Protection par ransomware

ONTAP 9

NetApp
March 22, 2023

Table des matières

Protection par ransomware . . . 1
Présentation de la protection autonome contre les ransomwares . . . 1
Cas d’utilisation et considérations relatives à la protection autonome contre les ransomwares . . . 3
Activation de la protection autonome contre les ransomwares . . . 5
Activez la protection autonome par défaut contre les ransomwares dans les nouveaux volumes . . . 8
Mettez en pause la protection autonome contre les ransomwares pour exclure les événements des charges de travail de l’analyse . . . 9
Réagir à une activité anormale. . . . 9
Restaurez les données après une attaque par ransomware . . . 12
Modifiez les options des copies Snapshot automatiques . . . 16

Protection par ransomware

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.

La fonctionnalité ARP est activée avec les licences suivantes.

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 ARP par volume à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes 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 voulez pas compter sur une seule caractéristique, comme une ceinture de sécurité, pour vous protéger complètement dans un 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.

Alors que ONTAP inclut des fonctionnalités telles que FPolicy, les copies Snapshot, SnapLock et Active IQ Digital Advisor pour vous protéger contre les ransomwares, les informations suivantes se concentrent sur la fonctionnalité intégrée ONTAP ARP avec des fonctionnalités d'apprentissage machine.

Pour en savoir plus sur les autres fonctionnalités d'ONTAP anti-ransomware, consultez la page suivante : "Tr-4572 : solution NetApp pour ransomware"

Détection de ONTAP ARP

Il existe deux types d'attaques par ransomware :

1. Refus de service aux fichiers par cryptage de données. L'attaquant maintient l'accès à ces données à moins qu'une rançon ne soit payée.
2. Vol de données propriétaires sensibles. L'attaquant menace de publier ces données dans le domaine public à moins qu'une rançon ne soit payée.

La fonctionnalité ONTAP ARP traite le premier type avec un mécanisme de détection anti-ransomwares basé sur :

1. Identification des données entrantes comme cryptées ou en texte clair.
2. Les analyses, qui détectent
   - Données élevées *entropie* (évaluation du caractère aléatoire des données dans un fichier)
   - Augmentation de l'activité de volume anormale grâce au chiffrement des données
   - Extension non conforme au type d'extension normal

> Aucun système de détection ou de prévention par ransomware ne peut garantir la sécurité en cas d'attaque par ransomware. Même s'il est possible qu'une attaque ne soit pas détectée, NetApp ARP agit comme une couche de protection supplémentaire importante si le logiciel antivirus n'a pas détecté d'intrusion. 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.

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 par la suite, le volume peut être restauré vers cette copie Snapshot de façon proactive, afin de limiter au minimum la perte de données.

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.

Grâce à la connaissance des fichiers affectés et au moment de l'attaque, il est possible de restaurer de manière sélective les fichiers affectés à partir de différentes copies Snapshot, plutôt que de simplement restaurer l'ensemble du volume sur l'une des snapshots.

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

Prise en charge de la plateforme ONTAP :

- La fonctionnalité ARP (autonome ransomware protection) est disponible pour tous les systèmes ONTAP sur site, à partir de ONTAP 9.10.1.
- ARP n’est actuellement pas disponible pour ONTAP Select.
- ARP n’est actuellement pas disponible pour Amazon FSX ou les environnements Cloud Volumes ONTAP suivants :
  - AWS
  - Azure
  - Google Cloud

Charges de travail adaptées :

- 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, il y a plus de risques de faux positifs dans cette charge de travail.

- Images et vidéos

  Par exemple, les dossiers médicaux et les données EDA.

Depuis ONTAP 9.12.1, ARP est disponible pour les configurations suivantes :

- Volumes protégés par SnapMirror
- Les SVM sont protégés par SnapMirror
- SVM activé pour la migration (mobilité des données des SVM)

Charges de travail inappropriées :

- Workloads avec fréquence élevée de création ou de suppression de fichiers (des centaines de milliers de fichiers en quelques secondes, par exemple des charges de travail de test/développement)
- ARP dépend de la capacité à reconnaître une surtension inhabituelle dans l’activité de création ou de suppression de fichiers. Si l’application elle-même est la source de l’activité de fichier, elle ne peut pas être distinguée efficacement de l’activité ransomware
- Les charges de travail pour lesquelles l’application ou l’hôte crypte les données ARP dépendent de la distinction entre les données entrantes et cryptées. 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 (création, suppression et écrasement) et du type de fichier.

Configurations système non prises en charge :

- Environnements SAN
- Les environnements ONTAP S3

- VMDK sur NFS

Volume requis :

- Plein à moins de 100 %
- Le chemin de jonction doit être actif

Types de volume non pris en charge :

- Les volumes hors ligne
- Volumes restreints
- Volumes SnapLock
- Volumes FlexGroup
- Volumes FlexCache (la fonctionnalité anti-ransomwares est prise en charge sur les volumes FlexVol d'origine, mais pas sur les volumes en cache)
- Volumes SAN uniquement
- Volumes des machines virtuelles de stockage arrêtées
- Volumes root des VM de stockage

Interopérabilité SnapMirror et ARP

Depuis la version ONTAP 9.12.1, ARP est pris en charge sur les volumes de destination SnapMirror 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.

Considérations relatives aux performances ARP et à la fréquence

La fonctionnalité ARP peut avoir un impact minimal sur les performances du système, comme mesurée en débit et en IOPS de pointe. L'impact de la fonctionnalité anti-ransomwares est fortement tributaire des charges de travail des volumes. Pour les charges de travail standard ou 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.

Étant donné que l'analyse ARP est exécutée dans une séquence hiérarchisée, au fur et à mesure que le nombre de volumes protégés augmente, les analyses sont exécutées moins souvent sur chaque volume.

Fonctionnement des copies Snapshot automatiques en cas de détection d'un ransomware

Afin d'obtenir le meilleur point de récupération possible, ARP crée une copie Snapshot automatique dès qu'elle détecte une activité anormale du fichier. Cependant, ARP ne signale pas immédiatement une alerte, mais l'analytique doit s'exécuter et confirmer que l'activité suspecte correspond à un profil ransomware avant de générer une alerte. Ce processus peut prendre jusqu'à 60 minutes. Si l'analytique détermine que l'activité n'est pas suspecte, une alerte n'est pas générée, mais la copie Snapshot créée automatiquement reste présente dans le système de fichiers pendant au moins deux jours.

Depuis ONTAP 9.11.1, vous pouvez contrôler le nombre et la période de conservation des copies Snapshot ARP générées automatiquement en réponse aux attaques de ransomware suspectées. Découvrez comment "Modifiez les options des copies Snapshot automatiques".

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 passez ensuite en mode actif, dans lequel une activité anormale est signalée pour votre évaluation.

Ce dont vous avez besoin

- Une machine virtuelle de stockage activée pour NFS ou SMB (ou les deux).
- La licence correcte est installée pour votre version de ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.8-9.10.1	MT_EK_MGMT (gestion des clés mutualisée)
ONTAP 9.11.1 et versions ultérieures	Protection contre les ransomwares

- Charge de travail NAS avec les clients configurés
- Le volume à protéger doit avoir un Junction-path actif.
- Facultatif mais recommandé : le système EMS est configuré pour envoyer des notifications par e-mail, qui incluent des notifications d'activité ARP. Pour plus d'informations, voir "Configurez les événements EMS pour envoyer des notifications par e-mail".

Description de la tâche

La solution ARP NetApp inclut une période d'apprentissage initiale (également appelée « exécution sèche »), dans laquelle le système ONTAP apprend quelles extensions de fichier sont valides et utilise les données analysées pour développer des profils d'alerte. 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. En mode actif, si une extension de fichier est marquée comme anormale, mais que vous l'évaluez et que vous la marquez comme un faux positif, le profil d'alerte est affiné pour que l'extension ne soit pas marquée comme anormale dans les alertes futures.

Bien que vous puissiez passer du mode d'apprentissage au mode actif à tout moment, une période d'apprentissage de 30 jours est recommandée. Un changement précoce peut entraîner un trop grand nombre de faux positifs. Dans l'interface de ligne de commandes de ONTAP, vous pouvez utiliser `security anti-ransomware volume workload-behavior show` commande pour afficher les extensions de fichier détectées à ce jour. Il est recommandé de ne pas utiliser cet outil pour raccourcir la période d'apprentissage.

Vous pouvez activer ARP sur un volume existant ou créer un nouveau volume et activer ARP depuis le début.

> Dans les volumes existants, les modes d'apprentissage et actif s'appliquent uniquement aux données récemment écrites, et non aux données déjà 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.

Pour gérer cette fonctionnalité dans l'interface de ligne de commandes de ONTAP, vous pouvez utiliser `security anti-ransomware volume` commande. Vous pouvez également utiliser le `volume modify` commande avec `-anti-ransomware` paramètre.

Exemple 1. Étapes

System Manager

1. Cliquez sur **Storage > volumes**, puis sélectionnez le volume à protéger.
2. Dans l'onglet **Security** de la présentation **volumes**, cliquez sur **Status** pour passer de Désactivé à activé en mode d'apprentissage dans la zone **anti-ransomware**.
3. Lorsque la période d'apprentissage est terminée, passez ARP en mode actif.
   a. Cliquez sur **Storage > volumes**, puis sélectionnez le volume prêt pour le mode actif.
   b. Dans l'onglet **Security** de la vue d'ensemble **volumes**, cliquez sur **basculer** en mode actif dans la zone anti-ransomware.
4. Vous pouvez toujours vérifier l'état ARP du volume dans la case **anti-ransomware**. Pour afficher l'état ARP pour tous les volumes : dans le volet **volumes**, cliquez sur **Afficher/Masquer**, puis vérifiez que l'état **anti-ransomware** est coché.

CLI

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`*

   Vous pouvez également activer le ransomware avec le `volume modify` commande :

   `volume modify -volume` *`vol_name`* `-vserver` *`svm_name`* `-anti-ransomware-state dry-run`

   Sur l'interface de ligne de commandes, vous pouvez également créer un volume avec une protection anti-ransomwares 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`*

   > Vous devez toujours activer ARP au départ à l'état de fonctionnement à sec. En commençant par l'état actif, vous pouvez générer un nombre excessif de faux positifs.

2. Lorsque la période d'apprentissage est terminée, modifiez le volume protégé pour passer en mode actif :

   `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).

Ce dont vous aurez besoin

- La licence correcte est installée pour votre version de ONTAP.

Versions d'ONTAP	Licence
ONTAP 9.11.1 et versions ultérieures	Protection contre les ransomwares
ONTAP 9.8-9.10.1	MT_EK_MGMT (gestion des clés mutualisée)

Description de la tâche

Les nouveaux volumes sont créés par défaut avec ARP en mode désactivé, mais vous pouvez modifier ce paramètre dans System Manager et dans l'interface de ligne de commandes. Les volumes activés par défaut sont définis sur ARP en mode d'apprentissage.

L'activation de ARP par défaut pour les nouveaux volumes d'un SVM n'active pas automatiquement ARP pour les volumes existants de ce SVM. Découvrez comment "Activez ARP dans un volume existant".

Exemple 2. Étapes

System Manager

1. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage pour l'antivirus par défaut.
2. Dans l'onglet **Paramètres**, [dans la section **sécurité**], cliquez sur Dans la case **anti-ransomware**, cochez la case pour activer ARP pour les volumes NAS.

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]`

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.

Ce dont vous aurez besoin

- ARP s'exécute en mode apprentissage ou actif.

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 anti-ransomware pour interrompre l'analytique. 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.

Exemple 3. Étapes

System Manager

1. Cliquez sur **Storage > volumes**, puis sélectionnez le volume sur lequel vous souhaitez mettre ARP en pause.
2. Dans l'onglet sécurité de la vue d'ensemble des volumes, cliquez sur **Pause anti-ransomware** dans la zone **anti-ransomware**.

CLI

Suspendre ARP sur un volume :

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

Pour reprendre le traitement, utilisez `resume` paramètre.

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

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 attendue et acceptable, ou si une attaque est en cours.

Ce dont vous aurez besoin

- ARP s'exécute en mode actif.

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, vous pouvez répondre en marquant l'activité du fichier de l'une des deux façons suivantes :

- Faux positif

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

- Attaque par ransomware potentielle

  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 ; les journaux sont mis à jour avec les nouveaux types de fichiers et les utilisent pour une analyse future. Cependant, 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 de supprimer les avis. "En savoir plus sur la manière de procéder à une reprise après une attaque par ransomware".

Il n'y a aucun avertissement à effacer si vous avez restauré un volume entier.

Exemple 4. Étapes

System Manager

1. Lorsque vous recevez une notification “activité anormale”, cliquez sur le lien ou accédez à l’onglet **sécurité** de la présentation **volumes**.

   Les avertissements s’affichent dans le volet vue d’ensemble de la fenêtre événements.

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

   Dans l’onglet **sécurité**, cliquez sur Afficher **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	Cliquez sur **mettre à jour** et **Effacer les types de fichiers suspects** pour enregistrer votre décision et reprendre la surveillance normale contre les attaques par ransomware.
Attaques par ransomware potentielles	Répondez aux attaques et restaurez les données protégées. Cliquez ensuite sur **Update** et **Effacer les types de fichiers suspects** pour enregistrer votre décision et reprendre la surveillance ARP normale. + il n’y a pas de types de fichiers suspects 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 (ajout d'une nouvelle extension à la liste des personnes autorisées) et reprendre la surveillance normale anti-ransomware :
     `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 aux attaques et restaurez les données. Entrez ensuite 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.

Restaurez les données après une attaque par ransomware

Des copies Snapshot nommées « anti_ransomware_Backup » sont créées lorsque la protection autonome contre les ransomwares (ARP) détecte une attaque potentielle. Vous pouvez restaurer les données à partir de ces copies ARP ou d'autres copies Snapshot.

En cas d’attaque par ransomware, consultez l’article de la base de connaissances "Prévention et restauration des ransomwares dans ONTAP" pour plus d’informations sur la reprise et l’atténuation future.

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.

Ce dont vous aurez besoin

- ARP activé
- Rapports d’attaques par ransomware potentielles

Étapes

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

System Manager

1. Si vous souhaitez restaurer les données à partir de copies Snapshot antérieures, plutôt que à partir des copies ARP, vous devez procéder comme suit pour libérer le verrou anti-ransomware Snapshot. Si vous souhaitez effectuer une restauration à partir des copies ARP, il n'est pas nécessaire de libérer le verrou et vous pouvez ignorer cette étape.

Si une attaque système a été identifiée, procédez comme suit…	Si aucune attaque système n'a été identifiée, procédez comme suit…
a. Cliquez sur **Storage > volumes**. b. Sélectionnez **sécurité**, puis cliquez sur **Afficher les types de fichiers suspects** c. Marquez les fichiers comme « Faux positif » . d. Cliquez sur **mettre à jour** et **Effacer les types de fichiers suspects**	Pour libérer le verrouillage Snapshot, vous devez effectuer une restauration à partir des copies ARP avant d'effectuer une restauration à partir de copies Snapshot antérieures. Suivez les étapes 1 à 2-3 pour restaurer des données à partir des copies ARP, puis répétez le processus pour restaurer à partir de copies Snapshot antérieures.

2. Afficher les copies Snapshot dans des volumes :

   Cliquez sur **stockage > volumes**, sélectionnez le volume et cliquez sur **copies Snapshot**.

3. Cliquez sur ⋮ En regard de la copie Snapshot à restaurer, puis sélectionnez **Restaurer**.

CLI

1. Si vous souhaitez restaurer les données à partir de copies Snapshot antérieures, plutôt que à partir des copies ARP, vous devez procéder comme suit pour libérer le verrou anti-ransomware Snapshot. Si vous souhaitez effectuer une restauration à partir des copies ARP, il n'est pas nécessaire de libérer le verrou et vous pouvez ignorer cette étape.

```
It is only necessary to release the anti-ransomware Snaplock before
restoring from earlier Snapshot copies if you are using the `volume
snap restore`` command as outline below.  If you are restoring data
using Flex Clone, Single File Snap Restore or other methods, this is
not necessary.
```

Si une attaque système a été identifiée, procédez comme suit…	Si aucune attaque système n'a été identifiée, procédez comme suit…
Marquez l'attaque comme un « faux positif » et un « 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".	Pour libérer le verrouillage Snapshot, vous devez effectuer une restauration à partir des copies ARP avant d'effectuer une restauration à partir de copies Snapshot antérieures. Suivez les étapes 1 à 2-3 pour restaurer des données à partir des copies ARP, puis répétez le processus pour restaurer à partir de copies Snapshot antérieures.

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
```

Modifiez les options des copies Snapshot automatiques

Depuis ONTAP 9.11.1, vous pouvez utiliser l'interface de ligne de commandes pour contrôler le nombre et la période de conservation des copies Snapshot ARP (autonome ransomware protection) générées automatiquement en réponse aux attaques de ransomware suspectées.

Note: 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.

Les options suivantes pour les copies Snapshot automatiques peuvent être modifiées :

compte arw.snap.max
: 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.

arw.snap.create.interval.hours
: Spécifie l'intervalle (en heures) entre les copies snapshot ARP. Une nouvelle copie Snapshot est créée lorsqu'une attaque est suspectée et que la copie créée précédemment est plus ancienne que cet intervalle spécifié.

arw.snap.normal.retain.interval.hours
: Spécifie la durée (en heures) pendant laquelle une copie Snapshot ARP est conservée. Lorsqu'une copie snapshot ARP devient cet ancien, toute autre copie Snapshot ARP créée avant la dernière copie pour atteindre cet âge est supprimée. Aucune copie snapshot ARP ne peut être antérieure à cette durée.

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 sera supprimée si aucune attaque n'a été signalée sur le volume.

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 un nombre maximal de copies snapshot ARP, cet intervalle spécifié dans cette option est utilisé pour la création de la copie Snapshot ARP suivante, au lieu de arw.snap.create.interval.hours.

arw.surge.snap.interval.days
: Spécifie l'intervalle (en jours) entre les copies Snapshot de surtension ARP. Une nouvelle copie de surtension ARP Snapshot est créée en cas de forte augmentation du trafic d'E/S et si la dernière copie Snapshot ARP créée est plus ancienne que cet intervalle spécifié. Cette option indique également la durée (en jours) pendant laquelle une copie Snapshot de surtension ARP est conservée.

Procédure CLI

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

Pour afficher les paramètres de copie snapshot ARP actuels sélectionnés, entrez :
`vserver options -vserver svm_name -option-name arw_setting_name`

Pour modifier les paramètres de copie snapshot ARP, entrez :
`vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

Informations sur le copyright

Informations sur les marques commerciales