Protection autonome contre les ransomwares

ONTAP 9

NetApp
August 31, 2024

Sommaire

Protection autonome contre les ransomwares

Présentation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la fonctionnalité ARP (autonome ransomware protection) utilise l'analyse des workloads dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive les activités anormales qui pourraient indiquer une attaque par ransomware.

Lorsqu'une attaque est suspectée, ARP crée également de nouvelles copies Snapshot, en plus de la protection existante à partir de copies Snapshot planifiées.

Licences et activation

ARP requiert une licence. ARP est disponible avec le "Licence ONTAP ONE". Si vous ne disposez pas de la licence ONTAP One, d'autres licences sont disponibles pour utiliser ARP, qui varient selon votre version de ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.11.1 et versions ultérieures	Protection contre les ransomwares
ONTAP 9.10.1	MT_EK_MGMT (gestion des clés mutualisée)

- Si vous effectuez une mise à niveau vers ONTAP 9.11.1 ou version ultérieure et que ARP est déjà configuré sur votre système, vous n'avez pas besoin d'acheter la nouvelle licence anti-ransomware. Pour les nouvelles configurations ARP, la nouvelle licence est requise.
- Si vous effectuez une restauration depuis ONTAP 9.11.1 ou une version ultérieure vers ONTAP 9.10.1 et que vous avez activé ARP avec la licence anti-ransomware, un message d'avertissement s'affiche et vous devrez peut-être reconfigurer ARP. "Découvrez le rétablissement ARP".

Vous pouvez configurer le protocole ARP par volume à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP.

Stratégie ONTAP de protection contre les ransomwares

Une stratégie efficace de détection des ransomwares doit inclure plus d'une couche de protection unique

On pourrait comparer les caractéristiques de sécurité d'un véhicule. Vous ne vous fiez pas à une seule fonction, telle qu'une ceinture de sécurité, pour vous protéger complètement en cas d'accident. Les sacs gonflables, les freins antiblocage et l'avertissement de collision avant sont tous des dispositifs de sécurité supplémentaires qui permettront d'obtenir un meilleur résultat. La protection contre les ransomwares doit être vue de la même manière.

Tandis que ONTAP inclut des fonctionnalités comme FPolicy, les copies Snapshot, SnapLock et Active IQ Digital Advisor pour vous protéger contre les attaques par ransomware, les informations suivantes se concentrent sur la fonctionnalité intégrée ARP avec des fonctionnalités de machine learning.

Pour en savoir plus sur les autres fonctionnalités de ONTAP contre les ransomware, consultez "Ransomware

et le portefeuille de solutions de protection de NetApp".

Ce que le protocole ARP détecte

Le protocole ARP est conçu pour vous protéger contre les attaques par déni de service où l'attaquant conserve ses données jusqu'au paiement d'une rançon. ARP propose une détection en temps réel des ransomware basée sur :

- Identification des données entrantes comme cryptées ou en texte clair.
- Les analyses, qui détectent
  - **Entropy**: Une évaluation du caractère aléatoire des données dans un fichier
  - **Types d'extension de fichier** : extension non conforme au type d'extension normal
  - **File IOPS** : une augmentation de l'activité de volume anormale avec le chiffrement des données (à partir de ONTAP 9.11.1)

ARP peut détecter la propagation de la plupart des attaques par ransomware après le chiffrement d'un petit nombre de fichiers uniquement, l'action automatique pour protéger les données et vous avertir qu'une attaque suspectée a lieu.

> Aucun système de détection ou de prévention par ransomware ne peut garantir la sécurité en cas d'attaque par ransomware. Bien qu'il soit possible qu'une attaque ne soit pas détectée, ARP agit comme une couche supplémentaire importante de défense si un logiciel antivirus ne parvient pas à détecter une intrusion.

Modes d'apprentissage et actifs

ARP a deux modes :

- **Apprentissage** (ou mode de fonctionnement à sec)
- **Actif** (ou mode « activé »)

Lorsque vous activez ARP, il s'exécute en *mode d'apprentissage*. En mode apprentissage, le système ONTAP développe un profil d'alerte basé sur les zones analytiques : entropie, types d'extension de fichier et IOPS de fichier. Après avoir exécuté ARP en mode d'apprentissage pendant suffisamment de temps pour évaluer les caractéristiques de la charge de travail, vous pouvez passer en mode actif et commencer à protéger vos données. Une fois que le protocole ARP est passé en mode actif, ONTAP crée des copies Snapshot ARP pour protéger les données en cas de détection d'une menace.

Il est recommandé de laisser ARP en mode d'apprentissage pendant 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours.

En mode actif, si une extension de fichier est marquée comme anormale, vous devez évaluer l'alerte. Vous pouvez agir sur l'alerte pour protéger vos données ou marquer l'alerte comme un faux positif. Le fait de marquer une alerte comme un 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 marquez l'alerte comme un faux positif, vous ne recevrez pas d'alerte la prochaine fois que l'extension de fichier sera observée. 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.)

À partir de ONTAP 9.11.1, vous pouvez personnaliser les paramètres de détection pour ARP. Pour plus d'informations, voir Gérer les paramètres de détection d'attaque ARP.

Évaluation des menaces et copies Snapshot ARP

En mode actif, ARP évalue la probabilité de menace en fonction des données entrantes mesurées par rapport aux analyses apprises. Une mesure est attribuée lorsque ARP détecte une menace :

- **Faible** : la première détection d'une anomalie dans le volume (par exemple, une nouvelle extension de fichier est observée dans le volume).
- **Modéré**: Plusieurs fichiers avec la même extension de fichier jamais vu-avant sont observés.
  - Dans ONTAP 9.10.1, le seuil de remontée à modéré est de 100 fichiers ou plus. À partir de ONTAP 9.11.1, la quantité du fichier peut être modifiée ; sa valeur par défaut est 20.

En cas de menace faible, ONTAP détecte une anomalie et crée une copie Snapshot du volume pour créer le meilleur point de restauration. ONTAP ajoute au nom de la copie snapshot ARP le préfixe `Anti-ransomware-backup` pour le rendre facilement identifiable, par exemple `Anti_ransomware_backup.2022-12-20_1248`.

La menace passe au niveau modéré après l'exécution d'un rapport d'analytique par ONTAP qui détermine si l'anomalie correspond à un profil de ransomware. Les menaces qui restent au niveau bas sont consignées et visibles dans la section **événements** de System Manager. Lorsque la probabilité d'attaque est modérée, ONTAP génère une notification EMS vous invitant à évaluer la menace. ONTAP n'envoie pas d'alertes en cas de menaces faibles, mais à partir de ONTAP 9.14.1, vous pouvez le faire modifier les paramètres des alertes. Pour plus d'informations, voir Réagir à une activité anormale.

Vous pouvez afficher des informations sur une menace, quel que soit le niveau, dans la section **événements** de System Manager ou avec le `security anti-ransomware volume show` commande.

Les copies Snapshot ARP sont conservées pendant au moins deux jours. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de rétention. Pour plus d'informations, voir Modifiez les options des copies Snapshot.

Comment récupérer des données dans ONTAP après une attaque par ransomware

Lorsqu'une attaque est suspectée, le système prend une copie Snapshot du volume à ce moment-là et verrouille cette copie. Si l'attaque est confirmée ultérieurement, le volume peut être restauré à l'aide de la copie ARP Snapshot.

La suppression des copies Snapshot verrouillées ne peut pas être effectuée par des moyens normaux. Cependant, si vous décidez plus tard de marquer l'attaque comme un faux positif, la copie verrouillée sera supprimée.

En connaissant les fichiers affectés et l'heure de l'attaque, il est possible de restaurer de manière sélective les fichiers affectés à partir de plusieurs copies Snapshot, plutôt que de simplement restaurer le volume entier vers l'une des copies Snapshot.

ARP s'appuie donc sur la technologie de protection des données et de reprise après incident ONTAP éprouvée pour répondre aux attaques par ransomware. Pour plus d'informations sur la récupération de données, reportez-vous aux rubriques suivantes.

- "Restauration à partir de copies Snapshot (System Manager)"
- "Restauration de fichiers à partir de copies Snapshot (interface de ligne de commandes)"

- "Restauration intelligente par ransomware"

Cas d’utilisation et considérations relatives à la protection autonome contre les ransomwares

La protection anti-ransomware autonome (ARP) est disponible pour les charges de travail NAS à partir de ONTAP 9.10.1. 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 pour :

- Les bases de données sur le stockage NFS
- Répertoires locaux Windows ou Linux

  Comme les utilisateurs pouvaient créer des fichiers avec des extensions qui n’ont pas été détectées pendant la période d’apprentissage, les risques de faux positifs sont plus élevés 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 pour :

- Les workloads comportant une fréquence élevée de création ou de suppression de fichiers (des centaines de milliers de fichiers en quelques secondes, par exemple des workloads de test/développement).
- La détection des menaces par ARP dépend de sa capacité à reconnaître une augmentation inhabituelle de l’activité de création, de renommage ou de suppression de fichiers. Si l’application elle-même est la source de l’activité des fichiers, elle ne peut pas être efficacement distinguée de l’activité des ransomware.
- Charges de travail où l’application ou l’hôte chiffre les données.
  ARP dépend de la distinction des données entrantes comme chiffrées ou non chiffrées. Si l’application elle-même est en train de chiffrer les données, l’efficacité de la fonction est réduite. Toutefois, la fonction peut toujours fonctionner en fonction de l’activité du fichier (supprimer, écraser ou créer, ou créer ou renommer avec une nouvelle extension de fichier) et du type de fichier.

Configurations compatibles

ARP est disponible pour les volumes NFS et SMB dans les systèmes ONTAP sur site 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 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protégés avec SnapMirror asynchrone	✓	✓	✓	✓		
SVM protégé avec SnapMirror asynchrone (reprise après incident SVM)	✓	✓	✓	✓		
Mobilité des données des SVM (`vserver migrate`)	✓	✓	✓	✓		
Volumes FlexGroup	✓	✓	✓			
Vérification multi-administrateurs	✓	✓	✓			

Interopérabilité SnapMirror et ARP

À partir de ONTAP 9.12.1, ARP est pris en charge sur les volumes de destination SnapMirror asynchrones. ARP est **non** pris en charge avec SnapMirror Synchronous.

Si un volume source SnapMirror est compatible ARP, le volume de destination SnapMirror acquiert automatiquement l'état de configuration ARP (apprentissage, activation, etc.), les données d'entraînement ARP et le snapshot créé par ARP du volume source. Aucune activation explicite n'est requise.

Alors que le volume de destination se compose de copies Snapshot RO (lecture seule), aucun traitement ARP n'est effectué sur ses données. Toutefois, 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 pas de procédure d'apprentissage supplémentaire en plus de ce qui est déjà enregistré 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'entraînement et les copies Snapshot des volumes source vers les volumes de destination. Ainsi, lorsque le volume de destination SnapMirror est converti en RW, ARP sur le volume de destination doit être explicitement activé en mode apprentissage une fois la conversion terminée.

ARP et machines virtuelles

ARP est pris en charge avec les machines virtuelles (VM). La détection ARP se comporte différemment pour les modifications à l'intérieur et à l'extérieur de la machine virtuelle. ARP n'est pas recommandé pour les workloads avec des fichiers fortement entropie dans la machine virtuelle.

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 chiffré ou si une extension de fichier change. Les modifications d'extension de fichier détectables sont les suivantes :

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Modifications au sein de la machine virtuelle

Si l'attaque par ransomware cible la machine virtuelle et les fichiers à l'intérieur de la machine virtuelle sont modifiés sans effectuer de modifications à l'extérieur de la machine virtuelle, ARP détecte la menace si l'entropie par défaut de la machine virtuelle est faible (par exemple, fichiers .txt, .docx ou .mp4). Bien que ARP crée un instantané de protection dans ce scénario, il ne génère pas d'alerte de menace car les extensions de fichiers en dehors de la machine virtuelle n'ont pas été falsifiées.

Si, par défaut, les fichiers sont à haute entropie (par exemple, les fichiers .gzip ou protégés par mot de passe), les capacités de détection d'ARP sont limitées. ARP peut toujours prendre des snapshots proactifs dans ce cas ; cependant, aucune alerte ne sera déclenchée si les extensions de fichier n'ont pas été falsifiées en externe.

Configurations non prises en charge

ARP n'est pas pris en charge dans les configurations système suivantes :

- Les environnements ONTAP S3
- Environnements SAN

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

- Volumes FlexGroup (dans ONTAP 9.10.1 à 9.12.1. À partir de ONTAP 9.13.1, les volumes FlexGroup sont pris en charge)
- 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 SAN uniquement
- Volumes SnapLock

- SnapMirror synchrone
- SnapMirror asynchrone (non pris en charge uniquement dans ONTAP 9.10.1 et 9.11.1) SnapMirror asynchrone est pris en charge à partir de ONTAP 9.12.1. Pour plus d'informations, voir [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

Le protocole ARP peut avoir un impact minimal sur les performances du système, mesuré en débit et en pic d'IOPS. L'impact de la fonctionnalité ARP dépend des charges de travail de volume spécifiques. 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 :[*]
Ces données intensives en lecture ou compressées peuvent être compressées.	150	4 % des IOPS maximales
Des opérations d'écriture intensives et des données ne peuvent pas être compressées.	60	10 % des IOPS maximales

Pass:[*] 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.

L'analyse ARP étant exécutée selon une séquence prioritaire, à mesure que le nombre de volumes protégés augmente, l'analyse s'exécute moins souvent sur chaque volume.

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 le `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, et `security anti-ransomware volume attack clear-suspect` Commandes ARP à protéger. Chaque administrateur du groupe MAV doit approuver chaque nouvelle demande de règle et "Ajoutez à nouveau la règle MAV" Dans les paramètres MAV.

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

Étapes suivantes

- "Activation de la protection autonome contre les ransomwares"

- "Activez MAV pour les volumes protégés par ARP"

Activation de la protection autonome contre les ransomwares

Depuis ONTAP 9.10.1, la protection autonome contre les ransomwares (ARP) peut être activée sur les volumes nouveaux ou existants. Vous commencez par activer ARP en mode d'apprentissage, dans lequel le système analyse la charge de travail pour caractériser le comportement normal. Vous pouvez activer ARP sur un volume existant ou créer un nouveau volume et activer ARP depuis le début.

Description de la tâche

Vous devez toujours activer le protocole ARP au départ en mode d'apprentissage (ou d'exécution à sec). Le démarrage en mode actif peut entraîner des rapports faux positifs excessifs.

Il est recommandé de laisser ARP fonctionner en mode d'apprentissage pendant au moins 30 jours. À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur, qui peut se produire avant 30 jours. Pour plus d'informations, voir "Modes d'apprentissage et actifs".

> 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.

Avant de commencer

- Une VM de stockage (SVM) doit être activée pour NFS ou SMB (ou les deux).
- Le licence correcte Doit être installé pour votre version ONTAP.
- Vous devez avoir une charge de travail NAS avec des clients configurés.
- Le volume sur lequel vous souhaitez définir ARP doit être protégé et doit avoir un actif "chemin de jonction".
- Le volume doit être rempli à moins de 100 %.
- Il est recommandé de configurer le système EMS pour envoyer des notifications par e-mail, qui incluront des notifications d'activité ARP. Pour plus d'informations, voir "Configurez les événements EMS pour envoyer des notifications par e-mail".
- À partir de 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".

Activez ARP

Vous pouvez activer le protocole ARP 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 à protéger.
2. Dans l'onglet **sécurité** de la vue d'ensemble **volumes**, sélectionnez **État** pour passer de Désactivé à activé en mode apprentissage dans la zone **anti-ransomware**.
3. Lorsque la période d'apprentissage est terminée, passez ARP en mode actif.

   À partir de ONTAP 9.13.1, ARP détermine automatiquement la période d'apprentissage optimale et automatise le commutateur. C'est possible "Désactivez ce paramètre sur la machine virtuelle de stockage associée" si vous souhaitez contrôler manuellement le mode d'apprentissage en mode actif.

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

Le processus d'activation de ARP avec l'interface de ligne de commande diffère si vous l'activez sur un volume existant par rapport à un nouveau volume.

Activez ARP sur un volume existant

1. Modifiez un volume existant pour activer la protection par ransomware en mode d'apprentissage :

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

   Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

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

2. Lorsque la période d'apprentissage est terminée, 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
   active
   ```

3. Vérifiez l'état ARP du volume.

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

Activez ARP sur un nouveau volume

1. Créez un volume avec la protection anti-ransomware activée avant le provisionnement des données.

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

   Si vous utilisez ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif soit effectué automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, modifier le paramètre au niveau du SVM sur tous les volumes associés :

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

2. Lorsque la période d'apprentissage est terminée, 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
   active
   ```

3. Vérifiez l'état ARP du volume.

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

Activez la protection autonome par défaut contre les ransomwares dans les nouveaux volumes

Depuis ONTAP 9.10.1, vous pouvez configurer des machines virtuelles de stockage (SVM) de manière à ce que les nouveaux volumes soient activés par défaut pour le mode d'apprentissage ARP (autonome ransomware protection).

Description de la tâche

Par défaut, de nouveaux volumes sont créés avec ARP en mode désactivé. Vous pouvez modifier ce paramètre dans System Manager et via l'interface de ligne de commandes. Les volumes activés par défaut sont définis sur ARP en mode d'apprentissage (ou d'exécution à sec).

ARP ne sera activé que sur les volumes créés dans le SVM après avoir modifié le paramètre. ARP ne sera pas activé sur les volumes existants. Découvrez comment "Activez ARP dans un volume existant".

À partir de ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP et le passage du mode d'apprentissage au mode actif s'effectue automatiquement. Pour plus d'informations, voir "Modes d'apprentissage et actifs".

Avant de commencer

- Le licence correcte Doit être installé pour votre version ONTAP.
- Le volume doit être rempli à moins de 100 %.

- Les chemins de jonction doivent être actifs.
- À partir de la version ONTAP 9.13.1, il est recommandé d'activer la vérification multiadministrateur afin que deux administrateurs d'utilisateurs authentifiés minimum soient requis pour les opérations anti-ransomware. "En savoir plus >>".

Basculez ARP du mode d'apprentissage au mode actif

À partir de la ONTAP 9.13.1, l'apprentissage adaptatif a été ajouté à l'analyse ARP. Le passage du mode d'apprentissage au mode actif s'effectue automatiquement. La décision autonome prise par ARP de passer automatiquement du mode d'apprentissage au mode actif est basée 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
```

Après 30 jours d'apprentissage, un volume passe automatiquement en mode actif même si une ou plusieurs de ces conditions ne sont pas satisfaites. Autrement dit, si le commutateur automatique est activé, le volume passe en mode actif au bout de 30 jours maximum. La valeur maximale 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".

Étapes

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

System Manager

1. Sélectionnez **Storage > Storage VM**, puis sélectionnez la VM de stockage contenant les volumes que vous souhaitez protéger avec ARP.
2. Accédez à l'onglet **Paramètres**. Sous **sécurité**, localisez la mosaïque **anti-ransomware**, puis sélectionnez
3. Cochez la case pour activer ARP pour les volumes NAS. Cochez la case supplémentaire pour activer ARP sur tous les volumes NAS éligibles de la machine virtuelle de stockage.

> Si vous avez effectué une mise à niveau vers ONTAP 9.13.1, le **passage automatique du mode apprentissage au mode actif après un apprentissage suffisant** est activé automatiquement. Cela permet à ARP de déterminer l'intervalle de la période d'apprentissage optimale et d'automatiser le passage en mode actif. Désactivez le paramètre si vous souhaitez passer manuellement en mode actif.

CLI

1. Modifier un SVM existant pour activer ARP par défaut dans les nouveaux volumes :
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Au niveau de l'interface de ligne de commandes, vous pouvez également créer un nouveau SVM avec ARP activé par défaut pour les nouveaux volumes.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Si vous avez mis à niveau vers ONTAP 9.13.1 ou une version ultérieure, l'apprentissage adaptatif est activé de sorte que le changement d'état actif s'effectue automatiquement. Si vous ne souhaitez pas que ce comportement soit automatiquement activé, utilisez la commande suivante :

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

Mettez en pause la protection autonome contre les ransomwares pour exclure les événements des charges de travail 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 >>".

Description de la tâche

Lors d'une pause ARP, aucun événement n'est enregistré et aucune action n'est en cours pour les nouvelles écritures. Toutefois, le processus d'analytique continue pour les journaux précédents 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 **Pause anti-ransomware** dans la zone **anti-ransomware**.

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

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`*

3. **Si vous utilisez MAV (disponible avec ARP à partir de ONTAP 9.13.1) pour protéger vos paramètres ARP,** l'opération de pause vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. L'approbation doit être reçue de tous les administrateurs associés au groupe d'approbation MAV, 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`*`]`

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

À partir de la version ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des ransomwares sur un volume spécifique optimisé par la protection anti-ransomware autonome 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 anti-ransomware autonome (ARP) est en mode d'apprentissage, elle développe des valeurs de base pour les comportements de volume. Il s'agit d'entropie, d'extensions de fichiers et, à partir de ONTAP 9.11.1, d'IOPS. Ces données de base sont utilisées pour évaluer les menaces de ransomware. Pour plus d'informations sur ces critères, reportez-vous à la section Ce que le protocole ARP détecte.

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 fichier 24 heures et 20 sont des valeurs par défaut, qui peuvent être modifiées.)

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 instantané. Pour plus d'informations, voir [modify-alerts]

Certains volumes et charges de travail requièrent des paramètres de détection différents. Par exemple, votre volume ARP peut héberger de nombreux types d'extensions de fichiers. Dans ce cas, vous pouvez modifier le nombre de seuils pour les extensions de fichiers jamais vues à un nombre supérieur à la valeur par défaut de 20 ou désactiver les avertissements basés sur des extensions de fichiers jamais vues. À partir de ONTAP 9.11.1, vous pouvez modifier les paramètres de détection des attaques afin qu'ils s'adaptent mieux à vos workloads spécifiques.

Modifier les paramètres de détection d'attaque

Selon les comportements attendus de votre volume ARP, vous pouvez modifier les paramètres de détection d'attaque.

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
            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 : 20
       Never Seen before File Extensions Duration in Hour : 24
```

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

   Pour obtenir la liste complète des paramètres, reportez-vous à la section "Référence de commande ONTAP".

Signaler les surtensions connues

ARP continue de modifier les valeurs de base pour les paramètres de détection, même en mode actif. Si vous connaissez des surtensions dans votre activité de volume—des surtensions ou une surtension qui est caractéristique d'une nouvelle normale—vous devriez la signaler comme sûre. 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
   ```

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
   ```

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 une vérification multiadministrateur. Pour plus d'informations, voir Vérification multiadministrateur avec volumes protégés par ARP.

System Manager

Définir des alertes pour un volume

1. Accédez à **volumes**. Sélectionnez le volume individuel pour lequel vous souhaitez modifier les paramètres.
2. Sélectionnez l'onglet **sécurité**, puis **Paramètres de sécurité des événements**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'événement** à **Avis**.
4. Sélectionnez **Enregistrer**.

Définir des alertes pour un SVM

1. Naviguer jusqu'à **Storage VM** puis sélectionner le SVM pour lequel vous voulez activer les paramètres.
2. Sous la rubrique **sécurité**, repérez la carte **anti-ransomware**. Sélectionnez ⋮, puis **Modifier la gravité des événements ransomware**.
3. Pour recevoir des alertes pour **Nouvelle extension de fichier détectée** et **instantané de ransomware créé**, sélectionnez le menu déroulant sous l'en-tête **gravité**. Modifiez le paramètre de **ne pas générer l'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 -is
  -enabled-on-new-file-extension-seen true
  ```

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

  ```
  security anti-ransomware volume event-log modify -vserver svm_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 instantané 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.

Plus d'informations

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

Réagir à une activité anormale

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.

Description de la tâche

ARP affiche une liste des fichiers suspects lorsqu'il détecte une combinaison de données entropie élevée, une activité de volume anormale avec chiffrement des données et des extensions de fichier inhabituelles.

Lorsque l'avertissement est émis, répondez en désignant l'activité de fichier de l'une des deux manières suivantes :

- **Faux positif**

  Le type de fichier identifié est attendu dans votre charge de travail et peut être ignoré.

- **Attaque potentielle par ransomware**

  Le type de fichier identifié est inattendu dans votre charge de travail et doit être traité comme une attaque potentielle.

Dans les deux cas, la surveillance normale reprend après la mise à jour et la suppression des avis. ARP enregistre votre évaluation dans le profil d'évaluation des menaces, en utilisant votre choix pour surveiller les activités de fichiers suivantes.

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 être exécuté en mode actif.

Étapes

Vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour répondre à une tâche anormale.

System Manager

1. Lorsque vous recevez une notification d'activité anormale, suivez le lien. Vous pouvez également accéder à l'onglet **sécurité** de la présentation **volumes**.

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

2. Lorsqu'un message "activité de volume anormale détectée" s'affiche, consultez les fichiers suspects.

   Dans l'onglet **sécurité**, sélectionnez **Afficher les types de fichiers suspects**.

3. Dans la boîte de dialogue **types de fichiers suspects**, examinez chaque type de fichier et marquez-le comme "Faux positif" ou "attaque par ransomware potentielle".

Si vous avez sélectionné cette valeur…	Prendre cette action…
Faux positif	Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects** pour enregistrer votre décision et reprendre la surveillance ARP normale. ⓘ À partir de ONTAP 9.13.1, si vous utilisez MAV pour protéger vos paramètres ARP, l'opération Effacer-suspect vous invite à obtenir l'approbation d'un ou de plusieurs administrateurs supplémentaires. "L'approbation doit être reçue de tous les administrateurs" Associé au groupe d'approbation MAV ou l'opération échouera.
Attaques par ransomware potentielles	Répondez aux attaques et restaurez les données protégées. Sélectionnez ensuite **Update** et **Clear suspect File types** pour enregistrer votre décision et reprendre la surveillance ARP normale. Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier.

CLI

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: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

   Vous pouvez également vérifier les messages EMS :

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

2. Générez un rapport d'attaque et notez l'emplacement de sortie :

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   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 :

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Suivez l'une des actions suivantes en fonction de votre évaluation des extensions de fichier :

   - Faux positif

     Entrez la commande suivante pour enregistrer votre décision, en ajoutant la nouvelle extension à la liste de ceux autorisés et en redonnant une surveillance anti-ransomware normale :
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

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

   - 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, entrez la commande suivante pour enregistrer votre décision et reprendre la surveillance ARP normale :

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

Il n'existe aucun type de fichier suspect à effacer si vous avez restauré un volume entier. L'instantané de sauvegarde créé par ARP sera supprimé et le rapport d'attaque sera effacé.

5. 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.

6. 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]
   ```

Plus d'informations

- "Base de connaissances : comprendre les attaques de protection anti-ransomware autonomes et le snapshot de protection anti-ransomware autonome".

Restaurez les données après une attaque par ransomware

La protection anti-ransomware autonome (ARP) crée des copies Snapshot nommées `Anti_ransomware_backup` lorsqu'il détecte une menace potentielle de ransomware. Vous pouvez utiliser l'une de ces copies snapshot ARP ou une autre copie Snapshot de votre volume pour restaurer les données.

Description de la tâche

Si le volume possède des relations SnapMirror, répliquez manuellement toutes les copies miroir du volume immédiatement après la restauration à partir d'une copie Snapshot. Cette opération risque d'entraîner des copies miroir inutilisables qui doivent d'être supprimées et recréées.

Pour effectuer une restauration à partir d'une copie Snapshot autre que le `Anti_ransomware_backup` Instantané après l'identification d'une attaque système, vous devez d'abord libérer l'instantané ARP.

Si aucune attaque système n'a été signalée, vous devez d'abord restaurer à partir du `Anti_ransomware_backup` La copie Snapshot effectue ensuite une restauration ultérieure du volume à partir de la copie Snapshot de votre choix.

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'une copie Snapshot antérieure, vous devez d'abord libérer le verrouillage de l'instantané ARP.
   a. Sélectionnez **stockage > volumes**.
   b. Sélectionnez **sécurité** puis **Afficher les types de fichiers suspects**
   c. Marquez les fichiers comme « Faux positif » .
   d. Sélectionnez **mettre à jour** et **Effacer les types de fichiers suspects**
2. Afficher les copies Snapshot dans des volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.
3. Sélectionnez ⋮ en regard de la copie Snapshot à restaurer, puis **Restaurer**.

Restaurez si aucune attaque système n'a été identifiée

1. Afficher les copies Snapshot dans des volumes :

   Sélectionnez **stockage > volumes**, puis sélectionnez le volume et **copies Snapshot**.
2. Sélectionnez ⋮ -les Choisissez l' `Anti_ransomware_backup` instantané.
3. Sélectionnez **Restaurer**.
4. Revenez au menu **copies Snapshot**, puis choisissez la copie Snapshot que vous souhaitez utiliser. Sélectionnez **Restaurer**.

CLI

Restauration après une attaque système

1. Pour effectuer une restauration à partir de la copie ARP Snapshot, passez à l'étape 2. Pour restaurer des données à partir de copies Snapshot antérieures, vous devez libérer le verrouillage de l'instantané ARP.

   ⓘ Si vous utilisez la, vous devez libérer la fonctionnalité anti-ransomware SnapLock avant de restaurer vos données à partir de copies Snapshot antérieures `volume snap restore` comme décrit ci-dessous. Si vous restaurez des données à l'aide de Flex Clone, de Single File Snap Restore ou d'autres méthodes, cela n'est pas nécessaire.

   Marquer l'attaque comme « faux positif » et « suspect clair » :
   `anti-ransomware volume attack clear-suspect -vserver` *`svm_name`* `-volume` *`vol_name`* `[`*`extension identifiers`*`] -false-positive true`
   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 fichier
   `[-start-time` *`date_time`* `-end-time` *`date_time`*`]` Heures de début et de fin pour la plage de fichiers à effacer, sous la forme "MM/JJ/AAAA HH:MM:SS".
2. Lister les copies Snapshot dans un volume :

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

L'exemple suivant montre les copies 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'une copie 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 copies Snapshot dans un volume :

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

L'exemple suivant montre les copies 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'une copie 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
```

3. Répétez les étapes 1 et 2 pour restaurer le volume à l'aide de la copie Snapshot souhaitée.

Plus d'informations

- "Base de connaissances : prévention des ransomwares et restauration dans ONTAP"

Modifiez les options des copies Snapshot automatiques

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 pouvez uniquement modifier les options ARP snapshots sur une SVM de nœud.

Étapes

1. Pour afficher tous les paramètres de copie snapshot ARP actuels, entrez :
`vserver options -vserver` *`svm_name`* `arw*`

Le `vserver options` commande est une commande masquée. Pour afficher la page man, entrez `man vserver options` Sur l'interface de ligne de commandes de ONTAP.

2. Pour afficher les paramètres de copie snapshot ARP actuels sélectionnés, entrez :
`vserver options -vserver svm_name -option-name arw_setting_name`
3. Pour modifier les paramètres de copie snapshot ARP, entrez :
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   Les paramètres suivants peuvent être modifiés :

Réglage ARW	Description
`arw.snap.max.count`	Spécifie le nombre maximal de copies snapshot ARP pouvant exister dans un volume à tout moment. Les anciennes copies sont supprimées pour garantir que le nombre total de copies snapshot ARP se situe dans cette limite spécifiée. Le `-option-value` le paramètre accepte des entiers compris entre 3 et 8, inclus. La valeur par défaut est 6.
`arw.snap.create.interval.hours`	Spécifie l'intervalle *en heures* entre les copies snapshot ARP. Une nouvelle copie ARP Snapshot est créée lorsqu'une attaque basée sur l'entropie des données est suspectée et que la dernière copie ARP Snapshot créée est antérieure à l'intervalle spécifié. Le `-option-value` le paramètre accepte des entiers compris entre 1 et 48, inclus. La valeur par défaut est 4.
`arw.snap.normal.retain.interval.hours`	Spécifie la durée *en heures* pendant laquelle une copie snapshot ARP est conservée. Lorsqu'une copie snapshot ARP atteint le seuil de rétention, toute autre copie snapshot ARP créée avant d'être supprimée. Il ne peut exister plus d'une copie snapshot ARP antérieure au seuil de rétention. Le `-option-value` le paramètre accepte des entiers compris entre 4 et 96, inclus. La valeur par défaut est 48.
`arw.snap.max.retain.interval.days`	Spécifie la durée maximale *en jours* pendant laquelle une copie snapshot ARP peut être conservée. Toute copie snapshot ARP antérieure à cette durée est supprimée lorsqu'aucune attaque n'est signalée sur le volume. L'intervalle de rétention maximal pour les copies snapshot ARP est ignoré si une menace modérée est détectée. La copie snapshot ARP créée en réponse à la menace est conservée jusqu'à ce que vous ayez répondu à la menace. Le marquage d'une menace comme faux positif entraîne la suppression des copies Snapshot ARP sur le volume. Le `-option-value` le paramètre accepte des entiers compris entre 1 et 365, inclus. La valeur par défaut est 5.

Réglage ARW	Description
`arw.snap.create.interval.hours.post.max.count`	Spécifie l'intervalle *en heures* entre les copies snapshot ARP lorsque le volume contient déjà le nombre maximal de copies snapshot ARP. Lorsque le nombre maximum est atteint, une copie snapshot ARP est supprimée pour faire place à une nouvelle copie. La nouvelle vitesse de création de copie Snapshot ARP peut être réduite pour conserver l'ancienne copie à l'aide de cette option. Si le volume contient déjà le nombre maximal de copies snapshot ARP, l'intervalle spécifié dans cette option est utilisé pour la création de la copie Snapshot ARP suivante, au lieu de `arw.snap.create.interval.hours`. Le `-option-value` le paramètre accepte des entiers compris entre 4 et 48, inclus. La valeur par défaut est 8.
`arw.surge.snap.interval.days`	Spécifie l'intervalle *en jours* entre les copies snapshot ARP créées en réponse aux pics d'E/S. ONTAP crée une copie snapshot ARP en cas de surcharge du trafic d'E/S et lorsque la dernière copie Snapshot ARP créée est antérieure à l'intervalle spécifié. Cette option spécifie également la période de rétention *in Day* pour les copies snapshot de surtension ARP. Le `-option-value` le paramètre accepte des entiers compris entre 1 et 365, inclus. La valeur par défaut est 5.
`arw.snap.new.extns.interval.hours`	Cette option spécifie l'intervalle *en heures* entre les copies snapshot ARP créées lorsqu'une nouvelle extension de fichier est détectée. Une nouvelle copie snapshot ARP est créée lorsque Une nouvelle extension de fichier est observée ; l'instantané précédent créé lors de l'observation d'une nouvelle extension de fichier est plus ancien que cet intervalle spécifié. Sur une charge de travail qui crée fréquemment de nouvelles extensions de fichiers, cet intervalle permet de contrôler la fréquence des copies Snapshot ARP. Cette option existe indépendamment de `arw.snap.create.interval.hours`, Qui spécifie l'intervalle pour les copies Snapshot ARP basées sur l'entropie des données. Le `-option-value` le paramètre accepte des entiers compris entre 24 et 8760. La valeur par défaut est 48.

Informations sur le copyright

Informations sur les marques commerciales