Utiliser la résilience aux ransomwares

NetApp Ransomware Resilience

NetApp
February 27, 2026

Sommaire

Utiliser la résilience aux ransomwares

Accéder à la NetApp Ransomware Resilience

Pour accéder à NetApp Ransomware Resilience, vous devez vous connecter via la NetApp Console.

Pour vous connecter à la console, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion au cloud NetApp à l'aide de votre e-mail et d'un mot de passe. "En savoir plus sur la connexion" .

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

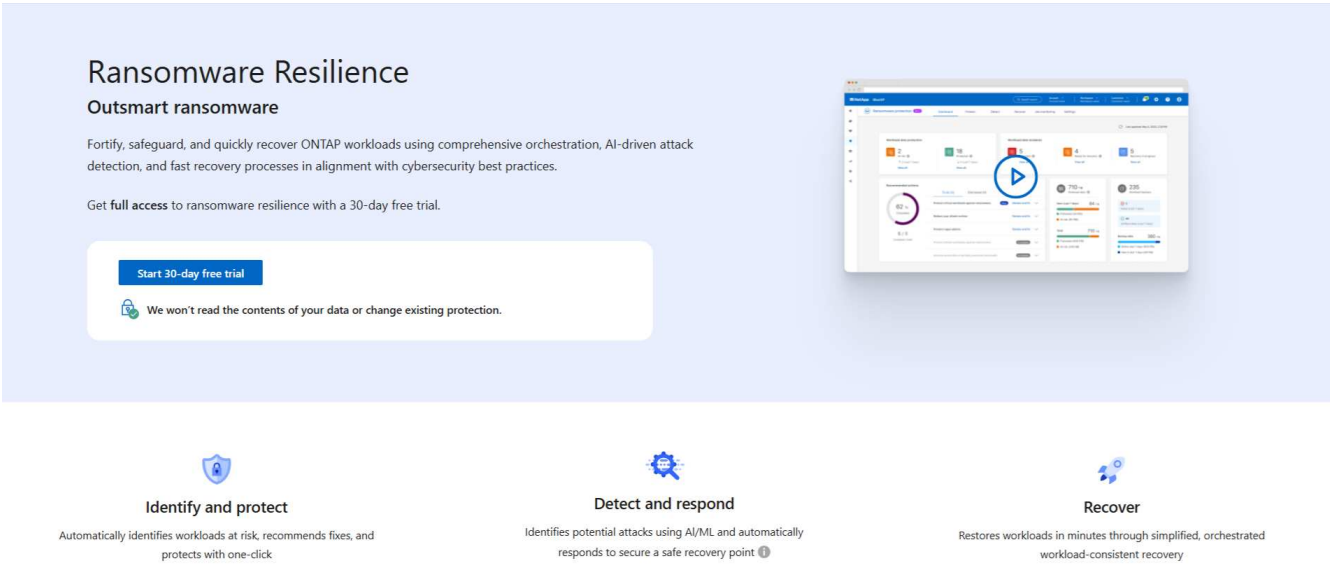
1. Ouvrez un navigateur Web et accédez à"la console" .

   La page de connexion à la console apparaît.

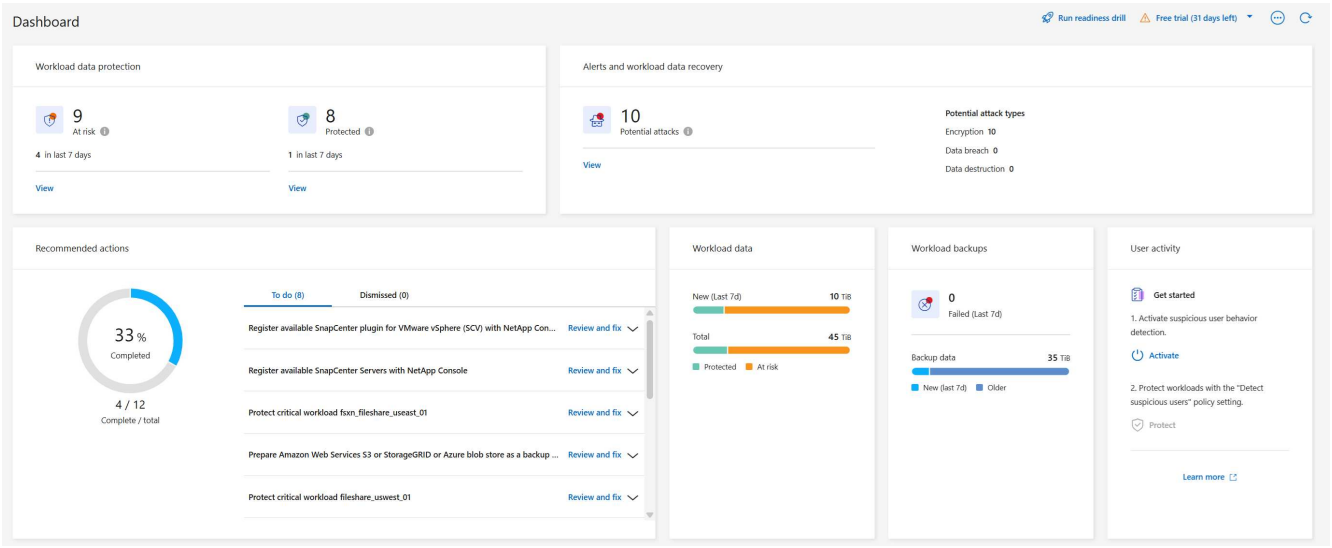
2. Connectez-vous à la console.
3. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.

   Si c'est la première fois que vous vous connectez à ce service, la page de destination apparaît.

   Si vous n'avez pas d'agent de console ou si ce n'est pas celui pour ce service, vous devez en déployer un. "Apprenez à configurer un agent de console" .



Sinon, le tableau de bord de résilience aux ransomwares apparaît.



4. Si vous ne l'avez pas déjà fait, sélectionnez l'option **Découvrir les charges de travail**.

   "Découvrir les charges de travail" .

Surveillez l'état de la charge de travail dans NetApp Ransomware Resilience

Le tableau de bord NetApp Ransomware Resilience offre un aperçu rapide de l'état de protection de vos charges de travail. Vous pouvez rapidement déterminer les charges de travail à risque ou protégées, identifier celles impactées par un incident ou en cours de récupération, et évaluer l'étendue de la protection en regardant la quantité de stockage protégée ou à risque.

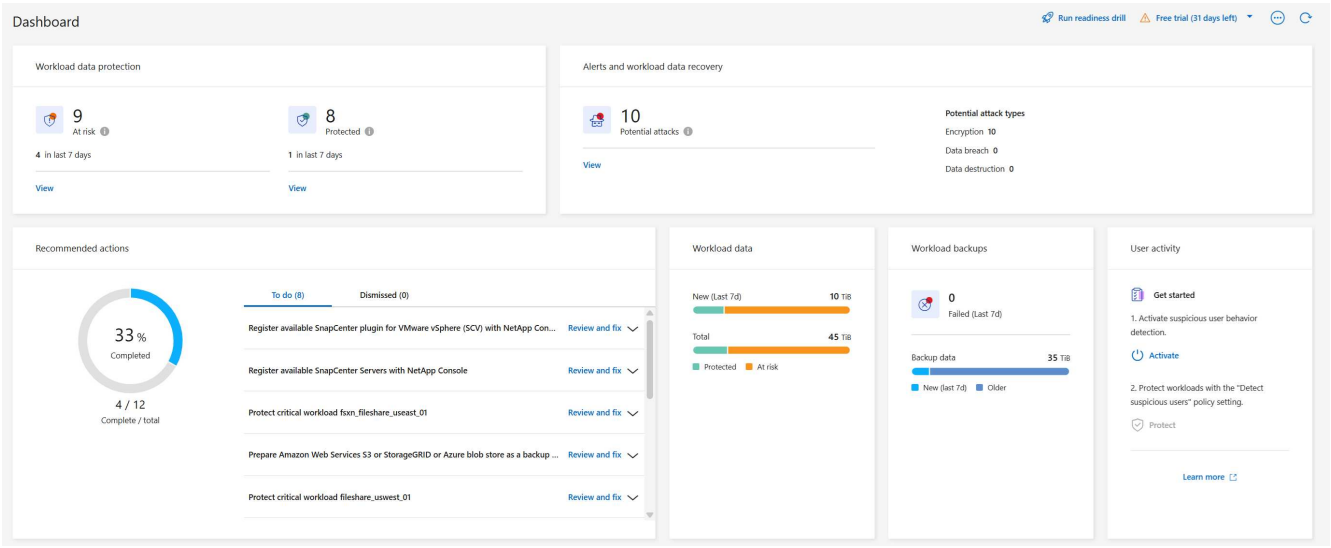
Utilisez le tableau de bord pour consulter les suggestions de protection, modifier les paramètres et télécharger des rapports.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Examinez l'état de santé de la charge de travail à l'aide du tableau de bord

Étapes

1. Une fois que la console a détecté vos charges de travail, le tableau de bord Ransomware Resilience affiche l'état de protection des données de la charge de travail.



2. Depuis le tableau de bord, vous pouvez effectuer les actions suivantes dans chacun des volets :

   - **Protection des données de charge de travail** : sélectionnez **Afficher tout** pour voir toutes les charges de travail à risque ou protégées sur la page Protection. Les charges de travail sont menacées lorsque les niveaux de protection ne correspondent pas à une politique de protection. "Protéger les charges de travail" .

     Sélectionnez l'info-bulle « i » pour voir des conseils sur ces données. Pour augmenter la limite de charge de travail, sélectionnez **Augmenter la limite de charge de travail** dans cette note. En sélectionnant cette option, vous accédez à la page d'assistance de la console où vous pouvez créer un ticket de cas.

   - **Alertes et récupération des données de charge de travail** : sélectionnez **Afficher tout** pour voir les incidents actifs qui ont eu un impact sur votre charge de travail, qui sont prêts à être récupérés une fois les incidents neutralisés ou qui sont en cours de récupération. "Répondre à une alerte détectée" .
     - Un incident est classé dans l'un des états suivants :
       - Nouveau
       - Rejeté
       - Rejeter
       - Résolu
     - Une alerte peut avoir l'un des statuts suivants :
       - Nouveau
       - Inactif
     - Une charge de travail peut avoir l'un des états de restauration suivants :
       - Restauration nécessaire
       - En cours
       - Restauré
       - Échec
   - **Actions recommandées** : Pour augmenter la protection, examinez chaque recommandation, puis sélectionnez **Examiner et corriger**.

Voir "Consultez les suggestions de protection sur le tableau de bord" ou "Protéger les charges de travail".

Ransomware Resilience affiche de nouvelles recommandations depuis votre dernière visite sur le tableau de bord avec l'étiquette « Nouveau » pendant 24 heures. Les actions apparaissent par ordre de priorité, la plus importante en haut. Examinez, agissez ou ignorez chaque recommandation.

Le nombre total d'actions n'inclut pas les actions que vous avez rejetées.

- **Données de charge de travail** : Surveillez les changements dans la couverture de protection au cours des 7 derniers jours.
- **Sauvegardes de charge de travail** : surveillez les modifications dans les sauvegardes de charge de travail créées par Ransomware Resilience qui ont échoué ou se sont terminées avec succès au cours des 7 derniers jours.

Consultez les recommandations de protection sur le tableau de bord

Ransomware Resilience évalue la protection de vos charges de travail et recommande des actions pour améliorer cette protection.

Vous pouvez consulter une recommandation et agir en conséquence, ce qui modifie le statut de la recommandation sur Terminé. Ou, si vous souhaitez agir plus tard, vous pouvez le rejeter. Le rejet d'une action déplace la recommandation vers une liste d'actions rejetées, que vous pouvez consulter ultérieurement.

Voici un échantillon des recommandations proposées par Ransomware Resilience.

Recommandation	Description	Comment résoudre
Ajoutez une politique de protection contre les ransomwares.	La charge de travail n'est actuellement pas protégée.	Affecter une politique à la charge de travail. "Protégez les charges de travail contre les attaques de ransomware" .
Connectez-vous au SIEM pour signaler les menaces.	Envoyez des données à un système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces.	Saisissez les informations du serveur SIEM/XDR pour activer la détection des menaces. Consultez "Se connecter à un SIEM".
Améliorer la posture de sécurité du système	NetApp Digital Advisor a identifié au moins un risque de sécurité élevé ou critique.	Passez en revue tous les risques de sécurité dans NetApp Digital Advisor. Se référer à "Documentation du Digital Advisor" .
Renforcer une politique.	Certaines charges de travail peuvent ne pas bénéficier d'une protection suffisante. Renforcez la protection des charges de travail avec une politique.	Augmentez la rétention, ajoutez des sauvegardes, appliquez des sauvegardes immuables, bloquez les extensions de fichiers suspectes, activez la détection sur le stockage secondaire et bien plus encore. "Protégez les charges de travail contre les attaques de ransomware" .

Recommandation	Description	Comment résoudre
Préparez <fournisseur de sauvegarde> comme destination de sauvegarde pour sauvegarder vos données de charge de travail.	La charge de travail n'a actuellement aucune destination de sauvegarde.	Ajoutez des destinations de sauvegarde à cette charge de travail pour la protéger. Consultez "Ajouter une destination de sauvegarde".
Protégez les charges de travail des applications critiques ou très importantes contre les ransomwares.	La page Protéger affiche les charges de travail d'application critiques ou très importantes (en fonction du niveau de priorité attribué) qui ne sont pas protégées.	Attribuez une politique à ces charges de travail. "Protégez les charges de travail contre les attaques de ransomware" .
Protégez les charges de travail de partage de fichiers critiques ou très importantes contre les ransomwares.	La page Protection affiche les charges de travail critiques ou très importantes du type Partage de fichiers ou Banque de données qui ne sont pas protégées.	Attribuez une stratégie à chaque charge de travail. Voir "Protégez les charges de travail contre les attaques de ransomware". Voir "Protégez les charges de travail contre les attaques de ransomware". Voir "Protégez les charges de travail contre les attaques de ransomware".
Consultez les nouvelles alertes.	De nouvelles alertes existent.	Consultez les nouvelles alertes. "Répondre à une alerte de ransomware détectée" .

Étapes

1. Dans le volet Actions recommandées de Ransomware Resilience, sélectionnez une recommandation, puis **Vérifier et corriger**.
2. Pour annuler l'action jusqu'à plus tard, sélectionnez **Annuler**.

   La recommandation disparaît de la liste des tâches à effectuer et apparaît dans la liste des tâches rejetées.

   Vous pouvez ultérieurement transformer un élément rejeté en élément à faire. Lorsque vous marquez un élément comme terminé ou que vous transformez un élément abandonné en action À faire, le nombre total d'actions augmente de 1.

3. Pour consulter les informations sur la manière d'agir sur la base des recommandations, sélectionnez l'icône **information**.

Exporter les données de protection vers des fichiers CSV

Vous pouvez exporter des données et télécharger des fichiers CSV qui affichent les détails de la protection, des alertes et de la récupération.

Vous pouvez télécharger des fichiers CSV à partir de l'une des options du menu principal :

- **Protection** : contient l'état et les détails de toutes les charges de travail, y compris le nombre total de charges de travail que Ransomware Resilience marque comme protégées ou à risque.
- **Alertes** : inclut l'état et les détails de toutes les alertes, y compris le nombre total d'alertes et d'instantanés automatisés.

- **Récupération** : inclut l'état et les détails de toutes les charges de travail qui doivent être restaurées, y compris le nombre total de charges de travail que Ransomware Resilience marque comme « Restauration nécessaire », « En cours », « Échec de la restauration » et « Restaurée avec succès ».

Le téléchargement d'un fichier CSV à partir d'une page inclut uniquement les données de cette page.

Les fichiers CSV incluent des données pour toutes les charges de travail sur tous les systèmes de console.

Étapes

1. Depuis le tableau de bord de résilience aux ransomwares, sélectionnez **Actualiser** L'option située en haut à droite permet d'actualiser les données qui apparaîtront dans les fichiers.
2. Effectuez l'une des opérations suivantes :
   - Sur la page, sélectionnez **Télécharger** option.
   - Dans le menu Résilience aux ransomwares, sélectionnez **Rapports**.
3. Si vous avez sélectionné l'option **Rapports**, sélectionnez l'un des fichiers nommés préconfigurés, puis sélectionnez **Télécharger (CSV)** ou **Télécharger (JSON)**.

Accéder à la documentation technique

Vous pouvez accéder à la documentation technique de Ransomware Resilience à partir de"docs.netapp.com" ou depuis Ransomware Resilience.

Étapes

1. Depuis le tableau de bord de résilience aux ransomwares, sélectionnez la verticale *Actions* option.
2. Sélectionnez l'une de ces options :
   - **Quoi de neuf** pour afficher les informations sur les fonctionnalités des versions actuelles ou précédentes dans les notes de version.
   - **Documentation** pour afficher la page d'accueil de la documentation sur la résilience aux ransomwares et cette documentation.

Protéger et détecter

Vérifier l'état de la protection dans NetApp Ransomware Resilience

NetApp Ransomware Resilience Le tableau de bord de protection offre une vue d'ensemble de l'état de protection et de la préparation de vos charges de travail. Utilisez le tableau de bord de protection pour obtenir des informations sur ce qui est protégé, ce qui nécessite une protection et quelle est la portée de la protection.

Une fois que vous aurez compris l'étendue de votre protection actuelle, "Vous pouvez créer et appliquer des stratégies de protection contre les ransomwares à vos charges de travail".

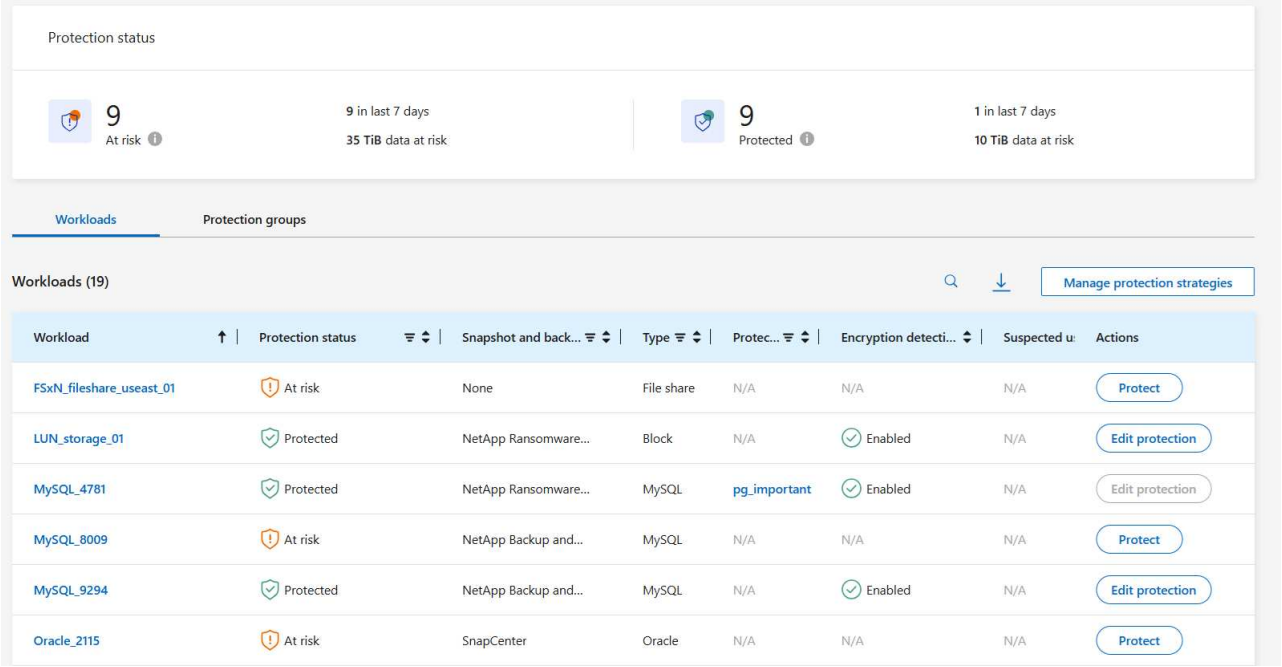
Afficher la protection sur une charge de travail

L'une des premières étapes de la protection des charges de travail consiste à afficher vos charges de travail actuelles et leur état de protection. Vous pouvez voir les types de charges de travail suivants :

- Charges de travail des applications
- Bloquer les charges de travail
- Charges de travail de partage de fichiers
- Charges de travail des machines virtuelles

Étapes

1. Dans le menu de navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.
2. Effectuez l'une des opérations suivantes :
   - Dans le volet Protection des données du tableau de bord, sélectionnez **Afficher tout**.
   - Dans le menu, sélectionnez **Protection**.



3. À partir de cette page, vous pouvez afficher et modifier les détails de protection de la charge de travail.

> Consultez "Ajouter une stratégie de protection contre les ransomwares" pour en savoir plus sur l'utilisation de Ransomware Resilience lorsqu'il existe déjà une politique de protection avec Backup and Recovery.

Comprendre le tableau de bord de protection

Le tableau de bord de protection dans Ransomware Resilience affiche des informations détaillées sur les charges de travail (par exemple, nom et type de charge de travail, agent Console, système et machine virtuelle de stockage) en plus des indications sur l'état de la protection. Utilisez le tableau de bord de protection pour examiner et gérer la préparation des charges de travail face aux ransomwares. Les colonnes suivantes sont particulièrement utiles pour comprendre votre posture de protection :

État de protection : une charge de travail peut afficher l'un des états de protection suivants pour indiquer si une politique est appliquée ou non :

- **Protégé** : Une politique est appliquée. ARP (ou ARP/AI selon la version ONTAP) est activé sur tous les volumes liés à la charge de travail.
- **À risque** : Aucune politique n'est appliquée. Si une charge de travail n'a pas de stratégie de détection principale activée, elle est « à risque » même si une stratégie de capture instantanée et de sauvegarde est activée.
- **En cours** : Une politique est en cours d'application mais pas encore finalisée.
- **Échec** : Une politique est appliquée mais ne fonctionne pas.

État de la détection:

+ Ransomware Resilience fournit des informations sur l'étendue des politiques de détection des ransomwares que vous avez configurées sur vos charges de travail. Consultez l'étendue de la détection à l'aide des champs suivants.

- **État de détection du chiffrement**
- **Statut de détection du comportement suspect de l'utilisateur**
- **Bloquer les extensions de fichiers suspectes**

Stratégies de capture instantanée, de réplication et de sauvegarde : Cette colonne indique le produit ou le service qui gère la stratégie. S'il n'y a pas de stratégie, le champ affiche N/A.

Importance

Ransomware Resilience attribue une importance ou une priorité à chaque charge de travail lors de la découverte en fonction d'une analyse de chaque charge de travail. L'importance de la charge de travail est déterminée par les fréquences d'instantanés suivantes :

- **Critique** : Plusieurs copies instantanées sont effectuées par heure (plan de protection très agressif)
- **Important** : Les copies instantanées sont créées moins fréquemment qu'une fois par heure, mais plus fréquemment qu'une fois par jour.
- **Standard** : Des copies instantanées sont prises plus d'une fois par jour.

Exposition de la vie privée : Sélectionnez cette option pour "analyser les informations personnellement identifiables avec NetApp Data Classification".

Destination de réplication : Si vous avez configuré la réplication par instantané, les noms des machines virtuelles de stockage de destination et des systèmes sont affichés. S'il n'y a pas de réplication, ce champ affiche "N/A".

Destination de sauvegarde : Si vous avez configuré une stratégie de protection contre les ransomwares avec des sauvegardes, le nom du système de destination de sauvegarde est indiqué ici.

Prochaines étapes

- "Protégez les charges de travail avec des stratégies de protection contre les ransomwares"
- "Gérer les groupes de protection"
- "Rechercher des données personnelles identifiables"

Ajouter une destination de sauvegarde dans NetApp Ransomware Resilience

Lorsque NetApp Ransomware Resilience découvre des charges de travail, si des sauvegardes sont configurées, Ransomware Resilience reconnaît les destinations de sauvegarde. Si vous prévoyez d'utiliser des sauvegardes comme partie de votre "stratégie de protection contre les ransomwares" mais que vous n'avez pas configuré de destinations de sauvegarde sur la charge de travail, vous devez ajouter une destination de sauvegarde dans NetApp Ransomware Resilience pour améliorer la cyber-résilience.

Vous pouvez choisir l'une des destinations de sauvegarde suivantes :

- NetApp StorageGRID
- Amazon Web Services (AWS)
- Plateforme Google Cloud
- Microsoft Azure

> Les destinations de sauvegarde ne sont pas disponibles pour les charges de travail dans Amazon FSx for NetApp ONTAP et Azure NetApp Files. Effectuez des opérations de sauvegarde à l'aide des solutions de sauvegarde natives : FSx for ONTAP backup service ou Azure NetApp Files backups.

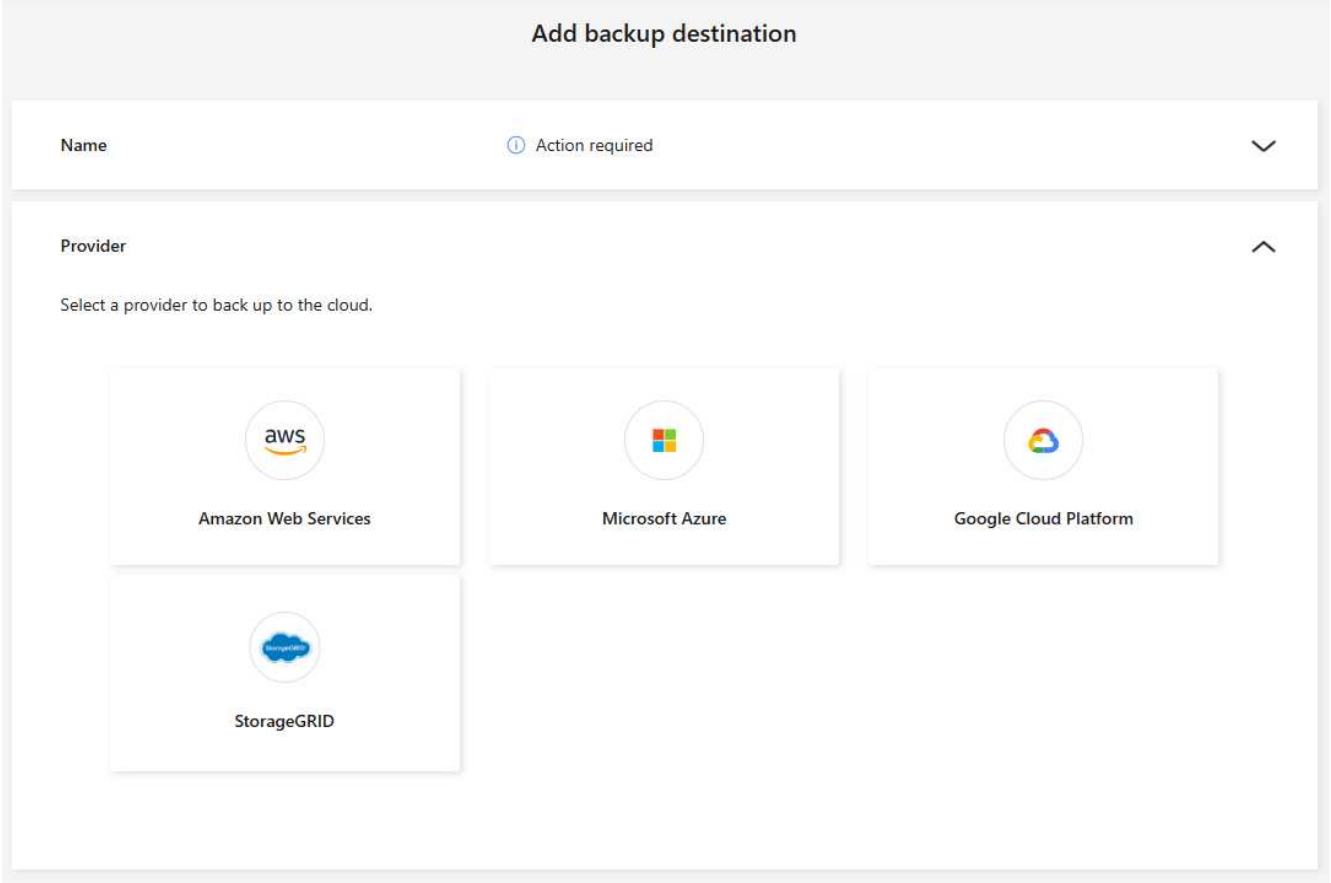
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Ajouter StorageGRID comme destination de sauvegarde

Pour configurer NetApp StorageGRID comme destination de sauvegarde, saisissez les informations suivantes.

Étapes

1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans la tuile **Backup Destinations**, sélectionnez **View**.
3. Sélectionnez **Ajouter**.
4. Entrez un nom pour la destination de sauvegarde.

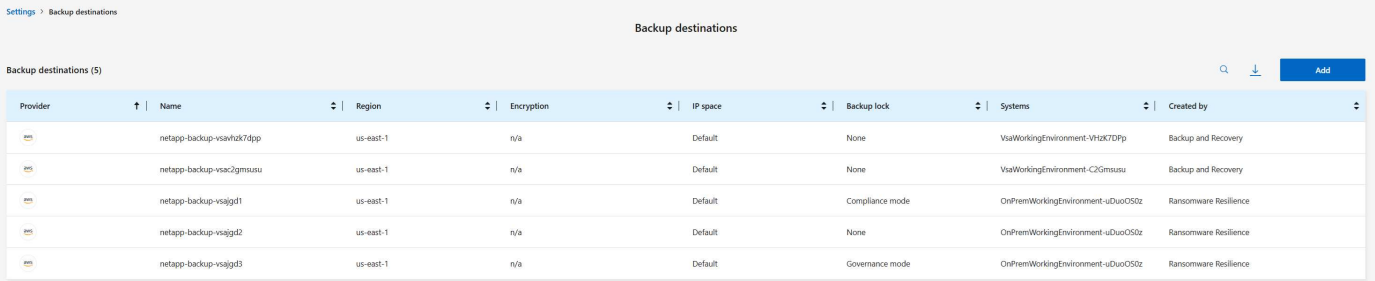


5. Sélectionnez * StorageGRID*.
6. Sélectionnez la flèche vers le bas à côté de chaque paramètre pour consulter les champs obligatoires :
   - **Paramètres du fournisseur**:
     - Choisissez de **créer un nouveau bucket** ou **d'apporter votre propre bucket**.
     - Fournissez le **domaine complet (FQDN) du nœud de passerelle** et le **port**.
     - Fournissez les informations d'identification StorageGRID : **Clé d'accès** et **Clé secrète**.
   - **Réseau** : Choisissez l'espace IP.
     - L'espace IP est le cluster dans lequel résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
   - **Verrouillage de sauvegarde**

     Choisissez si vous souhaitez configurer le verrouillage des sauvegardes. Avec le verrouillage des sauvegardes, les copies sont protégées contre toute modification ou suppression et analysées pour détecter les menaces de type ransomware. Vous ne pouvez pas modifier ce paramètre après avoir configuré la destination de sauvegarde. **Si vous ne souhaitez pas de verrouillage des sauvegardes, sélectionnez** None**.** Sélectionnez **Governance mode** pour permettre aux utilisateurs disposant d'autorisations spécifiques d'écraser ou de supprimer les fichiers de sauvegarde protégés pendant la période de conservation. **Sélectionnez** Compliance mode** pour empêcher les utilisateurs d'écraser ou de supprimer les fichiers de sauvegarde protégés pendant la période de conservation.
7. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.



Ajouter Amazon Web Services comme destination de sauvegarde

Pour configurer AWS comme destination de sauvegarde, saisissez les informations suivantes.

Pour plus d'informations sur la gestion de votre stockage AWS dans la console, consultez "Gérez vos buckets Amazon S3".

Étapes

1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans la tuile **Backup Destinations**, sélectionnez **View**.
3. Sélectionnez **Ajouter**.
4. Sélectionnez **Amazon Web Services**.
5. Sélectionnez la flèche vers le bas à côté de chaque paramètre et saisissez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur**:
     - Créez un nouveau bucket, sélectionnez un bucket existant s'il en existe déjà un dans la console ou apportez votre propre bucket qui stockera les sauvegardes.
     - Compte AWS, région, clé d'accès et clé secrète pour les informations d'identification AWS

       "Si vous souhaitez apporter votre propre seau, reportez-vous à Ajouter des seaux S3" .
   - **Cryptage** : si vous créez un nouveau compartiment S3, saisissez les informations de clé de cryptage fournies par le fournisseur. Si vous avez choisi un bucket existant, les informations de chiffrement sont déjà disponibles.

     Les données du bucket sont chiffrées par défaut avec des clés gérées par AWS. Vous pouvez continuer à utiliser les clés gérées par AWS ou gérer le chiffrement de vos données à l'aide de vos propres clés.
   - **Réseau** : Choisissez l'espace IP et indiquez si vous utiliserez un point de terminaison privé.
     - L'espace IP est le cluster dans lequel résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
     - Vous pouvez également choisir si vous utiliserez un point de terminaison privé AWS (PrivateLink) que vous avez précédemment configuré.

       Si vous souhaitez utiliser AWS PrivateLink, reportez-vous à "AWS PrivateLink pour Amazon S3" .
   - **Verrouillage de sauvegarde** : choisissez si vous souhaitez que Ransomware Resilience protège les sauvegardes contre toute modification ou suppression. Cette option utilise la technologie NetApp DataLock. Chaque sauvegarde sera verrouillée pendant la période de conservation, ou pendant un minimum de 30 jours, plus une période tampon pouvant aller jusqu'à 14 jours.

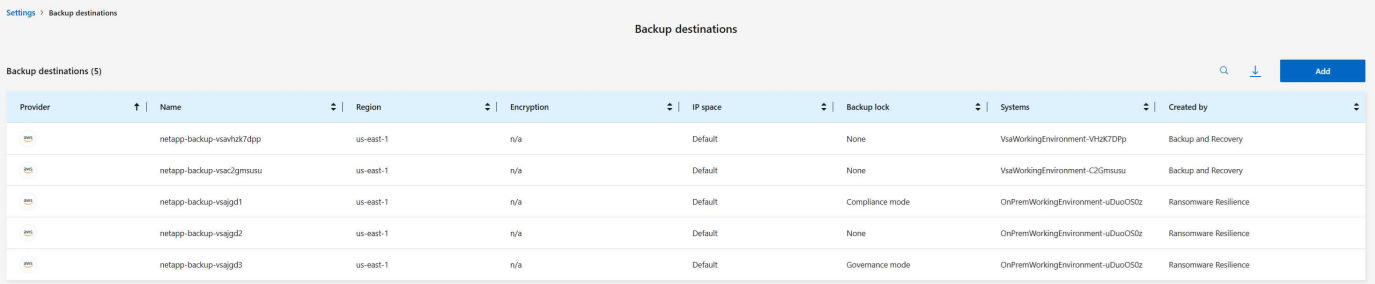
Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pourrez pas modifier ce paramètre après la configuration de la destination de sauvegarde.

- **Mode de gouvernance** : des utilisateurs spécifiques (avec l'autorisation s3:BypassGovernanceRetention) peuvent écraser ou supprimer des fichiers protégés pendant la période de conservation.
- **Mode de conformité** : les utilisateurs ne peuvent pas écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation.

6. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.



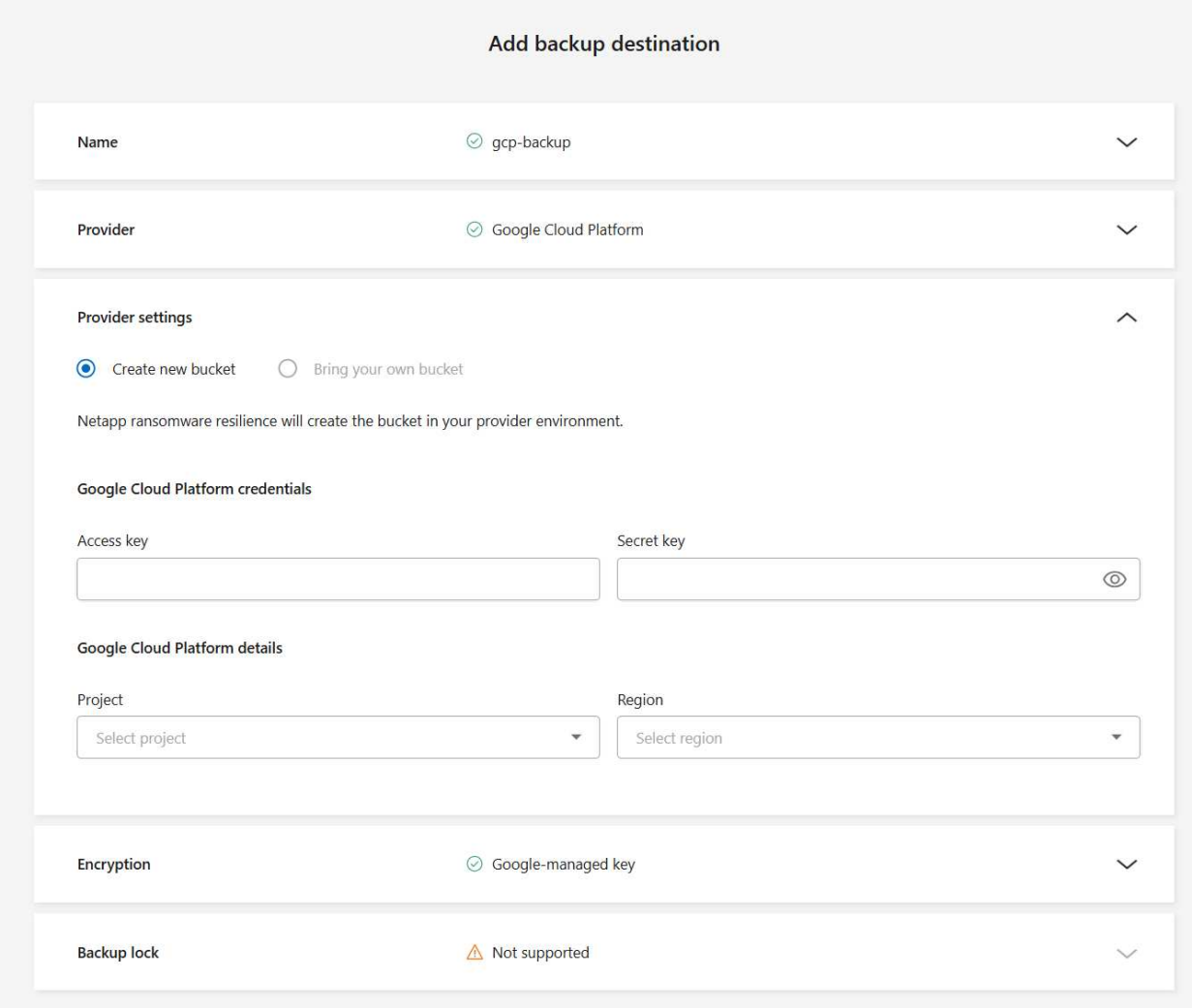
Ajouter Google Cloud Platform comme destination de sauvegarde

Pour configurer Google Cloud Platform (GCP) comme destination de sauvegarde, saisissez les informations suivantes.

Pour plus d'informations sur la gestion de votre stockage GCP dans la console, consultez "Options d'installation de l'agent de console dans Google Cloud".

Étapes

1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans la tuile **Backup Destinations**, sélectionnez **View**.
3. Sélectionnez **Ajouter**.
4. Entrez un nom pour la destination de sauvegarde.
5. Sélectionnez **Google Cloud Platform**.
6. Sélectionnez la flèche vers le bas à côté de chaque paramètre et saisissez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur**:
     - Choisissez de **créer un nouveau bucket** ou **d'apporter votre propre bucket**.
     - Fournissez les identifiants Google Cloud Platform : **Clé d'accès** et **Clé secrète**.
     - Sélectionnez votre **Project** et la **Region** dans laquelle il se trouve.



- **Cryptage** : Si vous créez un nouveau bucket, saisissez les informations de clé de cryptage fournies par le fournisseur. Si vous avez choisi un bucket existant, les informations de chiffrement sont déjà disponibles.

  Les données du bucket sont chiffrées par défaut avec des clés gérées par Google. Vous pouvez conserver ce paramètre par défaut en sélectionnant **Google-managed keys** ou utiliser **Customer-managed keys**.

7. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.

Ajouter Microsoft Azure comme destination de sauvegarde

Pour configurer Azure comme destination de sauvegarde, saisissez les informations suivantes.

Pour plus de détails sur la gestion de vos informations d'identification Azure et de vos abonnements à la place de marché dans la console, reportez-vous à "Gérez vos informations d'identification Azure et vos abonnements à la place de marché" .

Étapes

1. Dans Ransomware Resilience, sélectionnez **Paramètres**.

2. Dans la tuile **Backup Destinations**, sélectionnez **View**.
3. Sélectionnez **Ajouter**.
4. Sélectionnez **Azure**.
5. Sélectionnez la flèche vers le bas à côté de chaque paramètre et saisissez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur**:
     - Créez un nouveau compte de stockage, sélectionnez-en un existant s'il en existe déjà un dans la console ou apportez votre propre compte de stockage qui stockera les sauvegardes.
     - Indiquez l'ID de l'application (client), le secret client et l'ID du répertoire (tenant). Sélectionnez **Authenticate**.
     - Sélectionnez l'abonnement Azure, la région et le groupe de ressources de votre abonnement Azure.

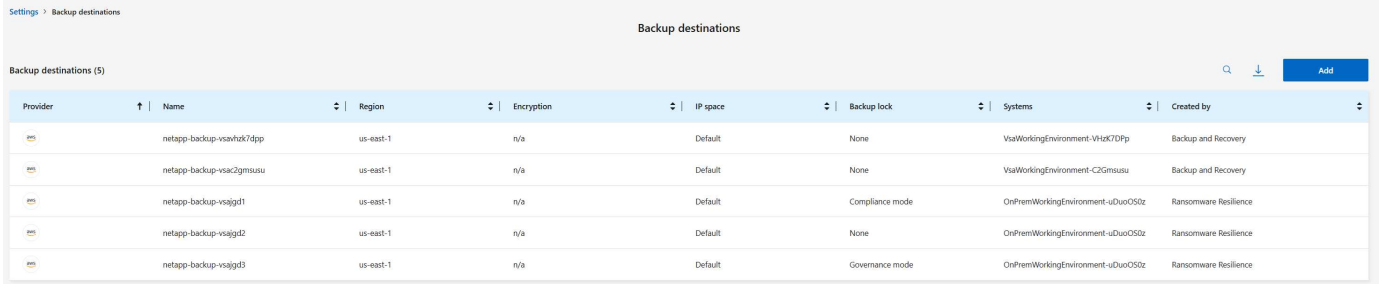
       "Si vous souhaitez utiliser votre propre compte de stockage, reportez-vous à la section Ajouter des comptes de stockage Azure Blob." .
   - **Chiffrement** : Par défaut, les données sont chiffrées à l'aide d'une clé gérée par Microsoft. Sélectionnez **Clé gérée par Microsoft** pour conserver cette option ; sinon, choisissez **Clé gérée par le client** pour utiliser vos propres clés pour le chiffrement.
   - **Réseau** : Choisissez l'espace IP et indiquez si vous utiliserez un point de terminaison privé.
     - L'espace IP est le cluster dans lequel résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
     - Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré.

       Si vous souhaitez utiliser Azure PrivateLink, reportez-vous à "Azure PrivateLink" .
   - **Verrouillage de sauvegarde**

     Choisissez si vous souhaitez configurer le verrouillage des sauvegardes. Avec le verrouillage des sauvegardes, les copies sont protégées contre toute modification ou suppression et analysées pour détecter les menaces de type ransomware. Vous ne pouvez pas modifier ce paramètre après avoir configuré la destination de sauvegarde. **Si vous ne souhaitez pas de verrouillage des sauvegardes, sélectionnez** None**.** Sélectionnez **Governance mode** pour permettre aux utilisateurs disposant d'autorisations spécifiques d'écraser ou de supprimer les fichiers de sauvegarde protégés pendant la période de conservation. **Sélectionnez** Compliance mode** pour empêcher les utilisateurs d'écraser ou de supprimer les fichiers de sauvegarde protégés pendant la période de conservation.
6. Sélectionnez **Ajouter**.

Résultat

La nouvelle destination de sauvegarde est ajoutée à la liste des destinations de sauvegarde.



Protégez les charges de travail avec les stratégies de protection NetApp Ransomware Resilience

Les stratégies de protection contre les ransomwares sont un élément clé de NetApp Ransomware Resilience : elles permettent la détection, la protection et la réplication. Les stratégies de protection sont un élément essentiel de votre posture de cybersécurité.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Comprendre les stratégies de protection contre les ransomwares

Les stratégies de protection contre les ransomwares englobent *détection*, *protection* et *réplication*.

- **Les politiques de détection** permettent d'identifier les menaces de type ransomware.
- **Les politiques de protection** incluent les politiques de capture instantanée et de sauvegarde. Les politiques de détection et de capture instantanée sont nécessaires dans une stratégie de protection. Les politiques de sauvegarde sont facultatives.

  Si vous utilisez d'autres produits NetApp pour protéger votre charge de travail, Ransomware Resilience les découvre et offre la possibilité de :

  - utiliser une politique de détection de ransomware et continuer à utiliser les politiques de snapshot et de sauvegarde créées par d'autres outils NetApp , ou
  - utilisez Ransomware Resilience pour gérer la détection, les instantanés et les sauvegardes.
- Les **stratégies de réplication** vous permettent de répliquer les instantanés de Ransomware Resilience vers un site secondaire. Les calendriers de réplication peuvent être définis sur des fréquences horaires, quotidiennes, hebdomadaires ou mensuelles.

  Actuellement, vous ne pouvez répliquer les instantanés que vers un stockage ONTAP local.

Si vous configurez des stratégies de protection pour Amazon FSxN pour ONTAP et Azure NetApp Files, consultez "les limitations de chaque service".

Pour une gestion et une protection améliorées de votre patrimoine de données, vous pouvez créer "groupes de charges de travail" pour protéger collectivement les volumes sous une seule stratégie.

Politiques de protection avec d'autres services gérés par NetApp

Au-delà de la résilience aux ransomwares, vous pouvez utiliser NetApp Backup and Recovery pour gérer la protection des partages de fichiers et des partages de fichiers de machines virtuelles.

Les informations de protection des services de Backup & Recovery apparaissent dans Ransomware Resilience. Vous pouvez ajouter des stratégies de détection à ces services avec Ransomware Resilience. L'ajout d'une stratégie de protection avec Ransomware Resilience remplace les stratégies de protection existantes.

Ransomware Resilience détecte également les politiques de protection de SnapCenter pour VMware pour les banques de données de machines virtuelles et de SnapCenter pour Oracle. Vous ne pouvez pas utiliser ces

services pour effectuer une restauration avec Ransomware Resilience.

Si une politique de détection de ransomware est gérée par Autonomous Ransomware Protection (ARP ou ARP/AI, selon la version ONTAP) et FPolicy dans ONTAP, ces charges de travail sont protégées et continueront d'être gérées par ARP et FPolicy.

> Les destinations de sauvegarde ne sont pas disponibles pour les charges de travail dans Amazon FSx for NetApp ONTAP ou Azure NetApp Files. Effectuez les opérations de sauvegarde à l'aide du service de sauvegarde FSx for ONTAP. Vous définissez les stratégies de sauvegarde pour les charges de travail dans FSx for ONTAP dans AWS, et non dans Ransomware Resilience. Les stratégies de sauvegarde apparaissent dans Ransomware Resilience et restent inchangées par rapport à AWS.

Politiques de protection pour les charges de travail non protégées par les applications NetApp

Si votre charge de travail n'est pas gérée par Backup and Recovery ou Ransomware Resilience, elle peut avoir des instantanés pris dans le cadre d'ONTAP ou d'autres produits. Si la protection FPolicy d'ONTAP est en place, vous pouvez modifier la protection FPolicy à l'aide d'ONTAP.

Politiques de détection prédéfinies

Vous pouvez choisir l'une des politiques prédéfinies de résilience aux ransomwares suivantes, qui sont alignées sur l'importance de la charge de travail.

> La stratégie **Extension utilisateur de chiffrement** est la seule stratégie prédéfinie qui prend en charge la détection des comportements suspects des utilisateurs.

+ La **stratégie de réplication critique** est la seule stratégie prédéfinie qui prend en charge la réplication des instantanés vers ONTAP.

Niveau politique	Instantané	Fréquence	Rétention (jours)	Nombre de copies d'instantané	Nombre maximal de copies d'instantané
Politique de charge de travail critique	Quart d'heure	Toutes les 15 minutes	3	288	309
	Tous les jours	Tous les 1 jour	14	14	309
	Hebdomadaire	Toutes les 1 semaine	35	5	309
	Mensuel	Tous les 30 jours	60	2	309
Politique importante relative à la charge de travail	Quart d'heure	Toutes les 30 minutes	3	144	165
	Tous les jours	Tous les 1 jour	14	14	165
	Hebdomadaire	Toutes les 1 semaine	35	5	165
	Mensuel	Tous les 30 jours	60	2	165

Niveau politique	Instantané	Fréquence	Rétention (jours)	Nombre de copies d'instantané	Nombre maximal de copies d'instantané
Politique de charge de travail standard	Quart d'heure	Toutes les 30 minutes	3	72	93
	Tous les jours	Tous les 1 jour	14	14	93
	Hebdomadaire	Toutes les 1 semaine	35	5	93
	Mensuel	Tous les 30 jours	60	2	93
Extension utilisateur de chiffrement	Quart d'heure	Toutes les 30 minutes	3	72	93
	Tous les jours	Tous les 1 jour	14	14	93
	Hebdomadaire	Toutes les 1 semaine	35	5	93
	Mensuel	Tous les 30 jours	60	2	93
Politique de réplication critique	Quart d'heure	Toutes les 15 minutes	3	288	309
	Tous les jours	Tous les 1 jour	14	14	309
	Hebdomadaire	Toutes les 1 semaine	35	5	309
	Mensuel	Tous les 30 jours	60	2	309

Ajouter une stratégie de protection contre les ransomwares

Il existe trois approches pour ajouter une stratégie de protection contre les ransomwares :

- **Créez une stratégie de protection contre les ransomwares si vous n'avez pas de politiques de snapshot ou de sauvegarde.**

  La stratégie de protection contre les ransomwares comprend :

  - Politique d'instantané
  - Politique de détection des ransomwares
  - Politique de sauvegarde
- **Remplacez les politiques d'instantané ou de sauvegarde existantes de la protection Backup and Recovery par des stratégies de protection gérées par Ransomware Resilience.**

  La stratégie de protection contre les ransomwares comprend :

  - Politique d'instantané

- Politique de détection des ransomwares
- Politique de sauvegarde

- **Créez une politique de détection pour les charges de travail avec des politiques de snapshot et de sauvegarde existantes gérées dans d'autres produits ou services NetApp .**

  La politique de détection ne modifie pas les politiques gérées dans d'autres produits.

  La politique de détection active la protection autonome contre les ransomwares et la protection FPolicy si elles sont déjà activées dans d'autres services. En savoir plus sur"Protection autonome contre les ransomwares" ,"Sauvegarde et récupération" , et"Politique ONTAP" .

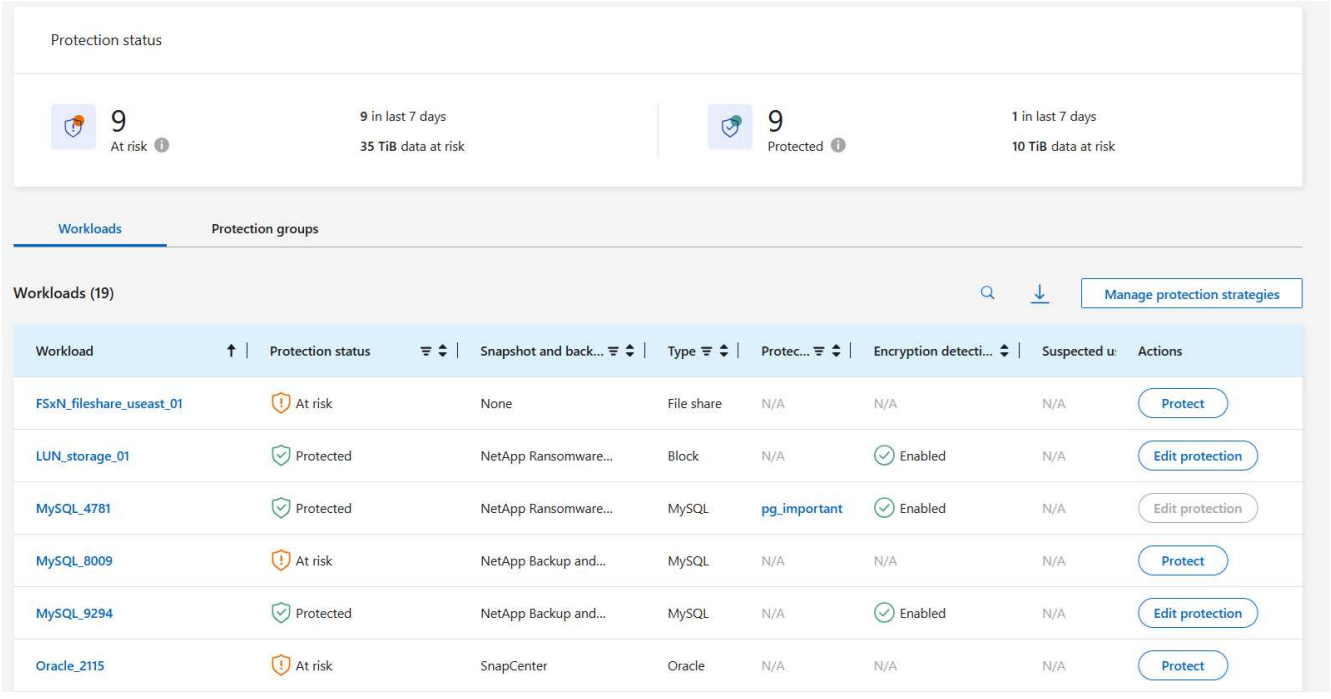
Créer une stratégie de protection contre les ransomwares (si vous n'avez pas de politiques de capture instantanée ou de sauvegarde)

Si les stratégies de capture instantanée ou de sauvegarde n'existent pas sur la charge de travail, vous pouvez créer une stratégie de protection contre les ransomwares, qui peut inclure les stratégies suivantes que vous créez dans Ransomware Resilience :

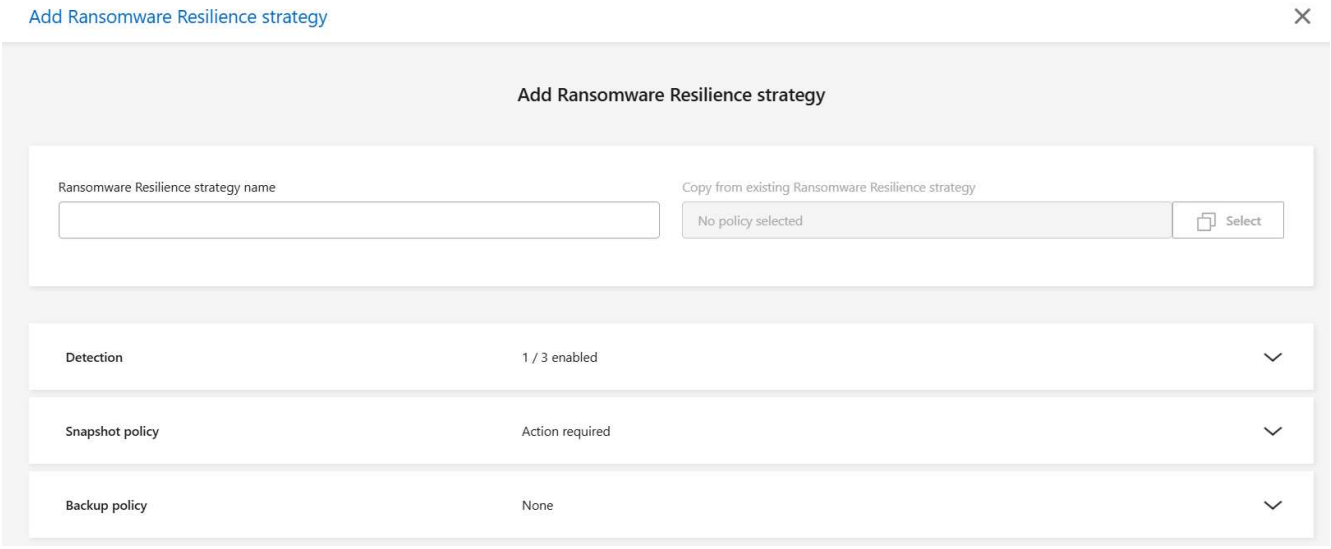
- Politique d'instantané
- Politique de sauvegarde
- Politique de détection des ransomwares
- Réplication secondaire vers ONTAP

Étapes pour créer une stratégie de protection contre les ransomwares

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.



2. Depuis la page Protection, sélectionnez une charge de travail, puis **Protéger**.
3. Depuis la page Stratégies de protection contre les ransomwares, sélectionnez **Ajouter**.



4. Saisissez un nouveau nom de stratégie ou saisissez un nom existant pour le copier. Si vous entrez un nom existant, choisissez celui que vous souhaitez copier et sélectionnez **Copier**.

> Si vous choisissez de copier et de modifier une stratégie existante, Ransomware Resilience ajoute « _copy » au nom d'origine. Vous devez modifier le nom et au moins un paramètre pour le rendre unique.

5. Pour chaque élément, sélectionnez la **flèche vers le bas**.

   - **Politique de détection**:
     - **Politique** : Choisissez l'une des politiques de détection prédéfinies.
     - **Détection primaire** : Activez la résilience aux ransomwares pour détecter les attaques potentielles de ransomware.
     - **Détection de comportement utilisateur suspect** : activez la détection du comportement utilisateur pour transmettre les événements d'activité utilisateur à Ransomware Resilience et détecter les événements suspects, tels que les violations de données.
     - **Bloquer les extensions de fichiers** : Activez la résistance aux ransomwares pour bloquer les extensions de fichiers suspectes connues. Ransomware Resilience effectue des copies instantanées automatisées lorsque la détection principale est activée.

       Si vous souhaitez modifier les extensions de fichiers bloquées, modifiez-les dans le Gestionnaire système.

   - **Politique d'instantané**:
     - **Nom de base de la politique d'instantané** : sélectionnez une politique ou sélectionnez **Créer** et saisissez un nom pour la politique d'instantané.
     - **Verrouillage des instantanés** : activez cette option pour verrouiller les copies d'instantanés sur le stockage principal afin qu'elles ne puissent pas être modifiées ou supprimées pendant une certaine période, même si une attaque de ransomware parvient à atteindre la destination de stockage de sauvegarde. Ceci est également appelé *stockage immuable*. Cela permet un temps de restauration plus rapide.

       Lorsqu'un instantané est verrouillé, le délai d'expiration du volume est défini sur le délai d'expiration de la copie de l'instantané.

Le verrouillage de copie d'instantané est disponible avec ONTAP 9.12.1 et versions ultérieures. Pour en savoir plus sur SnapLock, reportez-vous à "SnapLock dans ONTAP" .

- **Planifications d'instantanés** : Choisissez les options de planification, le nombre de copies d'instantanés à conserver et sélectionnez pour activer la planification.
  - **Politique de réplication** :
- **Nom de base de la stratégie de réplication** : Saisissez un nouveau nom ou choisissez-en un existant. Le nom de base est le préfixe ajouté à tous les instantanés.
- **Planifications de réplication** : Activez les fréquences que vous souhaitez (horaire, quotidienne, hebdomadaire ou mensuelle) et définissez la valeur de rétention (le nombre d'instantanés répliqués à conserver) pour chaque planification activée.
  - **Politique de sauvegarde**:
- **Nom de base de la politique de sauvegarde** : saisissez un nouveau nom ou choisissez un nom existant.
- **Planifications de sauvegarde** : Choisissez les options de planification pour le stockage secondaire et activez la planification.

Pour activer le verrouillage des sauvegardes sur le stockage secondaire, configurez vos destinations de sauvegarde à l'aide de l'option **Paramètres**. Pour plus de détails, consultez "Configurer les paramètres".

6. Sélectionnez **Ajouter**.

Ajoutez une stratégie de détection aux charges de travail disposant de stratégies de capture instantanée et de sauvegarde existantes gérées par Backup and Recovery

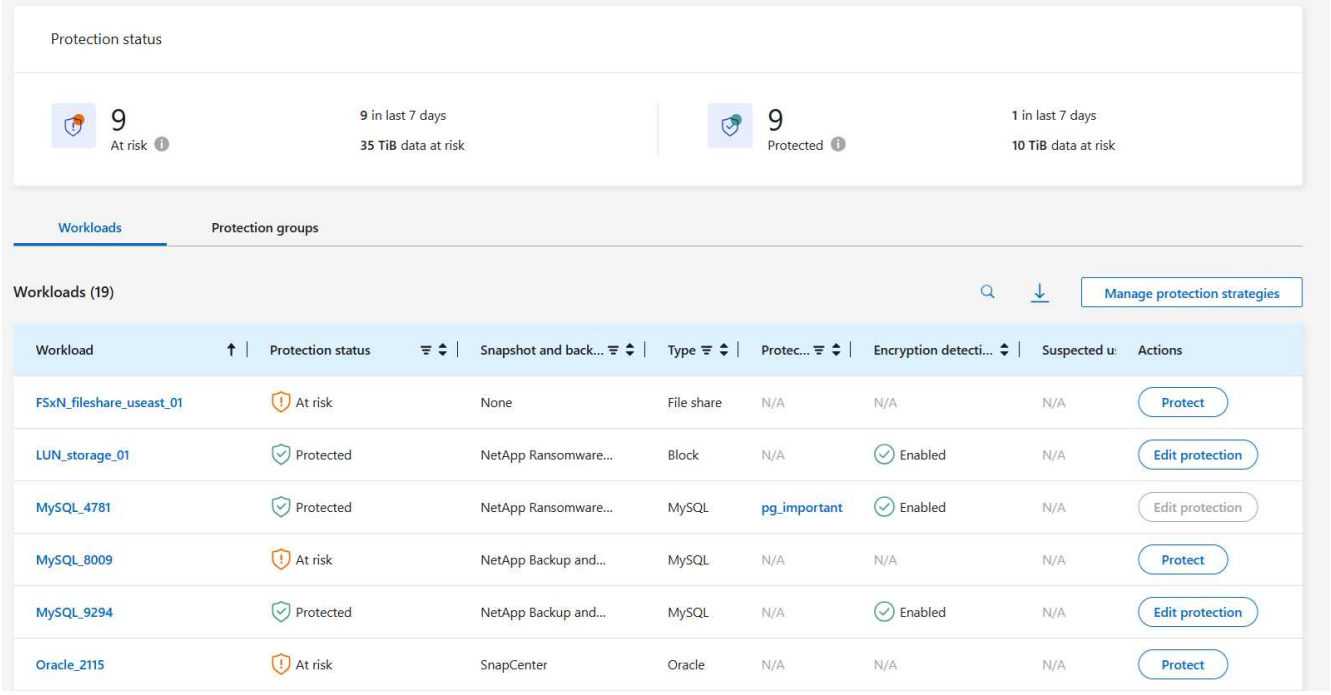
Ransomware Resilience vous permet d'attribuer une stratégie de détection ou une stratégie de protection aux charges de travail bénéficiant déjà d'une protection par instantané et sauvegarde gérée dans d'autres NetApp products or services. Backup and Recovery utilise des stratégies qui régissent les instantanés, la réplication vers un stockage secondaire ou les sauvegardes vers un stockage objet.

Ajouter une politique de détection aux charges de travail avec des politiques de sauvegarde ou de snapshot existantes

Si vous disposez déjà de stratégies d'instantané ou de sauvegarde avec Backup and Recovery, vous pouvez ajouter une stratégie pour détecter les attaques de ransomware. Pour gérer la protection et la détection avec Ransomware Resilience, voir Protégez-vous grâce à la résilience contre les ransomwares.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.



2. Depuis la page Protection, sélectionnez une charge de travail, puis sélectionnez **Protéger**.
3. Ransomware Resilience détecte s'il existe des politiques de Backup and Recovery actives.
4. Pour laisser votre NetApp Backup and Recovery existant en place et appliquer uniquement une politique de *détection*, laissez la case **Remplacer les politiques existantes** décochée.
5. Sélectionnez les paramètres de détection que vous souhaitez :
   - **Détection du chiffrement**
   - **Détection des comportements utilisateurs suspects**
   - **Bloquer les extensions de fichiers suspectes**
6. Sélectionnez **Suivant**.
7. Si vous avez sélectionné **Détection des comportements suspects des utilisateurs** comme paramètre de détection, sélectionnez l'agent d'activité utilisateur ou "ou en créer un".

   L'agent d'activité utilisateur héberge les nouveaux collecteurs de données. Ransomware Resilience crée automatiquement le collecteur de données pour transmettre les événements d'activité des utilisateurs à Ransomware Resilience afin de détecter les comportements anormaux des utilisateurs.

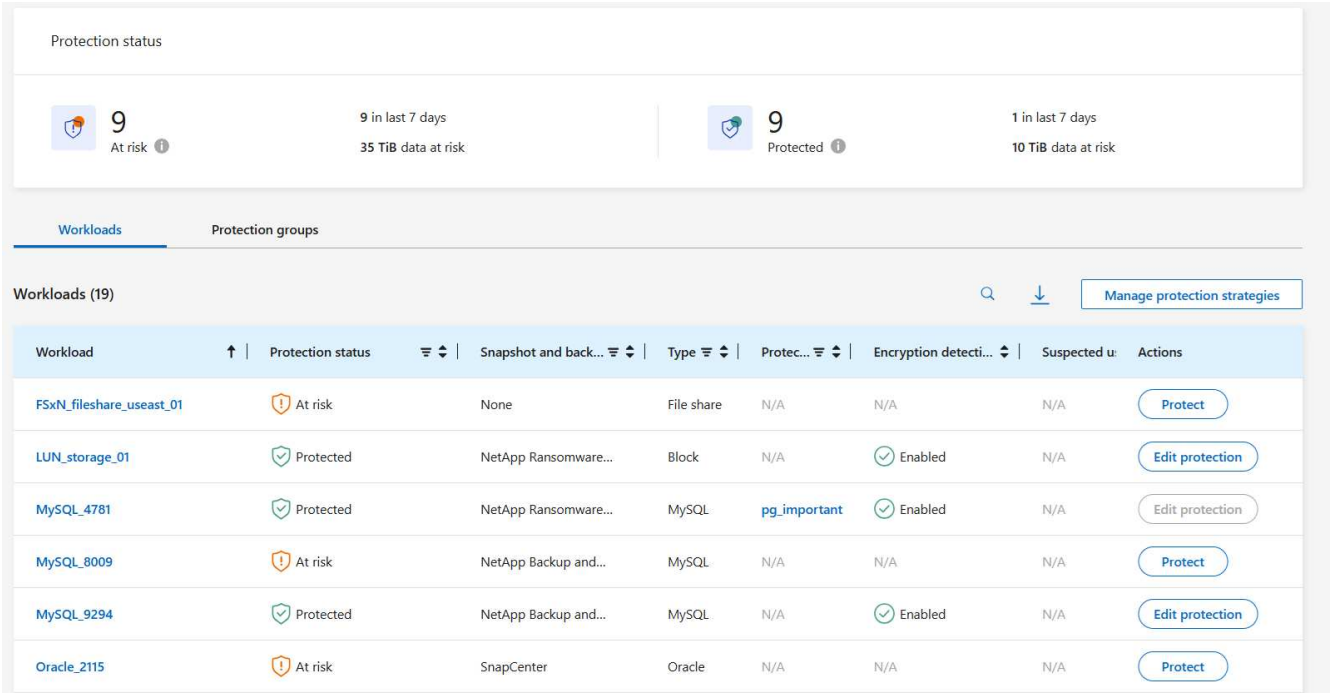
8. Sélectionnez **Suivant**.
9. Revoyez vos choix. Sélectionnez **Créer** pour activer la détection.
10. Sur la page Protection, vérifiez l'**état de détection** pour confirmer que la détection est active.

Remplacer les politiques de sauvegarde ou de snapshot existantes par une stratégie de protection contre les ransomwares

Vous pouvez remplacer vos politiques de sauvegarde ou de snapshot existantes par une stratégie de protection contre les ransomwares. Cette approche supprime votre protection gérée en externe et configure la détection et la protection dans Ransomware Resilience.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.



2. Depuis la page Protection, sélectionnez une charge de travail, puis sélectionnez **Protéger**.
3. Ransomware Resilience détecte s'il existe des politiques de Backup and Recovery actives. Pour remplacer les politiques existantes, cochez la case **Remplacer les politiques existantes**. Lorsque vous cochez la case, Ransomware Resilience remplace la liste des politiques de détection par des politiques de détection.
4. Choisissez une politique de protection. Si aucune politique de protection n'existe, sélectionnez **Ajouter** pour créer une nouvelle politique. Pour plus d'informations sur la création d'une politique, voirCréer une politique de protection . Sélectionnez **Suivant**.
5. Si votre stratégie inclut la réplication, sélectionnez le **système de destination** et la **VM de stockage de destination**. Sélectionnez **Suivant**.
6. Sélectionnez une destination de sauvegarde ou créez-en une nouvelle. Sélectionnez **Suivant**.
   a. Si votre stratégie de protection inclut la détection du comportement des utilisateurs, sélectionnez un agent d'activité utilisateur dans votre environnement pour héberger les nouveaux collecteurs de données. Ransomware Resilience crée automatiquement le collecteur de données pour transmettre les événements d'activité des utilisateurs à Ransomware Resilience afin de détecter les comportements anormaux des utilisateurs.
7. Passez en revue la nouvelle stratégie de protection, puis sélectionnez **Protéger** pour l'appliquer.
8. Sur la page Protection, vérifiez l'**état de détection** pour confirmer que la détection est active.

Attribuer une politique différente

Vous pouvez remplacer la politique existante par une autre.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sur la ligne de charge de travail, sélectionnez **Modifier la protection**.
3. Si la charge de travail possède une stratégie de sauvegarde et de restauration existante que vous souhaitez conserver, décochez **Remplacer les stratégies existantes**. Pour remplacer les stratégies

existantes, cochez **Remplacer les stratégies existantes**.

4. Dans la page Politiques, sélectionnez la flèche vers le bas correspondant à la politique que vous souhaitez attribuer pour consulter les détails.
5. Sélectionnez la politique que vous souhaitez attribuer.
6. Sélectionnez **Protéger** pour terminer la modification.

Gérer les stratégies de protection contre les ransomwares

Vous pouvez supprimer une stratégie de ransomware.

Afficher les charges de travail protégées par une stratégie de protection contre les ransomwares

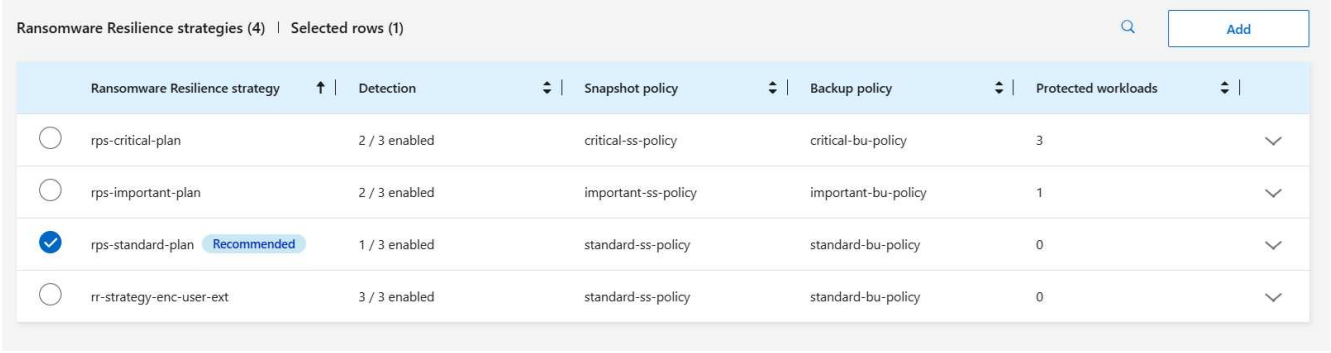
Avant de supprimer une stratégie de protection contre les ransomwares, vous souhaiterez peut-être afficher les charges de travail protégées par cette stratégie.

Vous pouvez afficher les charges de travail à partir de la liste des stratégies ou lorsque vous modifiez une stratégie spécifique.

Étapes pour visualiser les stratégies

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez **Gérer les stratégies de protection**.

   La page Stratégies de protection contre les ransomwares affiche une liste de stratégies.



3. Sur la page Stratégies de protection contre les ransomwares, dans la colonne Charges de travail protégées, sélectionnez la flèche vers le bas à la fin de la ligne.

Supprimer une stratégie de protection contre les ransomwares

Vous pouvez supprimer une stratégie de protection qui n'est actuellement associée à aucune charge de travail.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez **Gérer les stratégies de protection**.
3. Dans la page Gérer les stratégies, sélectionnez les *Actions* option pour la stratégie que vous souhaitez supprimer.
4. Dans le menu Actions, sélectionnez **Supprimer la politique**.

Configurer la détection de l’activité de l’utilisateur

Découvrez la détection de l’activité des utilisateurs dans NetApp Ransomware Resilience

Grâce à la détection de l’activité de l’utilisateur, NetApp Ransomware Resilience vous permet de gérer les incidents liés aux ransomwares au niveau de l’utilisateur, en stoppant des événements tels que les violations de données et les suppressions à grande échelle.

NetApp Ransomware Resilience fournit une détection de violation de données basée sur l’IA en surveillant l’activité utilisateur suspecte. Des augmentations soudaines de l’activité de lecture et des schémas d’accès à l’activité de lecture sont utilisées pour déterminer une intention malveillante. Une fois détectée, Ransomware Resilience génère automatiquement des alertes dans la NetApp Console, par e-mail et dans tout écosystème de sécurité configuré (par exemple, SIEM).

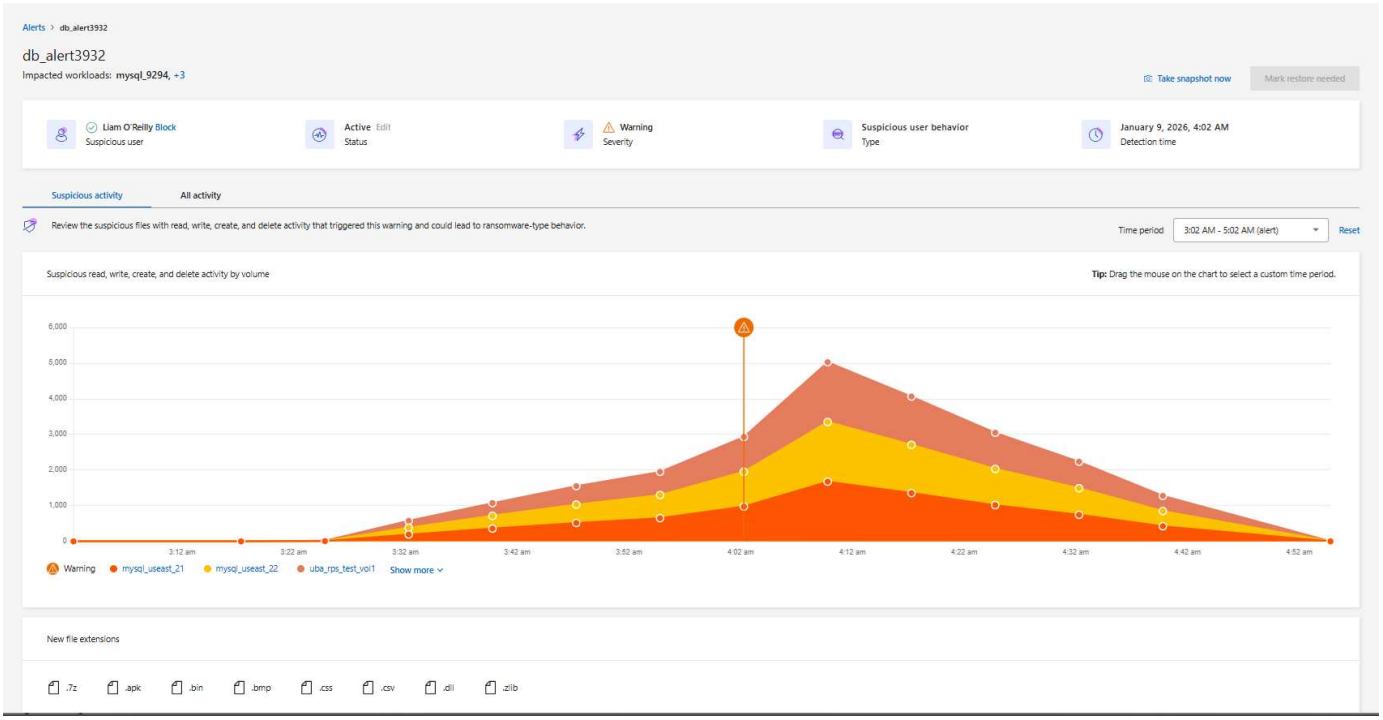
Grâce à la détection et à l’alerte en cas de comportement utilisateur suspect, Ransomware Resilience vous avertit des tentatives de violation et de destruction de données ainsi que des schémas qui semblent suspects. Dans chaque alerte, Ransomware Resilience identifie un utilisateur que vous pouvez bloquer.

Ransomware Resilience détecte l’activité suspecte des utilisateurs en analysant les événements d’activité des utilisateurs générés par FPolicy dans ONTAP. Pour collecter des données d’activité utilisateur, vous devez déployer un ou plusieurs agents d’activité utilisateur. L’agent est un serveur Linux ou une machine virtuelle avec connectivité aux appareils de votre locataire.

La détection de l’activité des utilisateurs n’est actuellement pas prise en charge pour les charges de travail SAN. Vous pouvez utiliser la détection de l’activité des utilisateurs avec les charges de travail NAS dans Amazon FSxN for ONTAP, Cloud Volumes ONTAP et ONTAP.

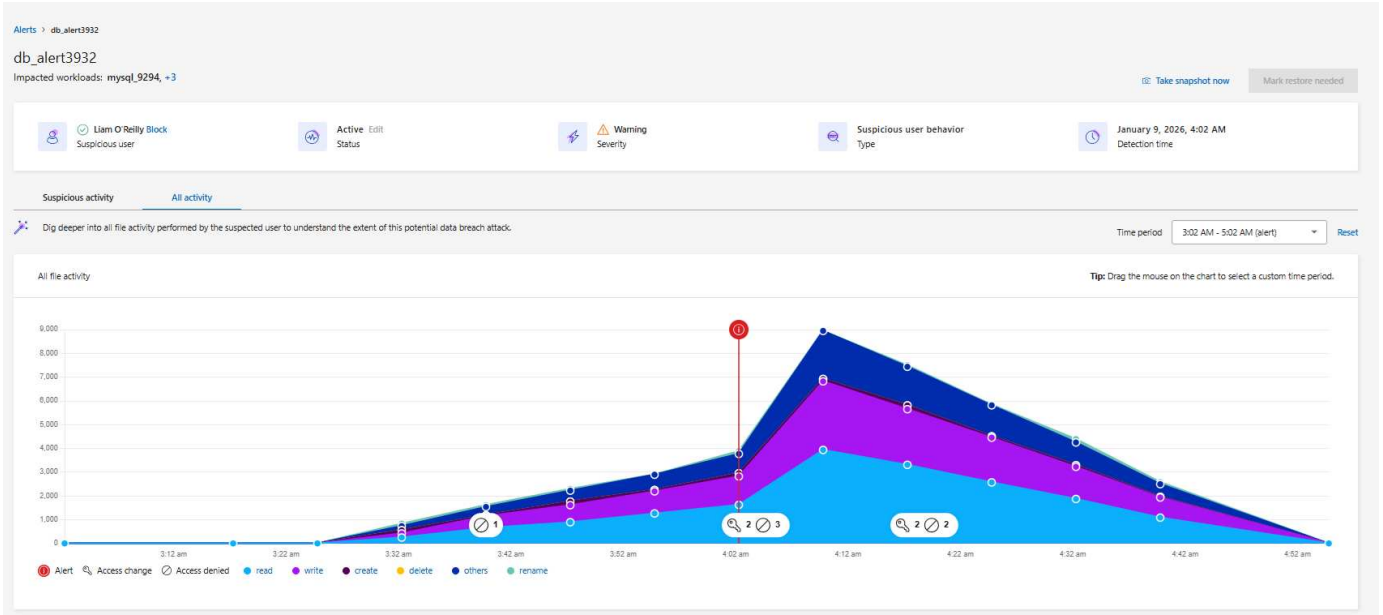
Analyse forensique des activités suspectes des utilisateurs

Ransomware Resilience propose une analyse forensique des comportements des utilisateurs : listes et graphiques montrant quand une activité suspecte a eu lieu et quand des notifications ont été envoyées. Ces éléments détaillent la fréquence des activités suspectes sur les fichiers, répertoires, volumes et charges de travail au fil du temps pour aider à retracer les événements. Vous pouvez également observer l’apparition de nouvelles extensions de fichiers.



.

Vous pouvez comparer l'activité suspecte avec une vue de toute l'activité. Dans la vue de toute l'activité, vous pouvez observer les événements de lecture, d'écriture, de renommage, de déplacement, de création et de suppression, en plus des événements de modification d'accès et d'accès refusé.



.

Composants

Il existe trois composants clés dans la détection de l'activité de comportement utilisateur suspecte de NetApp Ransomware Resilience.

- L'**agent d'activité utilisateur** est un environnement d'exécution pour les collecteurs de données. Vous devez configurer l'agent d'activité utilisateur.

- Le **collecteur de données** partage les événements d'activité des utilisateurs avec Ransomware Resilience. Le collecteur de données est créé automatiquement lorsque vous "mettre en place une stratégie de protection contre les ransomwares avec détection des activités suspectes des utilisateurs".
- Le **connecteur d'annuaire utilisateur** permet d'associer les noms d'utilisateur aux identifiants d'utilisateur, créant une plus grande clarté lors de la réponse à un comportement utilisateur suspect. Vous devez configurer le connecteur d'annuaire utilisateur.

Ransomware Resilience et Data Infrastructure Insights

La détection des comportements suspects des utilisateurs de Ransomware Resilience est une intégration avec Data Infrastructure Insights (DII) Workload Security et utilise "Points de terminaison DII". Vous n'avez besoin d'aucune configuration DII pour activer la détection des comportements des utilisateurs dans Ransomware Resilience. Pour activer la détection des comportements des utilisateurs, "créez l'agent et les collecteurs requis et activez la stratégie de protection contre les ransomwares appropriée".

Si vous utilisez déjà NetApp Data Infrastructure Insights (DII) Workload Security, il est recommandé d'utiliser les mêmes agents Workload Security pour Ransomware Resilience. Il n'est pas nécessaire de déployer des agents Workload Security distincts pour Ransomware Resilience, cependant, l'utilisation des mêmes agents Workload Security nécessite une relation de couplage entre l'organisation de la Ransomware Resilience Console et le locataire DII Storage Workload Security. Contactez votre responsable de compte pour activer ce couplage.

Prochaines étapes

- "Exigences relatives à la détection de l'activité comportementale des utilisateurs"
- "Configurer les agents et détecteurs d'activité du comportement utilisateur"

Exigences relatives à la détection du comportement des utilisateurs dans NetApp Ransomware Resilience

NetApp Ransomware Resilience la détection du comportement des utilisateurs vous permet de répondre aux événements de ransomware au niveau de l'utilisateur. Vous devez créer un ensemble d'agents pour activer la détection du comportement des utilisateurs. Avant d'activer la détection, vous devez vous assurer que vous répondez aux exigences du système d'exploitation, du serveur et du réseau décrites afin que Ransomware Resilience puisse détecter et signaler correctement les événements.

Prise en charge du fournisseur de cloud

Les données d'activité suspecte des utilisateurs peuvent être stockées dans AWS et Azure dans les régions suivantes :

Fournisseur de cloud	Région
AWS	• Asie-Pacifique (Sydney) (ap-sud-est-2) • Europe (Francfort) (eu-central-1) • États-Unis Est (Virginie du Nord) (us-east-1)
Azuré	Est des États-Unis

Configuration requise pour le système d'exploitation

La détection des comportements suspects des utilisateurs est prise en charge avec les systèmes d'exploitation suivants :

Système opérateur	Versions prises en charge
AlmaLinux	9.4 (64 bits) à 9.5 (64 bits) et 10 (64 bits), y compris SELinux
CentOS	CentOS Stream 9 (64 bits)
Debian	11 (64 bits), 12 (64 bits), y compris SELinux
OpenSUSE Leap	15.3 (64 bits) à 15.6 (64 bits)
Oracle Linux	8.10 (64 bits) et 9.1 (64 bits) à 9.6 (64 bits), y compris SELinux
Chapeau rouge	8.10 (64 bits), 9.1 (64 bits) à 9.6 (64 bits) et 10 (64 bits), y compris SELinux
Rocheux	Rocky 9.4 (64 bits) à 9.6 (64 bits), y compris SELinux
SUSE Enterprise Linux	15 SP4 (64 bits) à 15 SP6 (64 bits), y compris SELinux
Ubuntu	20.04 LTS (64 bits), 22.04 LTS (64 bits) et 24.04 LTS (64 bits)

L'ordinateur que vous utilisez pour l'agent d'activité de l'utilisateur ne doit pas exécuter d'autres logiciels au niveau de l'application. Un serveur dédié est recommandé.

Le `unzip` Cette commande est requise pour l'installation. Le `sudo su -` Cette commande est nécessaire pour l'installation, l'exécution des scripts et la désinstallation.

Configuration requise pour le serveur

Le serveur doit répondre aux exigences minimales suivantes :

- **Processeur** : 4 cœurs
- **RAM** : 16 Go de RAM
- **Espace disque** : 36 Go d'espace disque libre

Recommandations serveur

- Allouez de l'espace disque supplémentaire pour permettre la création du système de fichiers. Assurez-vous qu'il y a au moins 35 Go d'espace libre dans le système de fichiers. + Si `/opt` Il s'agit d'un dossier monté depuis un stockage NAS ; les utilisateurs locaux doivent avoir accès à ce dossier. La création de l'agent d'activité utilisateur peut échouer si les utilisateurs locaux ne disposent pas des autorisations nécessaires.
- Il est recommandé d'installer l'agent d'activité utilisateur sur un système distinct de votre environnement NetApp Ransomware Resilience. Si vous les installez sur la même machine, vous devez prévoir 50 à 55 Go d'espace disque. Pour Linux, allouez 25 à 30 Go d'espace à `/opt/netapp` et 25 Go à `var/log/netapp`.

- Il est recommandé de synchroniser l'heure à la fois sur le système ONTAP et sur la machine de l'agent d'activité utilisateur à l'aide du protocole NTP (Network Time Protocol) ou du protocole SNTP (Simple Network Time Protocol).

règles d'accès au réseau cloud

Veuillez consulter les règles d'accès au réseau cloud pour votre zone géographique concernée (Asie-Pacifique, Europe ou États-Unis).

Lors de l'installation initiale, remplacez le `<site_name>` par une autorisation de caractère générique (`*`. Après que l'agent est activé et pleinement opérationnel, vous pouvez remplacer l'autorisation par le nom du site. Contactez votre représentant NetApp pour le nom du site.

L'agent d'activité utilisateur utilise la technologie NetApp Data Insights Infrastructure, d'où l'utilisation de points de terminaison `cloudinsights`. Pour plus d'informations, consultez

Déploiements d'agents d'activité utilisateur basés en APAC

Protocole	Port	Source	Destination	Description
HTTPS (TCP)	443	Agent d'activité utilisateur	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Accès à la résilience face aux ransomwares

Déploiements d'agents d'activité utilisateur basés en Europe

Protocole	Port	Source	Destination	Description
HTTPS (TCP)	443	Agent d'activité utilisateur	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accès à la résilience face aux ransomwares

Déploiements d'agents d'activité utilisateur basés aux États-Unis

Protocole	Port	Source	Destination	Description
HTTPS (TCP)	443	Agent d'activité utilisateur	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Accès à la résilience face aux ransomwares

Règles du réseau

Protocole	Port	Source	Destination	Description
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agent d'activité utilisateur	URL du serveur LDAP	Se connecter à LDAP
HTTPS (TCP)	443	Agent d'activité utilisateur	Adresse IP de gestion du cluster ou de la SVM (selon la configuration du collecteur SVM)	Communication API avec ONTAP

Protocole	Port	Source	Destination	Description
TCP	35000 - 55000	Données SVM Adresses IP LIF	Agent d’activité utilisateur	Communication d' ONTAP à l’agent d’activité utilisateur pour les événements Fpolicy. Ces ports doivent être ouverts vers l’agent d’activité utilisateur pour ONTAP puisse lui envoyer des événements, y compris tout pare-feu sur l’agent d’activité utilisateur lui-même (le cas échéant). **REMARQUE :** Vous n’avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez doivent se situer dans cette plage. Il est recommandé de commencer par réserver 100 ports et d’augmenter ce nombre si nécessaire.

Protocole	Port	Source	Destination	Description
TCP	35000-55000	IP de gestion de cluster	Agent d'activité utilisateur	Communication de l'adresse IP de gestion du cluster ONTAP à l'agent d'activité utilisateur pour les **événements EMS**. Ces ports doivent être ouverts vers l'agent d'activité utilisateur pour ONTAP puisse lui envoyer des événements EMS, y compris tout pare-feu sur l'agent d'activité utilisateur lui-même. **REMARQUE :** Vous n'avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez doivent se situer dans cette plage. Il est recommandé de commencer par réserver 100 ports et d'augmenter ce nombre si nécessaire.
SSH	22	Agent d'activité utilisateur	Gestion des clusters	Nécessaire pour le blocage des utilisateurs CIFS/SMB.

Étape suivante

- "Configurer les agents d'activité utilisateur et les collecteurs"

Configurer les agents et les collecteurs pour la détection de l'activité des utilisateurs dans NetApp Ransomware Resilience

NetApp Ransomware Resilience détection de l'activité utilisateur vous aide à prévenir les événements de ransomware au niveau de l'utilisateur. Pour activer la détection des comportements suspects des utilisateurs dans Ransomware Resilience, vous devez installer au moins un agent d'activité utilisateur, ce qui crée un environnement de collecte de données pour surveiller le comportement des utilisateurs à la recherche de schémas aberrants ressemblant à des événements de ransomware.

Un agent d'activité utilisateur héberge un collecteur de données et un connecteur d'annuaire utilisateur, qui envoient tous deux des données vers un emplacement SaaS pour analyse.

- Le **collecteur de données** recueille les données d'activité des utilisateurs depuis ONTAP. Le collecteur de données est créé automatiquement lorsque vous créez une stratégie de protection avec détection du comportement des utilisateurs.
- Le **connecteur d'annuaire utilisateur** se connecte à votre annuaire pour associer les identifiants utilisateur aux noms d'utilisateur. Vous devez configurer le connecteur d'annuaire utilisateur.

L'agent d'activité utilisateur, le collecteur de données et le connecteur d'annuaire utilisateur peuvent tous être gérés depuis le tableau de bord des paramètres de NetApp Ransomware Resilience.

> Si vous utilisez déjà NetApp Data Infrastructure Insights (DII) Workload Security, il est recommandé d'utiliser les mêmes agents Workload Security pour Ransomware Resilience. Il n'est pas nécessaire de déployer des agents Workload Security distincts pour Ransomware Resilience, cependant, l'utilisation des mêmes agents Workload Security nécessite une relation de couplage entre l'organisation de la Ransomware Resilience Console et le locataire DII Storage Workload Security. Contactez votre responsable de compte pour activer ce couplage.

+ Si vous n'utilisez *pas* DII, suivez les instructions de configuration ici.

Avant de commencer

- Assurez-vous de respecter les "exigences relatives au système d'exploitation, au serveur et au réseau".

Rôle Console requis Pour activer la détection des activités utilisateur suspectes, vous devez disposer du **rôle Organization admin**. Pour les configurations ultérieures relatives aux activités utilisateur suspectes, vous devez disposer du **rôle Ransomware Resilience user behavior admin**. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console".

Assurez-vous que chaque rôle est appliqué au niveau de l'organisation.

Créer un agent d'activité utilisateur

Les agents d'activité utilisateur sont des environnements exécutables pour "collecteurs de données" ; les collecteurs de données partagent les événements d'activité utilisateur avec Ransomware Resilience. Vous devez créer au moins un agent d'activité utilisateur pour activer la détection des activités utilisateur suspectes.

Étapes

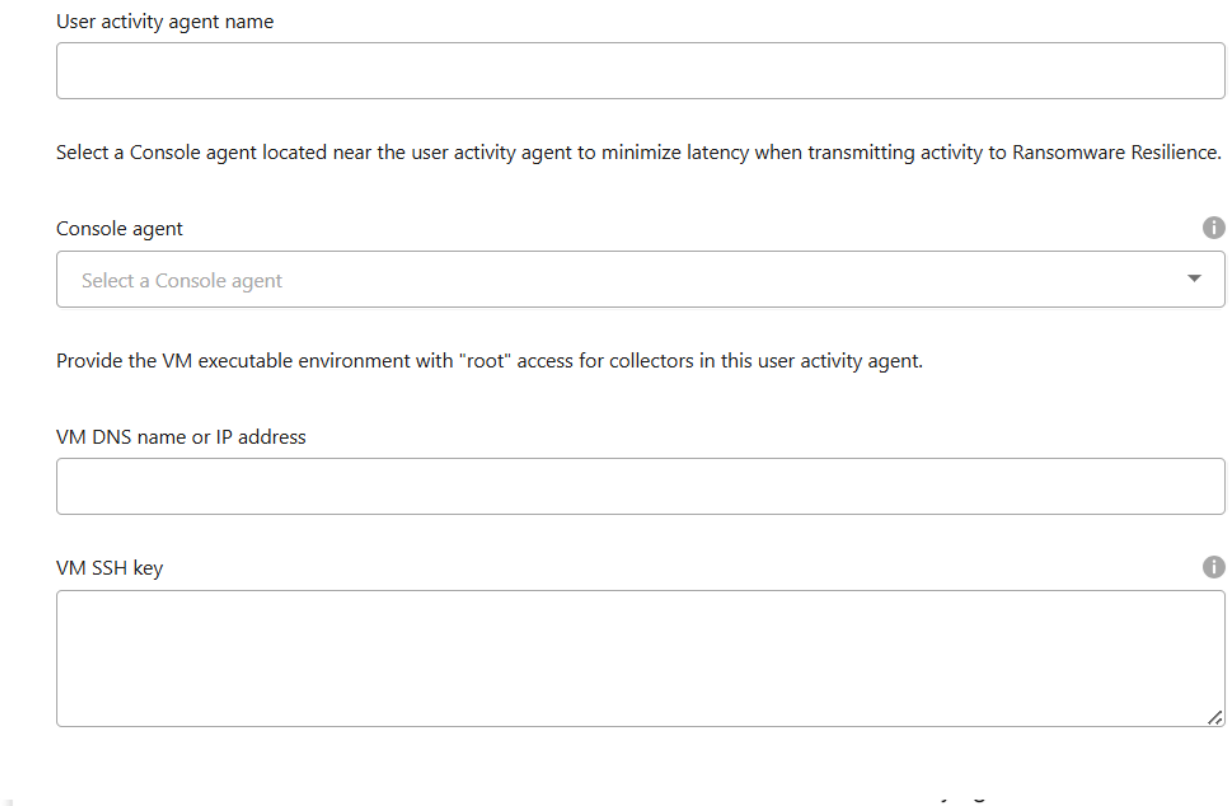
1. Si c'est la première fois que vous créez un agent d'activité utilisateur, accédez au **Tableau de bord**. Dans la mosaïque **Activité utilisateur**, sélectionnez **Activer**.

   Si vous ajoutez un agent d'activité utilisateur supplémentaire, accédez à **Paramètres**, recherchez la vignette **Activité utilisateur**, puis sélectionnez **Gérer**. Sur l'écran Activité utilisateur, sélectionnez l'onglet **Agents d'activité utilisateur** puis **Ajouter**.

2. Sélectionnez un **fournisseur Cloud** puis une **région**. Sélectionnez **Suivant**.
3. Fournissez les détails de l'agent d'activité de l'utilisateur :
   - **Nom de l'agent d'activité utilisateur**
   - **Agent de console** - L'agent de console doit se trouver sur le même réseau que l'agent d'activité utilisateur et disposer d'une connectivité SSH à l'adresse IP de l'agent d'activité utilisateur.
   - **Nom DNS ou adresse IP de la VM**

- **Clé SSH de la VM** - Saisissez la clé SSH au format suivant :

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```



4. Sélectionnez **Suivant**.
5. Vérifiez vos paramètres. Sélectionnez **Activer** pour terminer l'ajout de l'agent d'activité utilisateur.
6. Vérifiez que l'agent d'activité utilisateur a bien été créé. Dans la vignette Activité utilisateur, un déploiement réussi s'affiche comme **Running**.

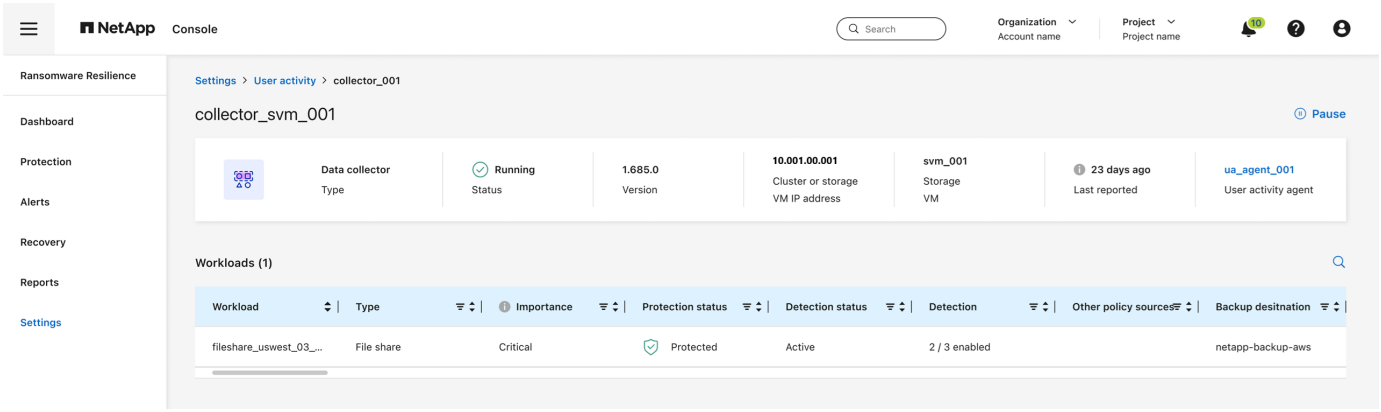
Résultat

Une fois l'agent d'activité utilisateur créé avec succès, retournez dans le menu **Paramètres** puis sélectionnez **Gérer** dans la vignette Activité utilisateur. Sélectionnez l'onglet **Agents d'activité utilisateur** puis sélectionnez l'agent d'activité utilisateur pour afficher des détails à son sujet, y compris les collecteurs de données et les connecteurs d'annuaire utilisateur.

Ajouter un collecteur de données

Des collecteurs de données sont créés automatiquement lorsque vous activez une stratégie de protection contre les ransomwares avec détection des activités suspectes des utilisateurs. Pour plus d'informations, consultez "ajouter une politique de détection".

Vous pouvez consulter les détails du collecteur de données. Dans Paramètres, sélectionnez **Gérer** dans la mosaïque Activité utilisateur. Sélectionnez l'onglet **Collecteur de données** puis sélectionnez le collecteur de données pour afficher ses détails ou le mettre en pause.



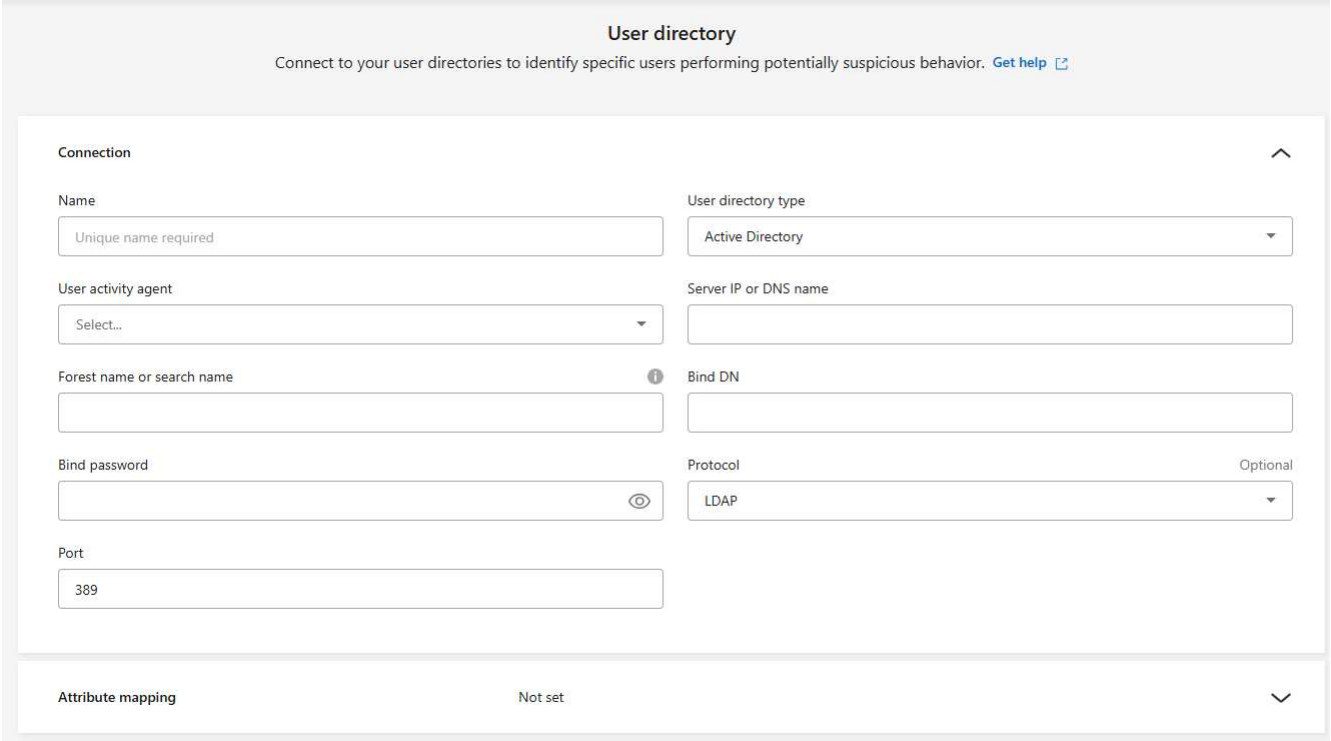
Créer un connecteur d'annuaire utilisateur

Pour mapper les ID utilisateur aux noms d'utilisateur, vous devez créer un connecteur d'annuaire utilisateur.

Étapes

1. Dans Ransomware Resilience, accédez à **Paramètres**.
2. Dans la mosaïque Activité utilisateur, sélectionnez **Gérer**.
3. Sélectionnez l'onglet **Connecteurs d'annuaire utilisateur** puis **Ajouter**.
4. Configurez la connexion. Saisissez les informations requises pour chaque champ.

Champ	Description
Nom	Saisissez un nom unique pour le connecteur d'annuaire utilisateur
Type de répertoire utilisateur	Le type de répertoire
Adresse IP du serveur ou nom de domaine	L'adresse IP ou le nom de domaine pleinement qualifié (FQDN) du serveur hébergeant la connexion
Nom de la forêt ou nom de recherche	Vous pouvez spécifier le niveau de forêt de la structure de répertoires comme nom de domaine direct (par exemple, `unit.company.com`) ou un ensemble de noms distinctifs relatifs (par exemple : `DC=unit,DC=company,DC=com`). Vous pouvez également saisir un `OU` filtrer par unité organisationnelle ou par un `CN` limiter à un utilisateur spécifique (par exemple : `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).
BIND DN	Le DN BIND est un compte utilisateur autorisé à effectuer des recherches dans l'annuaire, tel que utilisateur@domaine.com. L'utilisateur doit disposer de l'autorisation « Lecture seule du domaine ».
Mot de passe BIND	Le mot de passe de l'utilisateur a été fourni dans BIND DN
Protocole	Le champ protocole est facultatif. Vous pouvez utiliser LDAP, LDAPS ou LDAP sur StartTLS.
Port	Saisissez le numéro de port que vous avez choisi



Fournissez les détails du mappage des attributs :

- **Nom d'affichage**
- **SID** (si vous utilisez LDAP)
- **Nom d'utilisateur**
- **ID Unix** (si vous utilisez NFS)
- Si vous sélectionnez **Inclure les attributs facultatifs**, vous pouvez également ajouter une adresse e-mail, un numéro de téléphone, un rôle, un état, un pays, un département, une photo, un DN de responsable ou des groupes. Sélectionnez **Avancé** pour ajouter une requête de recherche facultative.

5. Sélectionnez **Ajouter**.
6. Revenez à l'onglet Connecteurs d'annuaire utilisateur pour vérifier l'état de votre connecteur d'annuaire utilisateur. Si la création est réussie, l'état du connecteur d'annuaire utilisateur s'affiche comme **En cours d'exécution**.

Supprimer un connecteur d'annuaire utilisateur

Étapes

1. Dans Ransomware Resilience, accédez à **Paramètres**.
2. Localisez la mosaïque Activité utilisateur, sélectionnez **Gérer**.
3. Sélectionnez l'onglet **Connecteur d'annuaire utilisateur**.
4. Identifiez le connecteur d'annuaire utilisateur que vous souhaitez supprimer. Dans le menu d'action en fin de ligne, sélectionnez les trois points … puis **Supprimer**.
5. Dans la boîte de dialogue contextuelle, sélectionnez **Supprimer** pour confirmer.

Exclure les utilisateurs des alertes

S'il existe certains utilisateurs de confiance dont le comportement pourrait déclencher des alertes de comportement utilisateur, vous pouvez les exclure des alertes.

Étapes

1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans le tableau de bord Paramètres, repérez la carte User activity puis sélectionnez **Manage**.
3. Sélectionnez l'onglet **Excluded users**.
4. Pour consulter les utilisateurs individuellement dans l'interface utilisateur, choisissez **Select manually**. Pour importer une liste d'utilisateurs exclus, sélectionnez **Upload**.
   a. Si vous avez sélectionné **Select manually**, cochez la case en regard des noms des utilisateurs spécifiques que vous souhaitez exclure.
   b. Si vous sélectionnez **Upload**, vous devez d'abord télécharger un fichier CSV contenant la liste de tous les utilisateurs. Sélectionnez **Download** pour accéder à la liste.

      Examinez le fichier CSV. Supprimez les noms de tous les utilisateurs pour lesquels vous souhaitez maintenir la détection. Lorsque la liste ne contient plus que les noms des utilisateurs que vous souhaitez exclure de la détection, enregistrez-la. Sélectionnez **Importer** pour localiser le fichier, puis choisissez-le.
5. Sélectionnez **Ajouter** pour terminer l'ajout des utilisateurs à la liste d'exclusion.
6. Dans l'onglet **Utilisateurs exclus**, les noms des utilisateurs retirés des alertes de détection du comportement des utilisateurs s'affichent désormais dans le tableau de bord.

Vous pouvez également exclure un utilisateur directement d'une alerte. Pour plus d'informations, consultez "Répondre aux alertes de ransomware".

Supprimer des utilisateurs de la liste des utilisateurs exclus

Vous pouvez réintégrer un utilisateur dans la détection après.

Étapes

1. Dans le tableau de bord Paramètres, repérez la carte User activity puis sélectionnez **Manage**.
2. Sélectionnez l'onglet **Excluded users**.
3. Repérez le nom de l'utilisateur que vous souhaitez supprimer de la liste des utilisateurs exclus. Sélectionnez le menu d'actions (… sur la ligne contenant le nom de l'utilisateur, puis **Supprimer**.
4. Dans la boîte de dialogue, sélectionnez **Remove** pour confirmer que vous souhaitez supprimer les utilisateurs sélectionnés.

Répondre aux alertes d'activité suspecte des utilisateurs

Une fois la détection des activités suspectes des utilisateurs configurée, vous pouvez suivre les événements sur la page des alertes. Pour plus d'informations, voir "Détecter les activités malveillantes et les comportements suspects des utilisateurs".

Gérer les groupes de protection dans NetApp Ransomware Resilience

NetApp Ransomware Resilience propose des groupes de protection pour faciliter la

gestion de votre patrimoine de données. Les groupes de protection sont des regroupements logiques de charges de travail. Ransomware Resilience peut protéger tous les volumes d'un groupe de protection en même temps avec une seule stratégie de protection, vous évitant d'appliquer une stratégie à chaque charge de travail.

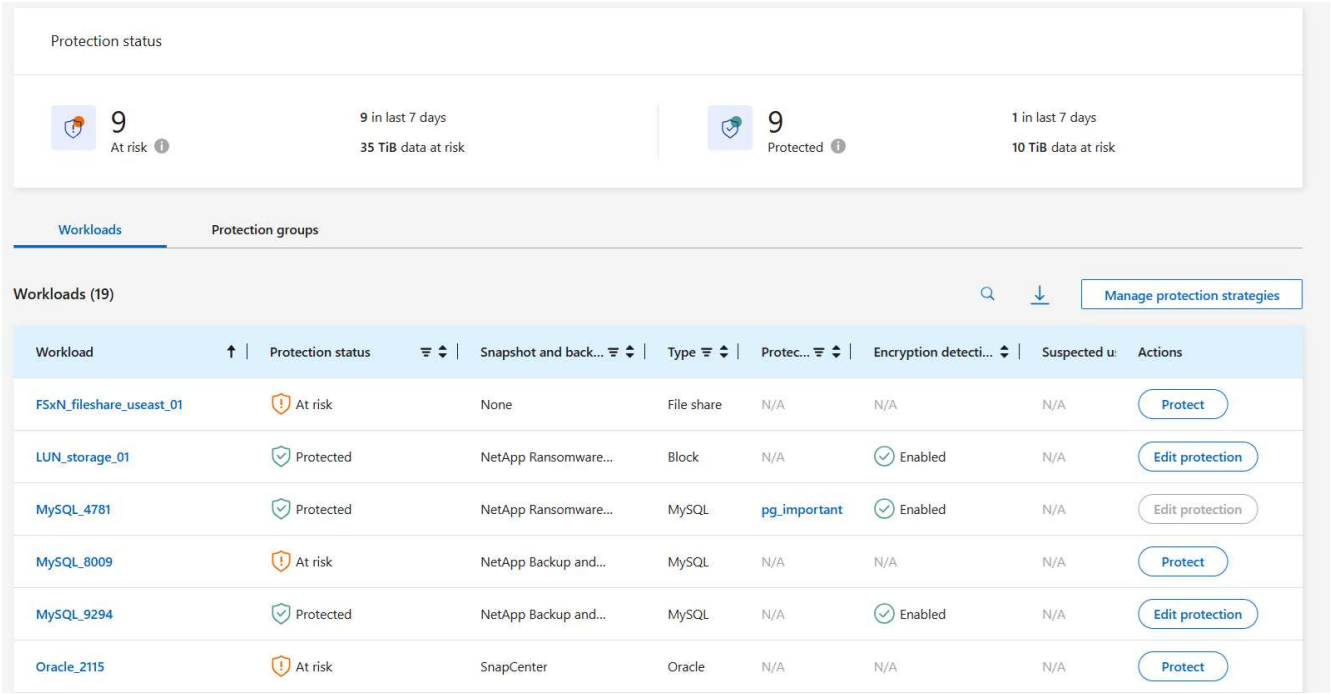
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Créer un groupe de protection

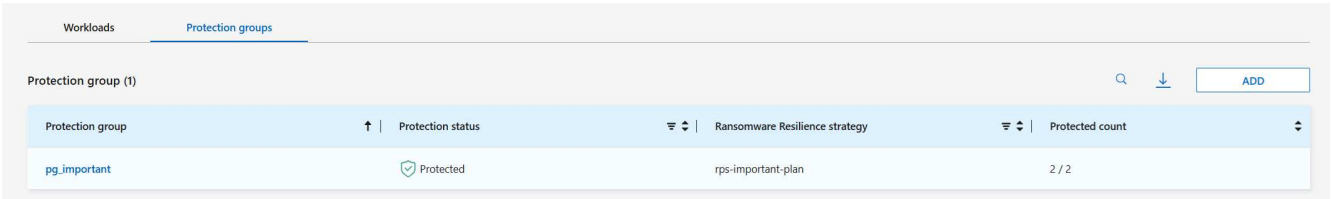
Vous pouvez créer des groupes quel que soit leur niveau de protection (c'est-à-dire, groupes non protégés et groupes protégés). Lorsque vous ajoutez une stratégie de protection à un groupe de protection, la nouvelle stratégie de protection remplace toute stratégie existante, y compris les stratégies gérées NetApp Backup and Recovery.

Étapes

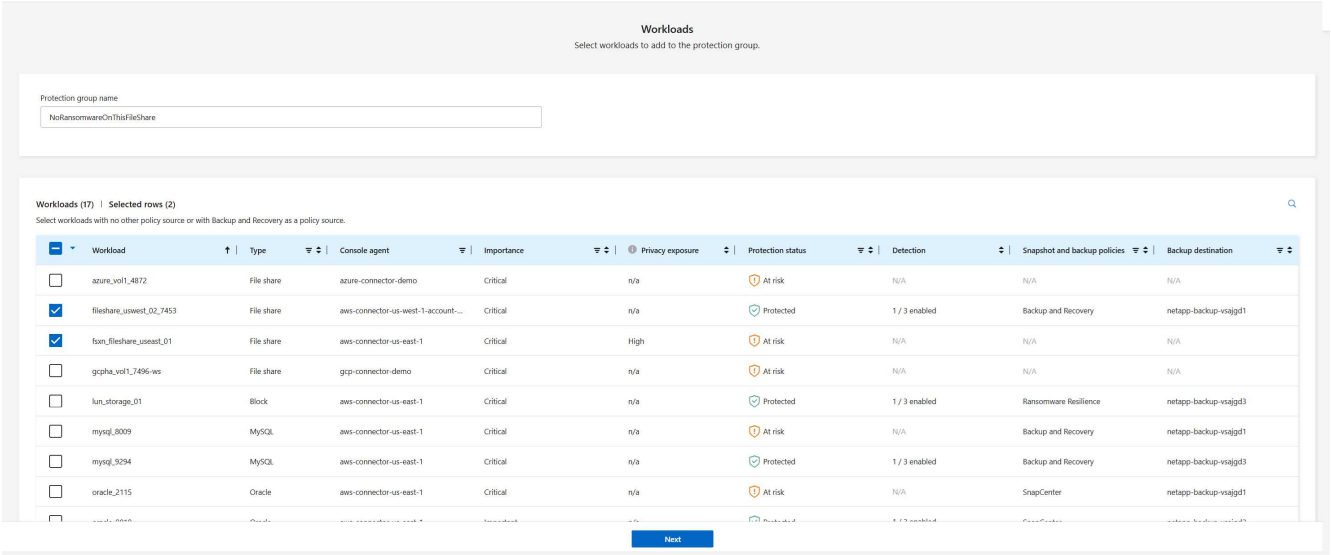
1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.



2. Dans le tableau de bord Protection, sélectionnez l'onglet **Protection groups**.



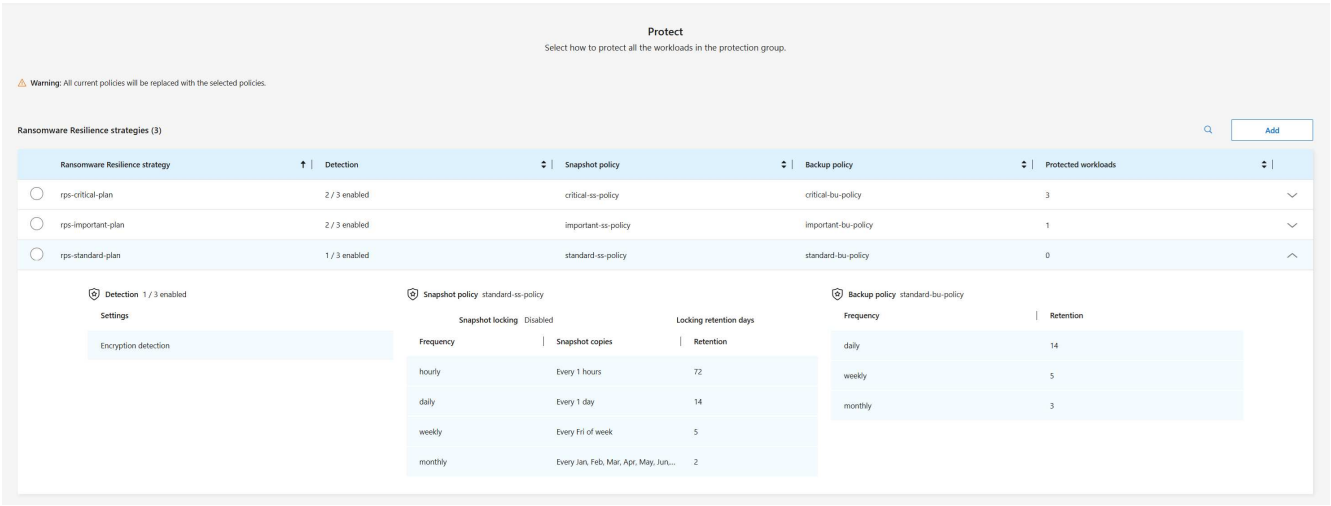
3. Sélectionnez **Ajouter**.



4. Entrez un nom pour le groupe de protection.
5. Sélectionnez les charges de travail à ajouter au groupe.

   Pour voir plus de détails sur les charges de travail, faites défiler vers la droite.

6. Sélectionnez **Suivant**.



7. Choisissez une stratégie de protection pour le groupe.
8. Si la stratégie de protection inclut la réplication, vérifiez les paramètres de réplication.
   a. Pour répliquer tous les instantanés vers la même destination, cochez **Utiliser la même destination pour chaque charge de travail**. Choisissez un **système de destination** et une **VM de stockage de destination** pour les charges de travail dans la section Agent de la console. + Pour utiliser des destinations différentes, décochez cette case. Examinez chaque charge de travail sous chaque agent de console et attribuez un **système de destination** et une **VM de stockage de destination** à chaque charge de travail. Sélectionnez **Suivant**.
9. Pour configurer une stratégie de sauvegarde, choisissez-en une puis sélectionnez **Suivant**.
10. Si votre politique de détection inclut la détection du comportement des utilisateurs, sélectionnez le collecteur de données que vous souhaitez utiliser, puis **Suivant**.

11. Passez en revue les sélections pour le groupe de protection.
12. Pour finaliser le groupe de protection, sélectionnez **Add**.

Lors de la consultation du tableau de bord de protection dans NetApp Ransomware Resilience, vous pouvez trier les charges de travail par groupe de protection.

Modifier la protection du groupe

Vous pouvez modifier la politique de détection sur un groupe existant.

Étapes

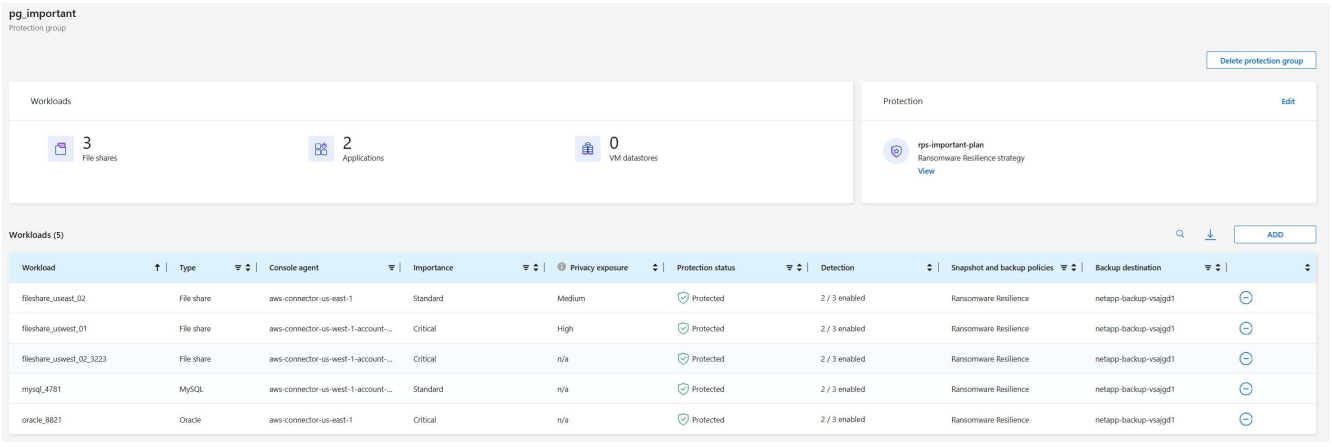
1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez l'onglet **Groupes de protection** puis sélectionnez le groupe dont vous souhaitez modifier la politique.
3. Depuis la page d'aperçu du groupe de protection, sélectionnez **Modifier la protection**.
4. Sélectionnez une politique de protection existante à appliquer ou sélectionnez **Ajouter** pour créer une nouvelle politique de protection. Pour plus d'informations sur l'ajout d'une politique de protection, consultez "Créer une politique de protection". Sélectionnez ensuite **Enregistrer**.
5. Dans l'aperçu de la destination de sauvegarde, sélectionnez une destination de sauvegarde existante ou **Ajoutez une nouvelle destination de sauvegarde**.
6. Sélectionnez **Suivant** pour examiner vos modifications.

Supprimer les charges de travail d'un groupe de protection

Vous pourriez avoir besoin ultérieurement de supprimer des charges de travail d'un groupe de protection existant.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez l'onglet **Groupes de protection**.
3. Sélectionnez le groupe à partir duquel vous souhaitez supprimer une ou plusieurs charges de travail.



4. Sur la page du groupe de protection, sélectionnez la charge de travail que vous souhaitez retirer du groupe et sélectionnez l'option **Actions** ⋯.
5. Dans le menu Actions, sélectionnez **Supprimer la charge de travail**.

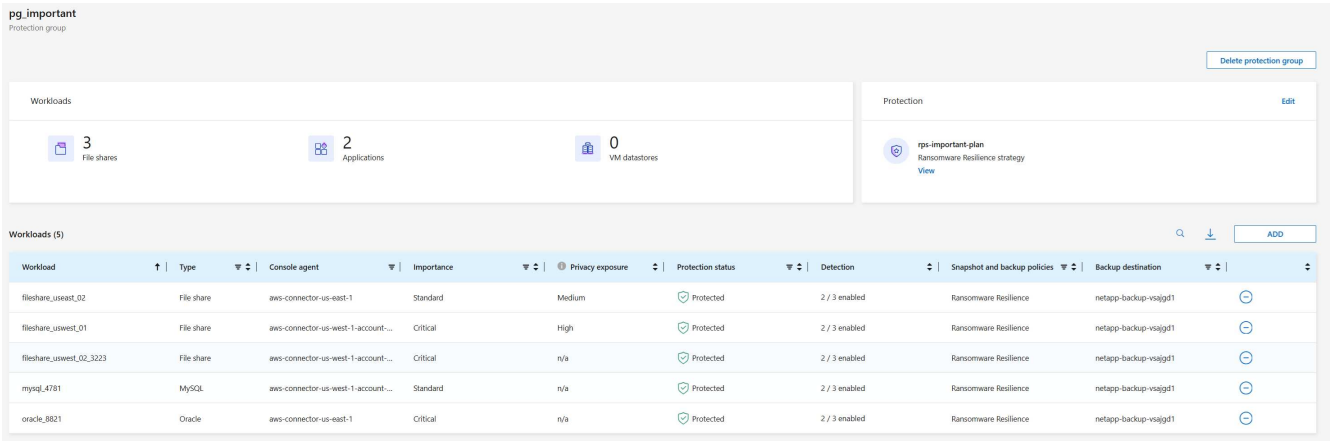
6. Confirmez que vous souhaitez supprimer la charge de travail et sélectionnez **Supprimer**.

Supprimer un groupe de protection

Lorsque vous supprimez un groupe de protection, Ransomware Resilience supprime le groupe et la stratégie de protection sur les charges de travail. Il ne supprime pas les charges de travail individuelles.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez l'onglet **Groupes de protection**.
3. Sélectionnez le groupe à partir duquel vous souhaitez supprimer une ou plusieurs charges de travail.



4. Depuis la page du groupe de protection sélectionné, en haut à droite, sélectionnez **Supprimer le groupe de protection**.
5. Confirmez que vous souhaitez supprimer le groupe et sélectionnez **Supprimer**.

Recherchez des informations personnelles identifiables avec la NetApp Data Classification dans Ransomware Resilience

Dans NetApp Ransomware Resilience, vous pouvez utiliser NetApp Data Classification pour analyser et classer les données dans une charge de travail de partage de fichiers. La classification des données vous aide à déterminer si l'ensemble de données contient des informations personnelles identifiables (PII), ce qui peut augmenter les risques de sécurité. La classification des données est un composant essentiel de la NetApp Console et est disponible sans frais supplémentaires.

"Classification des données"utilise le traitement du langage naturel basé sur l'IA pour l'analyse et la catégorisation des données contextuelles, fournissant des informations exploitables sur vos données pour répondre aux exigences de conformité, détecter les vulnérabilités de sécurité, optimiser les coûts et accélérer la migration.

Ce processus peut avoir un impact sur l'importance de la charge de travail pour vous aider à garantir que vous disposez de la protection appropriée.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Identifier l'exposition à la confidentialité grâce à la classification des données

Avant d'utiliser la classification des données dans Ransomware Resilience, vous devez"pour permettre à la classification des données d'analyser vos données" .

Vous pouvez déployer la classification des données dans la page Protection de Ransomware Resilience. Suivez la procédure pour identifier l'exposition à la confidentialité. Lorsque vous sélectionnez **Identifier l'exposition**, si vous n'avez pas déjà déployé la classification des données, une boîte de dialogue vous permet d'activer la classification des données.

Pour plus d'informations sur la classification des données, voir :

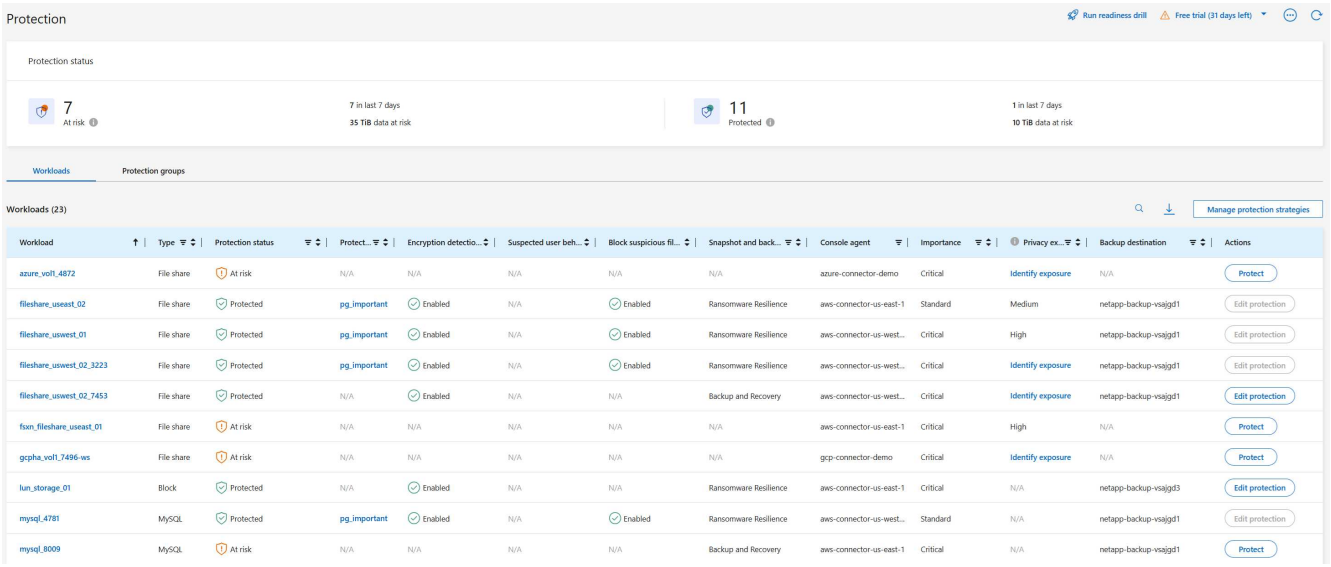
- "En savoir plus sur la classification des données"
- "Catégories de données privées"
- "Examinez les données stockées dans votre organisation"

Avant de commencer

L'analyse des données PII dans Ransomware Resilience est disponible si vous avez"Classification des données déployée" . La classification des données est disponible dans le cadre de la console sans frais supplémentaires et peut être déployée sur site ou dans le cloud client.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Dans la page Protection, recherchez une charge de travail de partage de fichiers dans la colonne Charge de travail.



3. Pour permettre à la classification des données d'analyser vos données à la recherche d'informations personnelles identifiables (PII), dans la colonne **Exposition à la confidentialité**, sélectionnez **Identifier l'exposition**.

> Si vous n'avez pas déployé Data CCassification, la sélection de **Identifier l'exposition** ouvre une boîte de dialogue pour déployer la classification des données. Sélectionnez **Déployer**. Après avoir déployé la classification des données, vous pouvez revenir à la page Protection puis sélectionner **Identifier l'exposition**.

Résultat

L'analyse peut prendre plusieurs minutes en fonction de la taille et du nombre de fichiers. Pendant l'analyse, la page Protection indique qu'elle identifie les fichiers et fournit un nombre de fichiers. Une fois l'analyse terminée, la colonne Exposition à la confidentialité évalue le niveau d'exposition comme Faible, Moyen ou Élevé.

Examiner l'exposition à la confidentialité

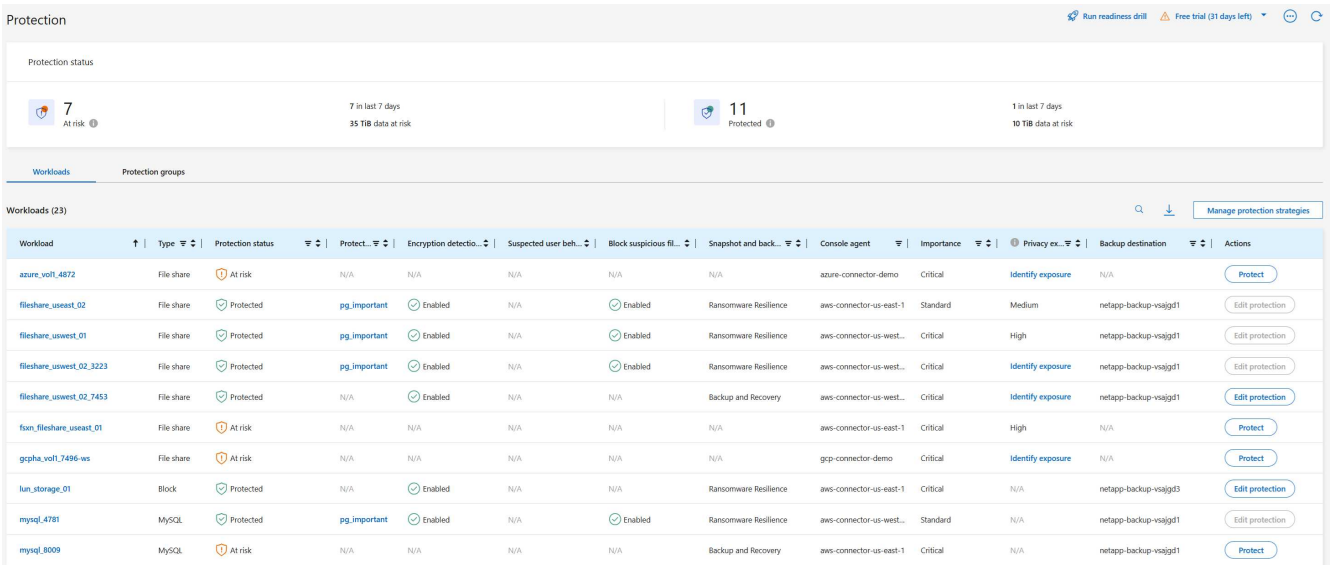
Après avoir analysé les données de classification pour les informations personnelles identifiables, évaluez le risque.

Les données PII sont classées selon l'une des trois désignations suivantes :

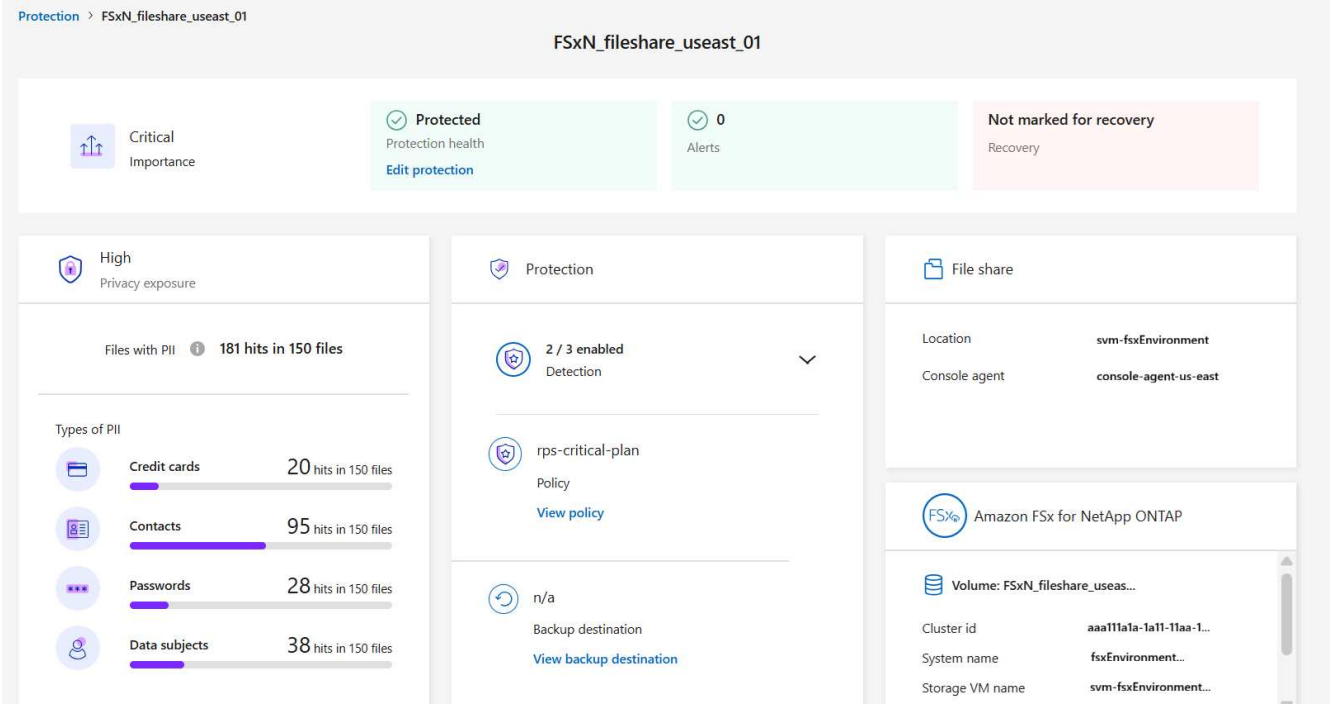
- **Élevé** : Plus de 70 % des fichiers contiennent des informations personnelles identifiables
- **Moyen** : Plus de 30 % et moins de 70 % des fichiers contiennent des informations personnelles identifiables
- **Faible** : Plus de 0 % et moins de 30 % des fichiers contiennent des informations personnelles identifiables

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Dans la page Protection, recherchez la charge de travail du partage de fichiers dans la colonne Charge de travail qui affiche un statut dans la colonne Exposition à la confidentialité.



3. Sélectionnez le lien de charge de travail dans la colonne Charge de travail pour voir les détails de la charge de travail.



4. Dans la page Détails de la charge de travail, examinez les détails de la mosaïque Exposition à la confidentialité.

Impact de l'exposition à la vie privée sur l'importance de la charge de travail

Les changements d'exposition à la confidentialité peuvent avoir un impact sur l'importance de la charge de travail.

En cas d'exposition à la vie privée :	À partir de cette exposition à la vie privée :	À cette exposition à la vie privée :	Ensuite, l'importance de la charge de travail fait ceci : .
Diminue	Élevé, moyen ou faible	Moyen, faible ou aucun	Reste le même
Augmente	Aucune	Faible	Reste au Standard
	Faible	Moyen	Changements de Standard à Important
	Faible ou moyen	Élevée	Changements de Standard ou Important à Critique

Pour plus d'informations

Pour plus de détails sur la classification des données, reportez-vous à la documentation sur la classification des données :

- "En savoir plus sur la classification des données"
- "Catégories de données privées"
- "Examinez les données stockées dans votre organisation"

Répondre et récupérer

Gérer les alertes dans NetApp Ransomware Resilience

Lorsque NetApp Ransomware Resilience détecte une attaque potentielle, une alerte s'affiche sur le tableau de bord et dans le menu Notifications. Ransomware Resilience prend immédiatement un snapshot. Lorsque vous recevez une alerte, examinez le risque potentiel dans l'onglet **Alerts** de Ransomware Resilience pour évaluer l'impact sur vos données et prévenir une éventuelle attaque de ransomware.

Si Ransomware Resilience détecte une attaque potentielle, une notification apparaît dans les paramètres de notification de la Console, et un courriel est envoyé aux adresses configurées. Le courriel contient des informations sur la gravité, la charge de travail impactée et un lien vers l'alerte dans l'onglet **Alerts** de Ransomware Resilience.

Vous pouvez ignorer les faux positifs ou décider de récupérer vos données immédiatement.

Si vous ignorez l'alerte, Ransomware Resilience apprend ce comportement, l'associe aux opérations normales et ne déclenche plus d'alerte.

Pour commencer à récupérer vos données, marquez l'alerte comme prête pour la récupération afin que votre administrateur de stockage puisse commencer le processus de récupération.

Chaque alerte peut inclure plusieurs incidents sur différents volumes et statuts. Passez en revue tous les incidents.

Comment les alertes sont générées

Ransomware Resilience s'appuie sur des données relatives aux modèles d'entropie des données, aux types d'extension de fichiers et au chiffrement pour produire des alertes. Les alertes sont basées sur les événements suivants :

- Violation de données
- Destruction de données
- Des extensions de fichiers ont été créées ou modifiées
- Création de fichier avec comparaison des taux détectés et attendus
- Suppression de fichiers avec comparaison des taux détectés et attendus
- Comportement utilisateur suspect
- Lorsque le cryptage est élevé, sans modification de l'extension de fichier

Pour les alertes de violation de données, de destruction de données et de comportement utilisateur suspect, vous devez configurer "détection de l'activité de l'utilisateur".

Types et statuts d'alerte

Les alertes ont l'un des deux statuts suivants : **New** ou **Inactive**.

Une alerte est classée comme l'un des types suivants :

- **Attaque potentielle** : Une alerte est classée comme attaque potentielle lorsque :
  - Autonomous Ransomware Protection détecte une nouvelle extension et l'occurrence se répète plus de 20 fois au cours des dernières 24 heures (comportement par défaut).
  - Des violations de données sont détectées.
  - Une destruction de données est détectée.
- **Avertissement** : Un avertissement se produit en fonction des comportements suivants :
  - La détection d'une nouvelle extension n'a pas été identifiée auparavant et le même comportement ne se répète pas suffisamment de fois pour le déclarer comme une attaque.
  - Une entropie élevée est observée.
  - L'activité de lecture, d'écriture, de renommage ou de suppression de fichiers a doublé par rapport aux niveaux normaux.

Pour les environnements SAN, les avertissements sont basés uniquement sur une entropie élevée.

Les preuves sont basées sur les informations de Autonomous Ransomware Protection dans ONTAP. Pour plus de détails, reportez-vous à "Présentation de la protection autonome contre les ransomwares" .

États d'alerte

Un incident d'alerte peut présenter les états suivants :

État	Description
Nouveau	Tous les incidents sont marqués « nouveaux » lorsqu'ils sont identifiés pour la première fois.
En cours de révision	Vous pouvez marquer manuellement un incident d'alerte comme « en cours d'examen » pendant que vous l'évaluez.
Rejeté	Si vous pensez qu'il ne s'agit pas d'une attaque de ransomware, vous pouvez changer le statut en « ignorée ». + ATTENTION : Après avoir ignoré une attaque, vous ne pouvez pas rétablir son statut. Si vous ignorez une charge de travail, toutes les copies de snapshots créées automatiquement en réponse à la potentielle attaque de ransomware seront définitivement supprimées.
Résolu	L'incident a été résolu.
Résolu automatiquement	Pour les alertes de faible priorité, l'incident est automatiquement résolu si aucune action n'a été entreprise à son sujet dans un délai de cinq jours.

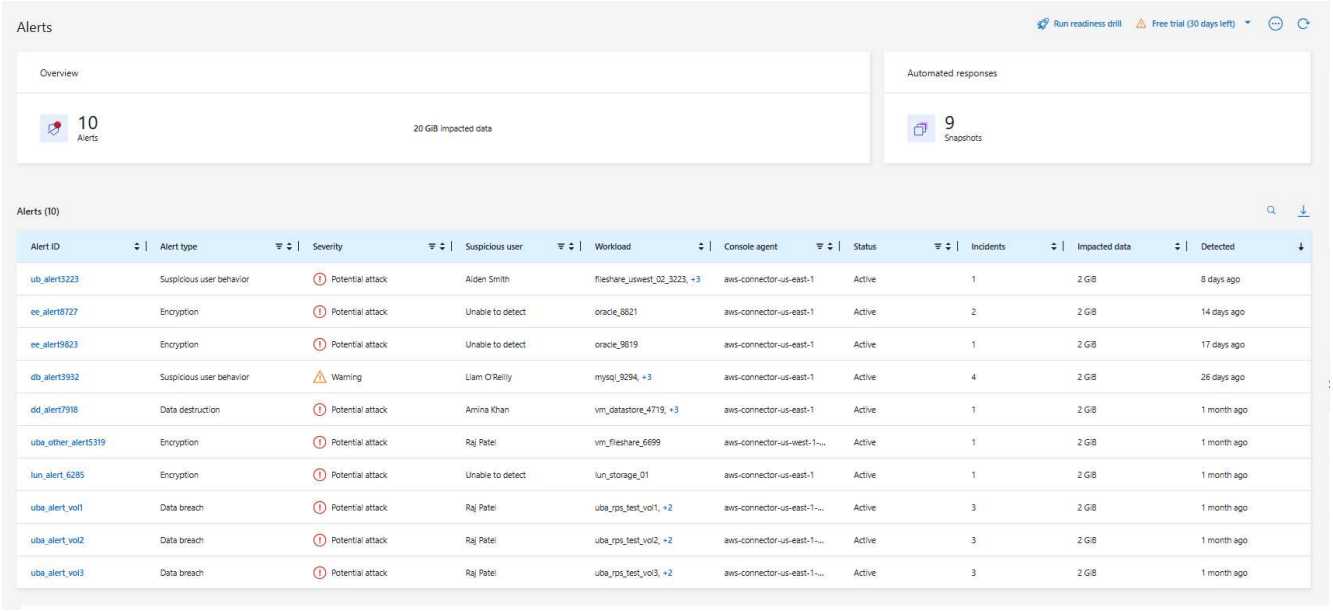
Afficher les alertes

Vous pouvez accéder aux alertes depuis le tableau de bord Ransomware Resilience ou depuis l'onglet **Alerts**.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

1. Dans le tableau de bord NetApp Ransomware Resilience, consultez le volet Alertes.
2. Sélectionnez **Afficher tout** sous l'un des statuts.
3. Sélectionnez une alerte pour examiner tous les incidents sur chaque volume pour chaque alerte.
4. Pour consulter des alertes supplémentaires, sélectionnez **Alerte** dans le fil d'Ariane en haut à gauche.
5. Consultez les alertes sur la page Alertes.



6. Continuez avec l'une des options suivantes :
   - Détecter les activités malveillantes et les comportements anormaux des utilisateurs .
   - Marquer les incidents de ransomware comme prêts à être récupérés (une fois les incidents neutralisés) .
   - Ignorer les incidents qui ne sont pas des attaques potentielles .

Répondre à un e-mail d'alerte

Lorsque Ransomware Resilience détecte une attaque potentielle, il envoie une notification par e-mail aux utilisateurs abonnés selon leurs préférences de notification d'abonnement configurées dans les paramètres de la NetApp Console. L'e-mail contient des informations sur l'alerte, y compris la gravité et les ressources impactées.

Pour configurer les notifications par e-mail dans la Console, consultez "Définir les paramètres de notification par e-mail".

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

1. Afficher l'e-mail.
2. Dans l'e-mail, sélectionnez **View alert** et connectez-vous à Ransomware Resilience.

La page Alertes apparaît.

3. Passez en revue tous les incidents sur chaque volume pour chaque alerte.
4. Pour consulter des alertes supplémentaires, sélectionnez **Alerte** dans le fil d'Ariane en haut à gauche.
5. Continuez avec l'une des options suivantes :
   - Détecter les activités malveillantes et les comportements anormaux des utilisateurs .
   - Marquer les incidents de ransomware comme prêts à être récupérés (une fois les incidents neutralisés) .
   - Ignorer les incidents qui ne sont pas des attaques potentielles .

Détecter les activités malveillantes et les comportements anormaux des utilisateurs

En consultant l'onglet Alertes, vous pouvez identifier s'il s'agit d'une activité malveillante ou d'un comportement anormal de l'utilisateur.

Pour afficher les alertes au niveau de l'utilisateur, vous devez avoir configuré un agent d'activité utilisateur et activé une stratégie de protection avec détection du comportement de l'utilisateur. La colonne **Utilisateur suspect** apparaît dans le tableau de bord Alertes uniquement lorsque la détection du comportement de l'utilisateur est activée. Pour activer la détection des utilisateurs suspects, voir "Activité utilisateur suspecte".

Afficher les activités malveillantes

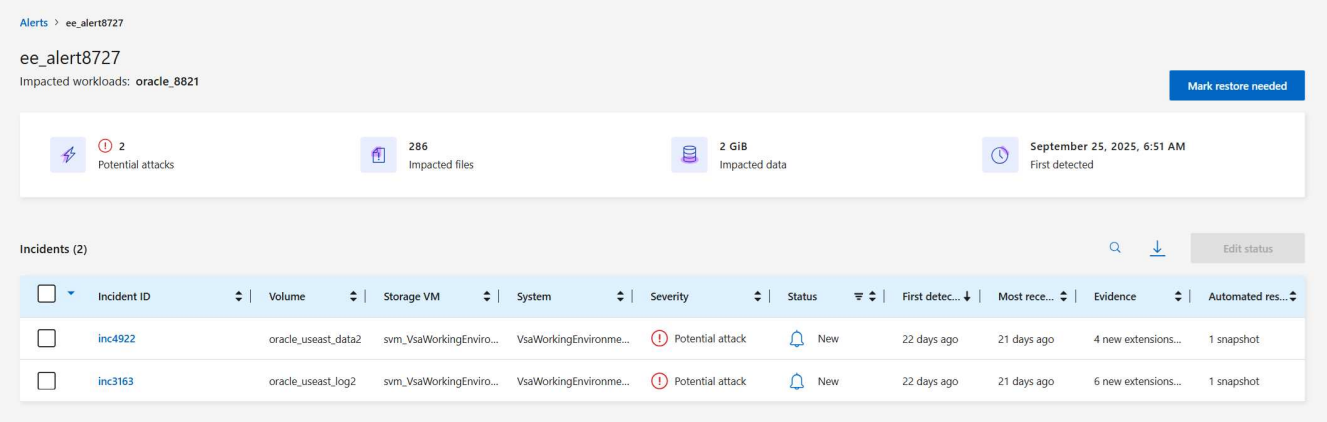
Lorsque la protection autonome contre les ransomwares déclenche une alerte dans NetApp Ransomware Resilience, vous pouvez consulter les détails suivants :

- Lorsque l'alerte a été déclenchée
- Lorsque l'accès a été modifié ou refusé
- Entropie des données entrantes
- Taux de création attendu de nouveaux fichiers par rapport au taux détecté
- Taux de suppression de fichiers attendu par rapport au taux détecté
- Taux de renommage attendu des fichiers par rapport au taux détecté
- Charges de travail, volumes, fichiers et répertoires impactés

> Ces détails sont visibles pour les charges de travail NAS. Pour les environnements SAN, seules les données d'entropie sont disponibles.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.
2. Sélectionnez une alerte.
3. Passez en revue les incidents dans l'alerte.



4. Sélectionnez un incident pour consulter les détails de l'incident.

Afficher le comportement anormal des utilisateurs

Si vous avez configuré la détection des utilisateurs suspects pour visualiser les comportements anormaux des utilisateurs, vous pouvez consulter les données au niveau de l'utilisateur et bloquer des utilisateurs spécifiques. Pour activer les paramètres relatifs aux utilisateurs suspects, voir "Configurer les agents et les collecteurs pour la détection de l'activité des utilisateurs".

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.
2. Sélectionnez une alerte.
3. Passez en revue les incidents dans l'alerte.
   a. Pour bloquer un utilisateur suspect dans votre environnement, sélectionnez **Block** à côté du nom de l'utilisateur.
   b. Pour désactiver les alertes concernant un utilisateur faisant l'objet d'une alerte que vous savez être fausse, sélectionnez les trois points (… puis **Exclure cet utilisateur de la surveillance**. Examinez la boîte de dialogue, puis sélectionnez **Exclure** pour confirmer.

> Pour réactiver les alertes d'un utilisateur, renvoyez l'alerte. Sélectionnez les trois points, puis **Inclure cet utilisateur dans la surveillance**. Vous pouvez également "Exclure les utilisateurs" depuis la surveillance.

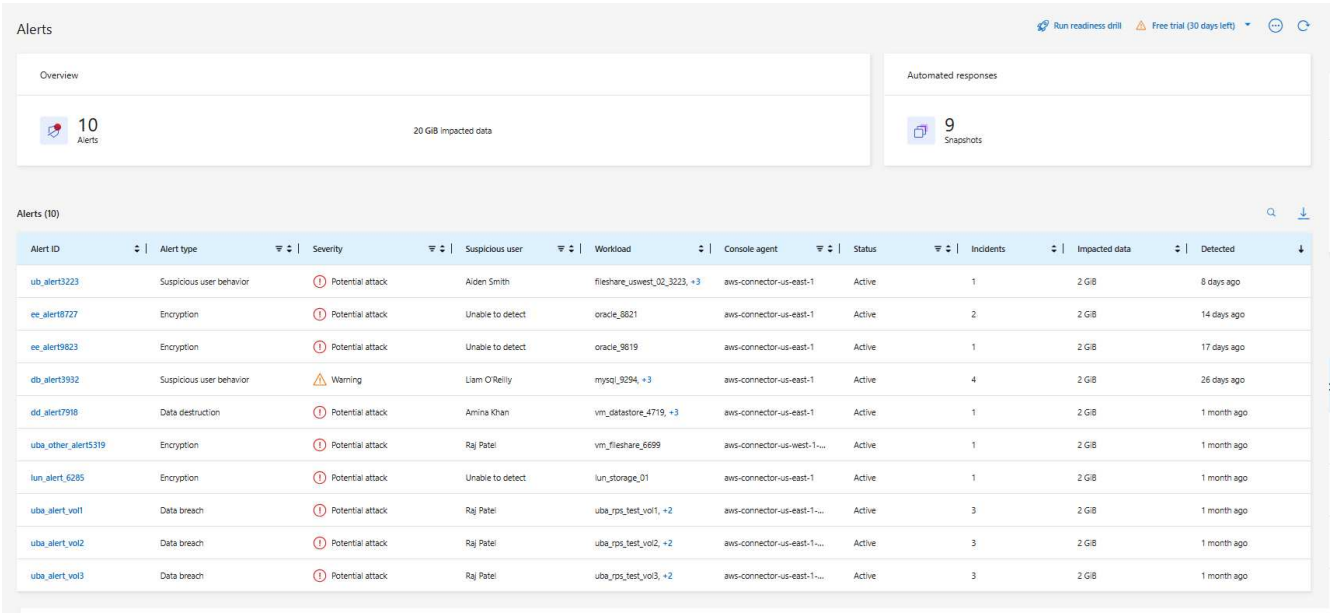
Marquer les incidents de ransomware comme prêts à être récupérés (une fois les incidents neutralisés)

Après avoir arrêté l'attaque, informez votre administrateur de stockage que les données sont prêtes afin qu'il puisse lancer le processus de récupération.

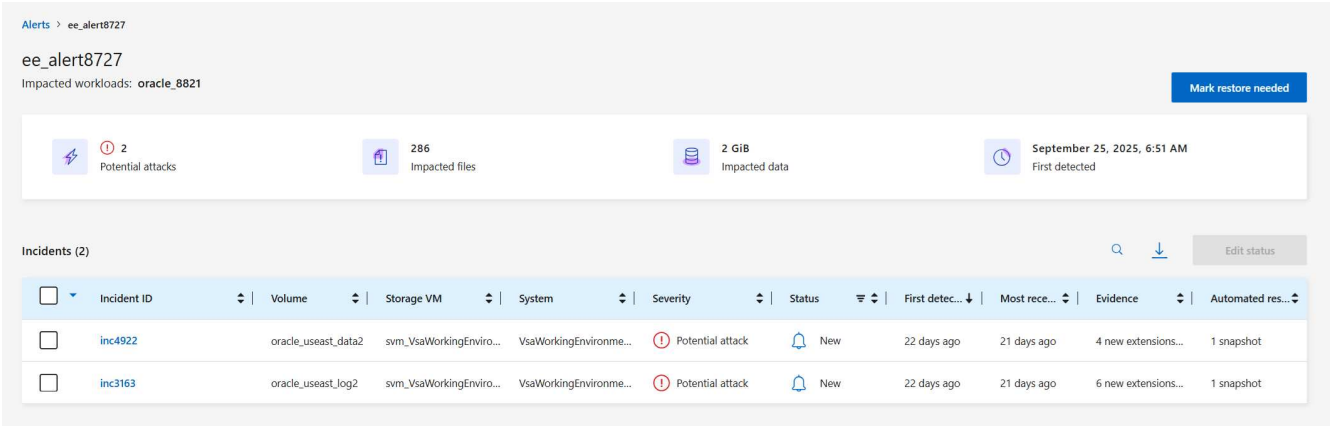
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.



2. Dans la page Alertes, sélectionnez l'alerte.
3. Passez en revue les incidents dans l'alerte.



4. Si vous déterminez que les incidents sont prêts à être récupérés, sélectionnez **Marquer comme restauration nécessaire**.
5. Confirmez l'action et sélectionnez **Marquer comme restauration nécessaire**.
6. Pour lancer la récupération de la charge de travail, sélectionnez **Récupérer** la charge de travail dans le message ou sélectionnez l'onglet **Récupération**.

Résultat

Une fois l'alerte marquée pour restauration, elle passe de l'onglet Alertes à l'onglet Récupération.

Ignorer les incidents qui ne sont pas des attaques potentielles

Après avoir examiné les incidents, vous devez déterminer si les incidents constituent des attaques potentielles. Si elles ne constituent pas de véritables menaces, elles peuvent être ignorées.

Vous pouvez ignorer les faux positifs ou décider de récupérer vos données immédiatement. Si vous ignorez l'alerte, Ransomware Resilience apprend ce comportement et l'associe à un fonctionnement normal, et ne déclenche plus d'alerte pour un tel comportement.

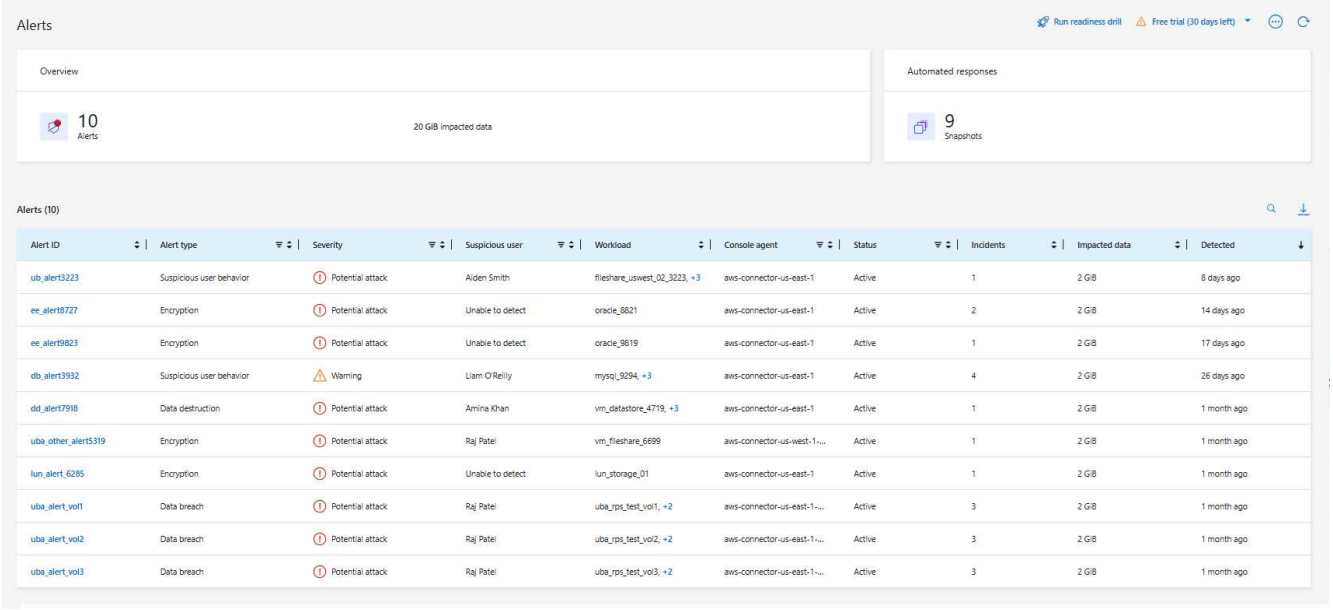
Si vous supprimez une charge de travail, toutes les copies instantanées prises automatiquement en réponse à une attaque potentielle de ransomware sont définitivement supprimées.

Si vous ignorez une alerte, vous ne pouvez pas modifier son statut ni annuler cette modification.

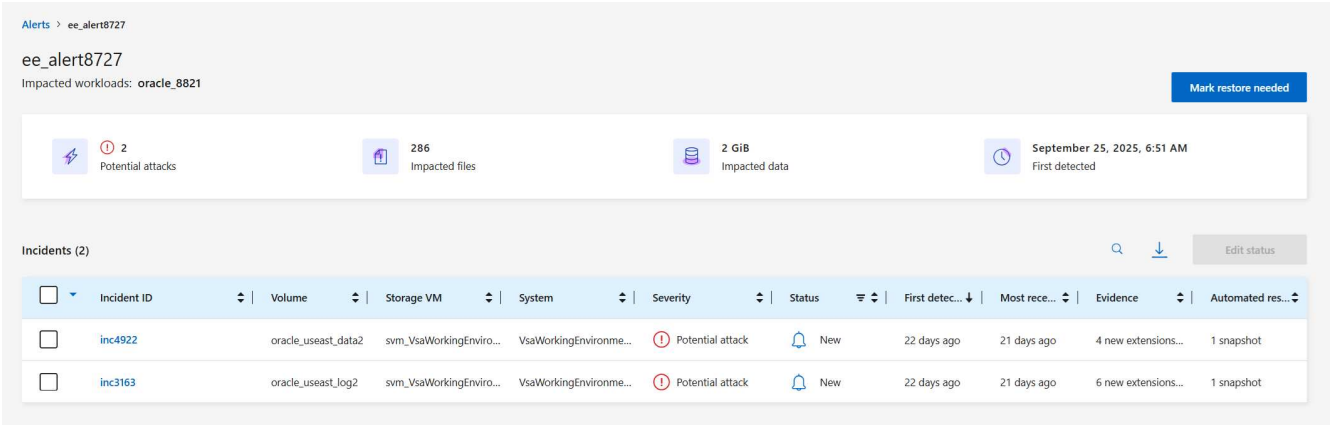
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

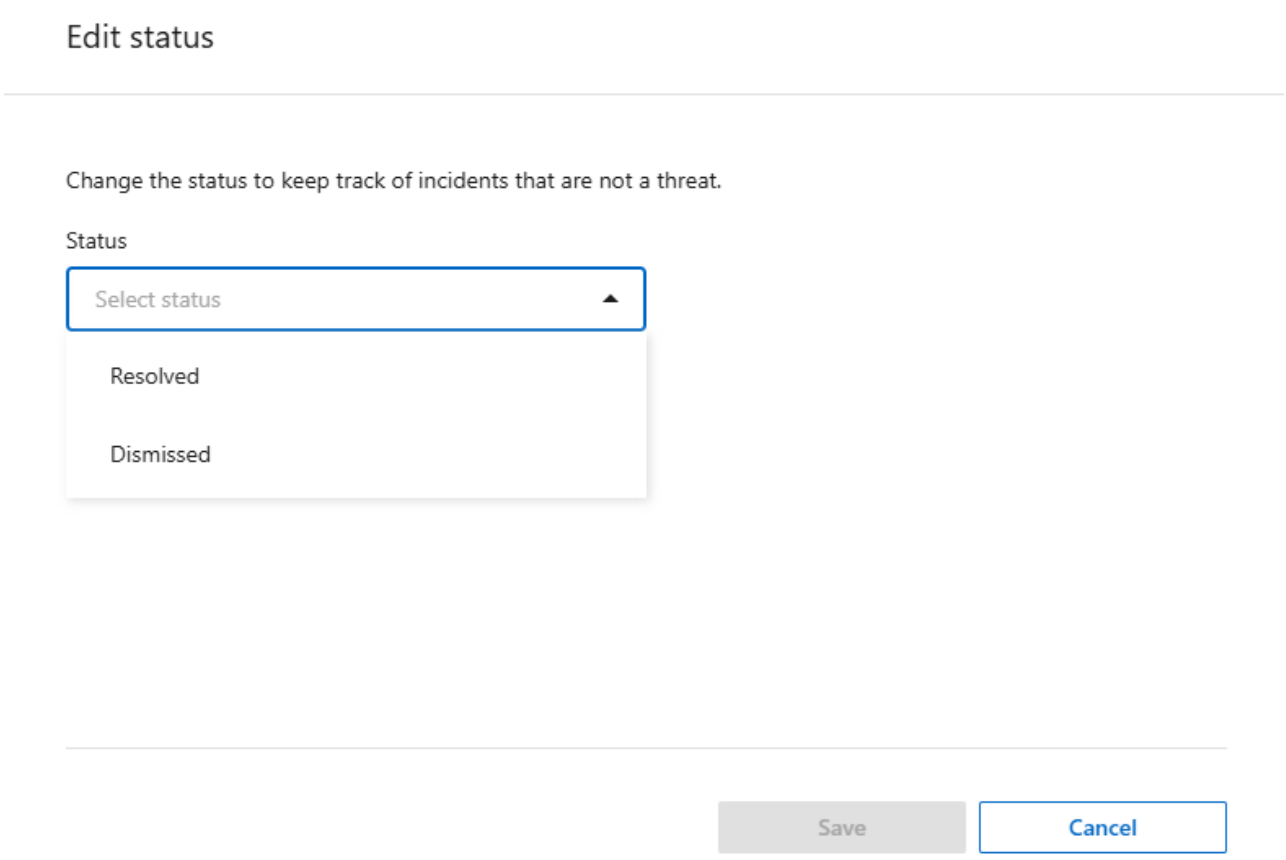
1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.



2. Dans la page Alertes, sélectionnez l'alerte.



3. Sélectionnez un ou plusieurs incidents. Vous pouvez également sélectionner tous les incidents en cochant la case « ID de l'incident » en haut à gauche du tableau.
4. Si vous déterminez que l'incident ne constitue pas une menace, considérez-le comme un faux positif :
   - Sélectionnez l'incident.
   - Sélectionnez le bouton **Modifier le statut** au-dessus du tableau.



5. Dans la boîte de dialogue Modifier le statut, choisissez le statut **Rejeté**.

   Des informations supplémentaires concernant la charge de travail et la suppression des copies d'instantané apparaissent.

6. Sélectionnez **Enregistrer**.

   Le statut de l'incident ou des incidents passe à « Classé sans suite ».

Afficher la liste des fichiers concernés

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez afficher une liste des fichiers impactés. Vous pouvez accéder à la page Alertes pour télécharger une liste des fichiers impactés. Utilisez ensuite la page de récupération pour télécharger la liste et choisir les fichiers à restaurer.

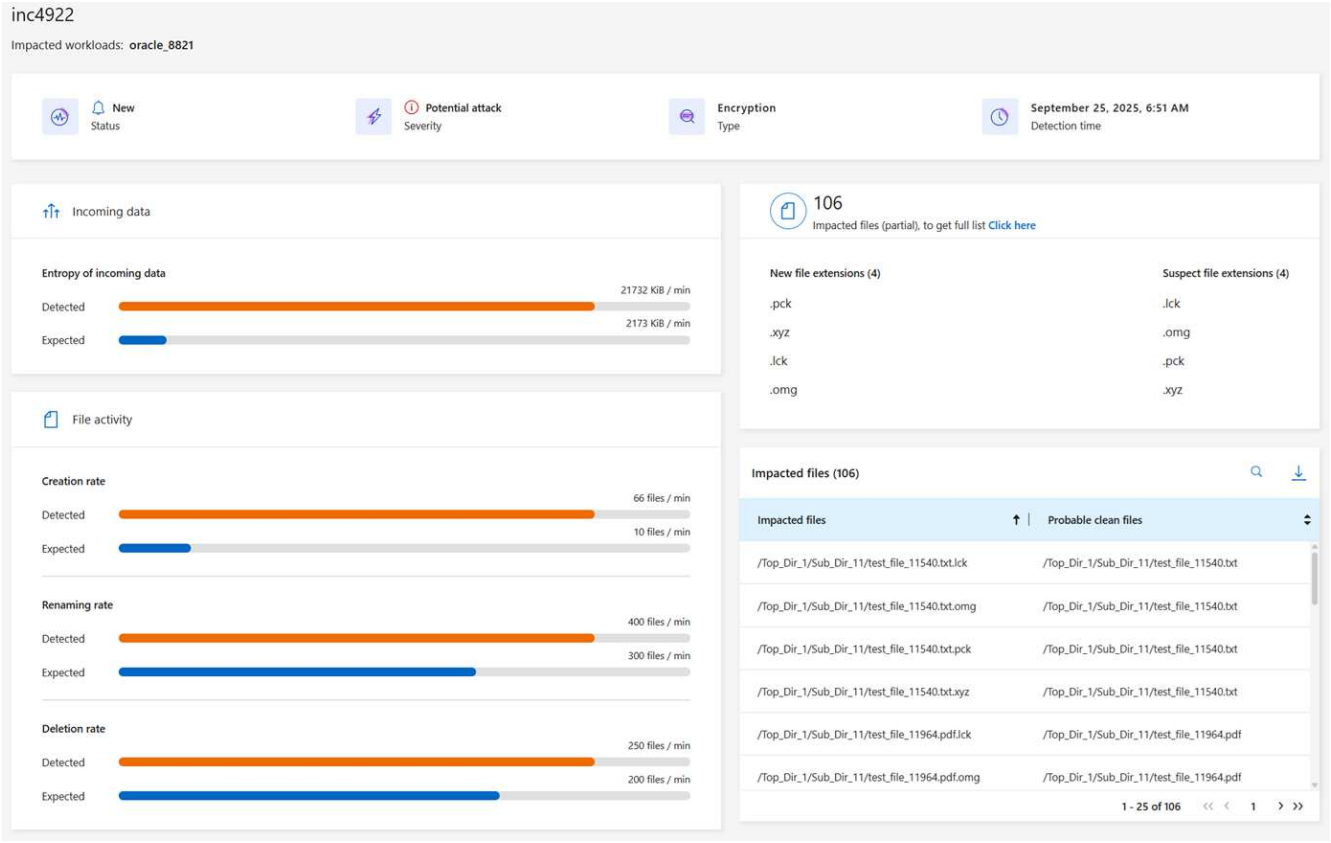
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

Utilisez la page Alertes pour récupérer la liste des fichiers impactés.

Si un volume comporte plusieurs alertes, vous devrez peut-être télécharger la liste CSV des fichiers concernés pour chaque alerte.

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.
2. Sur la page Alertes, triez les résultats par charge de travail pour afficher les alertes pour la charge de travail d'application que vous souhaitez restaurer.
3. Dans la liste des alertes pour cette charge de travail, sélectionnez une alerte.
4. Pour cette alerte, sélectionnez un seul incident.



5. Pour cet incident, sélectionnez l'icône de téléchargement pour télécharger la liste des fichiers impactés au format CSV.

Récupérez après une attaque de ransomware (après neutralisation des incidents) avec NetApp Ransomware Resilience

Une fois les charges de travail marquées « Restauration nécessaire », NetApp Ransomware Resilience recommande un point de récupération réel (RPA) et orchestre le flux de travail pour une récupération résistante aux pannes.

- Si l'application ou la VM est gérée par NetApp Backup and Recovery ou Ransomware Resilience, Ransomware Resilience effectue une restauration cohérente en cas de panne, où toutes les données qui se trouvaient dans le volume au même moment sont restaurées, par exemple, si le système a planté.

  Vous pouvez restaurer la charge de travail en sélectionnant tous les volumes, des volumes spécifiques ou des fichiers spécifiques.

La récupération de la charge de travail peut avoir un impact sur les charges de travail en cours d'exécution. Vous devez coordonner les processus de récupération avec les parties prenantes appropriées.

Une charge de travail peut avoir l'un des états de restauration suivants :

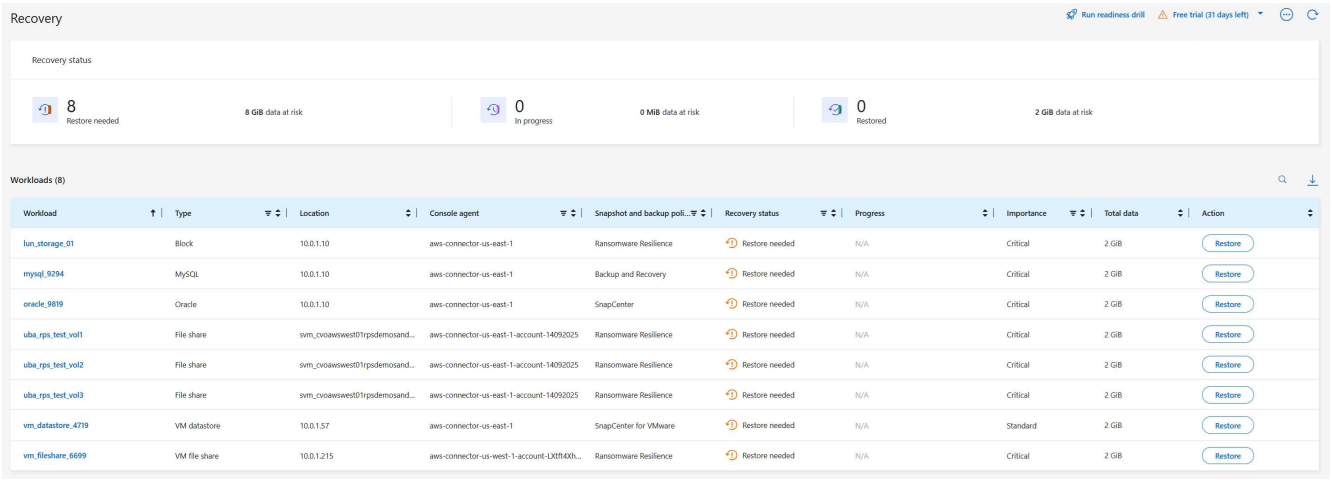
- **Restauration nécessaire** : La charge de travail doit être restaurée.
- **En cours** : L'opération de restauration est actuellement en cours.
- **Restauré** : La charge de travail a été restaurée.
- **Échec** : le processus de restauration de la charge de travail n'a pas pu être terminé.

Afficher les charges de travail prêtes à être restaurées

Passez en revue les charges de travail qui sont dans l'état de récupération « Restauration nécessaire ».

Étapes

1. Effectuez l'une des opérations suivantes :
   - Depuis le tableau de bord, consultez les totaux « Restore needed » dans le volet Alertes et sélectionnez **View all**.
   - Dans le menu, sélectionnez **Récupération**.
2. Consultez les informations sur la charge de travail dans la page **Récupération**.



Restaurer une charge de travail

Grâce à Ransomware Resilience, l'administrateur de stockage peut déterminer la meilleure façon de restaurer les charges de travail à partir du point de restauration recommandé ou du point de restauration préféré.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

L'administrateur du stockage de sécurité peut récupérer des données à différents niveaux :

- Récupérer tous les volumes
- Récupérer une application au niveau du volume ou au niveau du fichier et du dossier.
- Récupérer un partage de fichiers au niveau du volume, du répertoire ou du fichier/dossier.
- Récupérer à partir d'une banque de données au niveau d'une machine virtuelle.

Le processus diffère selon le type de charge de travail.

Étapes

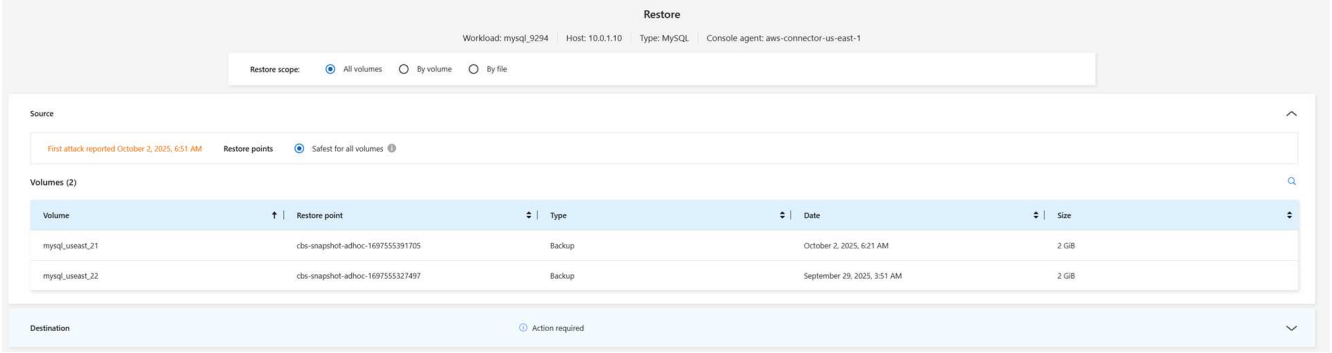
1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Consultez les informations sur la charge de travail dans la page **Récupération**.
3. Sélectionnez une charge de travail qui est dans l'état « Restauration nécessaire ».
4. Pour restaurer, sélectionnez **Restaurer**.
5. **Étendue de la restauration** : sélectionnez le type de restauration que vous souhaitez effectuer :
   - Tous les volumes
   - En volume
   - Par fichier : vous pouvez spécifier un dossier ou des fichiers uniques à restaurer.

   Pour les charges de travail SAN, vous ne pouvez restaurer que par charge de travail.

   Vous pouvez sélectionner jusqu'à 100 fichiers ou un seul dossier.
6. Continuez avec l'une des procédures suivantes selon que vous avez choisi l'application, le volume ou le fichier.

Restaurer tous les volumes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Sélectionnez une charge de travail qui est dans l'état « Restauration nécessaire ».
3. Pour restaurer, sélectionnez **Restaurer**.
4. Sur la page Restaurer, dans l'étendue de la restauration, sélectionnez **Tous les volumes**.



5. **Source** : Sélectionnez la flèche vers le bas à côté de Source pour voir les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

   Ransomware Resilience identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et affiche une indication « Le plus sûr pour tous les volumes ». Cela signifie que tous les volumes seront restaurés à partir d'une copie antérieure à la première attaque sur le premier volume détecté.
6. **Destination** : Sélectionnez la flèche vers le bas à côté de Destination pour voir les détails.
   a. Sélectionnez le système.
   b. Sélectionnez la machine virtuelle de stockage.

c. Sélectionnez l'agrégat.

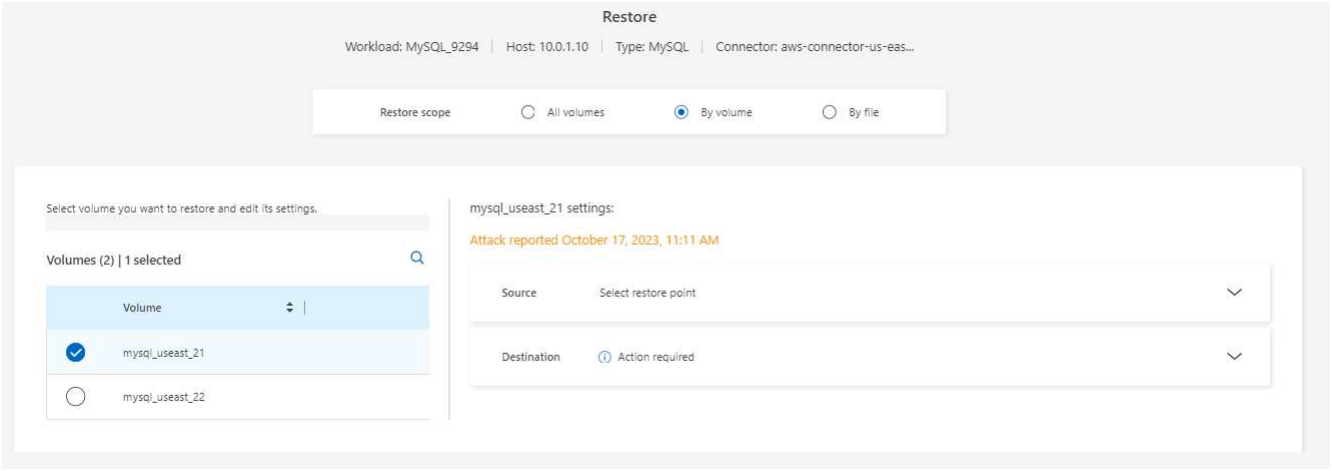
d. Modifiez le préfixe de volume qui sera ajouté à tous les nouveaux volumes.

> Le nouveau nom de volume apparaît sous la forme préfixe + nom de volume d'origine + nom de sauvegarde + date de sauvegarde.

7. Sélectionnez **Enregistrer**.
8. Sélectionnez **Suivant**.
9. Revoyez vos sélections.
10. Sélectionnez **Restaurer**.
11. Dans le menu supérieur, sélectionnez **Récupération** pour examiner la charge de travail sur la page de récupération où l'état de l'opération se déplace à travers les états.

Restaurer une charge de travail d'application au niveau du volume

1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Sélectionnez une charge de travail d'application qui est dans l'état « Restauration nécessaire ».
3. Pour restaurer, sélectionnez **Restaurer**.
4. Sur la page Restaurer, dans l'étendue de la restauration, sélectionnez **Par volume**.



5. Dans la liste des volumes, sélectionnez le volume que vous souhaitez restaurer.
6. **Source** : Sélectionnez la flèche vers le bas à côté de Source pour voir les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

> Ransomware Resilience identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et affiche une indication « Recommandé ».

7. **Destination** : Sélectionnez la flèche vers le bas à côté de Destination pour voir les détails.
   a. Sélectionnez le système.
   b. Sélectionnez la machine virtuelle de stockage.
   c. Sélectionnez l'agrégat.
   d. Vérifiez le nouveau nom du volume.

Le nouveau nom de volume apparaît comme le nom du volume d'origine + le nom de la sauvegarde + la date de sauvegarde.

8. Sélectionnez **Enregistrer**.
9. Sélectionnez **Suivant**.
10. Revoyez vos sélections.
11. Sélectionnez **Restaurer**.
12. Dans le menu supérieur, sélectionnez **Récupération** pour examiner la charge de travail sur la page de récupération où l'état de l'opération se déplace à travers les états.

Restaurer une charge de travail d'application au niveau du fichier

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez afficher une liste des fichiers impactés. Vous pouvez accéder à la page Alertes pour télécharger une liste des fichiers impactés. Utilisez ensuite la page de récupération pour télécharger la liste et choisir les fichiers à restaurer.

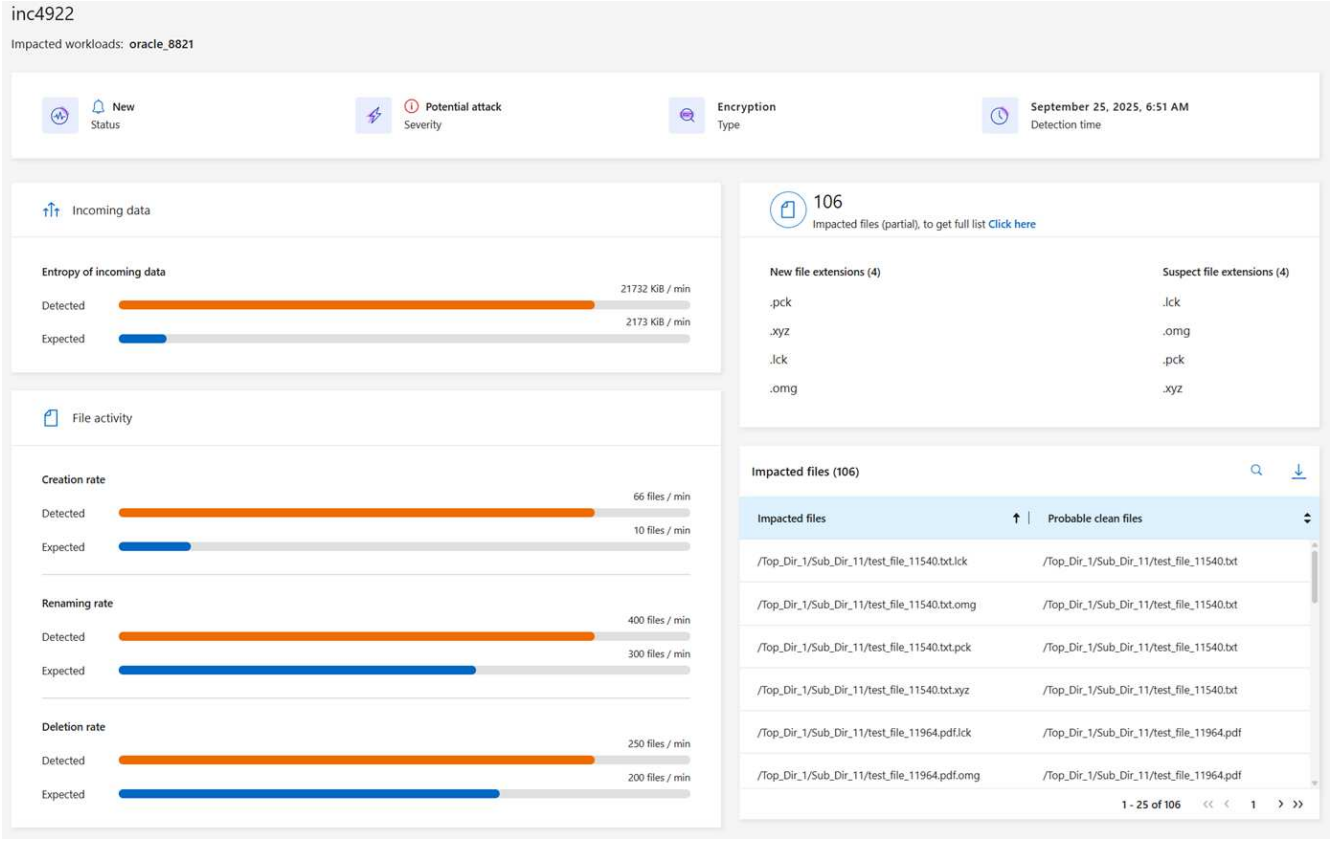
Vous pouvez restaurer une charge de travail d'application au niveau du fichier sur le même système ou sur un système différent.

Étapes pour obtenir la liste des fichiers impactés

Utilisez la page Alertes pour récupérer la liste des fichiers impactés.

Si un volume comporte plusieurs alertes, vous devrez télécharger la liste CSV des fichiers impactés pour chaque alerte.

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.
2. Sur la page Alertes, triez les résultats par charge de travail pour afficher les alertes pour la charge de travail d'application que vous souhaitez restaurer.
3. Dans la liste des alertes pour cette charge de travail, sélectionnez une alerte.
4. Pour cette alerte, sélectionnez un seul incident.



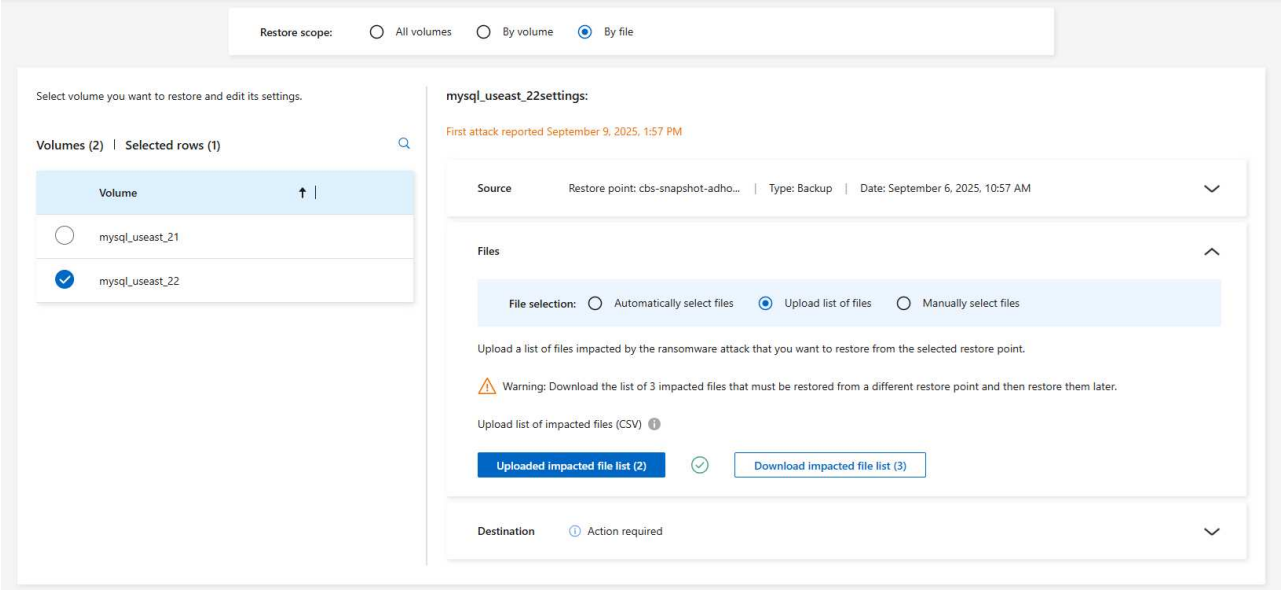
5. Pour voir la liste complète des fichiers, sélectionnez **Cliquez ici** en haut du volet Fichiers concernés.
6. Pour cet incident, sélectionnez l'icône de téléchargement et téléchargez la liste des fichiers impactés au format CSV.

Étapes pour restaurer ces fichiers

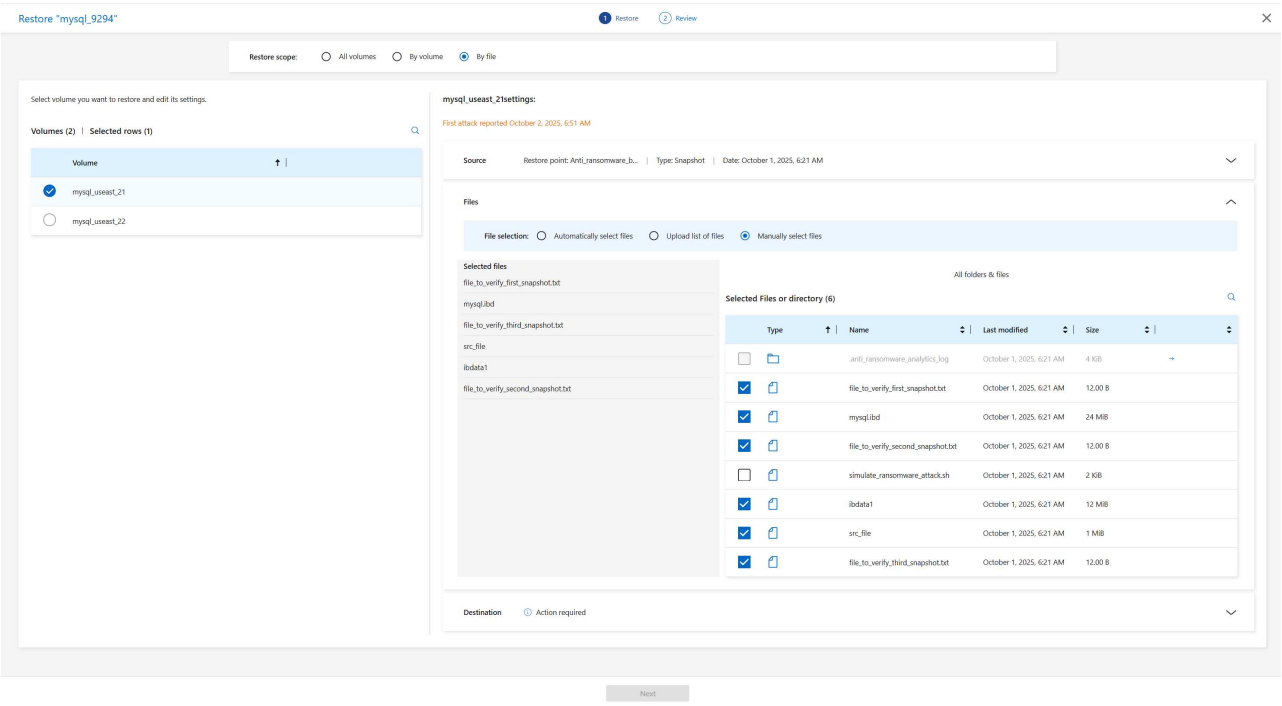
1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Sélectionnez une charge de travail d'application qui est dans l'état « Restauration nécessaire ».
3. Pour restaurer, sélectionnez **Restaurer**.
4. Sur la page Restaurer, dans l'étendue Restaurer, sélectionnez **Par fichier**.
5. Dans la liste des volumes, sélectionnez le volume qui contient les fichiers que vous souhaitez restaurer.
6. **Point de restauration** : sélectionnez la flèche vers le bas à côté de **Point de restauration** pour voir les détails. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

> La colonne Raison du volet Points de restauration indique la raison de l'instantané ou de la sauvegarde comme étant « Planifiée » ou « Réponse automatisée à un incident de ransomware ».

7. **Fichiers**:
   - **Sélectionner automatiquement les fichiers** : laissez Ransomware Resilience sélectionner les fichiers à restaurer.
   - **Télécharger la liste des fichiers** : Téléchargez un fichier CSV contenant la liste des fichiers impactés que vous avez reçus de la page Alertes ou que vous possédez. Vous pouvez restaurer jusqu'à 10 000 fichiers à la fois.



- **Sélectionner manuellement les fichiers** : sélectionnez jusqu'à 10 000 fichiers ou un seul dossier à restaurer.



Si des fichiers ne peuvent pas être restaurés à l'aide du point de restauration sélectionné, un message apparaît indiquant le nombre de fichiers qui ne peuvent pas être restaurés et vous permet de télécharger la liste de ces fichiers en sélectionnant **Télécharger la liste des fichiers impactés**.

8. **Destination** : Sélectionnez la flèche vers le bas à côté de Destination pour voir les détails.
   a. Choisissez où restaurer les données : emplacement source d'origine ou un autre emplacement que vous pouvez spécifier.

Bien que les fichiers ou répertoires d'origine soient écrasés par les données restaurées, les noms de fichiers et de dossiers d'origine restent les mêmes, sauf si vous spécifiez de nouveaux noms.

b. Sélectionnez le système.

c. Sélectionnez la machine virtuelle de stockage.

d. Saisissez éventuellement le chemin.

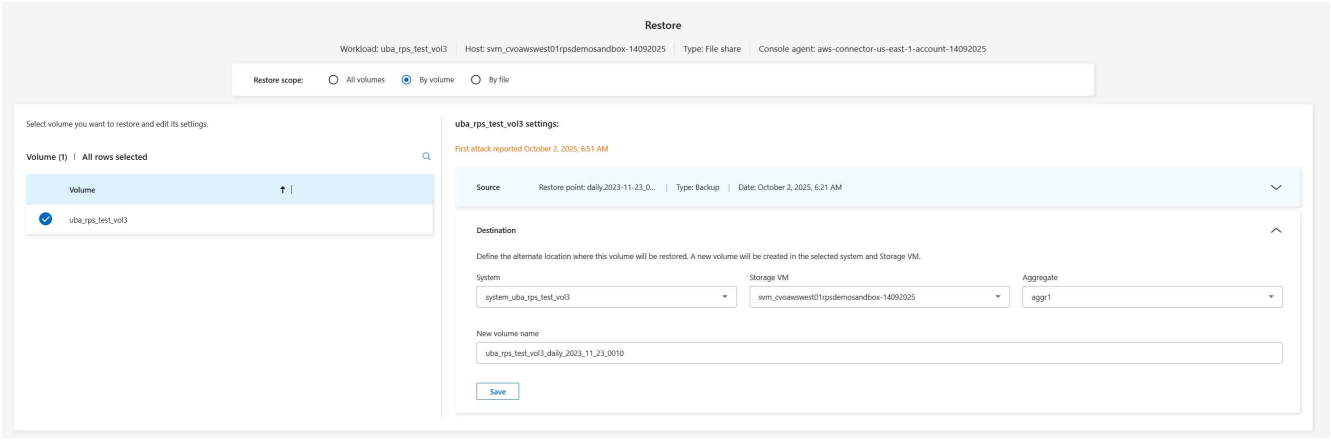
Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

e. Sélectionnez si vous souhaitez que les noms des fichiers ou du répertoire restaurés soient les mêmes que ceux de l'emplacement actuel ou des noms différents.

9. Sélectionnez **Suivant**.
10. Revoyez vos sélections.
11. Sélectionnez **Restaurer**.
12. Dans le menu supérieur, sélectionnez **Récupération** pour examiner la charge de travail sur la page de récupération où l'état de l'opération se déplace à travers les états.

Restaurer un partage de fichiers ou une banque de données

1. Après avoir sélectionné un partage de fichiers ou une banque de données à restaurer, sur la page Restaurer, dans l'étendue de la restauration, sélectionnez **Par volume**.



2. Dans la liste des volumes, sélectionnez le volume que vous souhaitez restaurer.
3. **Source** : Sélectionnez la flèche vers le bas à côté de Source pour voir les détails.

a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

Ransomware Resilience identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et affiche une indication « Recommandé ».

4. **Destination** : Sélectionnez la flèche vers le bas à côté de Destination pour voir les détails.

a. Choisissez où restaurer les données : emplacement source d'origine ou un autre emplacement que vous pouvez spécifier.

Bien que les fichiers ou répertoires d'origine soient écrasés par les données restaurées, les noms de fichiers et de dossiers d'origine restent les mêmes, sauf si vous spécifiez de nouveaux noms.

b. Sélectionnez le système.

c. Sélectionnez la machine virtuelle de stockage.

d. Saisissez éventuellement le chemin.

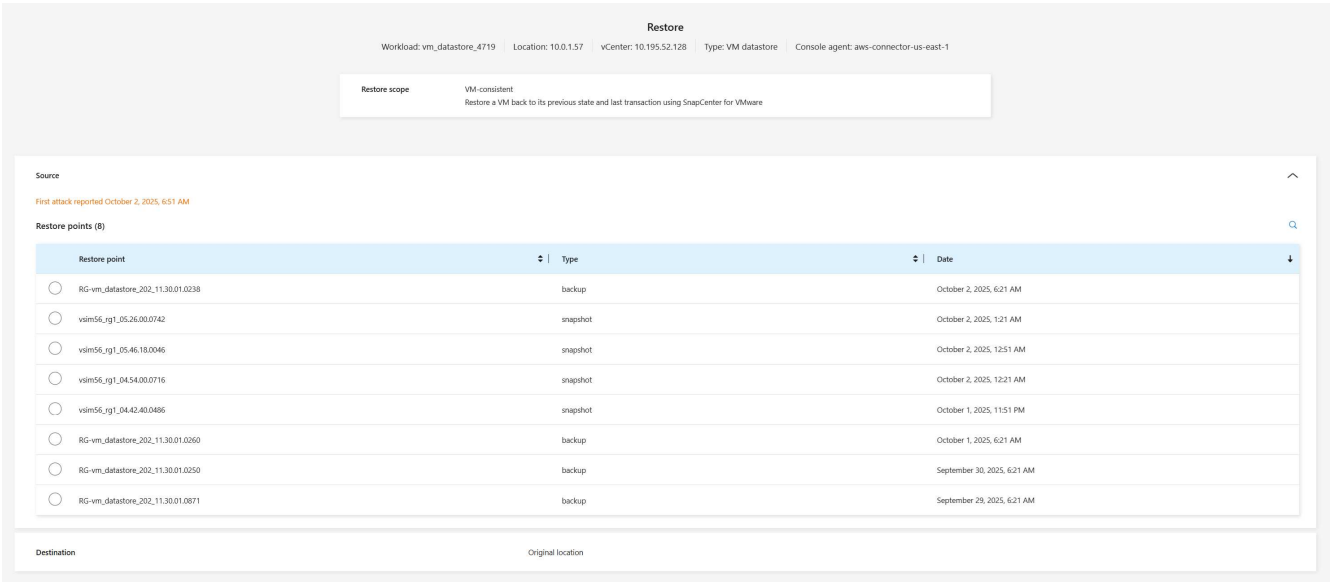
Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

5. Sélectionnez **Enregistrer**.
6. Revoyez vos sélections.
7. Sélectionnez **Restaurer**.
8. Dans le menu, sélectionnez **Récupération** pour examiner la charge de travail sur la page de récupération où l'état de l'opération se déplace à travers les états.

Restaurer un partage de fichiers VM au niveau de la VM

Sur la page de récupération, après avoir sélectionné une machine virtuelle à restaurer, continuez avec ces étapes.

1. **Source** : Sélectionnez la flèche vers le bas à côté de Source pour voir les détails.



2. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.
3. **Destination** : Vers l'emplacement d'origine.
4. Sélectionnez **Suivant**.
5. Revoyez vos sélections.
6. Sélectionnez **Restaurer**.
7. Dans le menu, sélectionnez **Récupération** pour examiner la charge de travail sur la page de récupération où l'état de l'opération se déplace à travers les états.

Effectuez un exercice de préparation aux attaques de ransomware dans NetApp Ransomware Resilience

Exécutez un exercice de préparation à une attaque par ransomware en simulant une attaque sur un nouvel exemple de charge de travail. Enquêter sur l'attaque simulée et récupérer la charge de travail. Utilisez cette fonctionnalité pour tester les notifications d'alerte, la réponse et la récupération. Exécutez l'exercice aussi souvent que nécessaire.

Vos données de charge de travail réelles ne sont pas affectées.

Vous pouvez exécuter des exercices de préparation sur les charges de travail NFS et CIFS (SMB).

Configurer un exercice de préparation aux attaques de ransomware

Avant d'exécuter une simulation, configurez un exercice sur la page Paramètres. Accédez à la page Paramètres à partir de l'option Actions dans le menu supérieur.

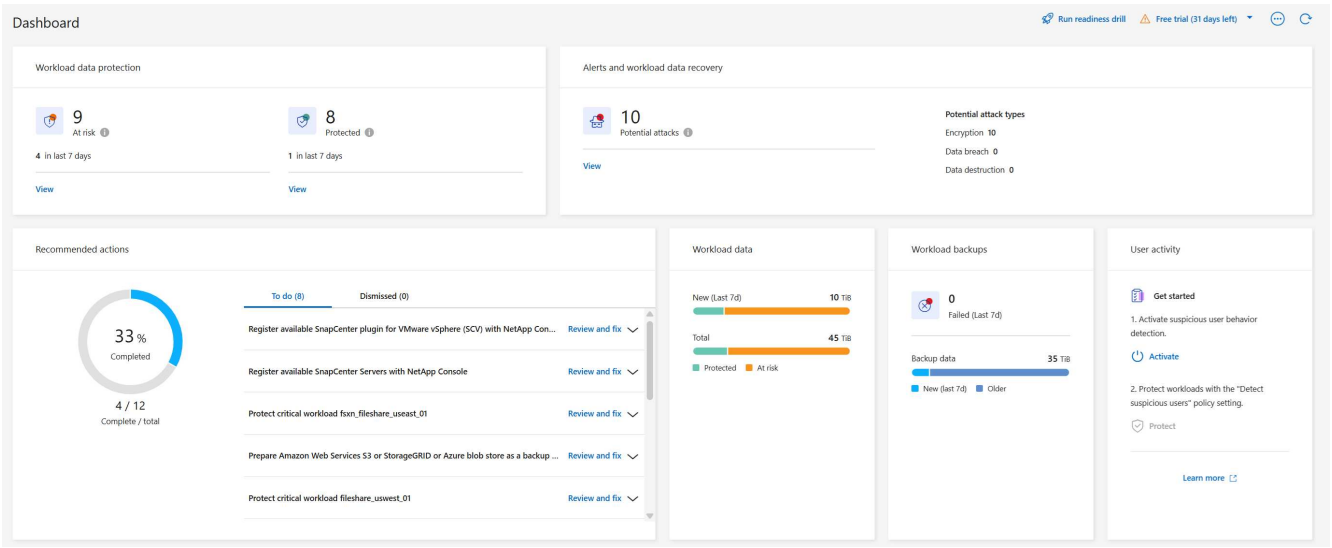
Vous devez saisir un nom d'utilisateur et un mot de passe dans les situations suivantes :

- Si des modifications du nom d'utilisateur ou du mot de passe ont eu lieu pour la machine virtuelle de stockage précédemment sélectionnée
- Si vous sélectionnez une autre machine virtuelle de stockage CIFS (SMB)
- Si vous entrez un nom de charge de travail de test différent

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

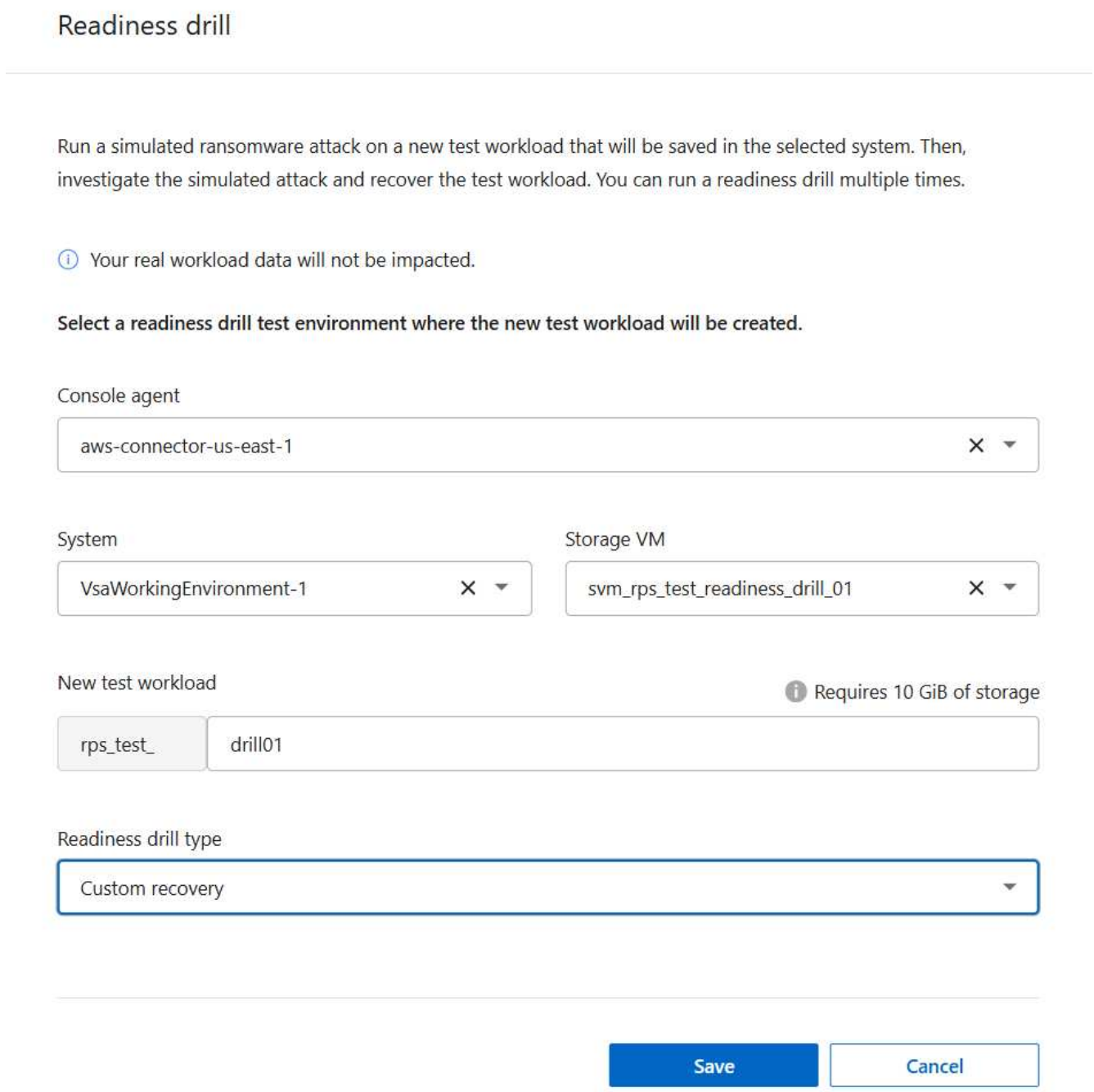
Étapes

1. Dans le menu NetApp Ransomware Resilience , sélectionnez le bouton **Exécuter l'exercice de préparation** en haut à droite.



2. Dans la carte d'exercice de préparation sur la page Paramètres, sélectionnez **Configurer**.

La console affiche la page Configurer l'exercice de préparation.



3. Procédez comme suit :
   a. Sélectionnez l'agent de console que vous souhaitez utiliser pour l'exercice de préparation.
   b. Sélectionnez un système de test.
   c. Sélectionnez un SVM de stockage de test.
   d. Si vous avez sélectionné une machine virtuelle de stockage CIFS (SMB), les champs **Nom d'utilisateur** et **Mot de passe** s'affichent. Saisissez le nom d'utilisateur et le mot de passe de la machine virtuelle de stockage.
   e. Sélectionnez le type d'exercice de préparation. Pour une récupération manuelle après une violation de

données de chiffrement, choisissez **Récupération personnalisée**. Pour récupérer une activité utilisateur suspecte, choisissez **Violation de données**.

f. Saisissez le nom d'une nouvelle charge de travail de test à créer. N'incluez pas de tirets dans le nom.

4. Sélectionnez **Enregistrer**.

Vous pouvez modifier la configuration de l'exercice de préparation ultérieurement à l'aide de la page Paramètres.

Démarrer un exercice de préparation

Après avoir configuré l'exercice de préparation, vous pouvez démarrer l'exercice.

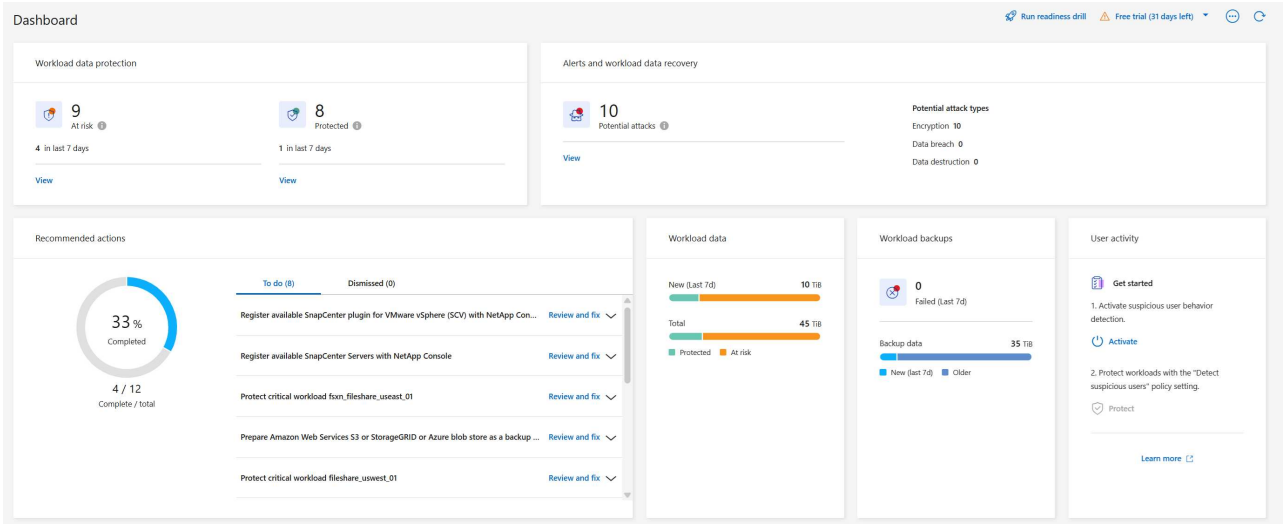
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Lorsque vous démarrez l'exercice de préparation, Ransomware Resilience ignore le mode d'apprentissage et démarre l'exercice en mode actif. L'état de détection de la charge de travail est Actif.

Une charge de travail peut avoir un statut de détection de ransomware **Mode d'apprentissage** lorsqu'une politique de détection est récemment attribuée et que Ransomware Resilience analyse les charges de travail.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Dans le menu Résilience aux ransomwares, sélectionnez le bouton **Exécuter l'exercice de préparation** en haut à droite.



   - OU, à partir de la page Paramètres, dans la carte d'exercice de préparation, sélectionnez **Démarrer**.

Vous ne pouvez pas modifier la configuration de l'exercice de préparation pendant que l'exercice est en cours d'exécution. Vous pouvez réinitialiser la perceuse pour l'arrêter et modifier la configuration.

Répondre à une alerte d'exercice de préparation

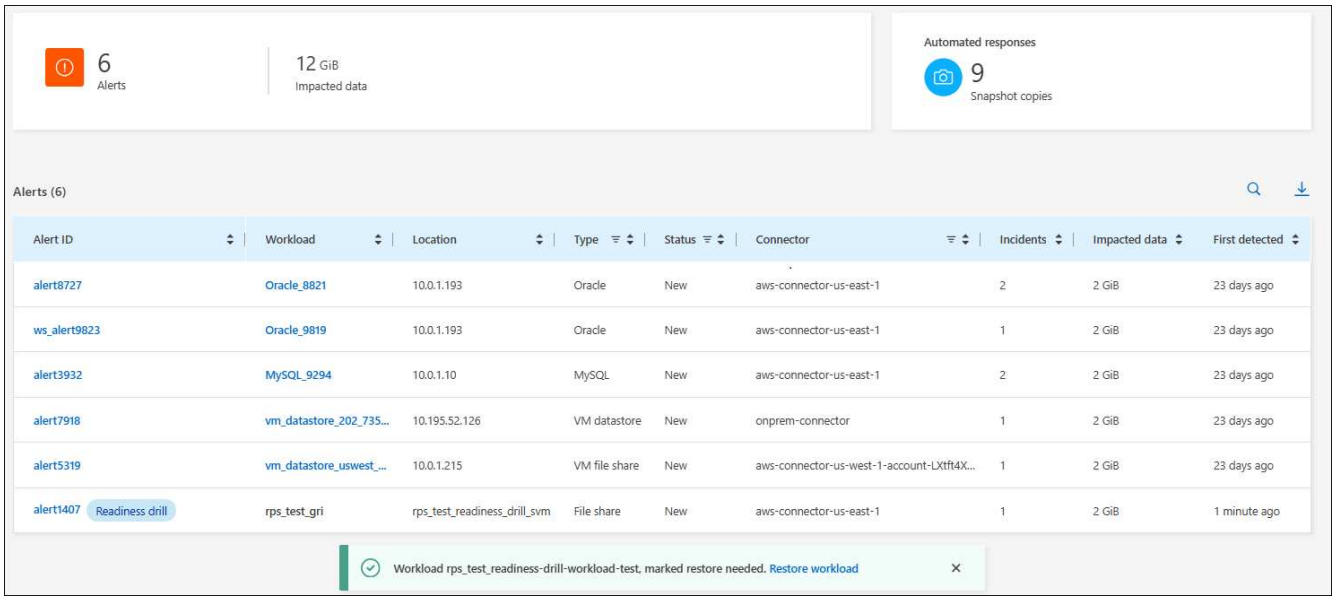
Testez votre état de préparation en répondant à une alerte d'exercice de préparation.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

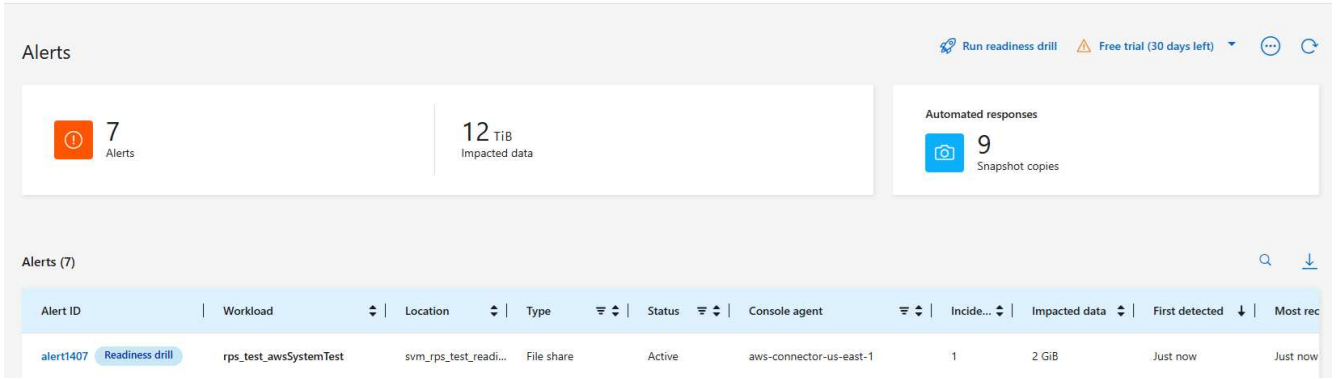
Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.

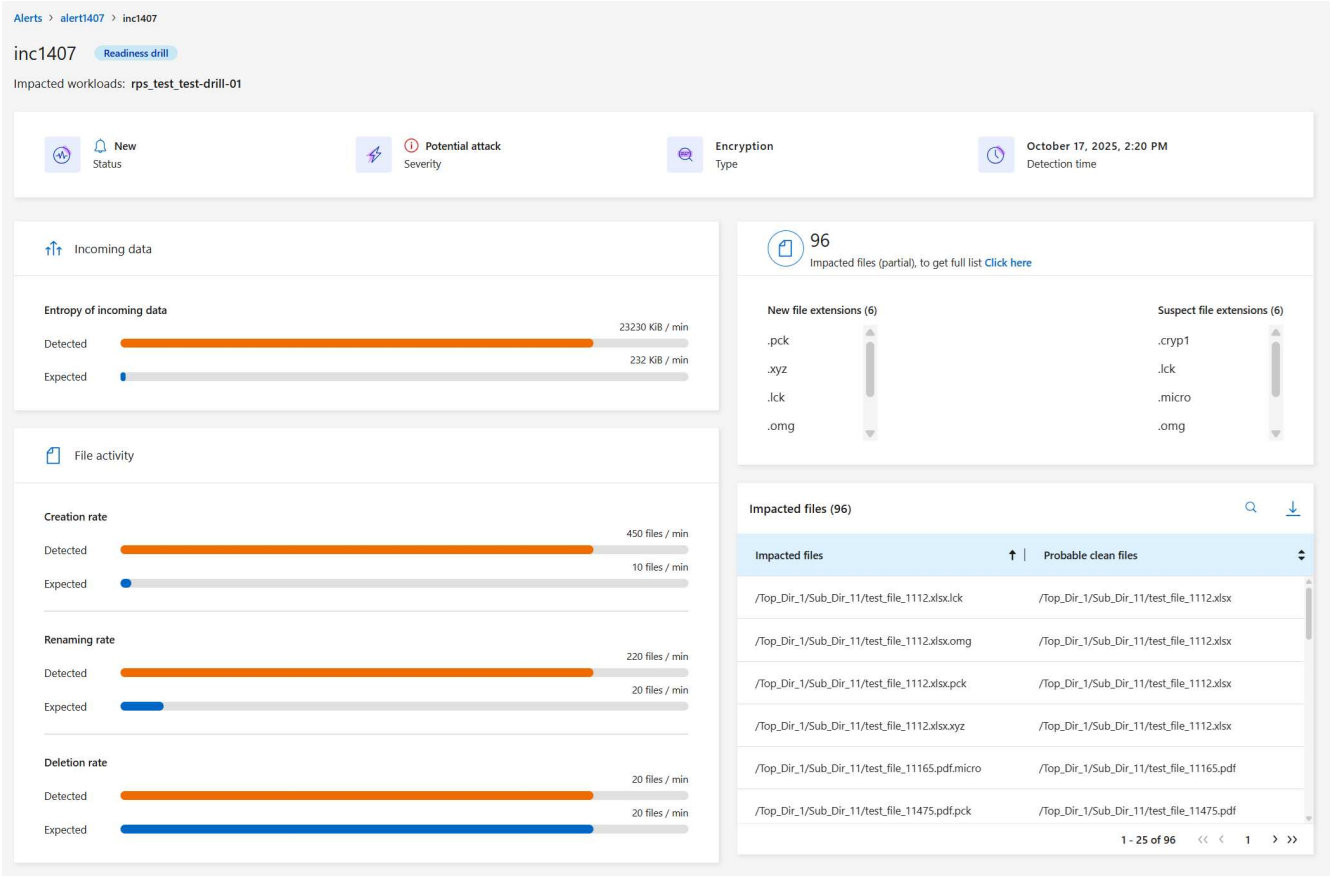
   La console affiche la page Alertes. Dans la colonne ID d'alerte, vous voyez « Exercice de préparation » à côté de l'ID.



2. Sélectionnez l'alerte avec l'indication « Exercice de préparation ». Une liste des alertes d'incident apparaît sur la page Détails des alertes.



3. Passez en revue les incidents d'alerte.
4. Sélectionnez un incident d'alerte.



Voici quelques éléments à rechercher :

- Regardez la gravité potentielle de l'attaque.

  Si la gravité indique qu'un utilisateur est suspecté d'activité malveillante, vérifiez le nom d'utilisateur. Vous pouvez également"bloquer l'utilisateur."

- Regardez l'activité du fichier et les processus suspects :
  - Regardez les données entrantes détectées par rapport aux données attendues.
  - Regardez le taux de création de fichiers détecté par rapport au taux attendu.
  - Regardez le taux de renommage de fichier détecté par rapport au taux attendu.
  - Regardez le taux de suppression par rapport au taux attendu.
- Regardez la liste des fichiers impactés. Regardez les extensions qui pourraient être à l'origine de l'attaque.
- Déterminez l'impact et l'ampleur de l'attaque en examinant le nombre de fichiers et de répertoires impactés.

Restaurer la charge de travail du test

Après avoir examiné l'alerte d'exercice de préparation, restaurez la charge de travail de test si nécessaire.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

1. Retourner à la page des détails de l'alerte.
2. Si la charge de travail de test doit être restaurée, procédez comme suit :
   - Sélectionnez **Marquer comme restauration nécessaire**.
   - Vérifiez la confirmation et sélectionnez **Marquer comme restauration nécessaire** dans la boîte de confirmation.
     - Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
     - Sélectionnez la charge de travail de test marquée « Exercice de préparation » que vous souhaitez restaurer.
     - Sélectionnez **Restaurer**.
     - Dans la page Restaurer, fournissez les informations pour la restauration :
   - Sélectionnez la copie instantanée source.
   - Sélectionnez le volume de destination.
3. Dans la page de révision de restauration, sélectionnez **Restaurer**.

   La console affiche l'état de la restauration de l'exercice de préparation comme « En cours » sur la page Récupération.

   Une fois la restauration terminée, la console modifie l'état de la charge de travail sur **Restauré**.

4. Examiner la charge de travail restaurée.

Pour plus de détails sur le processus de restauration, voir"Récupérer après une attaque de ransomware (après neutralisation des incidents)" .

Modifier le statut des alertes après l'exercice de préparation

Après avoir examiné l'alerte d'exercice de préparation et restauré la charge de travail, modifiez le statut de l'alerte si nécessaire.

Requiert le rôle de console Administrateur d'organisation, Administrateur de dossier ou de projet ou Administrateur de résilience aux ransomwares. "En savoir plus sur les rôles d'accès à la console pour tous les services" .

Étapes

1. Retourner à la page des détails de l'alerte.
2. Sélectionnez à nouveau l'alerte.
3. Indiquez le statut en sélectionnant **Modifier le statut** et modifiez le statut en l'un des suivants :
   - Rejeté : si vous pensez que l'activité n'est pas une attaque de ransomware, modifiez le statut sur Rejeté.

     Après avoir rejeté une attaque, vous ne pouvez pas la modifier à nouveau. Si vous supprimez une charge de travail, toutes les copies instantanées prises automatiquement en réponse à l'attaque potentielle du ransomware seront définitivement supprimées. Si vous ignorez l'alerte, l'exercice de préparation est considéré comme terminé.

   - Résolu : L'incident a été atténué.

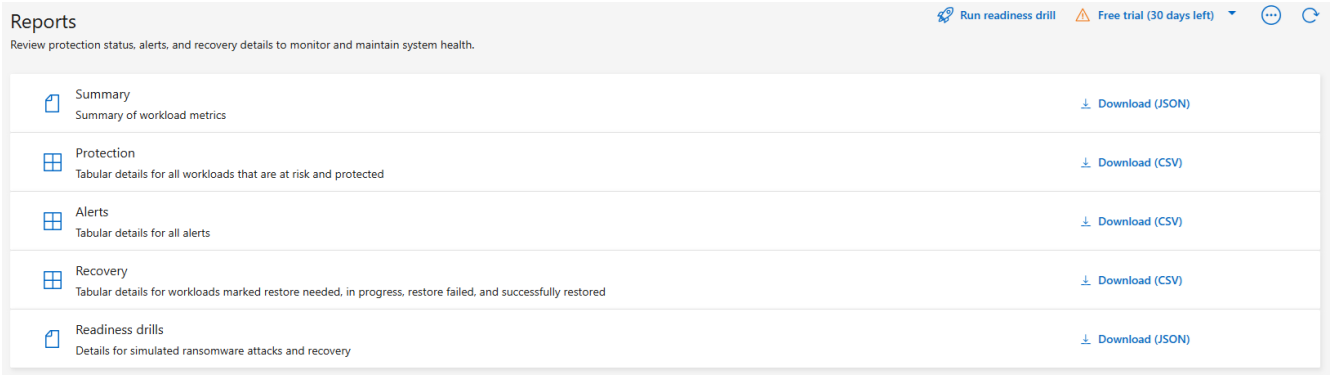
Rapports d’examen sur l’exercice de préparation

Une fois l’exercice de préparation terminé, vous souhaiterez peut-être consulter et enregistrer un rapport sur l’exercice.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d’administrateur d’organisation, d’administrateur de dossier ou de projet, d’administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Rapports**.



2. Sélectionnez **Exercices de préparation** et **Télécharger** pour télécharger le rapport d’exercice de préparation.

Connectez NetApp Ransomware Resilience au système de gestion des informations et des événements de sécurité (SIEM) pour l’analyse et la détection des menaces

Un système de gestion des événements et de la sécurité (SIEM) centralise les journaux et les données d’événements afin de fournir des informations sur les incidents de sécurité et la conformité. NetApp Ransomware Resilience prend en charge l’envoi automatique des données à votre SIEM pour une analyse et une détection des menaces simplifiées.

Ransomware Resilience prend en charge les SIEM suivants :

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

Avant d’activer SIEM dans Ransomware Resilience, vous devez configurer votre système SIEM.

Données d’événements envoyées à un SIEM

Ransomware Resilience peut envoyer les données d’événement suivantes à votre système SIEM :

- **contexte**:

- **os**: Il s'agit d'une constante avec la valeur ONTAP.
- **os_version** : la version d' ONTAP exécutée sur le système.
- **connector_id** : l'ID de l'agent de console qui gère le système.
- **cluster_id** : l'ID de cluster signalé par ONTAP pour le système.
- **svm_name** : Le nom du SVM où l'alerte a été trouvée.
- **volume_name** : Le nom du volume sur lequel l'alerte est trouvée.
- **volume_id** : l'ID du volume signalé par ONTAP pour le système.

- **incident**:
  - **incident_id** : l'ID d'incident généré par Ransomware Resilience pour le volume attaqué dans Ransomware Resilience.
  - **alert_id** : l'ID généré par Ransomware Resilience pour la charge de travail.
  - **gravité** : L'un des niveaux d'alerte suivants : « CRITIQUE », « ÉLEVÉ », « MOYEN », « FAIBLE ».
  - **description** : Détails sur l'alerte détectée, par exemple : « Une attaque potentielle de rançongiciel détectée sur la charge de travail arp_learning_mode_test_2630 »

Configurer AWS Security Hub pour la détection des menaces

Avant d'activer AWS Security Hub dans NetApp Ransomware Resilience, vous devez effectuer les étapes générales suivantes dans AWS Security Hub :

- Configurez les autorisations dans AWS Security Hub.
- Configurez la clé d'accès d'authentification et la clé secrète dans AWS Security Hub. (Ces étapes ne sont pas fournies ici.)

Étapes pour configurer les autorisations dans AWS Security Hub

1. Accédez à la **console AWS IAM**.
2. Sélectionnez **Politiques**.
3. Créez une politique à l'aide du code suivant au format JSON :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Configurer Microsoft Sentinel pour la détection des menaces

Avant d'activer Microsoft Sentinel dans NetApp Ransomware Resilience, vous devez effectuer les étapes générales suivantes dans Microsoft Sentinel :

- **Prérequis**
  - Activer Microsoft Sentinel.
  - Créez un rôle personnalisé dans Microsoft Sentinel.
- **Inscription**
  - Inscrivez-vous à Ransomware Resilience pour recevoir des événements de Microsoft Sentinel.
  - Créez un secret pour l'inscription.
- **Autorisations** : Attribuer des autorisations à l'application.
- **Authentification** : Saisissez les informations d'authentification pour l'application.

Étapes pour activer Microsoft Sentinel

1. Accédez à Microsoft Sentinel.
2. Créez un **espace de travail Log Analytics**.
3. Autorisez Microsoft Sentinel à utiliser l'espace de travail Log Analytics que vous venez de créer.

Étapes pour créer un rôle personnalisé dans Microsoft Sentinel

1. Accédez à Microsoft Sentinel.
2. Sélectionnez **Abonnement** > **Contrôle d'accès (IAM)**.
3. Saisissez un nom de rôle personnalisé. Utilisez le nom **Ransomware Resilience Sentinel Configurator**.
4. Copiez le JSON suivant et collez-le dans l'onglet **JSON**.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Vérifiez et enregistrez vos paramètres.

Étapes pour enregistrer Ransomware Resilience afin de recevoir les événements de Microsoft Sentinel

1. Accédez à Microsoft Sentinel.
2. Sélectionnez **Entra ID** > **Applications** > **Enregistrements d'applications**.
3. Pour le **Nom d'affichage** de l'application, saisissez « **Ransomware Resilience** ».
4. Dans le champ **Type de compte pris en charge**, sélectionnez **Comptes dans cet annuaire organisationnel uniquement**.
5. Sélectionnez un **index par défaut** où les événements seront poussés.
6. Sélectionnez **Révision**.
7. Sélectionnez **Enregistrer** pour enregistrer vos paramètres.

   Après l'enregistrement, le centre d'administration Microsoft Entra affiche le volet Présentation de l'application.

Étapes pour créer un secret pour l'enregistrement

1. Accédez à Microsoft Sentinel.
2. Sélectionnez **Certificats et secrets** > **Secrets client** > **Nouveau secret client**.
3. Ajoutez une description pour le secret de votre application.
4. Sélectionnez une **Expiration** pour le secret ou spécifiez une durée de vie personnalisée.

   La durée de vie d'un secret client est limitée à deux ans (24 mois) ou moins. Microsoft vous recommande de définir une valeur d'expiration inférieure à 12 mois.

5. Sélectionnez **Ajouter** pour créer votre secret.
6. Enregistrez le secret à utiliser dans l'étape d'authentification. Le secret ne s'affiche plus jamais après avoir quitté cette page.

Étapes pour attribuer des autorisations à l'application

1. Accédez à Microsoft Sentinel.
2. Sélectionnez **Abonnement** > **Contrôle d'accès (IAM)**.
3. Sélectionnez **Ajouter** > **Ajouter une attribution de rôle**.
4. Pour le champ **Rôles d'administrateur privilégiés**, sélectionnez **Ransomware Resilience Sentinel Configurator**.

Il s'agit du rôle personnalisé que vous avez créé précédemment.

5. Sélectionnez **Suivant**.
6. Dans le champ **Attribuer l'accès à**, sélectionnez **Utilisateur, groupe ou principal de service**.
7. Sélectionnez **Sélectionner les membres**. Ensuite, sélectionnez **Ransomware Resilience Sentinel Configurator**.
8. Sélectionnez **Suivant**.
9. Dans le champ **Ce que l'utilisateur peut faire**, sélectionnez **Autoriser l'utilisateur à attribuer tous les rôles à l'exception des rôles d'administrateur privilégié Propriétaire, UAA, RBAC (recommandé)**.
10. Sélectionnez **Suivant**.
11. Sélectionnez **Réviser et attribuer** pour attribuer les autorisations.

Étapes pour saisir les informations d'authentification pour l'application

1. Accédez à Microsoft Sentinel.
2. Entrez les informations d'identification :
   a. Saisissez l'ID du locataire, l'ID de l'application cliente et le secret de l'application cliente.
   b. Sélectionnez **Authenticate**.

   Une fois l'authentification réussie, un message « Authentifié » s'affiche.
3. Saisissez les détails de l'espace de travail Log Analytics pour l'application.
   a. Sélectionnez l'ID d'abonnement, le groupe de ressources et l'espace de travail Log Analytics.

Configurer Splunk Cloud pour la détection des menaces

Avant d'activer Splunk Cloud dans Ransomware Resilience, vous devez effectuer les étapes de haut niveau suivantes dans Splunk Cloud :

- Activez un collecteur d'événements HTTP dans Splunk Cloud pour recevoir des données d'événement via HTTP ou HTTPS à partir de la console.
- Créez un jeton de collecteur d'événements dans Splunk Cloud.

Étapes pour activer un collecteur d'événements HTTP dans Splunk

1. Accédez à Splunk Cloud.
2. Sélectionnez **Paramètres** > **Entrées de données**.
3. Sélectionnez **Collecteur d'événements HTTP** > **Paramètres globaux**.
4. Sur le bouton bascule Tous les jetons, sélectionnez **Activé**.
5. Pour que le collecteur d'événements écoute et communique via HTTPS plutôt que HTTP, sélectionnez **Activer SSL**.
6. Saisissez un port dans **Numéro de port HTTP** pour le collecteur d'événements HTTP.

Étapes pour créer un jeton de collecteur d'événements dans Splunk

1. Accédez à Splunk Cloud.
2. Sélectionnez **Paramètres** > **Ajouter des données**.

3. Sélectionnez **Moniteur** > **Collecteur d'événements HTTP**.
4. Saisissez un nom pour le jeton et sélectionnez **Suivant**.
5. Sélectionnez un **Index par défaut** où les événements seront poussés, puis sélectionnez **Réviser**.
6. Confirmez que tous les paramètres du point de terminaison sont corrects, puis sélectionnez **Soumettre**.
7. Copiez le jeton et collez-le dans un autre document pour le préparer pour l'étape d'authentification.

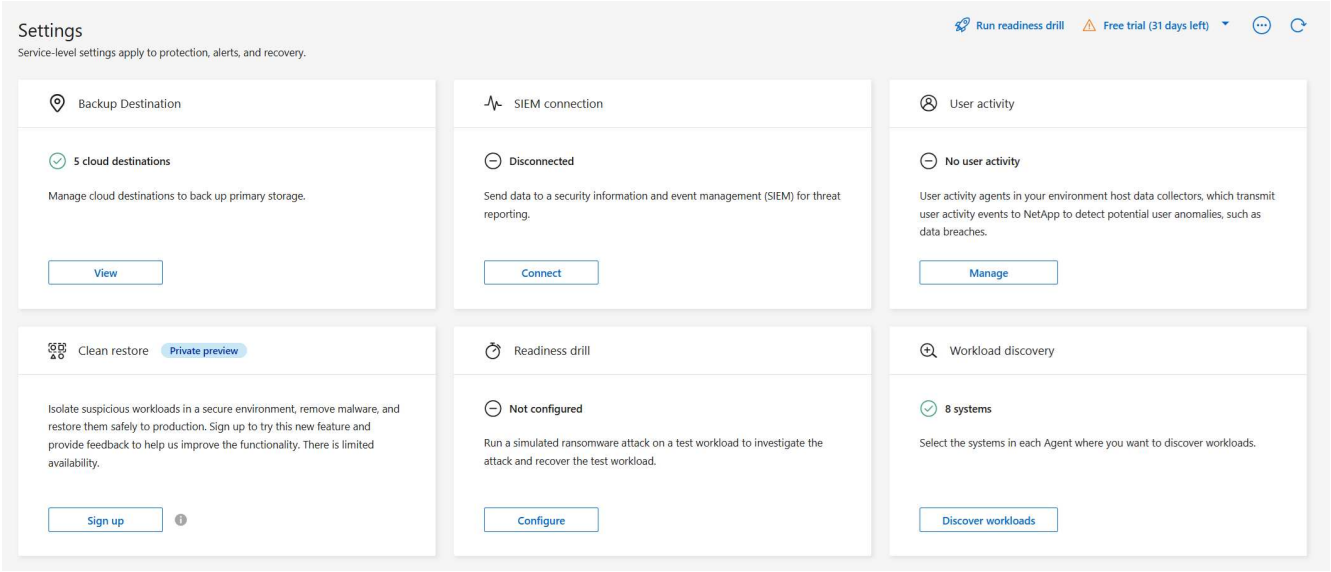
Connecter SIEM dans Ransomware Resilience

L'activation de SIEM envoie les données de Ransomware Resilience à votre serveur SIEM pour l'analyse des menaces et la création de rapports.

Étapes

1. Dans le menu de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.
2. Dans le menu Résilience aux ransomwares, sélectionnez la verticale … option en haut à droite.
3. Sélectionnez **Paramètres**.

   La page Paramètres apparaît.



4. Dans la page Paramètres, sélectionnez **Connecter** dans la mosaïque de connexion SIEM.

5. Choisissez l'un des systèmes SIEM.
6. Saisissez le jeton et les détails d'authentification que vous avez configurés dans AWS Security Hub ou Splunk Cloud.

   Les informations que vous saisissez dépendent du SIEM que vous avez sélectionné.

7. Sélectionnez **Activer**.

   La page Paramètres affiche « Connecté ».

Télécharger les rapports sur la NetApp Ransomware Resilience

NetApp Ransomware Resilience fournit des rapports aux formats CSV et JSON qui affichent des détails sur les volumes pris en charge et non pris en charge, les exercices de préparation aux attaques, la protection, les alertes et la récupération. Avec les rapports, vous pouvez enregistrer et consulter hors ligne des rapports sur les exercices, la posture de protection, les alertes et les événements de récupération.

Avant de télécharger les fichiers, actualisez le tableau de bord pour que vos rapports intègrent les données les plus récentes.

Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de résilience aux ransomwares ou de visualiseur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Quelles données pouvez-vous télécharger ? Vous pouvez télécharger des fichiers à partir de n'importe quelle option du menu principal :

- **Résumé** : Comprend des listes de charges de travail prises en charge et non prises en charge, des actions recommandées pour améliorer votre posture de cyber-résilience et des informations capturées dans le tableau de bord de résilience aux ransomwares.

- **Protection** : Comprend l'état et les détails de toutes les charges de travail, y compris le nombre total de charges de travail protégées et à risque.
- **Alertes** : inclut l'état et les détails de toutes les alertes, y compris le nombre total d'alertes et d'instantanés automatisés.
- **Récupération** : inclut l'état et les détails de toutes les charges de travail qui doivent être restaurées, y compris le nombre total de charges de travail marquées « Restauration nécessaire », « En cours », « Échec de la restauration » et « Restaurée avec succès ».
- **Rapports** : Vous pouvez exporter des données depuis n'importe quelle page et télécharger les fichiers.

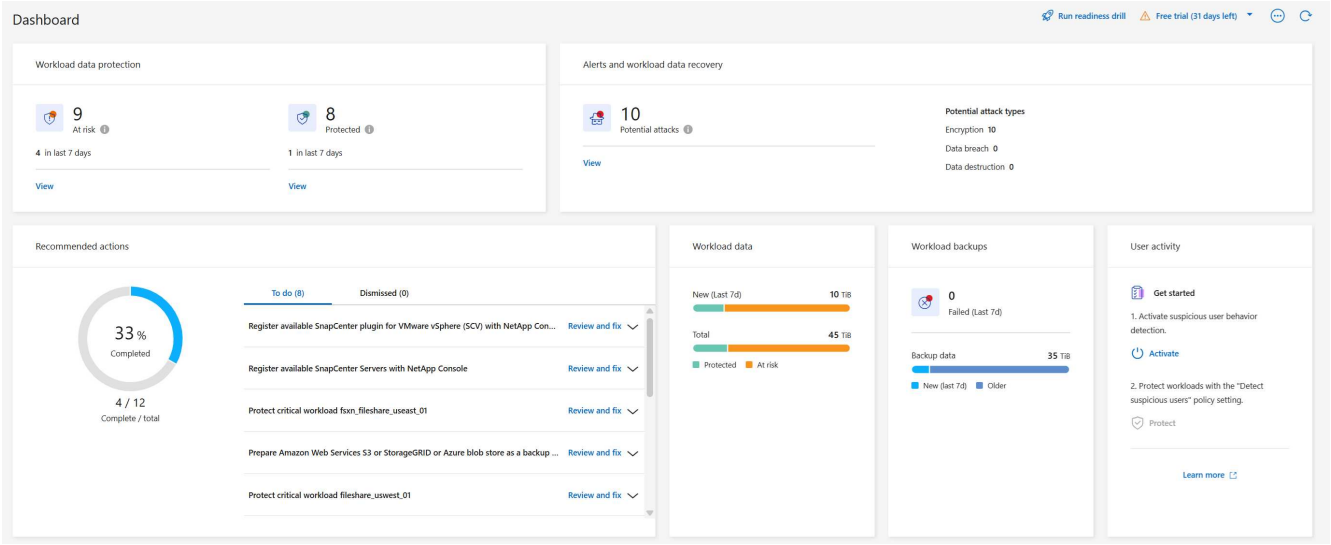
> Vous pouvez télécharger les rapports d'exercice de préparation uniquement à partir de la page **Rapports**.

Si vous téléchargez des fichiers CSV ou JSON à partir de la page Protection, Alertes ou Récupération, les données affichent uniquement les données de cette page.

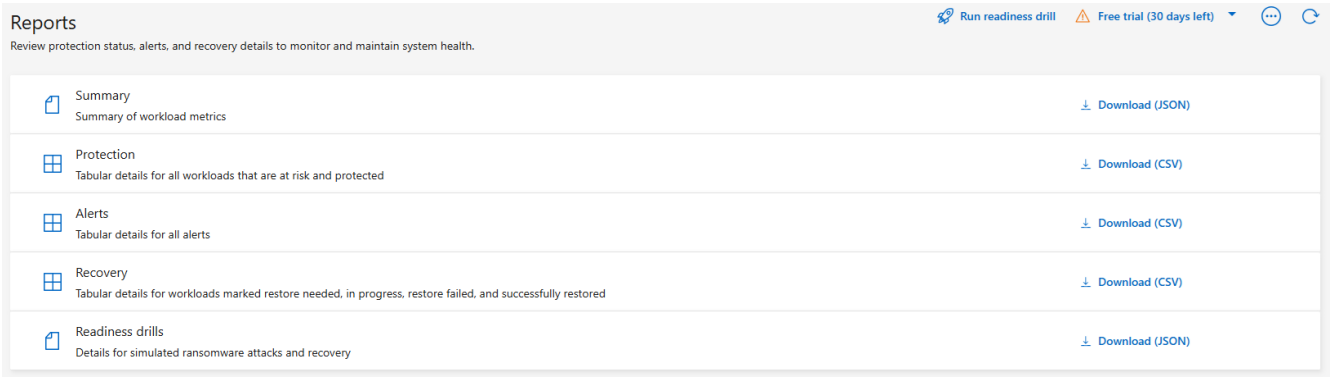
Les fichiers CSV ou JSON incluent des données pour toutes les charges de travail sur tous les systèmes de console.

Étapes

1. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.



2. Depuis le tableau de bord ou une autre page, sélectionnez l'option **Actualiser** en haut à droite pour actualiser les données qui apparaîtront dans les rapports.
3. Effectuez l'une des opérations suivantes :
   - Depuis la page, sélectionnez *Télécharger* option.
   - Dans le menu NetApp Ransomware Resilience , sélectionnez **Rapports**.
4. Si vous avez sélectionné l'option **Rapports**, sélectionnez l'un des noms de fichiers préconfigurés et sélectionnez **Télécharger**.


Reports
Review protection status, alerts, and recovery details to monitor and maintain system health.
Run readiness drill
Free trial (30 days left)
Summary
Summary of workload metrics
Download (JSON)
Protection
Tabular details for all workloads that are at risk and protected
Download (CSV)
Alerts
Tabular details for all alerts
Download (CSV)
Recovery
Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored
Download (CSV)
Readiness drills
Details for simulated ransomware attacks and recovery
Download (JSON)

Informations sur le copyright

Informations sur les marques commerciales