Protégez-vous contre les attaques par ransomware

ASA r2

NetApp
February 11, 2026

Sommaire

Protégez-vous contre les attaques par ransomware

Créez des instantanés inviolables pour vous protéger contre les attaques de ransomware sur les systèmes de stockage ASA r2

Pour une protection renforcée contre les attaques par ransomware, répliquez les snapshots sur un cluster distant, puis verrouillez les snapshots de destination pour les protéger contre toute tentative d'altération. Les snapshots verrouillés ne peuvent pas être supprimés accidentellement ou de manière malveillante. Vous pouvez utiliser des snapshots verrouillés pour restaurer des données si une unité de stockage n'est jamais compromise par une attaque par ransomware.

Initialiser l'horloge SnapLock Compliance

Avant de pouvoir créer des instantanés inviolables, vous devez initialiser l'horloge SnapLock Compliance sur vos clusters locaux et de destination.

Étapes

1. Sélectionnez **Cluster > Présentation**.
2. Dans la section **nœuds**, sélectionnez **initialiser horloge SnapLock Compliance**.
3. Sélectionnez **initialiser**.
4. Vérifiez que l'horloge de conformité est initialisée.
   a. Sélectionnez **Cluster > Présentation**.
   b. Dans la section **nœuds**, sélectionnez ; puis **SnapLock Compliance horloge**.

Et la suite ?

Après avoir initialisé l'horloge SnapLock Compliance sur vos clusters locaux et de destination, vous êtes prêt à "créer une relation de réplication avec des snapshots verrouillés".

Activez la protection autonome contre les ransomwares avec l'IA sur vos systèmes de stockage ASA r2

À partir d' ONTAP 9.17.1, vous pouvez utiliser la protection autonome contre les ransomwares avec intelligence artificielle (ARP/AI) pour protéger les données de votre système ASA r2. ARP/AI détecte rapidement les menaces potentielles de ransomware, crée automatiquement un instantané ARP pour protéger vos données et affiche un message d'avertissement dans le Gestionnaire système pour vous avertir de toute activité suspecte.

ARP améliore la cyber-résilience en adoptant un modèle d'apprentissage automatique pour l'analyse anti-ransomware qui détecte les formes de ransomware en constante évolution avec une précision de 98 % dans les environnements SAN. Le modèle d'apprentissage automatique d'ARP est pré-entraîné sur un vaste

ensemble de fichiers, à la fois avant et après une attaque par ransomware simulée. Cet entraînement gourmand en ressources est effectué en dehors d'ONTAP, et le modèle pré-entraîné résultant de cet entraînement est inclus sur la boîte avec ONTAP. Ce modèle n'est pas accessible ni modifiable. ARP/AI est actif immédiatement après l'activation ; il n'y a pas "période d'apprentissage".

> Aucun système de détection ou de prévention des ransomwares ne peut complètement garantir la sécurité contre une attaque de ransomware. Bien qu'une attaque puisse passer inaperçue, ARP/AI agit comme une couche de défense supplémentaire importante si le logiciel antivirus ne parvient pas à détecter une intrusion.

Description de la tâche

- Le support ARP/AI est inclus avec le "Licence ONTAP One" .
- ARP/AI n'est pas pris en charge sur les unités de stockage protégées par SnapMirror active sync, SnapMirror synchrone ou SnapLock.
- À partir de ONTAP 9.18.1, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage créées 12 heures après la mise à niveau vers ONTAP 9.18.1 ou l'initialisation d'un nouveau cluster ONTAP 9.18.1 ASA r2.
- Après avoir activé ARP/AI, vous devez "activer les mises à jour automatiques de vos fichiers de sécurité" pour recevoir automatiquement les nouvelles mises à jour de sécurité.

Activez ARP/AI sur toutes les unités de stockage du cluster

Si vous utilisez ONTAP 9.17.1, vous pouvez activer ARP/AI sur toutes les unités de stockage créées dans le cluster par défaut.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. À côté de **Anti-ransomware**, sélectionnez ⋮ puis sélectionnez **Activer sur toutes les unités de stockage existantes**.
3. Sélectionnez **Activer**.

Activez ARP/AI sur toutes les unités de stockage d'une machine virtuelle de stockage.

Si vous utilisez ONTAP 9.17.1, vous pouvez activer ARP/AI par défaut sur toutes les unités de stockage créées dans une storage virtual machine (VM). Cela signifie que toute nouvelle unité de stockage créée dans la storage VM aura ARP/AI activé automatiquement. Vous pouvez également appliquer ARP/AI aux unités de stockage existantes dans la storage VM.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans le Gestionnaire système, sélectionnez **Cluster > Machines virtuelles de stockage**.
2. Sélectionnez la machine virtuelle de stockage sur laquelle vous souhaitez activer ARP/AI.

3. Dans la section **Sécurité**, à côté de **Anti-ransomware**, sélectionnez ⋮ ; puis sélectionnez **Modifier les paramètres anti-ransomware**.
4. Sélectionnez **Activer l'anti-ransomware**.

   Cela active ARP/AI sur toutes les futures unités de stockage créées sur la machine virtuelle de stockage sélectionnée par défaut.

5. Pour appliquer ARP aux unités de stockage existantes sur la machine virtuelle de stockage sélectionnée, sélectionnez **Appliquer cette modification à toutes les unités de stockage existantes applicables sur cette machine virtuelle de stockage**.
6. Sélectionnez **Enregistrer**.

Résultat

Toutes les nouvelles unités de stockage que vous créez sur la machine virtuelle de stockage sont protégées par défaut contre les attaques de ransomware, et toute activité suspecte vous est signalée dans le Gestionnaire système.

Activer ARP/AI sur des unités de stockage spécifiques dans une machine virtuelle de stockage

Si vous utilisez ONTAP 9.17.1 et que vous ne souhaitez pas activer ARP/AI sur toutes les unités de stockage dans une storage VM, vous pouvez sélectionner les unités spécifiques que vous souhaitez activer.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez activer ARP/AI.
3. Sélectionner ⋮ ; puis sélectionnez **Activer l'anti-ransomware**.
4. Sélectionnez **Activer**.

Résultat

Les unités de stockage que vous avez sélectionnées sont protégées contre les attaques de ransomware et toute activité suspecte vous est signalée dans le Gestionnaire système.

Désactivez la protection autonome par défaut contre les ransomwares sur vos systèmes de stockage ASA r2

Lorsque vous initialisez un nouveau cluster ONTAP 9.18.1 ASA r2 ou que vous mettez à niveau votre cluster vers ONTAP 9.18.1, ARP/AI est automatiquement activé par défaut sur toutes les nouvelles unités de stockage après un délai de grâce de 12 heures. Si vous ne désactivez pas ARP/AI pendant le délai de grâce, il est activé pour l'ensemble du cluster pour les nouvelles unités de stockage à la fin du délai de grâce.

Les unités de stockage créées dans ONTAP 9.17.1 doivent être "activé manuellement" pour ARP/AI.

Étapes

Vous pouvez désactiver l'activation par défaut pendant ou après le délai de grâce initial de 12 heures.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Désactiver ARP:
   - Pour désactiver pendant le délai de grâce de 12 heures :
     i. Sous **Anti-ransomware**, sélectionnez **Ne pas activer** puis sélectionnez **Désactiver**.
   - Pour désactiver après le délai de grâce de 12 heures :
     i. Sous **Anti-ransomware**, sélectionnez puis désélectionnez **Enable for new storage units**.
     ii. Sélectionnez **Save**

CLI

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

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

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

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modifier les périodes de conservation des snapshots ARP/AI sur les systèmes de stockage ASA r2

Si la protection autonome contre les ransomwares avec intelligence artificielle (ARP/IA) détecte une activité anormale sur une ou plusieurs unités de stockage de votre système ASA r2, elle crée automatiquement un snapshot ARP pour protéger les données de l'unité. En fonction de votre capacité de stockage et des besoins de votre entreprise en matière de données, vous pouvez augmenter ou réduire la période de conservation par défaut du snapshot ARP. Par exemple, vous pouvez augmenter la période de conservation des applications critiques afin de bénéficier, si nécessaire, de périodes de conservation plus longues pour la récupération des données, ou réduire celle des applications non critiques pour économiser de l'espace de stockage.

La période de conservation par défaut de l'instantané ARP varie en fonction de l'action que vous entreprenez en réponse à l'activité anormale.

Si vous effectuez cette action…	Les instantanés ARP sont conservés par défaut pendant…
Marquer comme faux positif	12 heures

Si vous effectuez cette action…	Les instantanés ARP sont conservés par défaut pendant…
Marquer comme attaque potentielle par ransomware	7 jours
Ne prenez pas de mesures immédiates	10 jours

Les périodes de conservation par défaut peuvent être modifiées à l'aide de l'interface de ligne de commande (CLI) ONTAP . Voir "Modifier les options pour les instantanés automatiques ONTAP" pour connaître les étapes à suivre pour modifier la période de conservation par défaut.

Répondez à la protection autonome contre les ransomwares avec des alertes IA sur les systèmes de stockage ASA r2

Si la protection autonome contre les ransomwares avec intelligence artificielle (ARP/IA) détecte une activité anormale sur une ou plusieurs unités de stockage de votre système ASA r2, un avertissement s'affiche sur le tableau de bord du Gestionnaire système. Consultez l'avertissement, vérifiez l'activité et, si nécessaire, prenez les mesures nécessaires pour contrer toute menace potentielle pesant sur vos données.

Si un message d'avertissement ARP/AI s'affiche, avant d'agir, utilisez le vérificateur d'intégrité des applications approprié pour vérifier l'intégrité des données sur l'unité de stockage. Vérifier l'intégrité des données de l'unité de stockage vous permet de déterminer si l'activité est acceptable ou s'il s'agit d'une attaque potentielle par rançongiciel.

Si l'activité anormale est…	Alors fais ceci…
Acceptable	Marquer l'activité comme un faux positif.
Une attaque potentielle de ransomware	Marquez l'activité comme une attaque potentielle de ransomware.
Indéterminé	N'agissez pas immédiatement. Surveillez l'unité de stockage pendant 7 jours maximum. Si l'unité de stockage continue de fonctionner normalement, signalez l'activité comme un faux positif. Si l'unité de stockage continue de présenter une activité anormale, signalez-la comme une attaque potentielle par rançongiciel.

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.

   Si ARP a détecté une activité anormale sur une ou plusieurs unités de stockage, un message apparaît sous **Avertissements**.

2. Sélectionnez le message d'avertissement.
3. Sous **Aperçu des événements**, sélectionnez le message **Avertissements** qui indique le nombre d'unités de stockage présentant une activité anormale.
4. Sous **Unités de stockage avec activité anormale**, sélectionnez l'unité de stockage.

5. Sélectionnez **Sécurité**.

   S'il y a une activité anormale sur l'unité de stockage, un message s'affiche sous **Anti-ransomware**.

6. Sélectionnez **Choisir une action**.
7. Sélectionnez **Marquer comme faux positif** ou sélectionnez **Marquer comme attaque potentielle par ransomware**.

Et la suite ?

Si vous constatez des pics d'activité dans votre unité de stockage, qu'il s'agisse de pics ponctuels ou d'une augmentation caractéristique d'une nouvelle norme, vous devez les signaler comme étant sans danger. Le signalement manuel de ces pics comme étant sans danger contribue à améliorer la précision des évaluations des menaces d'ARP. Découvrez comment "signaler les pics connus d'ARP/IA".

Suspendez ou reprenez la protection autonome contre les ransomwares avec l'IA sur vos systèmes de stockage ASA r2

À partir d' ONTAP 9.17.1, vous pouvez utiliser la protection autonome contre les ransomwares avec intelligence artificielle (ARP/AI) pour protéger les données de votre système ASA r2. Si vous prévoyez un événement de charge de travail inhabituel, vous pouvez suspendre temporairement l'analyse ARP/AI afin d'éviter les détections de faux positifs d'attaques de ransomware. Une fois l'événement de charge de travail terminé, vous pouvez reprendre l'analyse ARP/AI.

Mettre en pause ARP/AI

Avant de commencer un événement de charge de travail inhabituel, vous devrez peut-être suspendre temporairement l'analyse ARP/AI pour éviter les détections faussement positives d'attaques de ransomware.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez suspendre ARP/AI.
3. Sélectionnez **Pause anti-ransomware**.

Résultat

L'analyse ARP/AI est suspendue pour les unités de stockage sélectionnées et aucune activité suspecte ne vous est signalée dans le Gestionnaire système jusqu'à ce que vous repreniez ARP/AI.

Reprendre ARP/AI

Si vous suspendez ARP/AI pendant une charge de travail inhabituelle, une fois votre charge de travail terminée, vous devez la reprendre pour protéger vos données contre les attaques de ransomware.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez reprendre ARP/AI.
3. Sélectionnez **Reprendre l'anti-ransomware**.

Résultat

L’analyse des attaques potentielles de ransomware reprend et les activités suspectes vous sont signalées dans le Gestionnaire système.

Informations sur le copyright

Informations sur les marques commerciales