaler comme étant sûres. La déclaration manuelle de ces surtensions comme étant sûres contribue à améliorer la précision des évaluations des menaces d'ARP.

Signaler une surtension ponctuelle

1. Si une surtension ponctuelle se produit dans des circonstances connues et que vous souhaitez que ARP signale une surtension similaire dans des circonstances futures, éliminez la poussée du comportement de la charge de travail :

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   <svm_name> -volume <volume_name>
   ```

   Pour en savoir plus, `security anti-ransomware volume workload-behavior clear-surge` consultez le "Référence de commande ONTAP".

Modifier la surtension de la ligne de base

1. Si une surtension signalée doit être considérée comme un comportement normal de l'application, signalez-la en tant que telle pour modifier la valeur de surtension de la ligne de base.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-
   surge -vserver <svm_name> -volume <volume_name>
   ```

   En savoir plus sur `security anti-ransomware volume workload-behavior update-baseline-from-surge` dans le "Référence de commande ONTAP" .

Configurez les alertes ARP

Depuis ONTAP 9.14.1, ARP vous permet de spécifier des alertes pour deux événements ARP :

- Observation de la nouvelle extension de fichier sur un volume
- Création d'un instantané ARP

Les alertes liées à ces deux événements peuvent être définies sur des volumes individuels ou pour l'ensemble du SVM. Si vous activez des alertes pour le SVM, les paramètres d'alerte ne sont hérités que par les volumes créés après l'activation de l'alerte. Par défaut, les alertes ne sont activées sur aucun volume.

Les alertes d'événements peuvent être contrôlées par vérification multi-administrateur. Pour plus d'informations, consultez la section "Vérification multiadministrateur avec volumes protégés par ARP" .

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour définir des alertes pour les événements ARP.

System Manager

Définir des alertes pour un volume

1. Accédez à **Volumes**. Sélectionnez le volume dont vous souhaitez modifier les paramètres.
2. Sélectionnez l'onglet **Sécurité** puis **Paramètres de gravité des événements**.
3. Pour recevoir des alertes en cas de **Nouvelle extension de fichier détectée** et de **Création d'un instantané de rançongiciel**, sélectionnez le menu déroulant sous **Gravité**. Modifiez le paramètre de **Ne pas générer d'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

Définir des alertes pour un SVM

1. Accédez à **Storage VM** puis sélectionnez la SVM pour laquelle vous souhaitez activer les paramètres.
2. Sous la rubrique **Sécurité**, recherchez la carte **Anti-ransomware**. Sélectionnez ⋮ puis **Modifier la gravité de l'événement Ransomware**.
3. Pour recevoir des alertes en cas de **Nouvelle extension de fichier détectée** et de **Création d'un instantané de rançongiciel**, sélectionnez le menu déroulant sous **Gravité**. Modifiez le paramètre de **Ne pas générer d'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

CLI

Définir des alertes pour un volume

- Pour définir des alertes pour une nouvelle extension de fichier :

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-new-file-extension-seen true`
```

- Pour définir des alertes pour la création d'un snapshot ARP :

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

- Confirmez vos paramètres à l'aide du `anti-ransomware volume event-log show` commande.

Définir des alertes pour un SVM

- Pour définir des alertes pour une nouvelle extension de fichier :

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-new-file-extension-seen true
```

- Pour définir des alertes pour la création d'un snapshot ARP :

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-snapshot-copy-creation true
```

- Confirmez vos paramètres à l'aide du `security anti-ransomware vserver event-log show` commande.

En savoir plus sur `security anti-ransomware vserver event-log` commandes dans le "Référence de commande ONTAP" .

Informations associées

- "Apprenez à comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome".
- "Référence de commande ONTAP"

Répondre à une activité anormale détectée par ONTAP ARP

Lorsque la protection autonome contre les attaques par ransomware (ARP) détecte une activité anormale dans un volume protégé, elle émet un avertissement. Vous devez évaluer la notification pour déterminer si l'activité est acceptable (faux positif) ou si une attaque semble malveillante. Après avoir classé l'attaque, vous pouvez effacer l'avertissement et les avis concernant les fichiers suspects.

Lorsque vous catégorisez une attaque, les instantanés ARP sont soit conservés pendant une période abrégée initiée par l'opération de catégorisation (ONTAP 9.16.1 et versions ultérieures), soit supprimés instantanément (ONTAP 9.15.1 et versions antérieures).

À partir d' ONTAP 9.11.1, vous pouvez modifier le "paramètres de conservation" pour les instantanés ARP.

Description de la tâche

ARP affiche une liste de fichiers suspects lorsqu'il détecte une combinaison d'entropie de données élevée, d'activité anormale du volume avec chiffrement des données et d'extensions de fichiers inhabituelles. À partir d' ONTAP 9.17.1, pour les environnements NAS et SAN, les pics d'entropie sont également signalés sur la page Anti-ransomware du Gestionnaire système.

Lorsqu'une notification d'avertissement ARP est émise, répondez en désignant l'activité de l'une des deux manières suivantes :

- **Faux positif**

  Le type de fichier identifié ou le pic d'entropie est attendu dans votre charge de travail et peut être ignoré.

- **Attaque potentielle par ransomware**

  Le type de fichier identifié ou le pic d'entropie est inattendu dans votre charge de travail et doit être traité comme une attaque potentielle.

La surveillance normale reprend après la mise à jour de votre décision et la suppression des notifications ARP.

ARP enregistre votre évaluation dans le profil d'évaluation des menaces et utilise votre choix pour surveiller les activités ultérieures du fichier.

Dans le cas d'une attaque suspectée, vous devez déterminer s'il s'agit d'une attaque, y répondre si c'est le cas et restaurer les données protégées avant d'effacer les notifications. "En savoir plus sur la manière de procéder à une reprise après une attaque par ransomware".

Si vous restaurez un volume entier, il n'y a pas d'avis à effacer.

Avant de commencer

ARP doit protéger activement un volume et non pas être en mode d'apprentissage ou d'évaluation.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour répondre à des activités anormales.

System Manager

1. Lorsque vous recevez une notification d'« activité anormale », suivez le lien. Vous pouvez également accéder à l'onglet « Sécurité » de la vue d'ensemble des « Volumes ».

   Les avertissements s'affichent dans le volet **vue d'ensemble** du menu **Events**.

2. Dans l'onglet **Sécurité**, examinez les types de fichiers suspects ou le rapport sur les pics d'entropie.
   - Pour les fichiers suspects, examinez chaque type de fichier dans la boîte de dialogue **Types de fichiers suspects** et marquez chacun d'eux individuellement.
   - Pour les pics d'entropie, examinez le rapport d'entropie.
3. Enregistrez votre réponse :

Si vous sélectionnez cette valeur…	Prendre cette action…
Faux positif	a. Effectuez l'une des opérations suivantes : ◦ Pour les avertissements de type de fichier, sélectionnez **Mettre à jour et effacer les types de fichiers suspects**. ◦ Pour les pics d'entropie, sélectionnez **Marquer comme faux positif**. Ces actions effacent les avertissements concernant les fichiers ou activités suspects. ARP reprend ensuite la surveillance normale du volume. Pour ARP/AI dans ONTAP 9.16.1 et les versions ultérieures, les instantanés ARP sont automatiquement supprimés après une période de conservation abrégée déclenchée par l'opération de catégorisation. Pour ONTAP 9.15.1 et versions antérieures, les snapshots ARP associés sont automatiquement supprimés après la suppression des types de fichiers suspects. ⓘ À partir d' ONTAP 9.13.1, si vous utilisez MAV pour protéger les paramètres ARP, l'opération de détection de suspect vous invite à obtenir l'approbation d'un ou plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" associé au groupe d'approbation MAV, sinon l'opération échouera.

Attaques par ransomware potentielles	a. Répondre à l'attaque : ◦ Pour les avertissements de type de fichier, marquez les fichiers sélectionnés comme **Attaque potentielle de ransomware** et "restaurez les données protégées" . ◦ Pour les pics d'entropie qui indiquent une attaque, sélectionnez **Marquer comme attaque potentielle par ransomware** et "restaurez les données protégées" . b. Une fois la restauration des données terminée, enregistrez votre décision et reprenez la surveillance ARP normale : ◦ Pour les avertissements de type de fichier, sélectionnez **Mettre à jour et effacer les types de fichiers suspects**. ◦ Pour les pics d'entropie, sélectionnez **Marquer comme attaque potentielle par ransomware** et sélectionnez **Enregistrer et ignorer**. ⓘ Il n'y a aucun avis de type de fichier suspect à effacer si vous avez restauré un volume entier. L'enregistrement de votre décision efface le rapport d'attaque. Pour ARP/AI dans ONTAP 9.16.1 et les versions ultérieures, les instantanés ARP sont automatiquement supprimés après une période de conservation abrégée déclenchée par l'opération de catégorisation. Pour ONTAP 9.15.1 et les versions antérieures, les snapshots ARP sont automatiquement supprimés après la restauration d'un volume.

CLI

Vérifiez l'attaque

1. Lorsque vous recevez une notification d'attaque par ransomware suspectée, vérifiez l'heure et la gravité de l'attaque :

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

Sortie d'échantillon :

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

Vous pouvez également vérifier les messages EMS :

```
event log show -message-name callhome.arw.activity.seen
```

2. Générer un rapport d'attaque et spécifier où l'enregistrer :

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

Exemple de commande :

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

Sortie d'échantillon :

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. Afficher le rapport sur un système client d'administration. Par exemple :

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

Agissez

1. Effectuez l'une des actions suivantes en fonction de votre évaluation des extensions de fichiers ou des pics d'entropie :

   - Faux positif

     Exécutez l'une des commandes suivantes pour enregistrer votre décision et reprendre la surveillance normale de la protection autonome contre les ransomwares :

     - Pour les extensions de fichiers :

```
anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension_identifiers>] -false
-positive true
```

     Utilisez le paramètre facultatif suivant pour identifier uniquement des extensions spécifiques comme de faux positifs :

     - `[-extension <text>, … ]`: Extensions de fichier

- Pour les pics d'entropie :

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
```

◦ Attaque par ransomware potentielle

Répondez à l'attaque et "Récupérez les données à partir de l'instantané de sauvegarde créé par ARP" Une fois les données récupérées, exécutez l'une des commandes suivantes pour enregistrer votre décision et reprendre la surveillance ARP normale :

- Pour les extensions de fichiers :

```
anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension identifiers>] -false
-positive false
```

Utilisez le paramètre facultatif suivant pour identifier uniquement des extensions spécifiques en tant que ransomware potentiel :

- `[-extension <text>, … ]`: Extension de fichier

- Pour les pics d'entropie :

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

Ce `clear-suspect` L'opération efface le rapport d'attaque. Aucun avis de type de fichier suspect n'est à effacer si vous avez restauré un volume entier. Pour ARP/AI dans ONTAP 9.16.1 et les versions ultérieures, les instantanés ARP sont automatiquement supprimés après une période de conservation abrégée déclenchée par l'opération de catégorisation. Pour ONTAP 9.15.1 et les versions antérieures, les instantanés ARP sont automatiquement supprimés après la restauration d'un volume ou la suppression d'un événement suspect.

2. À partir de la version 9.18.1, vous pouvez déterminer l'état de `clear-suspect` opération:

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

options MAV

1. Si vous utilisez MAV et un attendu `clear-suspect` L'opération nécessite des approbations supplémentaires, chaque approbateur de groupe MAV doit :

a. Afficher la demande :

```
security multi-admin-verify request show
```

b. Approuver la demande de reprise de la surveillance anti-ransomware classique :

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

La réponse du dernier approbateur de groupe indique que le volume a été modifié et qu'un faux positif est enregistré.

2. Si vous utilisez MAV et que vous êtes un approbateur de groupe MAV, vous pouvez également rejeter une demande claire-suspecte :

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

Informations associées

- "Base de connaissances NetApp : Comprendre les attaques de protection autonome contre les ransomwares et l'instantané de protection autonome contre les ransomwares"
- "Modifier les options d'instantanés automatiques"
- "sécurité anti-ransomware volume"
- "demande de vérification multi-administrateur de sécurité"

Restaurez les données à partir des snapshots ARP ONTAP après une attaque par ransomware

La protection autonome contre les ransomwares (ARP) crée des instantanés pour vous protéger contre une menace potentielle de ransomware. Vous pouvez utiliser l'un de ces instantanés ARP ou un autre instantané de votre volume pour restaurer vos données.

Description de la tâche

L'ARP crée des instantanés avec l'un des noms suivants ajoutés au début :

- `Anti_ransomware_periodic_backup` : Utilisé dans ONTAP 9.17.1 et versions ultérieures pour les instantanés créés à intervalles réguliers. Par exemple : `Anti_ransomware_periodic_backup.2025-06-01_1248` .
- `Anti_ransomware_attack_backup`:Utilisé dans ONTAP 9.17.1 et versions ultérieures pour les instantanés créés en réponse à des anomalies. Par exemple : `Anti_ransomware_attack_backup.2025-08-25_1248` .
- `Anti_ransomware_backup` : Utilisé dans ONTAP 9.16.1 et versions antérieures avec des instantanés

créés en réponse à des anomalies. Par exemple : `Anti_ransomware_backup.2022-12-20_1248` .

Pour restaurer à partir d'un instantané autre que le `Anti_ransomware` Après l'identification d'une attaque système, vous devez d'abord libérer l'instantané ARP.

Si aucune attaque système n'est signalée, vous devez d'abord restaurer à partir du `Anti_ransomware` instantané, puis effectuez une restauration ultérieure du volume à partir de l'instantané que vous choisissez.

> Si le volume protégé par ARP fait partie d'une relation SnapMirror , vous devrez mettre à jour manuellement toutes les copies miroir du volume après sa restauration à partir d'un snapshot. Si vous ignorez cette étape, les copies miroir risquent de devenir inutilisables et de devoir être supprimées puis recréées.

Avant de commencer

"Vous devez marquer l'attaque comme une attaque potentielle de ransomware" avant de restaurer les données à partir d'un instantané.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour restaurer vos données.

System Manager

Restauration après une attaque système

1. Pour effectuer une restauration à partir de l'instantané ARP, passez à l'étape 2. Pour effectuer une restauration à partir d'un snapshot antérieur, vous devez d'abord libérer le verrou sur le snapshot ARP.
   a. Sélectionnez **stockage > volumes**.
   b. Sélectionnez **sécurité** puis **Afficher les types de fichiers suspects**.
   c. Marquez les fichiers comme « attaque potentielle par ransomware ».
   d. Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects**.
2. Afficher les snapshots dans les volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.
3. Sélectionnez ⋮ en regard de l'instantané que vous souhaitez restaurer, puis **Restaurer**.

Restaurez si aucune attaque système n'a été identifiée

1. Afficher les snapshots dans les volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.
2. Sélectionner ⋮ puis choisissez le `Anti_ransomware` instantané.
3. Sélectionnez **Restaurer**.
4. Revenez au menu **copies Snapshot**, puis choisissez l'instantané que vous souhaitez utiliser. Sélectionnez **Restaurer**.

CLI

Restauration après une attaque système

Pour effectuer une restauration à partir de l'instantané ARP, passez à l'étape 2. Pour restaurer des données à partir de snapshots antérieurs, vous devez libérer le verrou sur le snapshot ARP.

> ⓘ Si vous utilisez la commande décrite ci-dessous, vous devez libérer la fonctionnalité anti-ransomware SnapLock avant de restaurer les données à partir de copies Snapshot antérieures `volume snapshot restore`. Si vous restaurez des données à l'aide de FlexClone, de la restauration par alignement de fichier unique ou d'autres méthodes, cela n'est pas nécessaire.

1. Marquer l'attaque comme une attaque potentielle de ransomware (`-false-positive false`) et effacer les fichiers suspects (`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   Utilisez l'un des paramètres suivants pour identifier les extensions :

   - `[-seq-no integer]` : Numéro de séquence du fichier dans la liste des suspects.
   - `[-extension text, … ]` : Extensions de fichiers

- `[-start-time date_time -end-time date_time]` : Heures de début et de fin de la plage de fichiers à effacer, sous la forme « MM/JJ/AAAA HH:MM:SS ».

2. Lister les snapshots dans un volume :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre le snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Restaurer le contenu d'un volume à partir d'un snapshot :

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

L'exemple suivant restaure le contenu de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Restaurez si aucune attaque système n'a été identifiée

1. Lister les snapshots dans un volume :

```
volume snapshot show -vserver <SVM> -volume <volume>
```

L'exemple suivant montre le snapshot dans `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurer le contenu d'un volume à partir d'un snapshot :

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

L'exemple suivant restaure le contenu de `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Pour en savoir plus, `volume snapshot` consultez le "Référence de commande ONTAP".

Informations associées

- "Base de connaissances NetApp : Prévention et récupération des ransomwares dans ONTAP"
- "Référence de commande ONTAP"

Ajuster les paramètres des instantanés ARP générés automatiquement

Depuis la version ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes pour contrôler les paramètres de conservation des copies Snapshot ARP (Autonomous ransomware protection) qui sont générées automatiquement en réponse à des attaques de ransomware suspectées.

Avant de commencer

Vous ne pouvez modifier les options des snapshots ARP que sur un "nœud SVM" et pas sur d'autres types de SVM.

Étapes

1. Afficher tous les paramètres de snapshot ARP actuels :

```
options -option-name arw*
```

2. Afficher les paramètres de snapshot ARP actuels sélectionnés :

```
options -option-name <arw_setting_name>
```

3. Modifier les paramètres de snapshot ARP :

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

Vous pouvez modifier les paramètres suivants :

Certaines des commandes décrites sont obsolètes depuis ONTAP 9.17.1. Les commandes introduites dans ONTAP 9.17.1 prennent en charge les environnements NAS et SAN.

Réglage	Description	Versions prises en charge
`arw.snap.max.count`	Spécifie le nombre maximal d'instantanés ARP pouvant exister dans un volume à un moment donné. Les copies plus anciennes sont supprimées afin de garantir que le nombre total d'instantanés ARP reste dans la limite spécifiée.	ONTAP 9.11.1 et versions ultérieures
`arw.snap.create.interval.hours`	Spécifie l'intervalle (en heures) entre les snapshots ARP. Un nouveau snapshot ARP est créé lorsqu'une attaque par entropie des données est suspectée et que le snapshot ARP le plus récent est plus ancien que l'intervalle spécifié.	ONTAP 9.11.1 et versions ultérieures
`arw.snap.normal.retain.interval.hours`	Spécifie la durée (en heures) de conservation d'un instantané ARP. Lorsqu'un instantané ARP atteint le seuil de conservation, il est supprimé.	• ONTAP 9.11.1 à ONTAP 9.16.1 • Obsolète dans ONTAP 9.17.1 et versions ultérieures

Réglage	Description	Versions prises en charge
`arw.snap.max.retain.interval.days`	Spécifie la durée maximale *en jours* pour laquelle un instantané ARP peut être conservé. Tout snapshot ARP antérieur à cette durée est supprimé lorsqu'aucune attaque n'est signalée sur le volume. L'intervalle de rétention maximal pour les instantanés ARP est ignoré si une menace modérée est détectée. L'instantané ARP créé en réponse à la menace est conservé jusqu'à ce que vous ayez répondu à la menace. Lorsque vous marquez une menace comme un faux positif, ONTAP supprime les instantanés ARP du volume.	• ONTAP 9.11.1 à ONTAP 9.16.1 • Obsolète dans ONTAP 9.17.1 et versions ultérieures
`arw.snap.create.interval.hours.post.max.count`	Spécifie l'intervalle (en heures) entre les snapshots ARP lorsque le volume contient déjà le nombre maximal de snapshots ARP. Lorsque ce nombre maximal est atteint, un snapshot ARP est supprimé pour laisser la place à une nouvelle copie. Cette option permet de réduire la vitesse de création du nouveau snapshot ARP afin de conserver l'ancienne copie. Si le volume contient déjà le nombre maximal de snapshots ARP, l'intervalle spécifié dans cette option est utilisé pour la création du prochain snapshot ARP, au lieu de `arw.snap.create.interval.hours` .	• ONTAP 9.11.1 à 9.16.1 • Obsolète dans ONTAP 9.17.1 et versions ultérieures
`arw.snap.low.encryption.retain.duration.hours`	Spécifie la durée de conservation *en heures* des instantanés ARP créés pendant les périodes de faible activité de chiffrement.	• ONTAP 9.17.1 et versions ultérieures
`arw.snap.new.extns.interval.hours`	Spécifie l'intervalle, en heures, entre les instantanés ARP créés lors de la détection d'une nouvelle extension de fichier. Un nouvel instantané ARP est créé lorsqu'une nouvelle extension de fichier est détectée ; l'instantané précédent, créé lors de l'observation d'une nouvelle extension de fichier, est antérieur à cet intervalle spécifié. Sur une charge de travail créant fréquemment de nouvelles extensions de fichier, cet intervalle permet de contrôler la fréquence des instantanés ARP. Cette option est disponible indépendamment de `arw.snap.create.interval.hours` , qui spécifie l'intervalle pour les instantanés ARP basés sur l'entropie des données.	• ONTAP 9.11.1 à ONTAP 9.16.1 • Obsolète dans ONTAP 9.17.1 et versions ultérieures

Réglage	Description	Versions prises en charge
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Spécifie l'intervalle (en heures) pendant lequel un instantané ARP est conservé par précaution après qu'un incident d'attaque a été signalé comme faux positif par l'administrateur. Après l'expiration de cette période de conservation préventive, l'instantané peut être supprimé selon la durée de conservation standard définie par les options. `arw.snap.normal.retain.interval.hours` et `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 et versions ultérieures
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Spécifie l'intervalle (en heures) pendant lequel un instantané ARP est conservé par précaution après qu'une attaque a été signalée comme réelle par l'administrateur. Après l'expiration de cette période de conservation préventive, l'instantané peut être supprimé selon la durée de conservation standard définie par les options. `arw.snap.normal.retain.interval.hours` et `arw.snap.max.retain.interval.days` .	• ONTAP 9.16.1 et versions ultérieures
`arw.snap.surge.interval.days`	Spécifie l'intervalle *en jours* entre les snapshots ARP créés en réponse aux pics d'E/S. ONTAP crée une copie de surtension de snapshot ARP lorsqu'il y a une surtension dans le trafic d'E/S et que le dernier instantané ARP créé est plus ancien que cet intervalle spécifié. Cette option spécifie également la période de rétention *in Day* pour un instantané de surtension ARP.	ONTAP 9.11.1 et versions ultérieures
`arw.high.encryption.alert.enabled`	Active les alertes pour les niveaux de chiffrement élevés. Lorsque cette option est activée, `on` (par défaut), ONTAP envoie une alerte lorsque le pourcentage de chiffrement dépasse le seuil spécifié dans `arw.high.encryption.percentage.threshold` .	ONTAP 9.17.1 et versions ultérieures
`arw.high.encryption.percentage.threshold`	Spécifie le pourcentage maximal de chiffrement d'un volume. Si le pourcentage de chiffrement dépasse ce seuil, ONTAP traite l'augmentation comme une attaque et crée un snapshot ARP. `arw.high.encryption.alert.enabled` doit être réglé sur `on` pour que cette option prenne effet.	ONTAP 9.17.1 et versions ultérieures
`arw.snap.high.encryption.retain.duration.hours`	Spécifie l'intervalle de durée de conservation *en heures* pour les instantanés créés lors d'un événement de seuil de chiffrement élevé.	ONTAP 9.17.1 et versions ultérieures

4. Si vous utilisez ARP avec un environnement SAN, vous pouvez également modifier les paramètres de période d'évaluation suivants :

Réglage	Description	Versions prises en charge
`arw.block_device.auto.learn.threshold.min_value`	Spécifie la valeur de pourcentage du seuil de chiffrement minimum pendant la phase d'apprentissage automatique de l'évaluation pour les périphériques de bloc.	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.auto.learn.threshold.max_value`	Spécifie la valeur de pourcentage du seuil de chiffrement maximal pendant la phase d'apprentissage automatique de l'évaluation pour les périphériques de bloc.	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.evaluation.phase.min_hours`	Spécifie l'intervalle minimum *en heures* pendant lequel la phase d'évaluation doit s'exécuter avant que le seuil de chiffrement ne soit défini.	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.evaluation.phase.max_hours`	Spécifie l'intervalle maximal *en heures* pendant lequel la phase d'évaluation doit s'exécuter avant que le seuil de chiffrement ne soit défini.	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	Spécifie la quantité minimale de données *en Go* qui doivent être ingérées pendant la phase d'évaluation avant que le seuil de chiffrement ne soit défini.	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.evaluation.phase.alert.enabled`	Indique si les alertes sont activées pour la phase d'évaluation d'ARP sur les périphériques de type bloc. La valeur par défaut est `True` .	ONTAP 9.17.1 et versions ultérieures
`arw.block_device.evaluation.phase.alert.threshold`	Spécifie le pourcentage de seuil pendant la phase d'évaluation d'ARP sur les périphériques de type bloc. Si le pourcentage de chiffrement dépasse ce seuil, une alerte est déclenchée.	ONTAP 9.17.1 et versions ultérieures

Informations associées

- "Évaluation des menaces et instantanés ARP"
- "Période d'évaluation de l'entropie SAN"

Mettez à jour la protection anti-ransomware autonome de ONTAP avec l'IA (ARP/ai)

Pour vous protéger contre les dernières menaces de ransomware, ARP/ai propose des mises à jour automatiques en dehors des cadences de version ONTAP régulières.

À partir d' ONTAP 9.16.1, les mises à jour de sécurité pour ARP/AI sont disponibles dans les téléchargements du logiciel System Manager, en plus des mises à jour système et du firmware. Si votre cluster ONTAP est déjà inscrit à "mises à jour automatiques du système et du micrologiciel" Vous serez automatiquement averti(e) des mises à jour de sécurité ARP/AI disponibles. Vous pouvez également modifier vos préférences de mise à jour afin ONTAP installe automatiquement les mises à jour de sécurité.

Si vous le souhaitezMettez à jour manuellement ARP/ai, vous pouvez télécharger les mises à jour à partir du site de support NetApp et les installer à l'aide de System Manager.

Description de la tâche

Vous ne pouvez mettre à jour ARP/AI qu'à l'aide du Gestionnaire système.

Sélectionnez une préférence de mise à jour pour ARP/ai

Dans le Gestionnaire système, les paramètres de la page Activer les mises à jour automatiques pour les fichiers de sécurité sont définis sur `Show notifications` Si vous êtes déjà inscrit aux mises à jour automatiques du micrologiciel et du système, vous pouvez modifier les paramètres de mise à jour. `Automatically update` Si vous préférez ONTAP applique automatiquement les dernières mises à jour, vous pouvez choisir d'afficher les notifications ou de les ignorer automatiquement. Si vous utilisez un dark web ou préférez effectuer les mises à jour manuellement,

Avant de commencer

Pour les mises à jour de sécurité automatiques, "AutoSupport et AutoSupport OnDemand doivent être activés et le protocole de transport doit être défini sur HTTPS".

Étapes

1. Dans System Manager, cliquez sur **Cluster > Paramètres > mises à jour logicielles**.
2. Dans la section **mises à jour logicielles**, sélectionnez →.
3. Sur la page **mises à jour logicielles**, sélectionnez l'onglet **toutes les autres mises à jour**.
4. Sélectionnez l'onglet **toutes les autres mises à jour** et cliquez sur **plus**.
5. Sélectionnez **Modifier les paramètres de mise à jour automatique**.
6. Sur la page Paramètres de mise à jour automatique, sélectionnez **fichiers de sécurité**.
7. Spécifiez l'action à effectuer pour les fichiers de sécurité (mises à jour ARP/ai).

   Vous pouvez choisir de mettre à jour, d'afficher les notifications ou de rejeter automatiquement les mises à jour.

   ⓘ Pour que les mises à jour de sécurité se mettent automatiquement à jour, AutoSupport et AutoSupport OnDemand doivent être activés et le protocole de transport doit être défini sur HTTPS.

8. Acceptez les conditions générales et sélectionnez **Enregistrer**.

Mettez à jour manuellement ARP/ai avec le dernier package de sécurité

Suivez la procédure appropriée selon que vous êtes enregistré ou non auprès de Active IQ Unified Manager.

ⓘ Assurez-vous d'installer uniquement une mise à jour ARP plus récente que votre version actuelle afin d'éviter toute rétrogradation ARP involontaire.

ONTAP 9.16.1 et versions ultérieures avec Digital Advisor

1. Dans System Manager, accédez à **Dashboard**.

   Dans la section **Santé**, un message s'affiche si des mises à jour de sécurité sont recommandées pour le cluster.

2. Cliquez sur le message d'alerte.
3. En regard des mises à jour de sécurité dans la liste des mises à jour recommandées, sélectionnez **actions**.
4. Cliquez sur **mettre à jour** pour installer la mise à jour immédiatement ou sur **planifier** pour la programmer ultérieurement.

   Si la mise à jour est déjà programmée, vous pouvez **la modifier** ou **la Annuler**.

ONTAP 9.16.1 et versions ultérieures sans conseiller numérique

1. Accédez au "Site de support NetApp"et connectez-vous.
2. Complétez les invites et téléchargez le package de sécurité que vous souhaitez utiliser pour mettre à jour votre ARP/ai de cluster.
3. Copiez les fichiers sur un serveur HTTP ou FTP de votre réseau ou dans un dossier local accessible par le cluster avec ARP/ai.
4. Dans System Manager, cliquez sur **Cluster > Paramètres > mises à jour logicielles**.
5. Dans **mises à jour logicielles**, sélectionnez l'onglet **toutes les autres mises à jour**.
6. Dans le volet **mises à jour manuelles**, cliquez sur **Ajouter des fichiers de sécurité** et ajoutez les fichiers à l'aide de l'une des préférences suivantes :
   - **Télécharger à partir du serveur** : saisissez l'URL du paquet de fichiers de sécurité.
   - **Télécharger à partir du client local** : accédez au fichier TGZ téléchargé.

   > Assurez-vous que le nom de fichier commence par `ontap_security_file_arpai_` et a `.tgz` une extension de fichier.

7. Cliquez sur **Ajouter** pour appliquer les mises à jour.

Vérifiez les mises à jour ARP/ai

Pour afficher un historique des mises à jour automatiques qui ont été rejetées ou qui n'ont pas pu être installées, procédez comme suit :

1. Dans System Manager, cliquez sur **Cluster > Paramètres > mises à jour logicielles**.
2. Dans la section **mises à jour logicielles**, sélectionnez →.
3. Sur la page **mises à jour logicielles**, sélectionnez l'onglet **toutes les autres mises à jour** et cliquez sur **plus**.
4. Sélectionnez **Afficher toutes les mises à jour automatiques**.

Informations associées

- "Découvrez ARP/IA"
- "Abonnements par e-mail aux mises à jour logicielles"

Informations sur le copyright

Informations sur les marques commerciales