Documentation sur la NetApp Ransomware Resilience

NetApp Ransomware Resilience

NetApp
February 17, 2026

Sommaire

Documentation sur la NetApp Ransomware Resilience

Notes de version

Nouveautés de NetApp Ransomware Resilience

Découvrez les nouveautés de NetApp Ransomware Resilience.

16 février 2026

Prise en charge d'Azure NetApp Files

Ransomware Resilience prend désormais en charge les systèmes Azure NetApp Files, vous permettant de détecter et de contrer efficacement les menaces de ransomware dans Azure NetApp Files. Lorsque vous découvrez des charges de travail, Ransomware Resilience présente désormais Azure NetApp Files et les affiche dans le tableau de bord de protection. La prise en charge de Ransomware Resilience pour Azure NetApp Files inclut des stratégies de détection et de protection uniquement avec des instantanés. La prise en charge d'Azure NetApp Files est actuellement en préversion.

Pour plus d'informations, consultez le lien : Pour plus d'informations, consultez "En savoir plus sur la résilience aux ransomwares".

Exclure les utilisateurs des alertes de comportement utilisateur

Ransomware Resilience permet désormais d'exclure des utilisateurs spécifiques des alertes de comportement utilisateur. Exclure des utilisateurs de confiance peut éviter les faux positifs et les alertes inutiles.

Pour plus d'informations, consultez le lien : Pour plus d'informations, consultez "Exclure les utilisateurs des alertes".

Prise en charge des groupes de protection pour l'activité des comportements des utilisateurs

Les groupes de protection Ransomware Resilience prennent désormais en charge les politiques de détection des comportements suspects des utilisateurs. Lorsque vous appliquez une stratégie de protection contre les ransomwares à un groupe de protection, elle applique une politique à l'ensemble des charges de travail, simplifiant la gestion de votre posture de cybersécurité.

Pour plus d'informations, voir "Créer un groupe de protection".

19 janvier 2026

Volumes non pris en charge

Les rapports de résilience aux ransomwares capturent désormais des informations sur les volumes pris en charge et non pris en charge dans le rapport **Résumé**. Utilisez ces informations pour diagnostiquer pourquoi certains volumes d'un système pourraient ne pas être éligibles à la protection contre les ransomwares.

Pour plus d'informations, voir "Télécharger les rapports dans Ransomware Resilience".

12 janvier 2026

Répliquer les instantanés sur ONTAP

Ransomware Resilience prend désormais en charge l'ajout de la réplication des snapshots vers un site

ONTAP secondaire. Avec des groupes de protection qui utilisent une stratégie de réplication, vous pouvez répliquer vers la même destination ou vers des destinations différentes pour chaque charge de travail. Vous pouvez créer une stratégie de protection contre les ransomwares qui inclut la réplication ou utiliser la stratégie prédéfinie.

Pour plus d'informations, voir "Protéger les charges de travail grâce à la résilience contre les ransomwares".

Exclure les charges de travail de la résilience aux ransomwares

Ransomware Resilience prend désormais en charge l'exclusion de certaines charges de travail d'un système de la protection et du tableau de bord Ransomware Resilience. Vous pouvez exclure les charges de travail après leur découverte, puis les réinclure si vous souhaitez ajouter une protection contre les ransomwares. Les charges de travail exclues ne vous seront pas facturées.

Pour plus d'informations, voir "Exclure les charges de travail".

Les alertes marquées comme étant en cours de révision

Ransomware Resilience vous permet désormais de marquer les alertes comme « En cours d'examen ». Utilisez l'étiquette « En cours d'examen » pour améliorer la clarté au sein de votre équipe lors du tri et de la gestion des menaces de ransomware actives.

Pour plus d'informations, voir "Gérer les alertes dans Ransomware Resilience".

8 décembre 2025

Le blocage des extensions est activé au niveau de la charge de travail.

Lorsque vous activez le blocage des extensions, celui-ci est désormais activé au niveau de la charge de travail et non plus au niveau de la machine virtuelle de stockage.

Modifier l'état d'alerte du comportement de l'utilisateur

Ransomware Resilience vous permet désormais de modifier le statut des alertes comportementales des utilisateurs. Vous pouvez ignorer et résoudre manuellement les alertes.

Pour plus d'informations, voir "Gérer les alertes dans Ransomware Resilience".

Prise en charge de plusieurs agents de console

Ransomware Resilience prend désormais en charge l'utilisation de plusieurs agents Console pour gérer les mêmes systèmes.

Pour plus d'informations sur les agents de console, consultez"Créer un agent de console" .

10 novembre 2025

Cette version comprend des améliorations générales.

06 octobre 2025

La BlueXP ransomware protection est désormais NetApp Ransomware Resilience

Le service de BlueXP ransomware protection a été renommé NetApp Ransomware Resilience.

BlueXP est désormais NetApp Console

La NetApp Console offre une gestion centralisée des services de stockage et de données dans les environnements sur site et dans le cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée.

Pour plus de détails sur ce qui a changé, consultez le "Notes de version de la NetApp Console" .

Détection de violation de données

Ransomware Resilience inclut un nouveau mécanisme de détection qui peut être activé en quelques étapes pour détecter les lectures anormales des utilisateurs comme indicateur précoce d'une violation de données. La résilience des ransomwares collecte et analyse les événements de lecture des utilisateurs en créant une base de référence historique, qui est un profil du comportement normal attendu à partir des données passées. Lorsque l'activité d'un nouvel utilisateur s'écarte considérablement de cette norme établie (comme une augmentation inattendue des lectures associée à des modèles de lecture suspects), une alerte est générée. Ransomware Resilience inclut un modèle d'IA pour détecter les modèles de lecture suspects.

Contrairement à la détection de chiffrement par ARP au niveau de la couche de stockage, la détection de l'anomalie de comportement de l'utilisateur est effectuée dans le service SaaS Ransomware Resilience en collectant les événements FPolicy.

> Vous devez utiliser le nouveau"Administrateur du comportement utilisateur de Ransomware Resilience et visualiseur du comportement utilisateur de Ransomware Resilience" rôles pour accéder aux paramètres de détection des comportements suspects des utilisateurs.

Pour plus d'informations, voir"Activer la détection des activités suspectes des utilisateurs" et"Afficher le comportement anormal des utilisateurs" .

Détections supplémentaires d'activités suspectes d'utilisateurs

En plus de la détection des violations de données, Ransomware Resilience détecte également les types d'alertes suivants en fonction de l'activité suspecte observée des utilisateurs :

- **Destruction de données - attaque potentielle** - Une alerte avec la gravité d'une attaque potentielle est créée lorsque le nombre de suppressions de fichiers dépasse la norme historique.
- **Comportement suspect de l'utilisateur - attaque potentielle** - Une alerte avec la gravité d'une attaque potentielle est créée lorsque des opérations de lecture, de renommage et de suppression dans une séquence similaire à une attaque de ransomware sont observées
- **Comportement suspect de l'utilisateur - Avertissement** - Une alerte avec la gravité d'un avertissement est créée lorsque le nombre total d'activités de fichiers (lecture, suppression, renommage, etc.) dépasse la norme historique

Nouveaux rôles d'utilisateur pour la détection des violations de données

Pour gérer les alertes d'activité utilisateur suspecte, Ransomware Resilience a introduit deux nouveaux rôles pour les administrateurs de l'organisation de la console afin d'accorder l'accès à la détection d'activité utilisateur suspecte : administrateur du comportement utilisateur Ransomware Resilience et visualiseur du comportement utilisateur Ransomware Resilience.

Vous devez être un administrateur du comportement utilisateur pour configurer les paramètres de comportement utilisateur suspect. Le rôle d'administrateur Ransomware Resilience n'est pas pris en charge pour la configuration des paramètres de comportement utilisateur suspect.

Pour plus d'informations, consultez la section "Accès basé sur les rôles NetApp Ransomware Resilience" .

12 août 2025

Cette version comprend des améliorations générales.

15 juillet 2025

Prise en charge de la charge de travail SAN

Cette version inclut la prise en charge des charges de travail SAN dans la BlueXP ransomware protection. Vous pouvez désormais protéger les charges de travail SAN en plus des charges de travail NFS et CIFS.

Pour plus d'informations, reportez-vous à "Conditions préalables à la BlueXP ransomware protection" .

Protection améliorée de la charge de travail

Cette version améliore le processus de configuration des charges de travail avec des stratégies de snapshot et de sauvegarde provenant d'autres outils NetApp tels que SnapCenter ou BlueXP backup and recovery. Dans les versions précédentes, la BlueXP ransomware protection détectait les politiques d'autres outils, vous permettant uniquement de modifier la politique de détection. Avec cette version, vous pouvez désormais remplacer les politiques de snapshot et de sauvegarde par les politiques de BlueXP ransomware protection ou continuer à utiliser les politiques d'autres outils.

Pour plus de détails, reportez-vous à"Protéger les charges de travail" .

Notifications par e-mail

Si la BlueXP ransomware protection détecte une attaque possible, une notification apparaît dans les notifications BlueXP et un e-mail est envoyé à l'adresse e-mail que vous avez configurée.

L'e-mail contient des informations sur la gravité, la charge de travail impactée et un lien vers l'alerte dans l'onglet **Alertes** de BlueXP ransomware protection .

Si vous avez configuré un système de gestion de la sécurité et des événements (SIEM) dans la BlueXP ransomware protection, le service envoie les détails des alertes à votre système SIEM.

Pour plus de détails, reportez-vous à"Gérer les alertes de ransomware détectées" .

9 juin 2025

Mises à jour de la page de destination

Cette version inclut des mises à jour de la page de destination pour la BlueXP ransomware protection qui facilitent le démarrage de l'essai gratuit et la découverte.

Mises à jour sur les exercices de préparation

Auparavant, vous pouviez exécuter un exercice de préparation aux ransomwares en simulant une attaque sur un nouvel exemple de charge de travail. Grâce à cette fonctionnalité, vous pouvez 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 et planifiez ces exercices aussi souvent que nécessaire.

Avec cette version, vous pouvez utiliser un nouveau bouton sur le tableau de bord de BlueXP ransomware protection pour exécuter un exercice de préparation aux ransomwares sur une charge de travail de test, ce qui vous permet de simuler plus facilement des attaques de ransomwares, d'étudier leur impact et de récupérer efficacement les charges de travail, le tout dans un environnement contrôlé.

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

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Activer les mises à jour de BlueXP classification

Avant d'utiliser la BlueXP classification dans le service de BlueXP ransomware protection , vous devez activer la BlueXP classification pour analyser vos données. La classification des données vous aide à trouver des informations personnelles identifiables (PII), ce qui peut augmenter les risques de sécurité.

Vous pouvez déployer la BlueXP classification sur une charge de travail de partage de fichiers à partir de la BlueXP ransomware protection. Dans la colonne **Exposition à la confidentialité**, sélectionnez l'option **Identifier l'exposition**. Si vous avez activé le service de classification, cette action identifie l'exposition. Sinon, avec cette version, une boîte de dialogue présente la possibilité de déployer la BlueXP classification. Sélectionnez **Déployer** pour accéder à la page de destination du service de BlueXP classification , où vous pouvez déployer ce service. W

Pour plus de détails, reportez-vous à "Déployer la BlueXP classification dans le cloud" et pour utiliser le service dans la BlueXP ransomware protection, reportez-vous à "Rechercher des informations personnelles identifiables avec la BlueXP classification" .

13 mai 2025

Signalement d'environnements de travail non pris en charge dans la BlueXP ransomware protection

Pendant le flux de travail de découverte, la BlueXP ransomware protection signale plus de détails lorsque vous passez la souris sur les charges de travail prises en charge ou non prises en charge. Cela vous aidera à comprendre pourquoi certaines de vos charges de travail ne sont pas détectées par le service de BlueXP ransomware protection .

Il existe de nombreuses raisons pour lesquelles le service ne prend pas en charge un environnement de travail. Par exemple, la version ONTAP de votre environnement de travail peut être inférieure à la version requise. Lorsque vous survolez un environnement de travail non pris en charge, une info-bulle affiche la raison.

Vous pouvez afficher les environnements de travail non pris en charge lors de la découverte initiale, où vous pouvez également télécharger les résultats. Vous pouvez également afficher les résultats de la découverte à partir de l'option **Découverte de charge de travail** dans la page Paramètres.

Pour plus de détails, reportez-vous à "Découvrez les charges de travail dans la BlueXP ransomware protection" .

29 avril 2025

Prise en charge d' Amazon FSx for NetApp ONTAP

Cette version prend en charge Amazon FSx for NetApp ONTAP. Cette fonctionnalité vous aide à protéger vos charges de travail FSx for ONTAP avec la BlueXP ransomware protection.

FSx for ONTAP est un service entièrement géré qui fournit la puissance du stockage NetApp ONTAP dans le cloud. Il offre les mêmes fonctionnalités, performances et capacités administratives que celles que vous utilisez sur site avec l'agilité et l'évolutivité d'un service AWS natif.

Les modifications suivantes ont été apportées au flux de travail de BlueXP ransomware protection :

- Discovery inclut les charges de travail dans les environnements de travail FSx pour ONTAP 9.15.
- L'onglet Protection affiche les charges de travail dans les environnements FSx for ONTAP . Dans cet environnement, vous devez effectuer des opérations de sauvegarde à l'aide du service de sauvegarde FSx for ONTAP . Vous pouvez restaurer ces charges de travail à l'aide des instantanés de BlueXP ransomware protection .

> Les politiques de sauvegarde pour une charge de travail exécutée sur FSx pour ONTAP ne peuvent pas être définies dans BlueXP. Toutes les politiques de sauvegarde existantes définies dans Amazon FSx for NetApp ONTAP restent inchangées.

- Les incidents d'alerte montrent le nouvel environnement de travail FSx pour ONTAP .

Pour plus de détails, reportez-vous à "En savoir plus sur la BlueXP ransomware protection" .

Pour plus d'informations sur les options prises en charge, reportez-vous à la "Limitations de la BlueXP ransomware protection" .

Rôle d'accès BlueXP requis

Vous avez désormais besoin de l'un des rôles d'accès suivants pour afficher, découvrir ou gérer la BlueXP ransomware protection: administrateur de l'organisation, administrateur de dossier ou de projet, administrateur de la protection contre les ransomwares ou visualiseur de protection contre les ransomwares.

"En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

14 avril 2025

Rapports d'exercices de préparation

Avec cette version, vous pouvez consulter les rapports d'exercices de préparation aux attaques de ransomware. Un exercice de préparation vous permet de simuler une attaque de ransomware sur un échantillon de charge de travail nouvellement créé. Ensuite, examinez l'attaque simulée et récupérez l'exemple de charge de travail. Cette fonctionnalité vous aide à savoir que vous êtes préparé en cas d'attaque réelle de ransomware en testant les processus de notification d'alerte, de réponse et de récupération.

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Nouveaux rôles et autorisations de contrôle d'accès basés sur les rôles

Auparavant, vous pouviez attribuer des rôles et des autorisations aux utilisateurs en fonction de leurs responsabilités, ce qui vous aide à gérer l'accès des utilisateurs à la BlueXP ransomware protection. Avec cette version, il existe deux nouveaux rôles spécifiques à la BlueXP ransomware protection avec des autorisations mises à jour. Les nouveaux rôles sont :

- Administrateur de la protection contre les ransomwares
- Visionneuse de protection contre les ransomwares

Pour plus de détails sur les autorisations, reportez-vous à "Accès aux fonctionnalités basé sur les rôles de BlueXP ransomware protection" .

Améliorations des paiements

Cette version inclut plusieurs améliorations au processus de paiement.

Pour plus de détails, reportez-vous à "Configurer les options de licence et de paiement" .

10 mars 2025

Simulez une attaque et répondez

Avec cette version, simulez une attaque de ransomware pour tester votre réponse à une alerte de ransomware. Cette fonctionnalité vous aide à savoir que vous êtes préparé en cas d'attaque réelle de ransomware en testant les processus de notification d'alerte, de réponse et de récupération.

Pour plus de détails, reportez-vous à "Effectuer un exercice de préparation aux attaques de ransomware" .

Améliorations du processus de découverte

Cette version inclut des améliorations aux processus de découverte et de redécouverte sélectives :

- Avec cette version, vous pouvez découvrir les charges de travail nouvellement créées qui ont été ajoutées aux environnements de travail précédemment sélectionnés.
- Vous pouvez également sélectionner de *nouveaux* environnements de travail dans cette version. Cette fonctionnalité vous aide à protéger les nouvelles charges de travail ajoutées à votre environnement.
- Vous pouvez effectuer ces processus de découverte au cours du processus de découverte initial ou dans l'option Paramètres.

Pour plus de détails, reportez-vous à "Découvrez les charges de travail nouvellement créées pour les environnements de travail précédemment sélectionnés" et "Configurer les fonctionnalités avec l'option Paramètres" .

Alertes déclenchées lorsqu'un cryptage élevé est détecté

Avec cette version, vous pouvez afficher des alertes lorsqu'un cryptage élevé est détecté sur vos charges de travail, même sans modifications d'extension de fichier élevées. Cette fonctionnalité, qui utilise l'IA ONTAP Autonomous Ransomware Protection (ARP), vous aide à identifier les charges de travail exposées au risque d'attaques de ransomware. Utilisez cette fonctionnalité et téléchargez la liste complète des fichiers impactés avec ou sans modifications d'extension.

Pour plus de détails, reportez-vous à "Répondre à une alerte de ransomware détectée" .

16 décembre 2024

Détectez les comportements anormaux des utilisateurs à l'aide de Data Infrastructure Insights Storage Workload Security

Avec cette version, vous pouvez utiliser Data Infrastructure Insights Storage Workload Security pour détecter les comportements anormaux des utilisateurs dans vos charges de travail de stockage. Cette fonctionnalité vous aide à identifier les menaces de sécurité potentielles et à bloquer les utilisateurs potentiellement malveillants pour protéger vos données.

Pour plus de détails, reportez-vous à "Répondre à une alerte de ransomware détectée" .

Avant d'utiliser Data Infrastructure Insights Storage Workload Security pour détecter un comportement utilisateur anormal, vous devez configurer l'option à l'aide de l'option **Paramètres** de BlueXP ransomware protection .

Se référer à "Configurer les paramètres de BlueXP ransomware protection" .

Sélectionnez les charges de travail à découvrir et à protéger

Avec cette version, vous pouvez désormais effectuer les opérations suivantes :

- Dans chaque connecteur, sélectionnez les environnements de travail dans lesquels vous souhaitez découvrir les charges de travail. Vous pourriez bénéficier de cette fonctionnalité si vous souhaitez protéger des charges de travail spécifiques dans votre environnement et pas d'autres.
- Lors de la découverte de charges de travail, vous pouvez activer la découverte automatique des charges de travail par connecteur. Cette fonctionnalité vous permet de sélectionner les charges de travail que vous souhaitez protéger.
- Découvrez les charges de travail nouvellement créées pour les environnements de travail précédemment sélectionnés.

Se référer à "Découvrir les charges de travail" .

7 novembre 2024

Activer la classification des données et rechercher des informations personnelles identifiables (PII)

Avec cette version, vous pouvez activer la BlueXP classification, un composant essentiel de la famille BlueXP , pour analyser et classer les données dans vos charges de travail de partage de fichiers. La classification des données vous aide à identifier si vos données contiennent des informations personnelles ou privées, ce qui peut augmenter les risques de sécurité. Ce processus a également un impact sur l'importance de la charge de travail et vous aide à garantir que vous protégez les charges de travail avec le niveau de protection approprié.

L'analyse des données PII dans la BlueXP ransomware protection est généralement disponible pour les clients qui ont déployé la BlueXP classification. La BlueXP classification est disponible dans le cadre de la plateforme BlueXP sans frais supplémentaires et peut être déployée sur site ou dans le cloud client.

Se référer à "Configurer les paramètres de BlueXP ransomware protection" .

Pour lancer l'analyse, sur la page Protection, cliquez sur **Identifier l'exposition** dans la colonne Exposition à la confidentialité.

"Recherchez des données sensibles personnellement identifiables avec la BlueXP classification" .

Intégration SIEM avec Microsoft Sentinel

Vous pouvez désormais envoyer des données à votre système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces à l'aide de Microsoft Sentinel. Auparavant, vous pouviez sélectionner AWS Security Hub ou Splunk Cloud comme SIEM.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

Essai gratuit maintenant 30 jours

Avec cette version, les nouveaux déploiements de la BlueXP ransomware protection bénéficient désormais d'un essai gratuit de 30 jours. Auparavant, la BlueXP ransomware protection offrait 90 jours d'essai gratuit. Si vous bénéficiez déjà de l'essai gratuit de 90 jours, cette offre se poursuit pendant 90 jours.

Restaurer la charge de travail de l'application au niveau du fichier pour Podman

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais afficher une liste des fichiers susceptibles d'avoir été affectés par une attaque et identifier ceux que vous souhaitez restaurer. Auparavant, si les connecteurs BlueXP d'une organisation (auparavant un compte) utilisaient Podman, cette fonctionnalité était désactivée. Il est désormais activé pour Podman. Vous pouvez laisser la BlueXP ransomware protection choisir les fichiers à restaurer, vous pouvez télécharger un fichier CSV qui répertorie tous les fichiers impactés par une alerte, ou vous pouvez identifier manuellement les fichiers que vous souhaitez restaurer.

"En savoir plus sur la récupération après une attaque de ransomware" .

30 septembre 2024

Regroupement personnalisé des charges de travail de partage de fichiers

Avec cette version, vous pouvez désormais regrouper les partages de fichiers en groupes pour faciliter la protection de votre parc de données. Le service peut protéger tous les volumes d'un groupe en même temps. Auparavant, vous deviez protéger chaque volume séparément.

"En savoir plus sur le regroupement des charges de travail de partage de fichiers dans les stratégies de protection contre les ransomwares" .

2 septembre 2024

Évaluation des risques de sécurité par Digital Advisor

La BlueXP ransomware protection collecte désormais des informations sur les risques de sécurité élevés et critiques liés à un cluster à partir de NetApp Digital Advisor. Si un risque est détecté, la BlueXP ransomware protection fournit une recommandation dans le volet **Actions recommandées** du tableau de bord : « Corriger une vulnérabilité de sécurité connue sur le cluster <nom>. » À partir de la recommandation sur le tableau de bord, cliquer sur **Examiner et corriger** suggère de consulter Digital Advisor et un article sur les vulnérabilités et expositions courantes (CVE) pour résoudre le risque de sécurité. S'il existe plusieurs risques de sécurité, consultez les informations dans Digital Advisor.

Se référer à "Documentation du Digital Advisor" .

Sauvegarde sur Google Cloud Platform

Avec cette version, vous pouvez définir une destination de sauvegarde sur un bucket Google Cloud Platform.

Auparavant, vous pouviez ajouter des destinations de sauvegarde uniquement à NetApp StorageGRID, Amazon Web Services et Microsoft Azure.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

Prise en charge de Google Cloud Platform

Le service prend désormais en charge Cloud Volumes ONTAP pour Google Cloud Platform pour la protection du stockage. Auparavant, le service prenait uniquement en charge Cloud Volumes ONTAP pour Amazon Web Services et Microsoft Azure ainsi que le NAS sur site.

"En savoir plus sur la BlueXP ransomware protection et les sources de données prises en charge, les destinations de sauvegarde et les environnements de travail" .

Contrôle d'accès basé sur les rôles

Vous pouvez désormais limiter l'accès à des activités spécifiques grâce au contrôle d'accès basé sur les rôles (RBAC). La BlueXP ransomware protection utilise deux rôles de BlueXP: administrateur de compte BlueXP et administrateur non-compte (spectateur).

Pour plus de détails sur les actions que chaque rôle peut effectuer, voir "Privilèges de contrôle d'accès basés sur les rôles" .

5 août 2024

Détection des menaces avec Splunk Cloud

Vous pouvez envoyer automatiquement des données à votre système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces. Avec les versions précédentes, vous pouviez sélectionner uniquement AWS Security Hub comme SIEM. Avec cette version, vous pouvez sélectionner AWS Security Hub ou Splunk Cloud comme SIEM.

"En savoir plus sur la configuration des paramètres de BlueXP ransomware protection" .

1er juillet 2024

Apportez votre propre permis de conduire (BYOL)

Avec cette version, vous pouvez utiliser une licence BYOL, qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp .

"En savoir plus sur la configuration des licences" .

Restaurer la charge de travail de l'application au niveau du fichier

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais afficher une liste des fichiers susceptibles d'avoir été affectés par une attaque et identifier ceux que vous souhaitez restaurer. Vous pouvez laisser la BlueXP ransomware protection choisir les fichiers à restaurer, vous pouvez télécharger un fichier CSV qui répertorie tous les fichiers impactés par une alerte, ou vous pouvez identifier manuellement les fichiers que vous souhaitez restaurer.

Avec cette version, si tous les connecteurs BlueXP d'un compte n'utilisent pas Podman, la fonction de restauration de fichier unique est activée. Sinon, il est désactivé pour ce compte.

"En savoir plus sur la récupération après une attaque de ransomware" .

Télécharger une liste des fichiers impactés

Avant de restaurer une charge de travail d'application au niveau du fichier, vous pouvez désormais accéder à la page Alertes pour télécharger une liste des fichiers impactés dans un fichier CSV, puis utiliser la page Récupération pour télécharger le fichier CSV.

"En savoir plus sur le téléchargement des fichiers concernés avant de restaurer une application" .

Supprimer le plan de protection

Avec cette version, vous pouvez désormais supprimer une stratégie de protection contre les ransomwares.

"En savoir plus sur la protection des charges de travail et la gestion des stratégies de protection contre les ransomwares" .

10 juin 2024

Verrouillage de copie instantanée sur le stockage principal

Activez cette option pour verrouiller les copies instantanées 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.

"En savoir plus sur la protection des charges de travail et l'activation du verrouillage des sauvegardes dans une stratégie de protection contre les ransomwares" .

Prise en charge de Cloud Volumes ONTAP pour Microsoft Azure

Cette version prend en charge Cloud Volumes ONTAP pour Microsoft Azure en tant que système en plus de Cloud Volumes ONTAP pour AWS et du NAS ONTAP sur site.

"Démarrage rapide de Cloud Volumes ONTAP dans Azure"

"En savoir plus sur la BlueXP ransomware protection" .

Microsoft Azure ajouté comme destination de sauvegarde

Vous pouvez désormais ajouter Microsoft Azure comme destination de sauvegarde avec AWS et NetApp StorageGRID.

"En savoir plus sur la configuration des paramètres de protection" .

14 mai 2024

Mises à jour des licences

Vous pouvez vous inscrire pour un essai gratuit de 90 jours. Bientôt, vous pourrez acheter un abonnement à la carte auprès d'Amazon Web Services Marketplace ou apporter votre propre licence NetApp .

"En savoir plus sur la configuration des licences" .

Protocole CIFS

Le service prend désormais en charge ONTAP sur site et Cloud Volumes ONTAP dans les systèmes AWS utilisant les protocoles NFS et CIFS. La version précédente ne prenait en charge que le protocole NFS.

Détails de la charge de travail

Cette version fournit désormais plus de détails sur les informations de charge de travail à partir des pages Protection et autres pour une meilleure évaluation de la protection de la charge de travail. À partir des détails de la charge de travail, vous pouvez consulter la politique actuellement attribuée et examiner les destinations de sauvegarde configurées.

"En savoir plus sur l'affichage des détails de la charge de travail dans les pages de protection" .

Protection et récupération cohérentes avec les applications et les machines virtuelles

Vous pouvez désormais effectuer une protection cohérente au niveau des applications avec le logiciel NetApp SnapCenter et une protection cohérente au niveau des machines virtuelles avec le SnapCenter Plug-in for VMware vSphere, en obtenant un état de repos et cohérent pour éviter toute perte de données potentielle ultérieure si une récupération est nécessaire. Si une récupération est nécessaire, vous pouvez restaurer l'application ou la machine virtuelle à l'un des états précédemment disponibles.

"En savoir plus sur la protection des charges de travail" .

Stratégies de protection contre les ransomwares

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 ce service :

- Politique d'instantané
- Politique de sauvegarde
- Politique de détection

"En savoir plus sur la protection des charges de travail" .

Détection des menaces

L'activation de la détection des menaces est désormais disponible à l'aide d'un système tiers de gestion de la sécurité et des événements (SIEM). Le tableau de bord affiche désormais une nouvelle recommandation « Activer la détection des menaces » qui peut être configurée sur la page Paramètres.

"En savoir plus sur la configuration des options de paramètres" .

Ignorer les alertes de faux positifs

Depuis l'onglet Alertes, vous pouvez désormais ignorer les faux positifs ou décider de récupérer vos données immédiatement.

"En savoir plus sur la réponse à une alerte de ransomware" .

État de détection

De nouveaux statuts de détection apparaissent sur la page Protection, indiquant le statut de la détection de

ransomware appliquée à la charge de travail.

"En savoir plus sur la protection des charges de travail et l'affichage des états de protection" .

Télécharger les fichiers CSV

Vous pouvez télécharger des fichiers CSV* à partir des pages Protection, Alertes et Récupération.

"En savoir plus sur le téléchargement de fichiers CSV à partir du tableau de bord et d'autres pages" .

Lien vers la documentation

Le lien vers la documentation est désormais inclus dans l'interface utilisateur. Vous pouvez accéder à cette documentation à partir du tableau de bord vertical **Actions***  **option. Sélectionnez *Quoi de neuf** pour afficher les détails dans les notes de publication ou **Documentation** pour afficher la page d'accueil de la documentation sur la BlueXP ransomware protection .

BlueXP backup and recovery

Le service de BlueXP backup and recovery n'a plus besoin d'être déjà activé sur le système. Voir "prérequis" . Le service de BlueXP ransomware protection permet de configurer une destination de sauvegarde via l'option Paramètres. Voir "Configurer les paramètres" .

Option Paramètres

Vous pouvez désormais configurer des destinations de sauvegarde dans les paramètres de BlueXP ransomware protection .

"En savoir plus sur la configuration des options de paramètres" .

5 mars 2024

Gestion des politiques de protection

En plus d'utiliser des politiques prédéfinies, vous pouvez désormais créer des politiques. "En savoir plus sur la gestion des politiques" .

Immuabilité sur le stockage secondaire (DataLock)

Vous pouvez désormais rendre la sauvegarde immuable dans le stockage secondaire à l'aide de la technologie NetApp DataLock dans le magasin d'objets. "En savoir plus sur la création de politiques de protection" .

Sauvegarde automatique sur NetApp StorageGRID

En plus d'utiliser AWS, vous pouvez désormais choisir StorageGRID comme destination de sauvegarde. "En savoir plus sur la configuration des destinations de sauvegarde" .

Fonctionnalités supplémentaires pour enquêter sur les attaques potentielles

Vous pouvez désormais afficher davantage de détails médico-légaux pour enquêter sur l'attaque potentielle détectée. "En savoir plus sur la réponse à une alerte de ransomware détectée" .

Processus de récupération

Le processus de récupération a été amélioré. Vous pouvez désormais récupérer volume par volume ou tous les volumes d'une charge de travail. "En savoir plus sur la récupération après une attaque de ransomware (après la neutralisation des incidents)" .

"En savoir plus sur la BlueXP ransomware protection" .

6 octobre 2023

Le service de BlueXP ransomware protection est une solution SaaS permettant de protéger les données, de détecter les attaques potentielles et de récupérer les données après une attaque de ransomware.

Pour la version préliminaire, le service protège les charges de travail applicatives d'Oracle, les banques de données de machines virtuelles et les partages de fichiers sur le stockage NAS sur site ainsi que sur Cloud Volumes ONTAP sur AWS (en utilisant le protocole NFS) au sein des organisations BlueXP individuellement et sauvegarde les données sur le stockage cloud Amazon Web Services.

Le service de BlueXP ransomware protection offre une utilisation complète de plusieurs technologies NetApp afin que votre administrateur de sécurité des données ou votre ingénieur des opérations de sécurité puisse atteindre les objectifs suivants :

- Affichez en un coup d'œil la protection contre les ransomwares sur toutes vos charges de travail.
- Obtenez un aperçu des recommandations de protection contre les ransomwares
- Améliorez votre posture de protection en fonction des recommandations de BlueXP ransomware protection .
- Attribuez des politiques de protection contre les ransomwares pour protéger vos principales charges de travail et vos données à haut risque contre les attaques de ransomwares.
- Surveillez la santé de vos charges de travail contre les attaques de ransomware à la recherche d'anomalies de données.
- Évaluez rapidement l'impact des incidents de ransomware sur votre charge de travail.
- Récupérez intelligemment des incidents de ransomware en restaurant les données et en garantissant qu'aucune réinfection à partir des données stockées ne se produise.

"En savoir plus sur la BlueXP ransomware protection" .

Limitations connues de NetApp Ransomware Resilience

Les limitations connues identifient les plates-formes, les appareils ou les fonctions qui ne sont pas pris en charge par cette version du produit ou qui n'interagissent pas correctement avec elle. Examinez attentivement ces limitations.

Problème d'option de réinitialisation de l'exercice de préparation

Si vous sélectionnez un volume ONTAP 9.11.1 pour l'exercice de préparation aux attaques de ransomware, Ransomware Resilience envoie une alerte. Si vous récupérez les données à l'aide de l'option « cloner sur volume » et réinitialisez la perceuse, l'opération de réinitialisation échoue.

Limitations Amazon FSx for NetApp ONTAP

Le système Amazon FSx for NetApp ONTAP est pris en charge dans Ransomware Resilience. Les limitations suivantes s'appliquent à Amazon FSx pour ONTAP:

- Les stratégies de sauvegarde ne sont pas prises en charge pour Amazon FSx for ONTAP. Dans cet environnement, vous devez effectuer les opérations de sauvegarde à l'aide d'Amazon FSx for ONTAP. Vous pouvez restaurer ces charges de travail grâce à Ransomware Resilience.
- Les opérations de restauration sont effectuées uniquement à partir de snapshots.

Limitations d'Azure NetApp Files

Azure NetApp Files est pris en charge dans Ransomware Resilience. Les limitations suivantes s'appliquent à Azure NetApp Files :

- Les stratégies de protection contre les ransomwares avec des politiques de sauvegarde ne sont pas prises en charge pour Azure NetApp Files. Vous pouvez utiliser la sauvegarde Azure NetApp Files à la place.
- Les stratégies de protection contre les ransomwares avec réplication ne sont pas prises en charge pour Azure NetApp Files.
- Lors du choix d'une stratégie de protection, assurez-vous que sa fréquence de création d'instantanés est compatible avec Azure NetApp Files. La fréquence de création d'instantanés la plus fréquente disponible dans Azure NetApp Files est horaire.

Commencer

En savoir plus sur la NetApp Ransomware Resilience

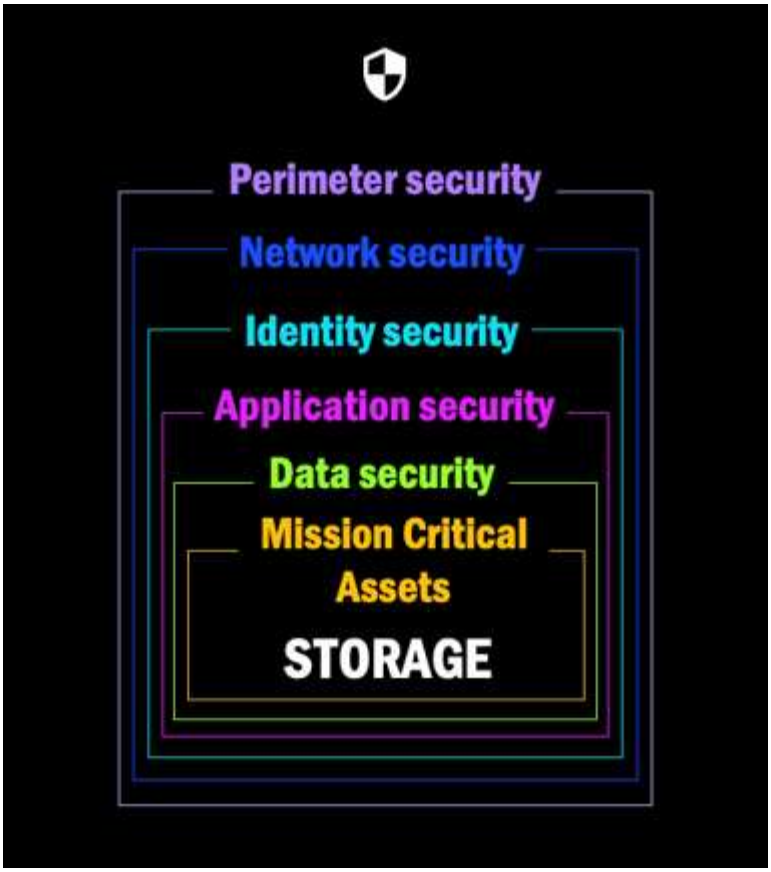
Les attaques de ransomware peuvent bloquer l'accès à vos données et les attaquants peuvent demander une rançon en échange de la divulgation des données ou de leur décryptage. Selon l'IDC, il n'est pas rare que les victimes de ransomware subissent plusieurs attaques de ransomware. L'attaque peut perturber l'accès à vos données pendant une durée allant d'un jour à plusieurs semaines.

NetApp Ransomware Resilience protège vos données contre les attaques de ransomware. Dans Ransomware Resilience, la protection est disponible pour les charges de travail applicatives d'Oracle, les banques de données VM et les partages de fichiers sur le stockage NAS sur site (utilisant les protocoles NFS et CIFS) et le stockage SAN (FC, iSCSI et NVMe), ainsi que pour Cloud Volumes ONTAP pour Amazon Web Services, Cloud Volumes ONTAP pour Google Cloud, Cloud Volumes ONTAP pour Microsoft Azure et Amazon FSx for NetApp ONTAP via la NetApp Console. Vous pouvez sauvegarder des données sur Amazon Web Services, Google Cloud, le stockage cloud Microsoft Azure et NetApp StorageGRID.

Résilience aux ransomwares au niveau de la couche de données

Votre posture de sécurité comprend généralement plusieurs couches de défense pour vous protéger contre une gamme de cybermenaces.

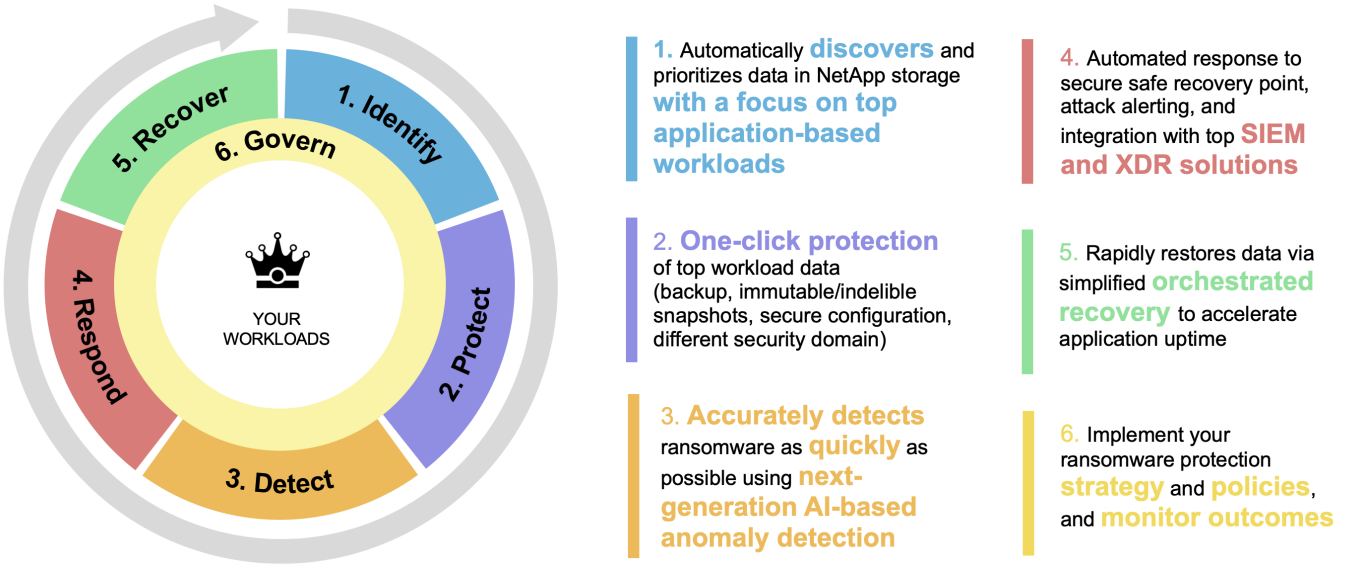
- **Couche la plus externe** : il s'agit de votre première ligne de défense utilisant des pare-feu, des systèmes de détection d'intrusion et des réseaux privés virtuels pour protéger les limites du réseau.
- **Sécurité du réseau** : Cette couche s'appuie sur la base de la segmentation du réseau, de la surveillance du trafic et du chiffrement.
- **Sécurité des identités** : utilise des méthodes d'authentification, des contrôles d'accès et une gestion des identités pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources sensibles.
- **Sécurité des applications** : protège les applications logicielles à l'aide de pratiques de codage sécurisées, de tests de sécurité et d'autoprotection des applications d'exécution.
- **Sécurité des données** : Protégez vos données grâce à des stratégies de protection des données, de sauvegarde et de récupération. La résilience aux ransomwares opère sur cette couche.



Ce que vous pouvez faire avec Ransomware Resilience

Ransomware Resilience offre une utilisation complète de plusieurs technologies NetApp afin que votre administrateur de stockage, administrateur de sécurité des données ou ingénieur des opérations de sécurité puisse atteindre les objectifs suivants :

- **Identifier** toutes les charges de travail basées sur des applications, des partages de fichiers ou gérées par VMware dans les systèmes NAS (NFS ou CIFS) et SAN (FC, iSCSI et NVMe) NetApp sur site, à travers la NetApp Console, les projets et les agents de console. Ransomware Resilience catégorise la priorité des données et vous fournit des recommandations pour améliorer la résilience des ransomwares.
- **Protégez** vos charges de travail en activant les sauvegardes, les copies instantanées et les stratégies de protection contre les ransomwares sur vos données.
- **Détecter** les anomalies qui pourraient être des attaques de ransomware.note de bas de page : [Bien qu'il soit possible qu'une attaque passe inaperçue, nos recherches indiquent que la technologie NetApp a permis un degré élevé de détection de certaines attaques de ransomware basées sur le chiffrement de fichiers.]
- Répondre aux potentielles attaques de ransomware en lançant automatiquement une capture instantanée verrouillée afin que la copie ne puisse pas être supprimée accidentellement ou malicieusement. Vos données de sauvegarde resteront immuables et protégées de bout en bout contre les attaques de ransomware, aussi bien à la source qu'à destination.
- **Récupérez** vos charges de travail qui contribuent à accélérer la disponibilité des charges de travail en orchestrant plusieurs technologies NetApp . Vous pouvez choisir de récupérer des volumes spécifiques. Ransomware Resilience fournit des recommandations sur les meilleures options.
- **Gouverner** : Mettez en œuvre votre stratégie de protection contre les ransomwares et surveillez les résultats.



Avantages de l'utilisation de Ransomware Resilience

Ransomware Resilience offre les avantages suivants :

- Découvre les charges de travail et leurs planifications de snapshots et de sauvegarde existantes, et classe leur importance relative.
- Évalue votre posture de protection contre les ransomwares et l'affiche dans un tableau de bord facile à comprendre.
- Fournit des recommandations sur les prochaines étapes en fonction de l'analyse de la posture de découverte et de protection.
- Applique les recommandations de protection des données basées sur l'IA/ML avec un accès en un clic.
- Protège les données dans les charges de travail applicatives telles que les datastores Oracle et VMware, ainsi que les partages de fichiers.
- Détecte les attaques de ransomware sur les données en temps réel sur le stockage principal à l'aide de la technologie d'IA.
- Lance des actions automatisées en réponse aux attaques potentielles détectées en créant des copies instantanées et en lançant des alertes sur une activité anormale.
- Applique une récupération organisée pour respecter les politiques RPO. Ransomware Resilience orchestre la récupération après des incidents de ransomware en utilisant plusieurs services de récupération NetApp , notamment NetApp Backup and Recovery (anciennement Cloud Backup) et SnapCenter.
- Utilise le contrôle d'accès basé sur les rôles (RBAC) pour gérer l'accès aux fonctionnalités et aux opérations.

Coût

Vous pouvez essayer Ransomware Resilience avec un essai gratuit de 30 jours. NetApp ne vous facture pas l'utilisation de la version d'essai de Ransomware Resilience.

Si vous disposez à la fois de Backup and Recovery et de Ransomware Resilience, toutes les données communes protégées par les deux produits sont facturées uniquement par Ransomware Resilience.

Après l'achat d'une licence ou d'un abonnement PayGo, toute charge de travail disposant d'une politique de

détection de ransomware (Autonomous Ransomware Protection) activée (découverte ou définie par Ransomware Resilience) et d'au moins une politique de snapshot ou de sauvegarde, Ransomware Resilience la classe comme « Protégée » et elle est comptabilisée dans la capacité achetée ou l'abonnement PayGo. Si une charge de travail est découverte sans politique de détection, même si elle dispose de politiques de sauvegarde ou de snapshot, elle est classée « À risque » et elle n'est pas comptabilisée dans la capacité achetée.

Les charges de travail protégées sont comptabilisées dans la capacité achetée ou dans l'abonnement après la fin de la période d'essai de 90 jours. Ransomware Resilience est facturé par Go pour les données associées aux charges de travail protégées avant les gains d'efficacité.

Licences

Avec Ransomware Resilience, vous pouvez utiliser différents plans de licence, notamment un essai gratuit, un abonnement à la carte ou apporter votre propre licence.

Ransomware Resilience nécessite une licence NetApp ONTAP One.

La licence Ransomware Resilience n'inclut pas de produits NetApp supplémentaires. Ransomware Resilience peut utiliser Backup and Recovery même si vous ne disposez pas de licence pour cela.

Pour détecter les comportements anormaux des utilisateurs, Ransomware Resilience utilise NetApp Autonomous Ransomware Protection, un modèle d'apprentissage automatique (ML) au sein ONTAP qui détecte l'activité des fichiers malveillants. Ce modèle est inclus dans la licence Ransomware Resilience.

Pour plus de détails, consultez la section "Configurer les licences" .

NetApp Console

La résilience aux ransomwares est accessible via la NetApp Console.

La NetApp Console fournit une gestion centralisée des services de stockage et de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise. La console est requise pour accéder aux services de données NetApp et les utiliser. En tant qu'interface de gestion, il vous permet de gérer de nombreuses ressources de stockage à partir d'une seule interface. Les administrateurs de console peuvent contrôler l'accès au stockage et aux services pour tous les systèmes de l'entreprise.

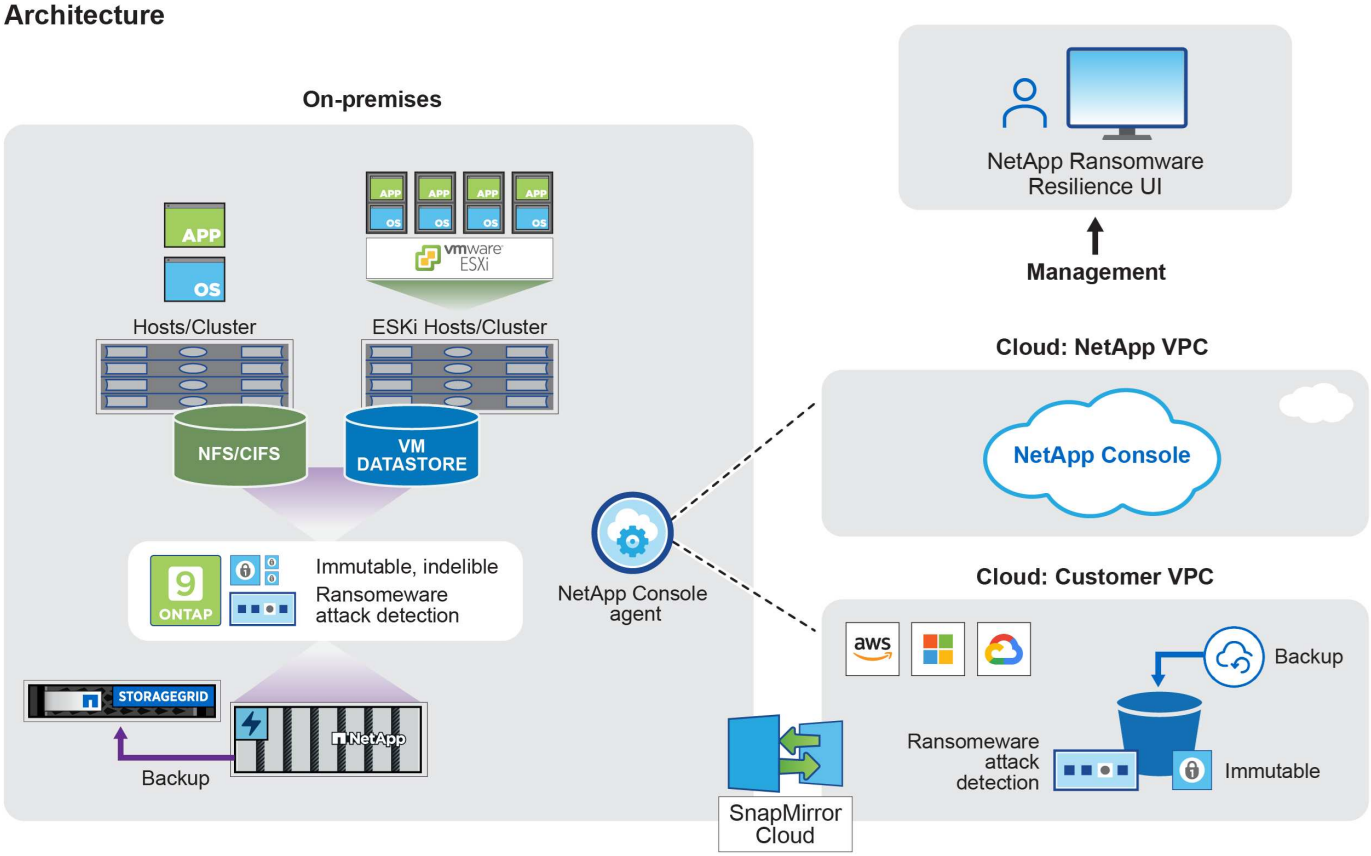
Vous n'avez besoin d'aucune licence ni d'abonnement pour commencer à utiliser NetApp Console et vous n'encourez des frais que lorsque vous déployez des agents Console dans votre cloud pour assurer la connectivité à vos systèmes de stockage ou aux services de données NetApp. Cependant, certains services de données NetApp accessibles depuis la Console sont sous licence ou nécessitent un abonnement.

En savoir plus sur le"NetApp Console" .

Comment fonctionne la résilience aux ransomwares

Ransomware Resilience utilise NetApp Backup and Recovery pour découvrir et définir des stratégies de snapshot et de sauvegarde pour les charges de travail de partage de fichiers, et SnapCenter ou SnapCenter pour VMware pour découvrir et définir des stratégies de snapshot et de sauvegarde pour les charges de travail des applications et des machines virtuelles. De plus, Ransomware Resilience utilise Backup and Recovery et SnapCenter / SnapCenter pour VMware pour effectuer une récupération cohérente au niveau des fichiers et des charges de travail.

Architecture



Fonctionnalité	Description
IDENTIFIER	• Recherche toutes les données NAS (protocoles NFS et CIFS) sur site du client, SAN (FC, iSCSI et NVMe) et Cloud Volumes ONTAP connectées à la console. • Identifie les données client des API de service ONTAP et SnapCenter et les associe aux charges de travail. En savoir plus sur "ONTAP" et "Logiciel SnapCenter" . • Découvre le niveau de protection actuel de chaque volume des copies instantanées NetApp et des politiques de sauvegarde, ainsi que toutes les capacités de détection intégrées. Ransomware Resilience associe ensuite cette posture de protection aux charges de travail en utilisant Backup and Recovery, les services ONTAP et les technologies NetApp telles que la protection autonome contre les ransomwares (ARP ou ARP/AI selon votre version ONTAP), FPolicy, les politiques de sauvegarde et les politiques de snapshot. Apprenez-en davantage sur "Protection autonome contre les ransomwares" , "NetApp Backup and Recovery" , et "Politique ONTAP" . • Attribue une priorité métier à chaque charge de travail en fonction des niveaux de protection découverts automatiquement et recommande des politiques de protection pour les charges de travail en fonction de leur priorité métier. La priorité de la charge de travail est basée sur les fréquences d'instantanés déjà appliquées à chaque volume associé à la charge de travail.
PROTÉGER	• Surveille activement les charges de travail et orchestre l'utilisation des API Backup and Recovery, SnapCenter et ONTAP en appliquant des politiques à chacune des charges de travail identifiées.

Fonctionnalité	Description
DÉTECTER	• Détecte les attaques potentielles avec un modèle d'apprentissage automatique (ML) intégré qui détecte le cryptage et les activités potentiellement anormaux. • Fournit une détection à double couche qui commence par détecter les attaques potentielles de ransomware dans le stockage principal et répond aux activités anormales en effectuant des copies instantanées automatisées supplémentaires pour créer les points de restauration de données les plus proches. Ransomware Resilience offre la possibilité d'approfondir les recherches pour identifier les attaques potentielles avec une plus grande précision sans affecter les performances des charges de travail principales. • Détermine les fichiers suspects spécifiques et les cartes qui attaquent les charges de travail associées, à l'aide des technologies ONTAP, Autonomous Ransomware Protection (ARP ou ARP/AI selon votre version ONTAP) et FPolicy.
RÉPONDRE	• Affiche des données pertinentes, telles que l'activité du fichier, l'activité de l'utilisateur et l'entropie, pour vous aider à effectuer des analyses médico-légales sur l'attaque. • Lance des copies instantanées rapides à l'aide des technologies et produits NetApp tels que ONTAP, Autonomous Ransomware Protection (ARP ou ARP/AI selon votre version ONTAP) et FPolicy.
RÉCUPÉRER	• Détermine le meilleur instantané ou la meilleure sauvegarde et recommande le meilleur point de récupération réel (RPA) en utilisant les technologies et services Backup and Recovery, ONTAP, Autonomous Ransomware Protection (ARP ou ARP/AI selon votre version ONTAP) et FPolicy. • Orchestre la récupération des charges de travail, notamment les machines virtuelles, les partages de fichiers, le stockage en blocs et les bases de données avec cohérence des applications.
GOUVERNER	• Attribue les stratégies de protection contre les ransomwares • Vous aide à surveiller les résultats.

Cibles de sauvegarde, systèmes et sources de données de charge de travail pris en charge

Ransomware Resilience prend en charge les cibles de sauvegarde, les systèmes et les sources de données suivants :

Cibles de sauvegarde prises en charge

- Amazon Web Services (AWS) S3
- Plateforme Google Cloud
- Blob Microsoft Azure
- NetApp StorageGRID

Systèmes pris en charge

Environnement	Protocole	Versions prises en charge
Amazon FSx for NetApp ONTAP*	CIFS, NFS et SAN	S/O
Azure NetApp Files	CIFS et NFS	S/O
Cloud Volumes ONTAP pour AWS	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
Cloud Volumes ONTAP pour Google Cloud Platform	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
Cloud Volumes ONTAP pour Microsoft Azure	CIFS et NFS	9.12.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
ONTAP (sur site)	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures

Amazon FSx for NetApp ONTAP utilise la protection autonome contre les ransomwares (ARP) et non ARP/AI. Pour plus d'informations sur la différence, voir"ARP/IA" .

> L'utilisation d'ARP/AI dans ONTAP nécessite ONTAP 9.16 ou une version supérieure. + ONTAP ne fournit pas de prise en charge de la protection contre les ransomwares pour les volumes FabricPool FlexCache, FlexGroup , les volumes de points de montage de groupes de cohérence, les volumes de chemin de montage, les volumes hors ligne et les volumes de protection des données (DP). Assurez-vous de consulter"Configurations prises en charge et non prises en charge dans ONTAP" .

Sources de données de charge de travail prises en charge

Ransomware Resilience protège les charges de travail basées sur les applications suivantes sur les volumes de données principaux :

- Stockage en bloc
- Bases de données:
  - Microsoft SQL Server
  - Oracle
  - PostgreSQL
- Partages de fichiers NetApp
- Banques de données VMware

Si vous utilisez SnapCenter ou SnapCenter pour VMware, toutes les charges de travail prises en charge par ces produits sont également identifiées dans Ransomware Resilience. Ransomware Resilience peut protéger et récupérer ces données de manière cohérente avec la charge de travail.

Termes clés

Il pourrait être utile de comprendre certains termes liés à la protection contre les ransomwares.

- **Protection** : La protection dans Ransomware Resilience signifie garantir que des instantanés et des sauvegardes immuables se produisent régulièrement dans un domaine de sécurité différent à l'aide de politiques de protection.
- **Charge de travail** : Une charge de travail dans Ransomware Resilience peut inclure des bases de données Oracle, des datastores VMware ou des partages de fichiers.

Conditions préalables à la NetApp Ransomware Resilience

Commencez par vérifier la préparation de votre environnement opérationnel, de votre accès réseau et de votre navigateur Web afin d'évaluer la NetApp Ransomware Resilience .

Pour utiliser Ransomware Resilience, assurez-vous de remplir les conditions préalables.

Systèmes pris en charge

Assurez-vous d'utiliser un système pris en charge :

Environnement	Protocole	Versions prises en charge
Amazon FSx for NetApp ONTAP*	CIFS, NFS et SAN	S/O
Azure NetApp Files	CIFS et NFS	S/O
Cloud Volumes ONTAP pour AWS	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
Cloud Volumes ONTAP pour Google Cloud Platform	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
Cloud Volumes ONTAP pour Microsoft Azure	CIFS et NFS	9.12.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures
ONTAP (sur site)	CIFS et NFS	9.11.1 et versions ultérieures
	SAN (FC, iSCSI et NVMe)	9.17.1 et versions ultérieures

Amazon FSx for NetApp ONTAP utilise la protection autonome contre les ransomwares (ARP) et non ARP/AI. Pour plus d'informations sur la différence, voir"ARP/IA" .

Configuration requise NetApp Console

La configuration de votre NetApp Console requiert :

- Un compte utilisateur de la NetApp Console avec des privilèges d'administrateur d'organisation pour la découverte des ressources.
- Une organisation et un système de console avec au moins un agent de console actif connecté à un"système pris en charge" .
  - Si vos clusters ONTAP locaux ou Cloud Volumes ONTAP dans AWS ou dans le cloud Azure ne sont pas configurés dans la console, consultez"Apprenez à configurer un agent de console" et"exigences standard de la console" .

> Si vous disposez de plusieurs agents de console dans une seule organisation de console, Ransomware Resilience analysera les ressources ONTAP sur tous les agents de console au-delà de celui actuellement sélectionné dans l'interface utilisateur de la console.

- L'agent de la console doit avoir le `cloudmanager-ransomware-protection` conteneur dans un état actif.
- Au moins un système de console avec un cluster ONTAP sur site NetApp ou Cloud Volumes ONTAP dans AWS ou Azure. Ransomware Resilience prend en charge les protocoles NAS (NFS et SMB) et SAN (iSCSI, FC et NVMe).
  - La résilience aux ransomwares est prise en charge avec les clusters ONTAP ou Cloud Volumes ONTAP avec la version ONTAP 9.11.1 ou supérieure.

> Pour utiliser Ransomware Resilience sur les charges de travail SAN, vous devez exécuter ONTAP 9.17.1 ou une version ultérieure.

Exigences ONTAP

- Vous devez utiliser ONTAP 9.11.1 ou une version ultérieure avec une licence ONTAP One activée sur l'instance ONTAP locale. Pour plus d'informations sur la prise en charge ONTAP , consultez"Présentation de la protection autonome contre les ransomwares" .
- Pour appliquer des configurations de protection (telles que l'activation de la protection autonome contre les ransomwares), Ransomware Resilience a besoin de droits d'administrateur sur le cluster ONTAP . Le cluster ONTAP aurait dû être intégré à l'aide des informations d'identification de l'utilisateur administrateur du cluster ONTAP uniquement.

> Si vous avez connecté un cluster ONTAP à la console avec des informations d'identification non administrateur, [vous devez mettre à jour les informations d'identification dans le cluster ONTAP](#update-non-admin-user-permissions-in-an-ontap-system).

Sauvegardes de données

- Un compte dans NetApp StorageGRID, AWS S3, Azure Blob ou Google Cloud Platform pour les cibles de sauvegarde avec les autorisations d'accès appropriées configurées.

  Se référer à la "Liste des autorisations AWS, Azure ou S3" pour plus de détails.

- NetApp Backup and Recovery n'a pas besoin d'être activé sur le système.

  Ransomware Resilience permet de configurer une destination de sauvegarde via l'option Paramètres. Voir "Configurer les paramètres" .

Exigences relatives aux comportements suspects des utilisateurs

Pour que Ransomware Resilience puisse fournir des alertes concernant un comportement utilisateur suspect, vous devez configurer un agent d'activité utilisateur. Pour installer un agent d'activité utilisateur, assurez-vous que votre système répond "les exigences".

Mettre à jour les autorisations des utilisateurs non administrateurs dans un système ONTAP

Si vous devez mettre à jour les autorisations des utilisateurs non administrateurs pour un système particulier, utilisez ces étapes de procédure.

1. Connectez-vous à la Console. Dans le tableau de bord, identifiez le système dont les autorisations utilisateur ONTAP doivent être mises à jour.
2. Sélectionnez le système pour afficher ses détails.
3. Sélectionnez **Afficher les informations supplémentaires** pour afficher le nom d'utilisateur.
4. Connectez-vous à l'interface de ligne de commande du cluster ONTAP en tant qu'utilisateur administrateur.
5. Afficher les rôles existants pour cet utilisateur :

```
security login show -user-or-group-name <username>
```

6. Modifier le rôle de l'utilisateur. Entrer:

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. Retournez à la NetApp Console pour utiliser la résilience face aux ransomwares.

Démarrage rapide pour NetApp Ransomware Resilience

Comprenez les étapes de haut niveau que vous devez suivre pour configurer la résilience aux ransomwares et protéger vos charges de travail.

Suivez les liens à chaque étape pour des informations détaillées.

Réviser les prérequis

Ces tâches nécessitent le rôle *Console admin*.

- "Assurez-vous d'avoir installé un agent de console"
- "Assurez-vous que votre système répond aux exigences"
- "Examiner les rôles des utilisateurs de Ransomware Resilience et attribuer des autorisations aux utilisateurs accédant à Ransomware Resilience"
- "Configurer les licences"

Démarrer avec Ransomware Resilience

Ces tâches nécessitent le rôle *Ransomware Resilience admin*.

- "Découvrir les charges de travail dans la console"
- "Afficher l'état de protection de la charge de travail sur le tableau de bord"
- "En option, effectuez un exercice de préparation aux attaques de ransomware"

3 **Configurer la protection et la détection dans Ransomware Resilience**

Ces tâches nécessitent le rôle *Ransomware Resilience admin*. La configuration d'une activité de comportement utilisateur suspecte nécessite le rôle supplémentaire *Ransomware Resilience user behavior admin*.

- "Protéger les charges de travail"
  - En option,"améliorer la protection en configurant la détection des activités suspectes des utilisateurs"
- Vous pouvez également configurer les destinations de sauvegarde :
  - "Préparez NetApp StorageGRID, Amazon Web Services, Google Cloud Platform ou Microsoft Azure comme destination de sauvegarde" .
  - "Configurer les destinations de sauvegarde"
- "Répondre à la détection d'attaques potentielles de ransomware"
- "Se remettre d'une attaque (après neutralisation des incidents)"

4 **Quelle est la prochaine étape ?**

Après avoir configuré la protection dans Ransomware Resilience, voici ce que vous pouvez faire ensuite.

- "Activer la classification des données pour identifier les risques de gouvernance et de sécurité"
- "Envoyer des alertes au SIEM"
- "Téléchargez des rapports d'alerte, de protection, d'exercice de préparation, de récupération ou de synthèse"

Configurer la NetApp Ransomware Resilience

Vous pouvez facilement déployer NetApp Ransomware Resilience. Avant de commencer, révisez"prérequis" pour garantir que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez l'une des destinations de sauvegarde suivantes :

- NetApp StorageGRID
- Amazon Web Services
- Plateforme Google Cloud
- Microsoft Azure

Après avoir configuré les options dans la destination de sauvegarde elle-même, vous la configurerez plus tard comme destination de sauvegarde dans Ransomware Resilience. Pour plus de détails sur la configuration de la destination de sauvegarde dans Ransomware Resilience, reportez-vous à"Configurer les destinations de

sauvegarde" .

Préparez StorageGRID pour devenir une destination de sauvegarde

Si vous souhaitez utiliser StorageGRID comme destination de sauvegarde, reportez-vous à "Documentation de StorageGRID" pour plus de détails sur StorageGRID.

Préparez AWS à devenir une destination de sauvegarde

- Configurez un compte dans AWS.
- Configure "Autorisations AWS" dans AWS.

Pour plus de détails sur la gestion de votre stockage AWS dans la console, reportez-vous à "Gérez vos buckets Amazon S3" .

Préparez Azure à devenir une destination de sauvegarde

- Configurez un compte dans Azure.
- Configure "Autorisations Azure" dans Azure.

Pour plus de détails sur la gestion de votre stockage Azure dans la console, reportez-vous à "Gérez vos comptes de stockage Azure" .

Configurer la NetApp Console

L'étape suivante consiste à configurer la console et la résilience aux ransomwares.

Revoir "Configuration requise pour la console en mode standard" .

Créer un agent de console

Contactez votre représentant commercial NetApp pour essayer ou utiliser ce service. Ensuite, lorsque vous utilisez l'agent de console, il inclura les fonctionnalités appropriées pour la résilience aux ransomwares.

Pour créer un agent de console à l'aide de Ransomware Resilience, contactez l'administrateur de votre organisation de console qui dispose des autorisations nécessaires pour créer des agents de console et reportez-vous à la documentation qui décrit "comment créer un agent de console" .

Si vous disposez de plusieurs agents de console, Ransomware Resilience analyse les données sur tous les agents de console au-delà de celui qui s'affiche actuellement dans la console. Ce service découvre tous les projets et tous les agents de console associés à cette organisation.

Accéder à la NetApp Ransomware Resilience

Connectez-vous à NetApp Ransomware Resilience 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

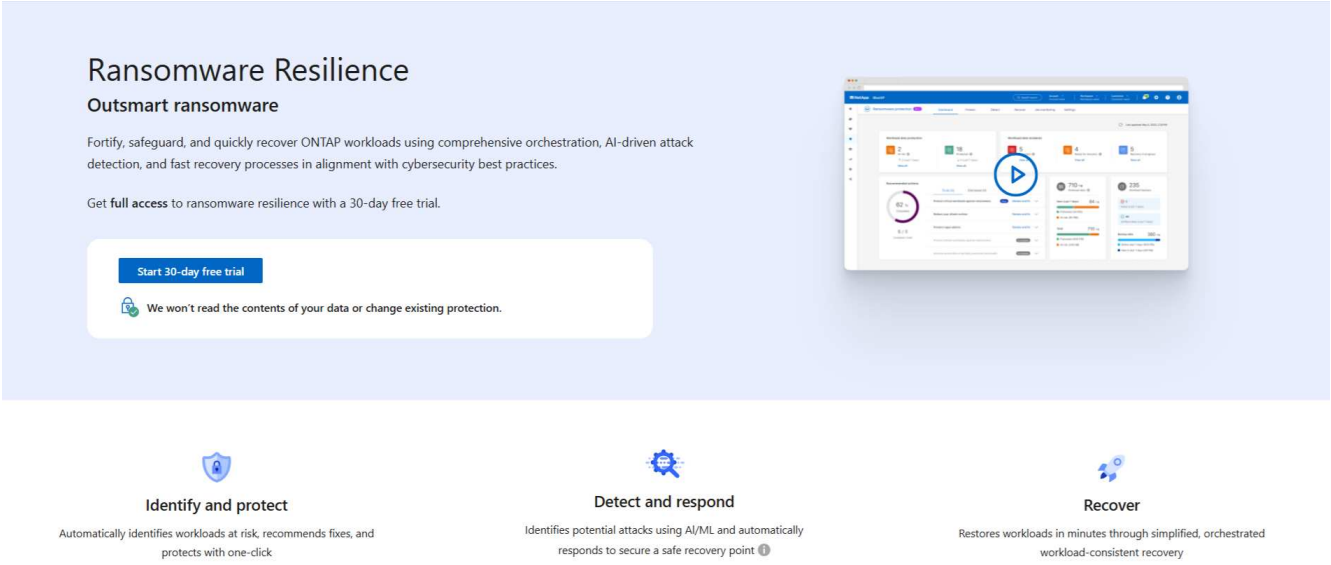
1. Ouvrez un navigateur Web et accédez à"la console" .

   La page de connexion à la console apparaît.

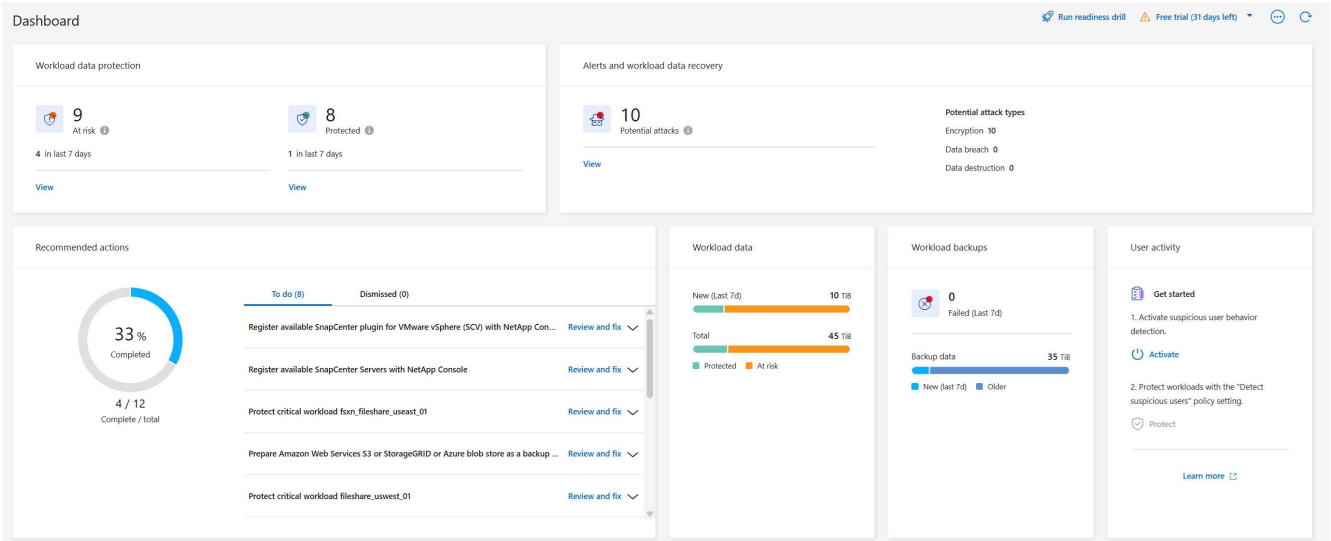
2. Connectez-vous à la console.
3. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.

   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" .

Configurer les licences pour NetApp Ransomware Resilience

Avec NetApp Ransomware Resilience, vous pouvez utiliser différents plans de licence.

Pour effectuer cette tâche, vous avez besoin du rôle d'administrateur d'organisation, de dossier ou de projet. "En savoir plus sur les rôles d'accès à la console" .

Types de licences

Ransomware Resilience est disponible avec les types de licences suivants :

- Essai gratuit de 30 jours
- Achetez un abonnement à la carte (PAYGO) avec Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace ou Azure Marketplace
- Apportez votre propre licence (BYOL) : un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp . Vous pouvez utiliser le numéro de série de la licence pour activer le BYOL dans la console.

Après avoir configuré votre BYOL ou acheté un abonnement PAYGO, vous pouvez voir la licence dans la section Licenses and subscriptions de la console.

Une fois l'essai gratuit terminé ou la licence ou l'abonnement expiré, vous pouvez toujours :

- Afficher les charges de travail et l'état de la charge de travail
- Supprimer des ressources telles que des politiques
- Exécutez toutes les opérations planifiées créées pendant la période d'essai ou sous la licence

Autres licences

La licence Ransomware Resilience n'inclut pas de produits NetApp supplémentaires. Cependant, Ransomware Resilience peut s'intégrer à NetApp Backup and Recovery, même si vous ne disposez pas d'une licence distincte pour Backup and Recovery.

> Si vous disposez à la fois de Backup and Recovery et de Ransomware Resilience, toutes les données communes protégées par les deux produits seront facturées uniquement par Ransomware Resilience.

Essayez Ransomware Resilience avec un essai gratuit de 30 jours

Vous pouvez essayer Ransomware Resilience avec un essai gratuit de 30 jours. Vous devez être administrateur de l'organisation de la console pour démarrer l'essai gratuit.

Les limites de capacité de stockage ne sont pas appliquées pendant l'essai.

Vous pouvez obtenir une licence ou vous abonner à tout moment et vous ne serez pas facturé avant la fin de

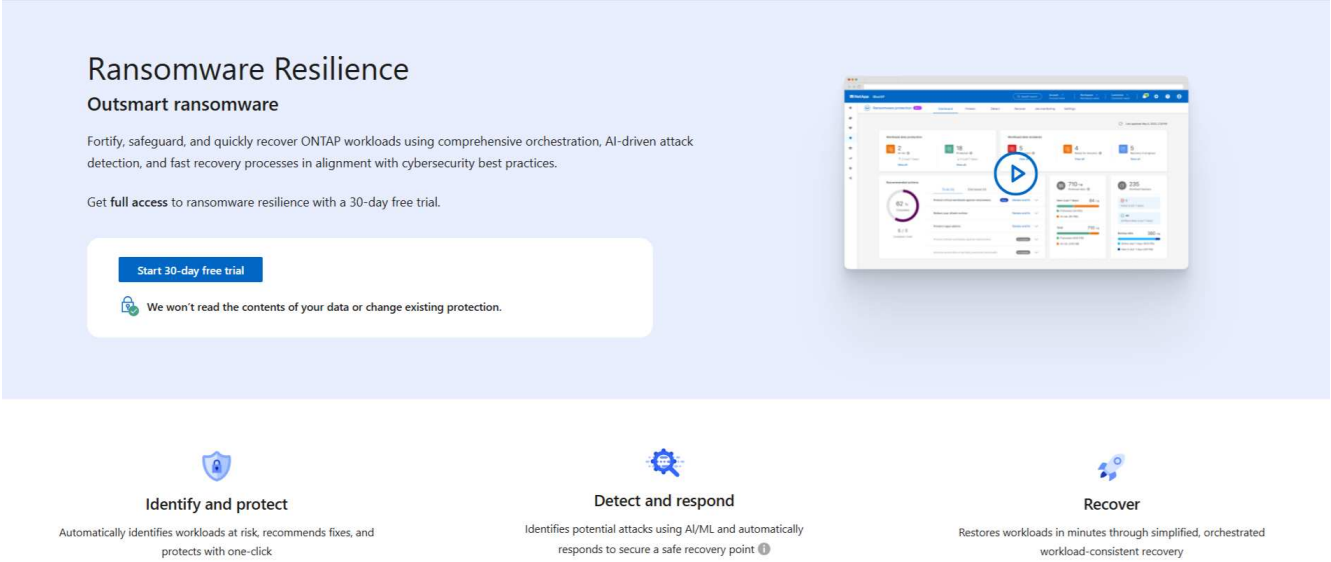
l'essai de 30 jours. Pour continuer après l'essai de 30 jours, vous devrez acheter une licence BYOL ou un abonnement PAYGO.

Pendant la période d'essai, vous bénéficiez de toutes les fonctionnalités.

Étapes

1. Accéder au "Console" .
2. Connectez-vous à la console.
3. Depuis la NetApp Console, sélectionnez **Protection** > **Résilience aux ransomwares**.

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



4. Si vous n'avez pas déjà ajouté un agent de console pour d'autres services,"ajouter un" .
5. Sur la page d'accueil de Ransomware Resilience, sélectionnez **Commencer par découvrir les charges de travail** pour découvrir vos charges de travail.

   Cette option n'est disponible que si vous avez installé avec succès un agent de console.

6. Pour consulter les informations sur l'essai gratuit, sélectionnez l'option déroulante en haut à droite.

Une fois la période d'essai terminée, obtenez un abonnement ou une licence

Une fois l'essai gratuit terminé, vous pouvez vous abonner via l'une des places de marché ou acheter une licence auprès de NetApp.

Si vous disposez déjà d'un abonnement PAYGO, la licence est automatiquement basculée vers l'abonnement une fois l'essai gratuit terminé.

Abonnez-vous via AWS Marketplace Abonnez-vous via Microsoft Azure Marketplace Abonnez-vous via Google Cloud Platform Marketplace Apportez votre propre permis de conduire (BYOL)

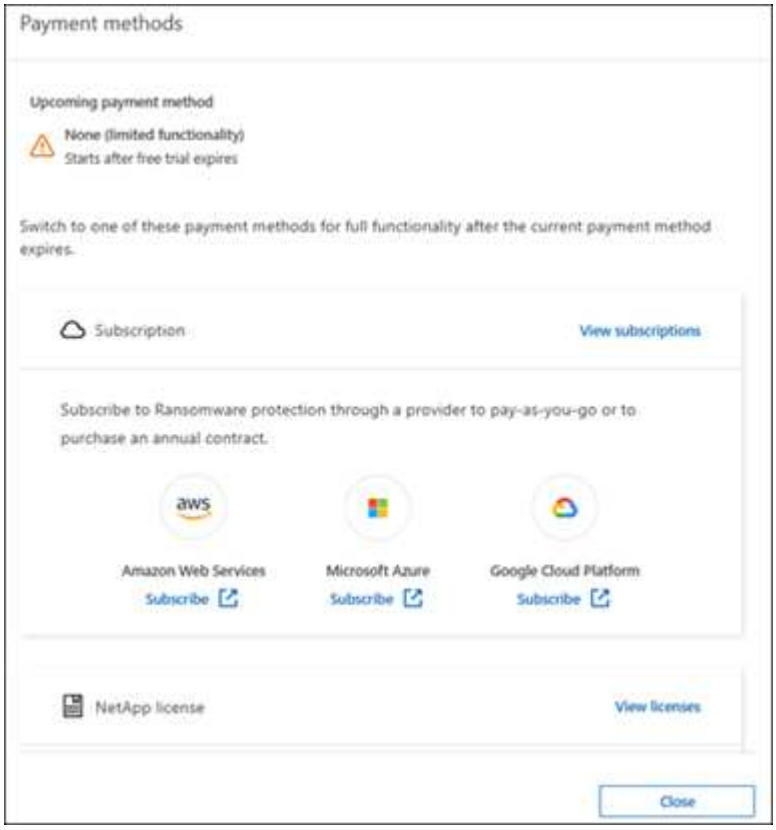
Abonnez-vous via AWS Marketplace

Cette procédure fournit un aperçu de haut niveau sur la manière de s'abonner directement sur AWS

Marketplace.

Étapes

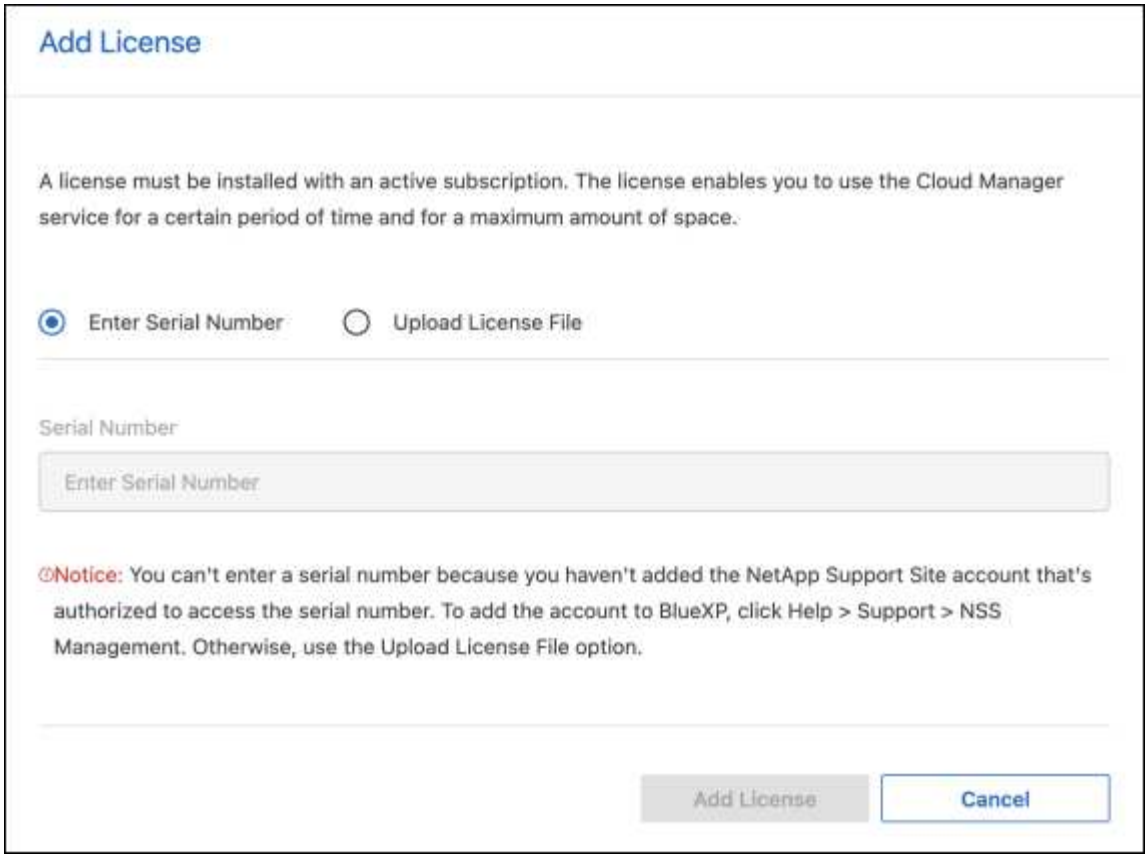
1. Dans Ransomware Resilience, effectuez l'une des opérations suivantes :
   - Si vous recevez un message indiquant que l'essai gratuit est sur le point d'expirer, sélectionnez **Afficher les modes de paiement**.
   - Si vous n'avez pas commencé l'essai, sélectionnez l'avis **Essai gratuit** en haut à droite puis **Afficher les modes de paiement**.



2. Sur la page Modes de paiement, sélectionnez **S'abonner** à **Amazon Web Services**.
3. Dans AWS Marketplace, sélectionnez **Afficher les options d'achat**.
4. Utilisez AWS Marketplace pour vous abonner à * NetApp Intelligent Services* et à **Ransomware Resilience**.
5. Lorsque vous revenez à Ransomware Resilience, un message indique que vous êtes abonné.

   Un e-mail vous est envoyé contenant le numéro de série de Ransomware Resilience et indiquant que Ransomware Resilience est abonné sur AWS Marketplace.

6. Retournez à la page des méthodes de paiement de Ransomware Resilience.
7. Ajoutez la licence à la console en sélectionnant **Ajouter une licence**.



8. Sur la page Ajouter une licence, sélectionnez **Entrer le numéro de série**, saisissez le numéro de série inclus dans l'e-mail qui vous a été envoyé, puis sélectionnez **Ajouter une licence**.
9. Pour afficher les détails de la licence, dans la navigation de gauche de la console, sélectionnez **Administration** > * Licenses and subscriptions*.
   - Pour voir les informations d'abonnement, sélectionnez **Abonnements**.
   - Pour voir les licences BYOL, sélectionnez **Licences de services de données**.
10. Retour à la résilience aux ransomwares. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.

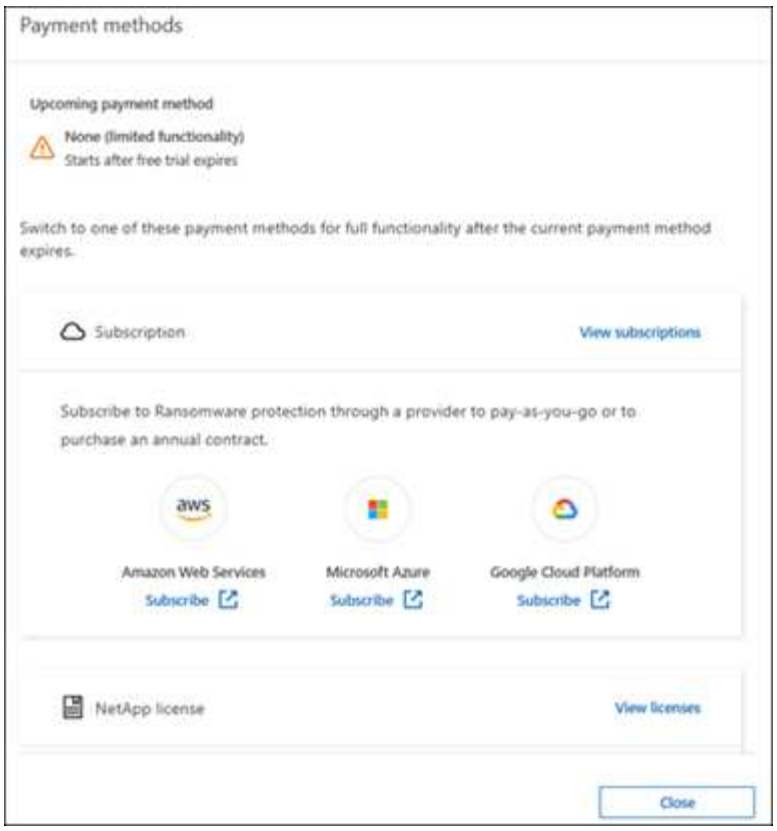
    Un message confirme qu'une licence a été ajoutée.

Abonnez-vous via Microsoft Azure Marketplace

Cette procédure fournit un aperçu de haut niveau de la manière de s'abonner directement sur la Place de marché Azure.

Étapes

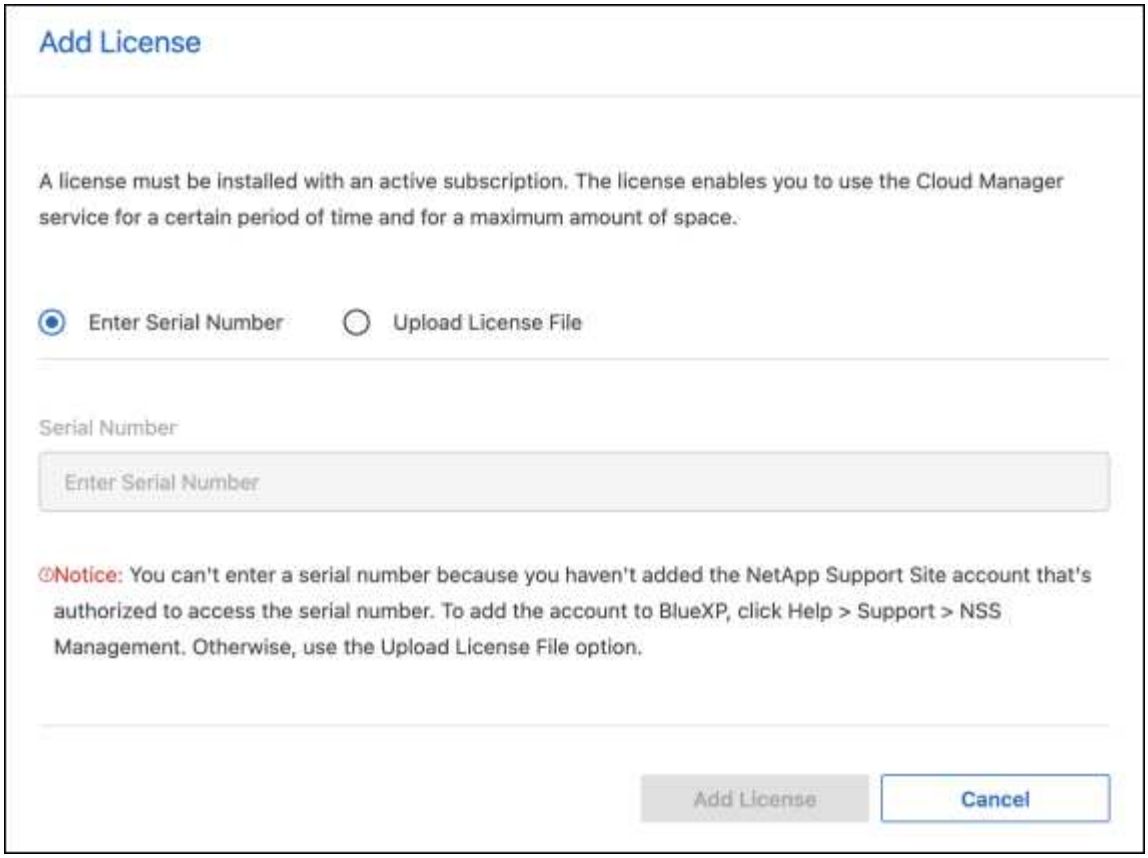
1. Dans Ransomware Resilience, effectuez l'une des opérations suivantes :
   - Si vous recevez un message indiquant que l'essai gratuit est sur le point d'expirer, sélectionnez **Afficher les modes de paiement**.
   - Si vous n'avez pas commencé l'essai, sélectionnez l'avis **Essai gratuit** en haut à droite puis **Afficher les modes de paiement**.



2. Sur la page Modes de paiement, sélectionnez **S'abonner** à **Microsoft Azure Marketplace**.
3. Dans la Place de marché Azure, sélectionnez **Afficher les options d'achat**.
4. Utilisez Azure Marketplace pour vous abonner à * NetApp Intelligent Services* et à **Ransomware Resilience**.
5. Lorsque vous revenez à Ransomware Resilience, un message indique que vous êtes abonné.

> Un e-mail vous est envoyé contenant le numéro de série de Ransomware Resilience et indiquant que Ransomware Resilience est abonné sur Azure Marketplace.

6. Retour à la page Méthodes de paiement de Ransomware Resilience.
7. Pour ajouter la licence, sélectionnez **Ajouter une licence**.



8. Sur la page Ajouter une licence, sélectionnez **Entrer le numéro de série** puis saisissez le numéro de série figurant dans l'e-mail qui vous a été envoyé. Sélectionnez **Ajouter une licence**.
9. Pour afficher les détails de la licence dans Licenses and subscriptions, dans la navigation de gauche de la console, sélectionnez **Gouvernance** > * Licenses and subscriptions*.
   - Pour voir les informations d'abonnement, sélectionnez **Abonnements**.
   - Pour voir les licences BYOL, sélectionnez **Licences de services de données**.
10. Retour à la résilience aux ransomwares. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.

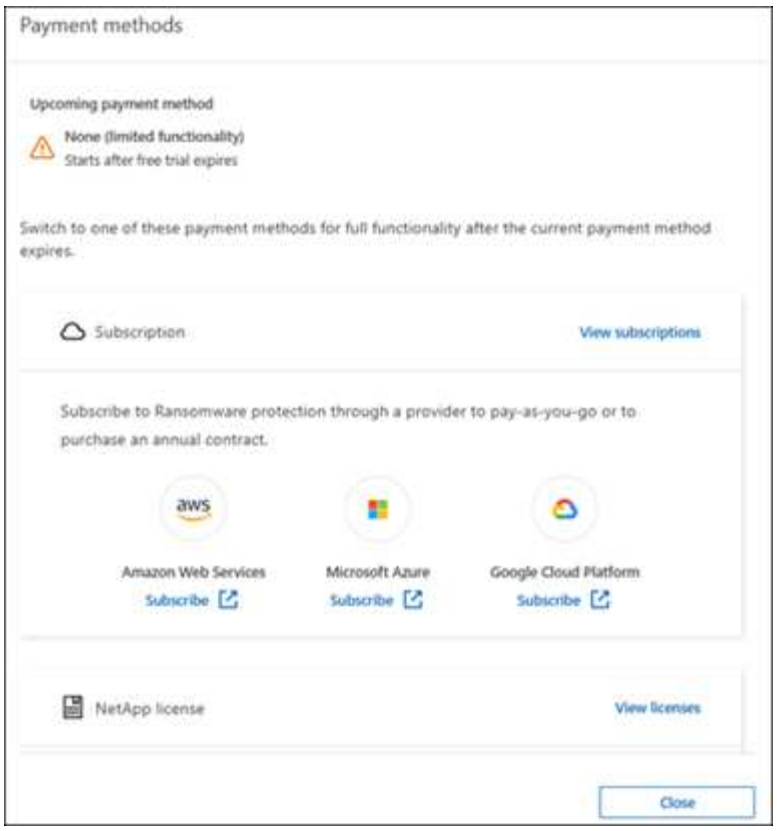
    Un message apparaît indiquant qu'une licence a été ajoutée.

Abonnez-vous via Google Cloud Platform Marketplace

Cette procédure fournit un aperçu de haut niveau sur la manière de s'abonner directement sur Google Cloud Platform Marketplace.

Étapes

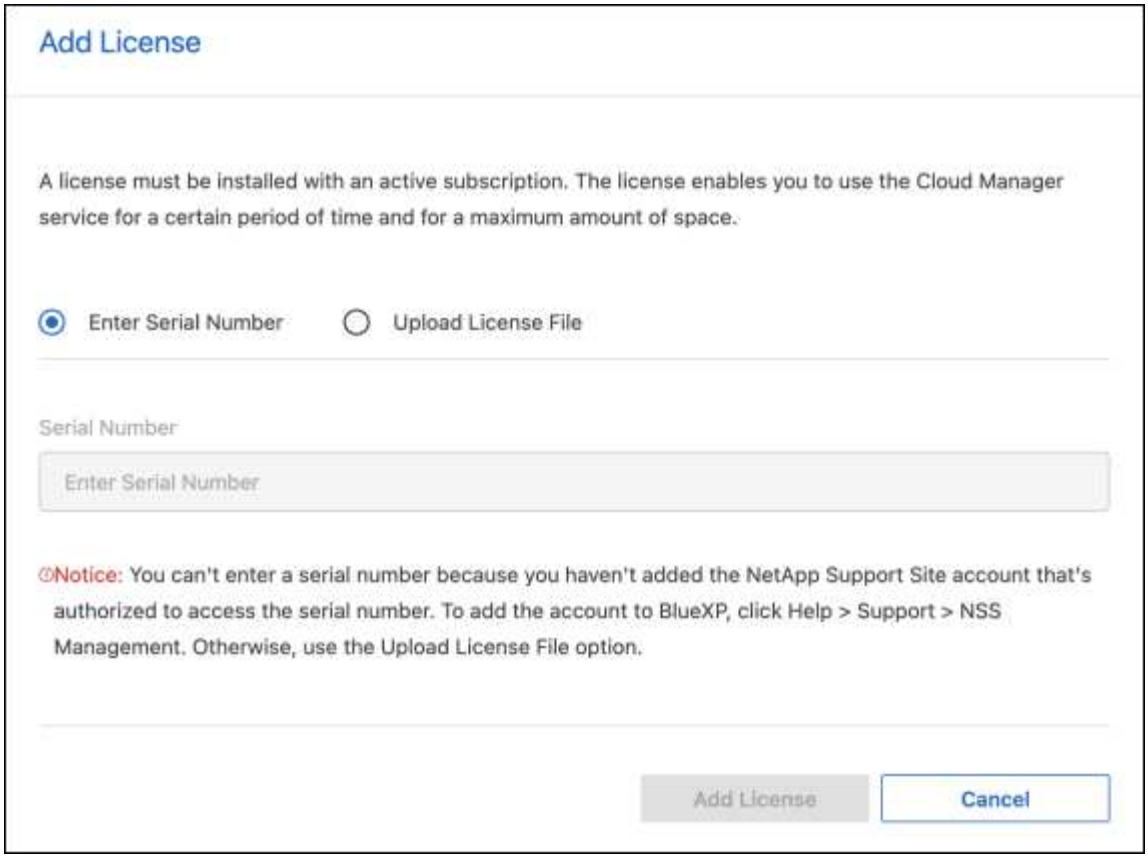
1. Dans Ransomware Resilience, effectuez l'une des opérations suivantes :
   - Si vous recevez un message indiquant que l'essai gratuit est sur le point d'expirer, sélectionnez **Afficher les modes de paiement**.
   - Si vous n'avez pas commencé l'essai, sélectionnez l'avis **Essai gratuit** en haut à droite puis **Afficher les modes de paiement**.



2. Sur la page Modes de paiement, sélectionnez **S'abonner** à Google Cloud Platform Marketplace*.
3. Dans Google Cloud Platform Marketplace, sélectionnez **S'abonner**.
4. Utilisez Google Cloud Platform Marketplace pour vous abonner à * NetApp Intelligent Services* et **Ransomware Resilience**.
5. Lorsque vous revenez à Ransomware Resilience, un message indique que vous êtes abonné.

> Un e-mail vous est envoyé contenant le numéro de série de Ransomware Resilience et indiquant que Ransomware Resilience est abonné sur Google Cloud Platform Marketplace.

6. Retour à la page Méthodes de paiement de Ransomware Resilience.
7. Pour ajouter la licence à la console, sélectionnez **Ajouter une licence**.



8. Dans la page Ajouter une licence, sélectionnez **Entrer le numéro de série**. Saisissez le numéro de série dans l'e-mail qui vous a été envoyé. Sélectionnez **Ajouter une licence**.
9. Pour afficher les détails de la licence, dans la navigation de gauche de la console, sélectionnez **Gouvernance** > * Licenses and subscriptions*.
   - Pour voir les informations d'abonnement, sélectionnez **Abonnements**.
   - Pour voir les licences BYOL, sélectionnez **Licences de services de données**.
10. Retour à la résilience aux ransomwares. Dans la navigation de gauche de la console, sélectionnez **Protection** > **Résilience aux ransomwares**.

    Un message apparaît indiquant qu'une licence a été ajoutée.

Apportez votre propre permis de conduire (BYOL)

Si vous souhaitez apporter votre propre licence (BYOL), vous devez acheter la licence, obtenir le fichier de licence NetApp (NLF), puis ajouter la licence à la console.

Ajoutez votre fichier de licence à la console

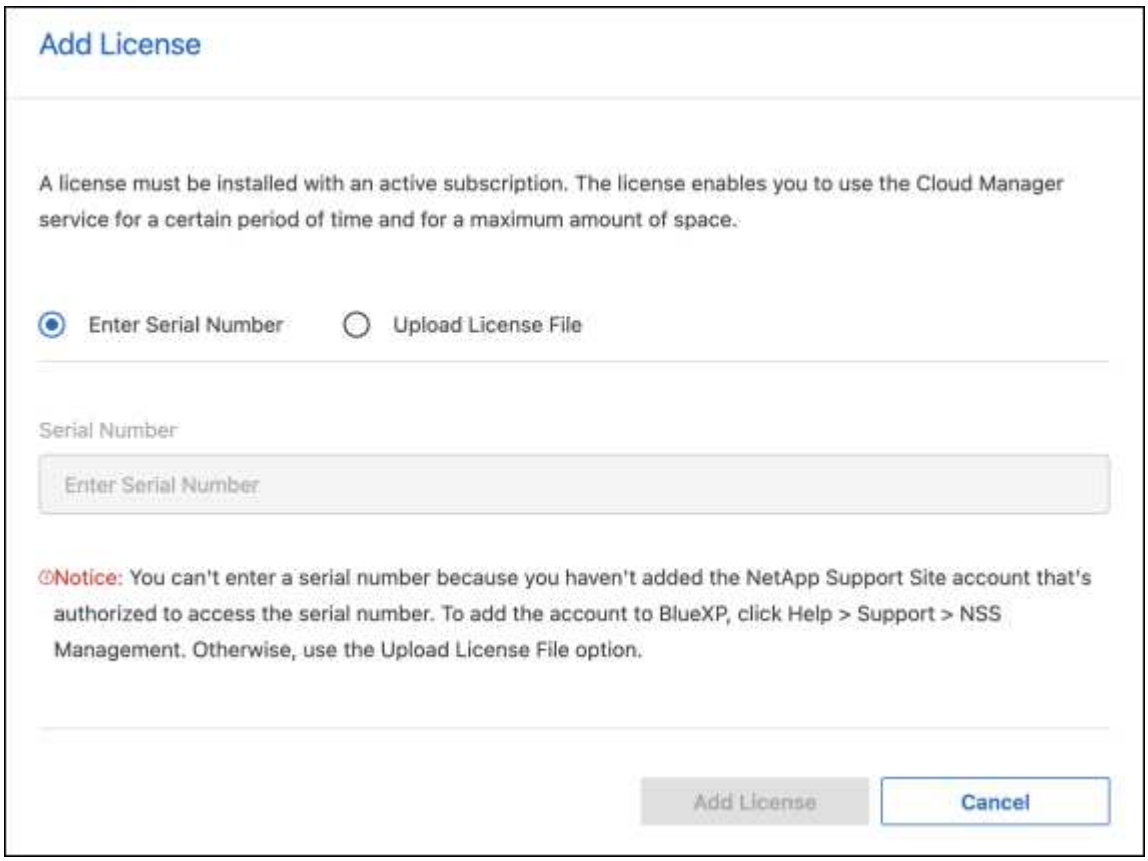
Après avoir acheté votre licence Ransomware Resilience auprès de votre représentant commercial NetApp , vous activez la licence en saisissant le numéro de série Ransomware Resilience et les informations de compte du site de support NetApp (NSS).

Avant de commencer

Vous avez besoin du numéro de série de Ransomware Resilience. Recherchez ce numéro sur votre bon de commande ou contactez l'équipe de compte pour obtenir ces informations.

Étapes

1. Après avoir obtenu la licence, revenez à Ransomware Resilience. Sélectionnez l'option **Afficher les modes de paiement** en haut à droite. Ou, dans le message indiquant que l'essai gratuit expire, sélectionnez **S'abonner ou acheter une licence**.
2. Sélectionnez **Ajouter une licence** pour accéder à la page Licences et abonnements de la console.
3. Dans l'onglet **Licences des services de données**, sélectionnez **Ajouter une licence**.



4. Sur la page Ajouter une licence, saisissez le numéro de série et les informations du compte du site de support NetApp .
   - Si vous disposez du numéro de série de la licence de la console et connaissez votre compte NSS, sélectionnez l'option **Entrer le numéro de série** et saisissez ces informations.

     Si votre compte de site de support NetApp n'est pas disponible dans la liste déroulante, "ajouter le compte NSS à la console" .

   - Si vous disposez du fichier de licence zvondolr (requis lors de l'installation sur un site sombre), sélectionnez l'option **Télécharger le fichier de licence** et suivez les instructions pour joindre le fichier.
5. Sélectionnez **Ajouter une licence**.

Résultat

La page Licenses and subscriptions indique que Ransomware Resilience dispose d'une licence.

Mettez à jour votre licence de console lorsqu'elle expire

Si la durée de votre licence approche de la date d'expiration ou si votre capacité sous licence atteint la limite, vous en serez averti dans l'interface utilisateur de Ransomware Resilience. Vous pouvez mettre à jour votre

licence Ransomware Resilience avant son expiration afin de ne pas interrompre votre capacité à accéder à vos données numérisées.

Ce message apparaît également dans Licenses and subscriptions et dans "Paramètres de notification" .

Étapes

1. Vous pouvez envoyer un e-mail au support pour demander une mise à jour de votre licence.

   Une fois la licence payée et enregistrée sur le site de support NetApp , la console met automatiquement à jour la licence. La page Licences des services de données reflétera le changement dans 5 à 10 minutes.

2. Si la console ne peut pas mettre à jour automatiquement la licence, vous devez télécharger manuellement le fichier de licence.
   a. Vous pouvez obtenir le fichier de licence sur le site de support NetApp .
   b. Dans la console, sélectionnez **Administration** > **Licenses and subscriptions**.
   c. Sélectionnez l'onglet **Licences des services de données**, sélectionnez l'icône **Actions…** pour le numéro de série que vous mettez à jour, puis sélectionnez **Mettre à jour la licence**.

Mettre fin à l'abonnement PAYGO

Si vous souhaitez mettre fin à votre abonnement PAYGO, vous pouvez le faire à tout moment.

Étapes

1. Dans Ransomware Resilience, en haut à droite, sélectionnez l'option de licence.
2. Sélectionnez **Afficher les modes de paiement**.
3. Dans les détails déroulants, décochez la case **Utiliser après l'expiration du mode de paiement actuel**.
4. Sélectionnez **Enregistrer**.

Plus d'informations

- "Documentation relative aux licences et abonnements de NetApp Console"

Découvrez les charges de travail dans NetApp Ransomware Resilience

Avant de pouvoir utiliser NetApp Ransomware Resilience, il est nécessaire de découvrir les données de charge de travail. Lors de la découverte, Ransomware Resilience analyse tous les volumes et fichiers des systèmes sur tous les agents et projets de console au sein d'une organisation.

Dans le tableau de bord Discovery, Ransomware Resilience affiche les configurations système prises en charge et celles qui ne le sont pas. Ransomware Resilience évalue les applications Oracle, les datastores VMware, les partages de fichiers et le stockage par blocs.

Ransomware Resilience ne détecte pas les charges de travail avec des volumes utilisant FlexGroup.

Ransomware Resilience vérifie votre protection de sauvegarde actuelle, vos copies instantanées et vos options de protection autonome contre les ransomwares NetApp . Ransomware Resilience détecte également les informations de protection de SnapCenter for VMware pour les banques de données de machines virtuelles, de SnapCenter for Oracle et de NetApp Backup and Recovery pour les partages de fichiers et les partages de fichiers de machines virtuelles. Il recommande ensuite des moyens d'améliorer votre protection contre les ransomwares.

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" .

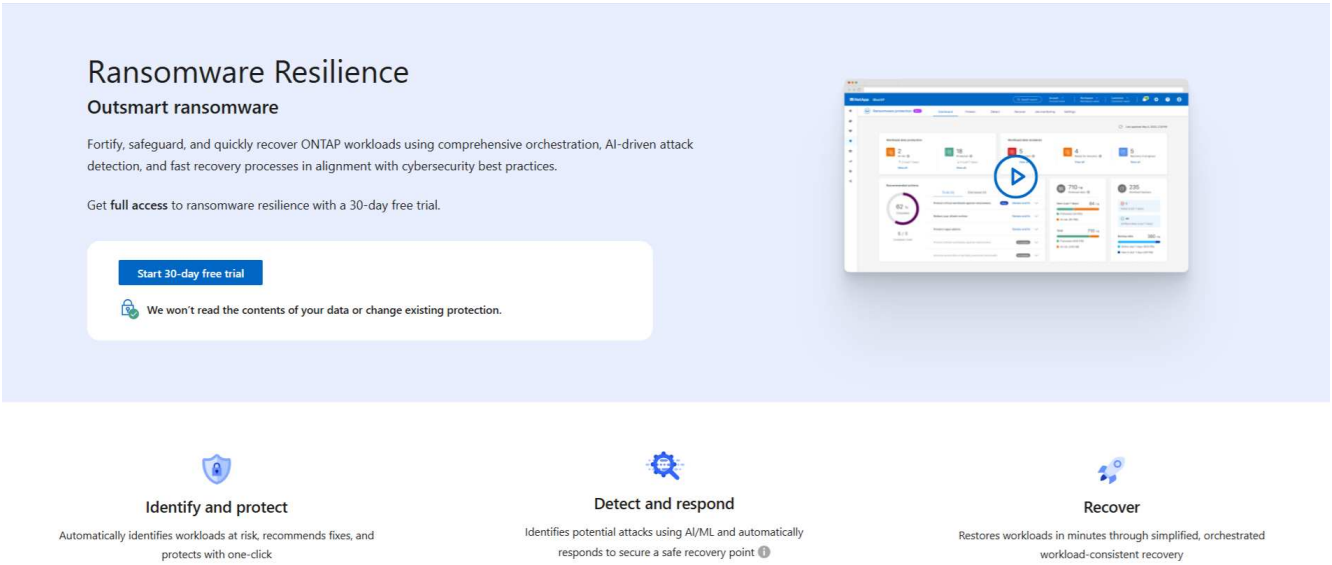
Sélectionnez les charges de travail à découvrir et à protéger

Dans chaque agent de console, sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.

Étapes

1. Depuis la NetApp Console, sélectionnez **Protection** > **Protection contre les ransomwares**.

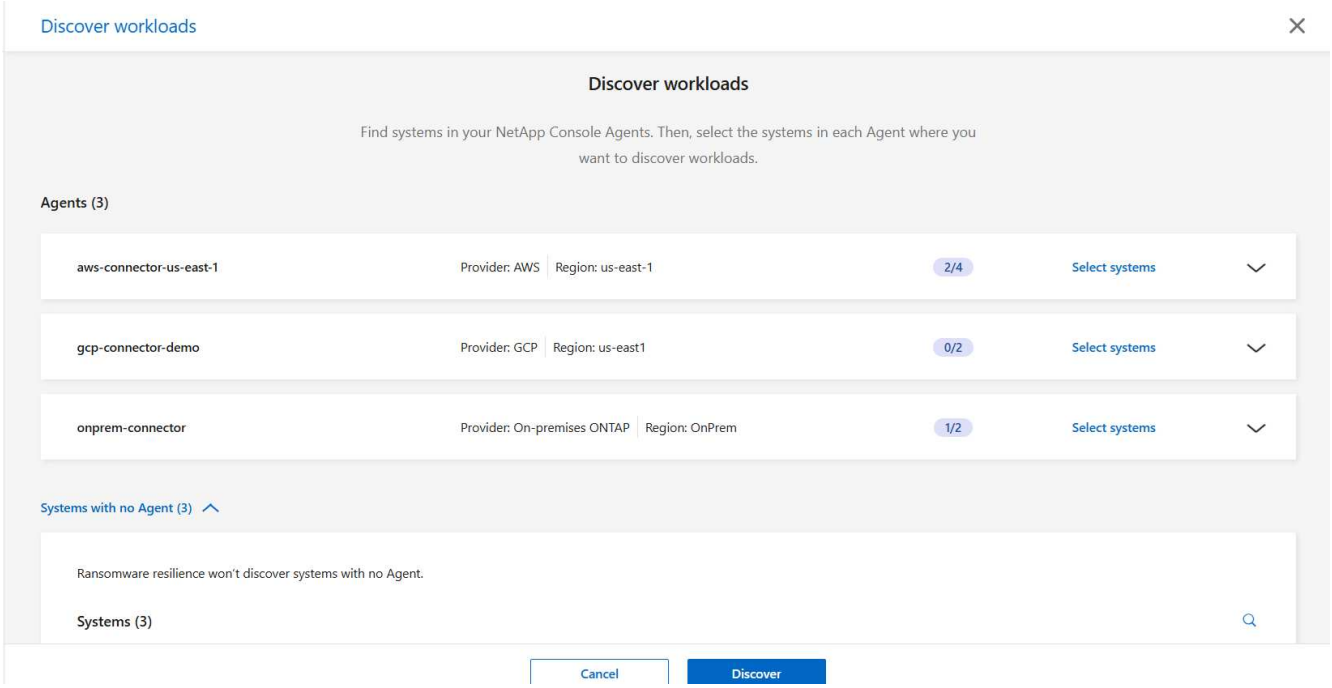
   S'il s'agit de votre première connexion, la page de destination apparaît.



   Si vous avez démarré l'essai gratuit, le libellé du bouton **Démarrer l'essai gratuit de 30 jours** devient **Commencer par découvrir les charges de travail**.

2. Depuis la page d'accueil initiale, sélectionnez **Commencer par découvrir les charges de travail**.

   Ransomware Resilience détecte à la fois les systèmes pris en charge et non pris en charge. Ce processus peut prendre quelques minutes.

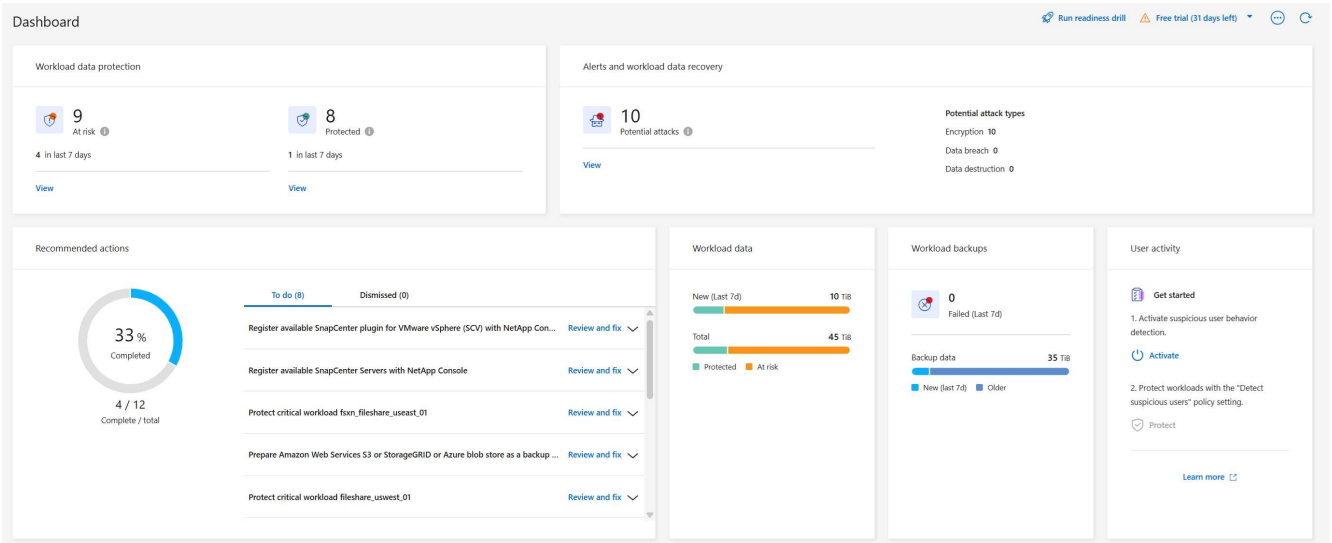


3. Pour découvrir les charges de travail d'un agent de console spécifique, sélectionnez **Sélectionner les systèmes** à côté de l'agent de console pour lequel vous souhaitez découvrir les charges de travail.
4. Sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.
5. Sélectionnez **Découvrir**.

   Ransomware Resilience ne découvre les données de charge de travail que lorsque vous sélectionnez le système. Le processus de découverte peut prendre plusieurs minutes.

6. Pour télécharger la liste des charges de travail découvertes, sélectionnez **Télécharger les résultats**.
7. Pour afficher le tableau de bord de résilience aux ransomwares, sélectionnez **Accéder au tableau de bord**.

   Le tableau de bord affiche l'état de la protection des données. Le nombre de charges de travail à risque ou protégées est mis à jour à mesure que de nouvelles charges de travail sont découvertes.



"Découvrez ce que le tableau de bord vous montre."

Découvrez les charges de travail nouvellement créées pour les systèmes précédemment sélectionnés

Si vous avez ajouté des charges de travail à un système précédemment découvert, vous devez relancer la découverte afin de protéger les nouvelles charges de travail.

Étapes

1. Pour identifier la date et l'heure de la dernière détection, consultez la date et l'heure indiquées à côté de l'icône **Actualiser** en haut à droite du tableau de bord de résilience aux ransomwares.
2. Depuis le tableau de bord, sélectionnez l'icône **Actualiser** pour trouver les nouvelles charges de travail.

> Si vous constatez que certains volumes ne s'affichent pas pour le système que vous avez découvert, il se peut qu'ils ne soient pas pris en charge. Pour trouver une liste des volumes non pris en charge, accédez au menu **Paramètres** puis sélectionnez le menu d'actions dans la carte Découverte de la charge de travail pour télécharger un rapport JSON des volumes pris en charge et non pris en charge.

Découvrez de nouveaux systèmes

Si vous avez déjà découvert des systèmes, vous pouvez en trouver de nouveaux ou des systèmes non sélectionnés auparavant.

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez l'option verticale " option category='inline-code'/> en haut à droite. Dans le menu déroulant, sélectionnez **Paramètres**.
2. Dans la carte Découverte de charge de travail, sélectionnez **Découvrir les charges de travail**. La découverte peut prendre quelques minutes. Une icône de chargement indique la progression.
3. Ransomware Resilience détecte les systèmes pris en charge et non pris en charge. Il ne prend pas en charge un système si sa version ONTAP est inférieure à la version requise. Lorsque vous survolez un système non pris en charge, une info-bulle affiche la raison. Sélectionnez les systèmes sur lesquels vous souhaitez découvrir les charges de travail.
4. Sélectionnez **Découvrir**.

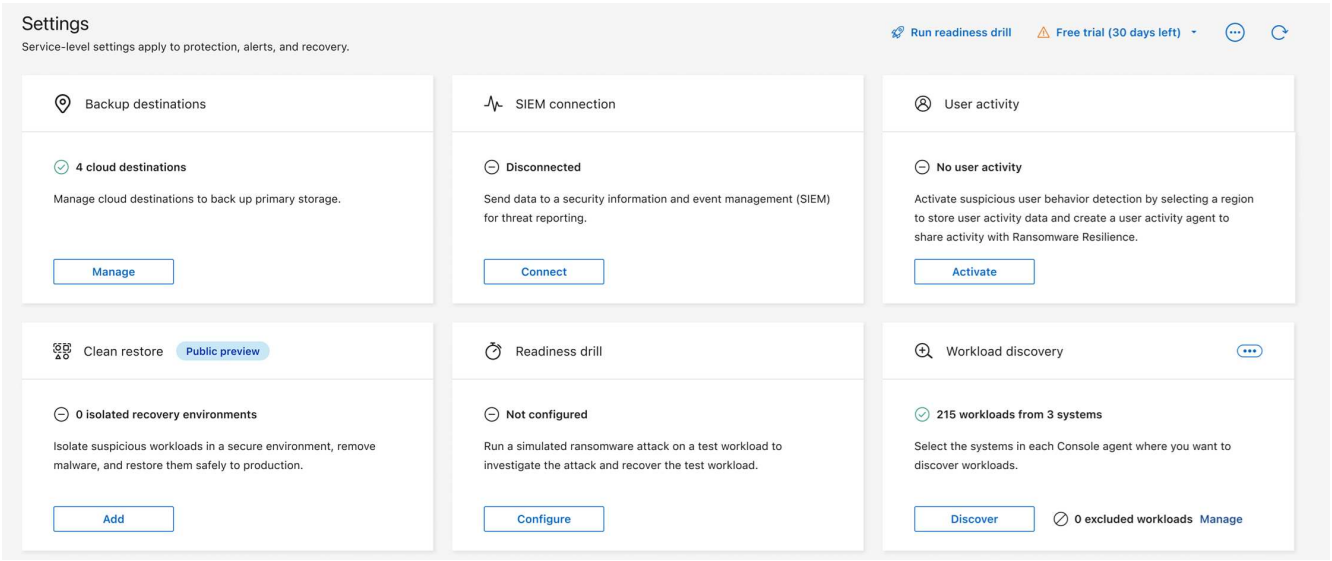
Exclure les charges de travail

La fonctionnalité de résilience aux ransomwares vous permet d'exclure certaines charges de travail d'un système de la protection et de la détection contre les ransomwares.

Vous ne pouvez exclure que les charges de travail prises en charge et qui ont été détectées avec succès. Vous pouvez modifier à tout moment la liste des charges de travail exclues. Vous n'êtes pas facturé pour les charges de travail exclues de la résilience aux ransomwares.

Ajouter des charges de travail à la liste des charges de travail exclues

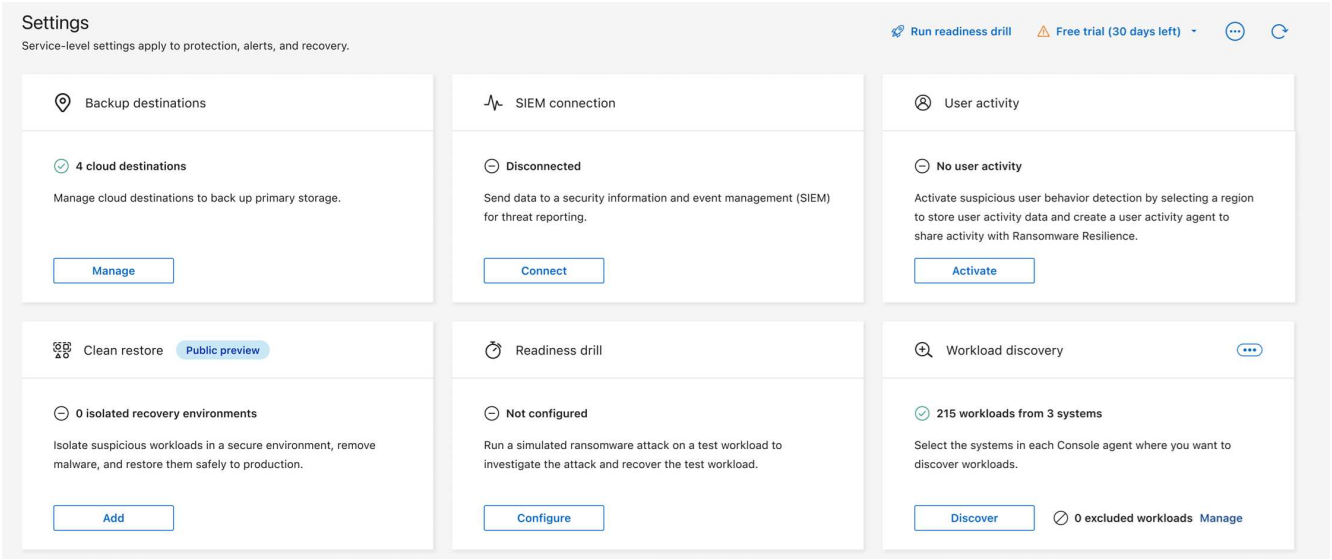
1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans le tableau de bord Paramètres, repérez le tableau de bord Découverte de la charge de travail. La carte indique le nombre de charges de travail exclues. Pour ajouter des charges de travail, à côté des charges de travail exclues, sélectionnez **Gérer**.



3. Sur la page Charges de travail exclues, sélectionnez **Ajouter**.
4. Sélectionnez les charges de travail que vous souhaitez exclure, puis **Ajouter**.
5. Consultez la page « Charges de travail exclues » pour connaître les charges de travail exclues. Pendant l'ajout de la charge de travail, un indicateur de progression s'affiche à côté de son nom. Si une charge de travail n'a pas pu être exclue avec succès, elle ne s'affiche pas sur la page.

Supprimer les charges de travail de la liste des charges de travail exclues

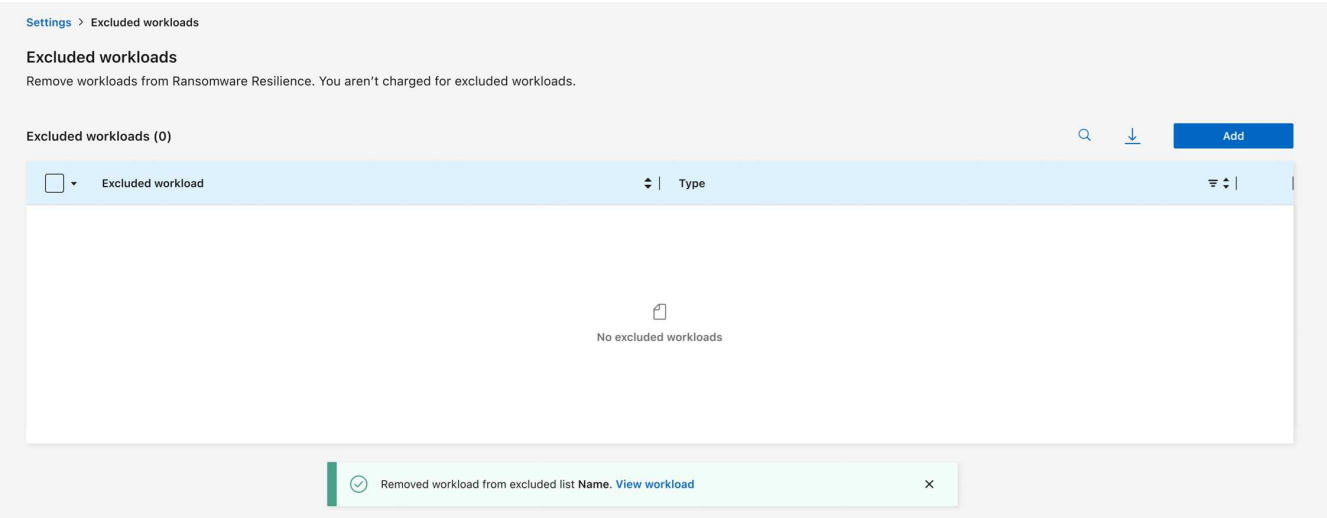
1. Dans Ransomware Resilience, sélectionnez **Paramètres**.
2. Dans le tableau de bord Paramètres, repérez le tableau de bord Découverte de la charge de travail. La carte indique le nombre de charges de travail exclues. À côté des charges de travail exclues, sélectionnez **Gérer**.



3. Pour supprimer une charge de travail individuelle, sélectionnez le menu d'actions correspondant à la charge de travail que vous souhaitez supprimer de la liste exclue.

   Pour supprimer plusieurs charges de travail, cochez la case en regard des charges de travail que vous souhaitez supprimer, puis **Supprimer de la liste des charges de travail exclues**.

4. Dans la boîte de dialogue, sélectionnez **Supprimer** pour confirmer que vous souhaitez supprimer les charges de travail de la liste d'exclusion.
5. Si la charge de travail est retirée avec succès de la liste des charges de travail exclues, un message de confirmation s'affiche sur la page des charges de travail exclues et la charge de travail n'apparaît plus dans la liste des charges de travail exclues. Si l'action échoue, un message d'erreur s'affiche ; veuillez réessayer.



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.

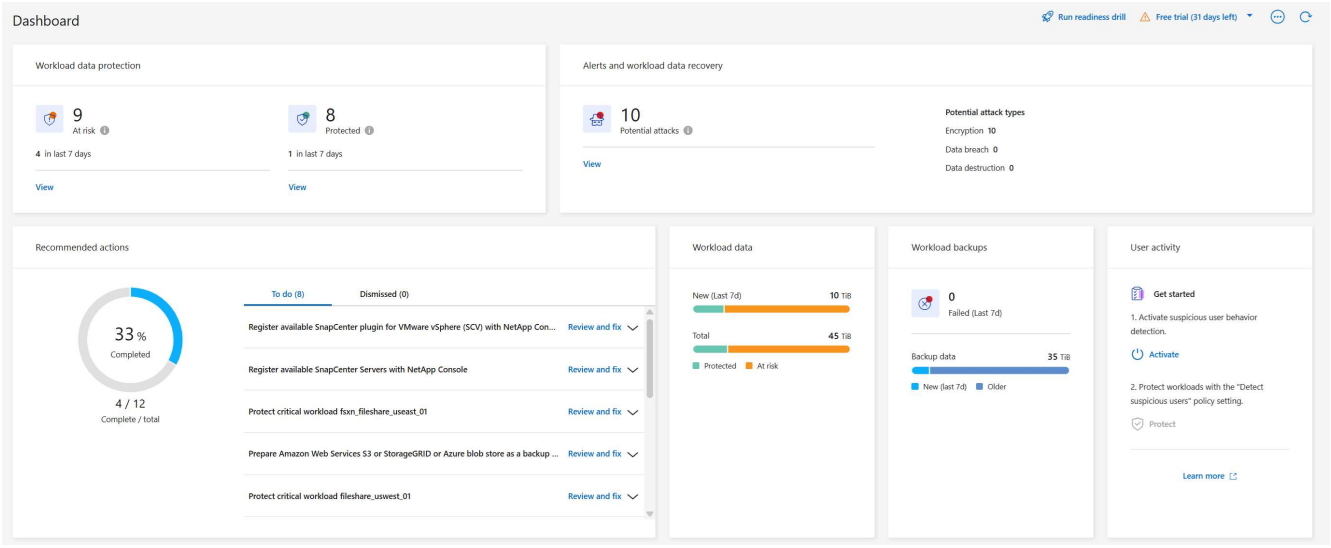
Vous devez saisir un nom d'utilisateur et un mot de passe dans les situations suivantes :

- 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" .

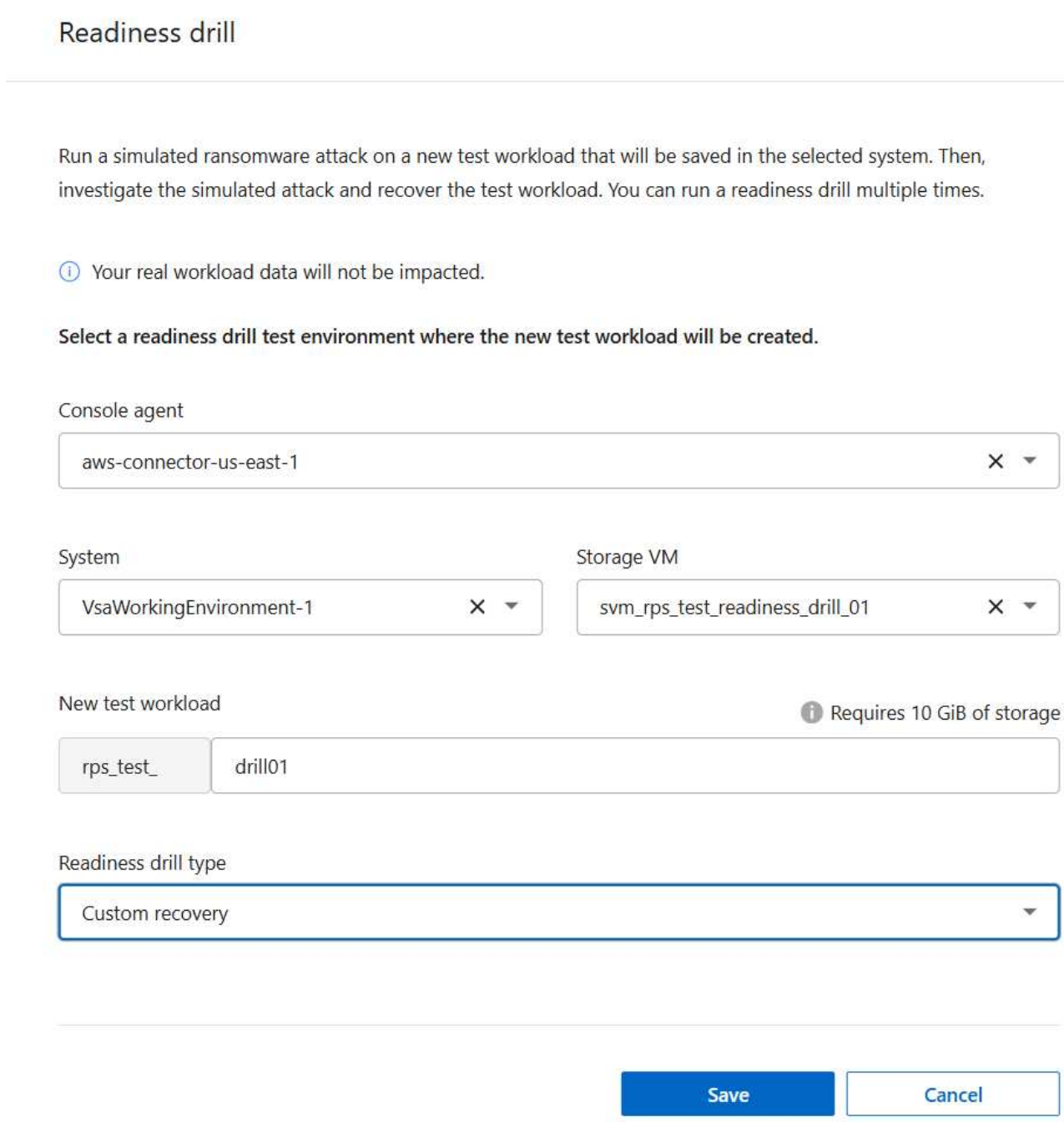
Étapes

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.

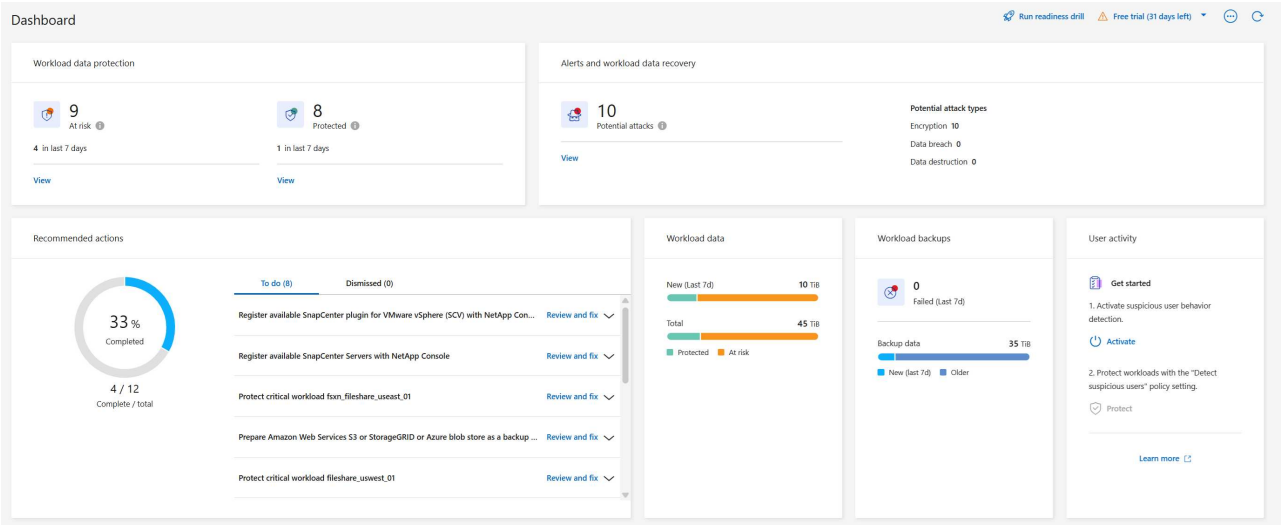
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

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

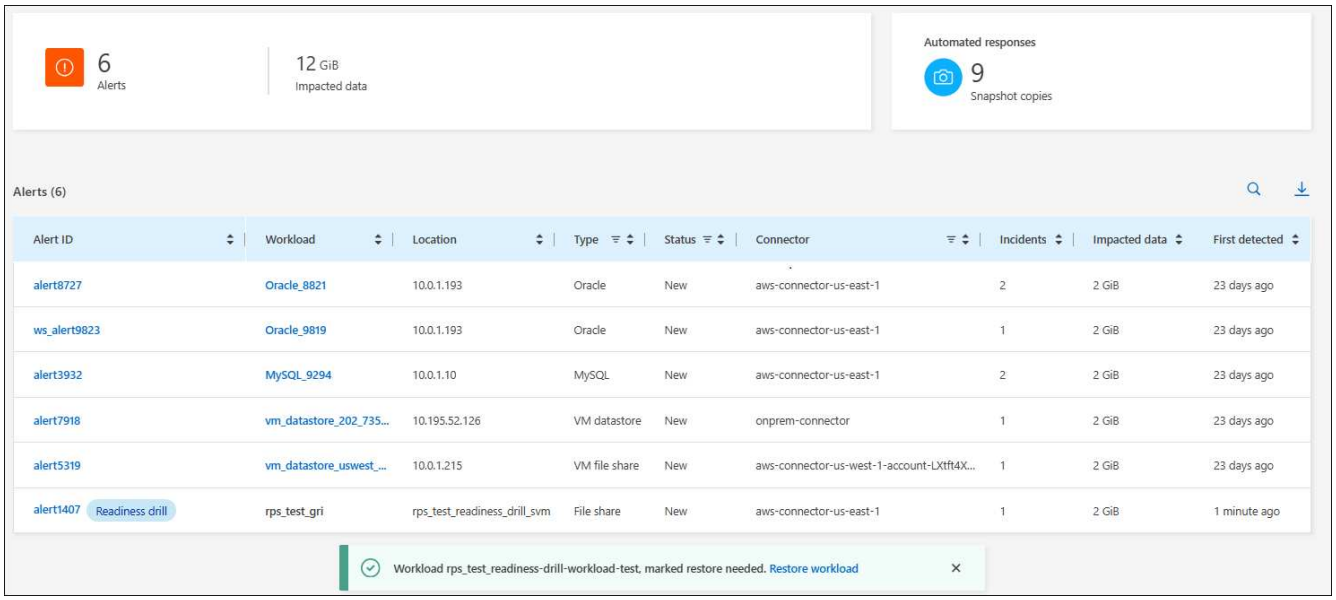
Testez votre état de préparation en répondant à une alerte d'exercice de préparation.

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" .

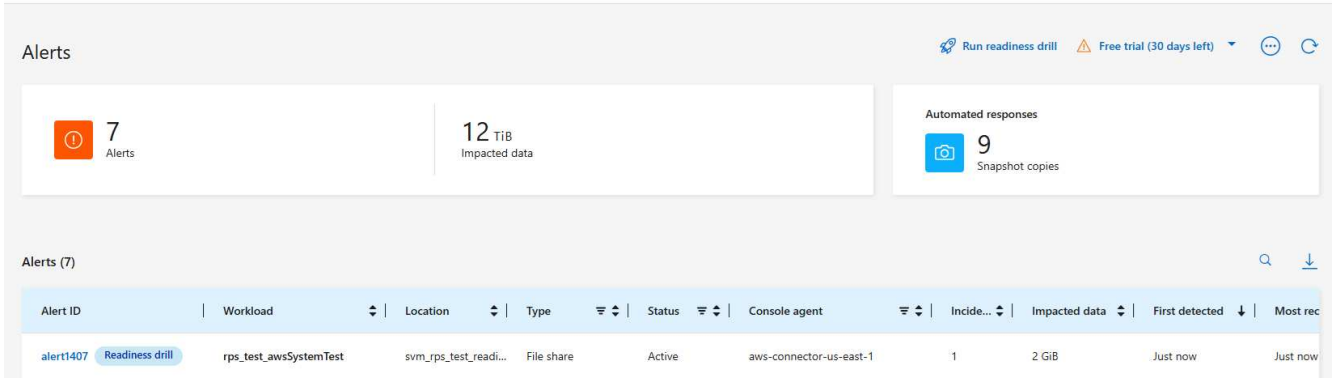
Étapes

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

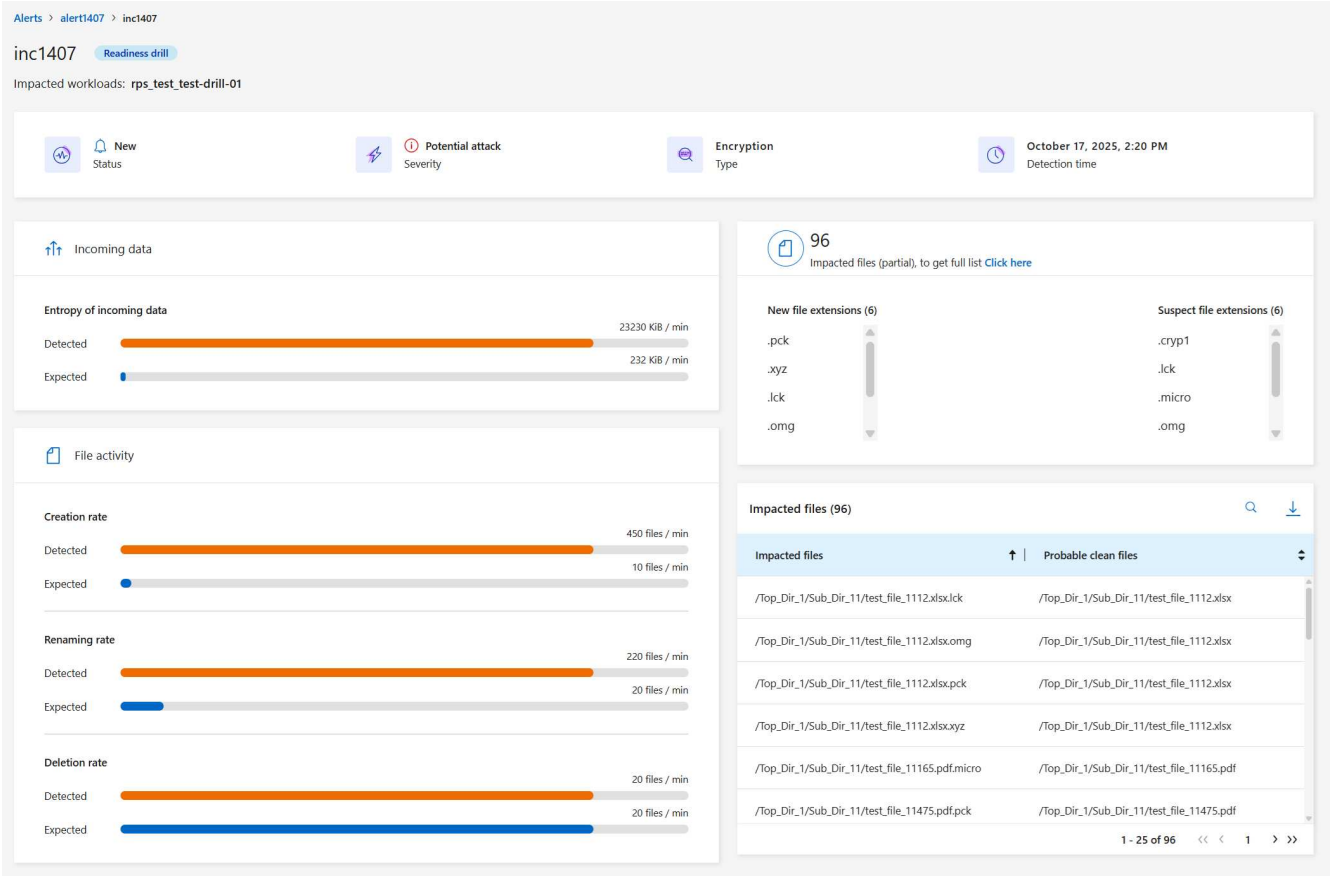
   La console affiche la page Alertes. Dans la colonne ID d'alerte, vous voyez « Exercice de préparation » à côté de l'ID.



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.

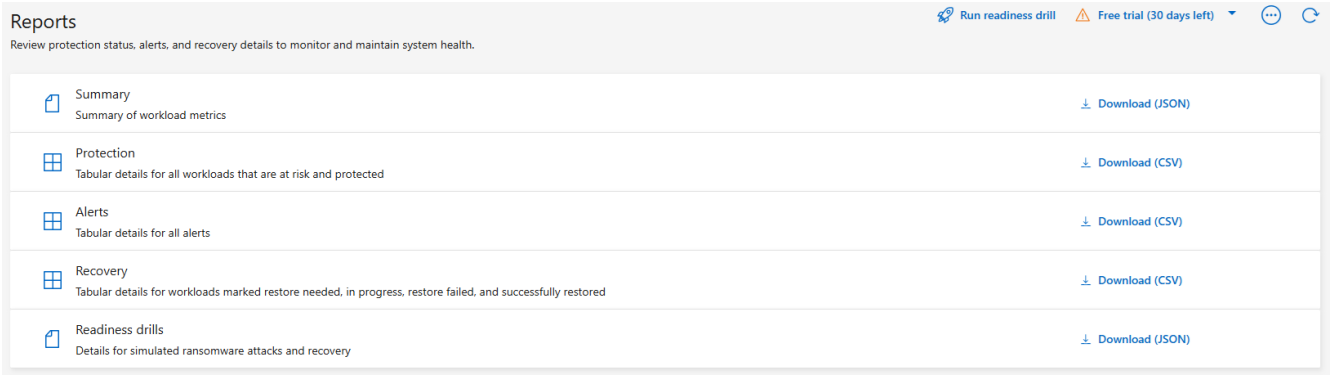
Rapports d’examen sur l’exercice de préparation

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.

Configurer les paramètres de protection dans NetApp Ransomware Resilience

Dans l’onglet Paramètres de NetApp Ransomware Resilience, vous pouvez configurer les destinations de sauvegarde, effectuer un exercice de préparation aux attaques, configurer la découverte des charges de travail ou configurer la détection des activités suspectes des utilisateurs.

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" .

Que pouvez-vous faire dans la page Paramètres ? Depuis la page Paramètres, vous pouvez effectuer les opérations suivantes :

- Simulez une attaque de ransomware en effectuant un exercice de préparation et répondez à une alerte de ransomware simulée. Pour plus de détails, consultez la section "Effectuer un exercice de préparation aux attaques de ransomware" .
- Configurer la découverte de charge de travail.
- Configurez le signalement des activités suspectes des utilisateurs. Pour plus d’informations, consultez "Activité utilisateur suspecte".
- Ajouter une destination de sauvegarde.

- Connectez votre système de gestion des événements et de la sécurité (SIEM) pour l'analyse et la détection des menaces. L'activation de la détection des menaces envoie automatiquement des données à votre SIEM pour l'analyse des menaces. Pour plus d'informations, voir "Connectez la résilience aux ransomwares NetApp à un SIEM".

Accéder directement à la page Paramètres

Vous pouvez facilement accéder à la page Paramètres à partir de l'option Actions près du menu supérieur.

1. Dans la résilience aux ransomwares, sélectionnez la verticale … option en haut à droite.
2. Dans le menu déroulant, sélectionnez **Paramètres**.

Simuler une attaque de ransomware

Réalisez un exercice de préparation aux ransomwares en simulant une attaque de ransomware sur une charge de travail d'échantillon nouvellement créée. Ensuite, examinez l'attaque simulée et récupérez l'exemple de charge de travail. Cette fonctionnalité vous aide à savoir que vous êtes préparé en cas d'attaque réelle de ransomware en testant les processus de notification d'alerte, de réponse et de récupération. Vous pouvez exécuter un exercice de préparation aux ransomwares plusieurs fois.

Pour plus de détails, reportez-vous à"Effectuer un exercice de préparation aux attaques de ransomware" .

Configurer la découverte de la charge de travail

Vous pouvez configurer la découverte de charges de travail pour découvrir automatiquement de nouvelles charges de travail dans votre environnement.

1. Dans la page Paramètres, recherchez la vignette **Découverte de charge de travail**.
2. Dans la mosaïque **Découverte de charge de travail**, sélectionnez **Découvrir les charges de travail**.

   Cette page affiche les agents de console avec des systèmes qui n'ont pas été sélectionnés précédemment, les agents de console nouvellement disponibles et les systèmes nouvellement disponibles. Cette page n'affiche pas les systèmes qui ont été précédemment sélectionnés.

3. Sélectionnez l'agent de console dans lequel vous souhaitez découvrir les charges de travail.
4. Consultez la liste des systèmes.
5. Cochez les systèmes sur lesquels vous souhaitez découvrir les charges de travail ou cochez la case en haut du tableau pour découvrir les charges de travail dans tous les environnements de charge de travail découverts.
6. Faites ceci pour d'autres systèmes si nécessaire.
7. Sélectionnez **Découvrir** pour que Ransomware Resilience découvre automatiquement les nouvelles charges de travail dans l'agent de console sélectionné.

Dans la carte Découverte de la charge de travail des Paramètres, sélectionnez le menu Actions … puis **Télécharger le rapport (JSON)** pour consulter la liste des charges de travail prises en charge et non prises en charge dans vos systèmes.

Ajouter une destination de sauvegarde

Ransomware Resilience peut identifier les charges de travail qui n'ont pas encore de sauvegardes ainsi que les charges de travail qui n'ont pas encore de destinations de sauvegarde attribuées.

Pour protéger ces charges de travail, vous devez ajouter une destination de sauvegarde. 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 ni dans Azure NetApp Files. Effectuez les opérations de sauvegarde à l'aide des solutions de sauvegarde natives : FSx for ONTAP backup service ou Azure NetApp Files backupss.

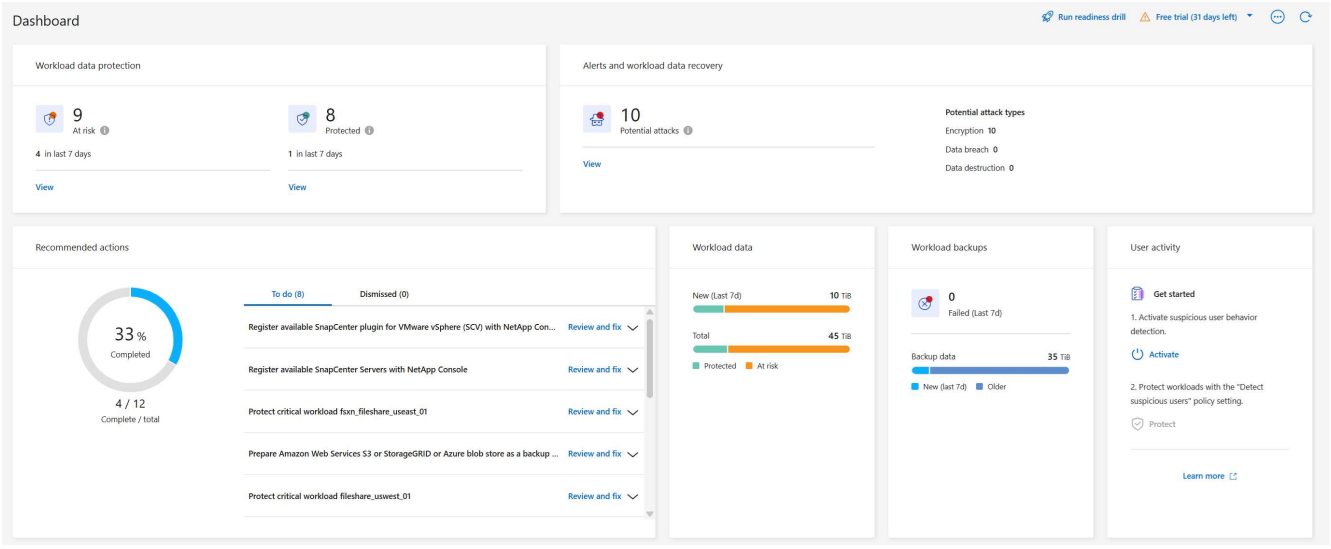
Vous pouvez ajouter une destination de sauvegarde en fonction d'une action recommandée à partir du tableau de bord ou en accédant à l'option Paramètres du menu.

Accéder aux options de destination de sauvegarde à partir des actions recommandées du tableau de bord

Le tableau de bord fournit de nombreuses recommandations. Une recommandation pourrait être de configurer une destination de sauvegarde.

Étapes

1. Dans le tableau de bord Résilience aux ransomwares, examinez le volet Actions recommandées.



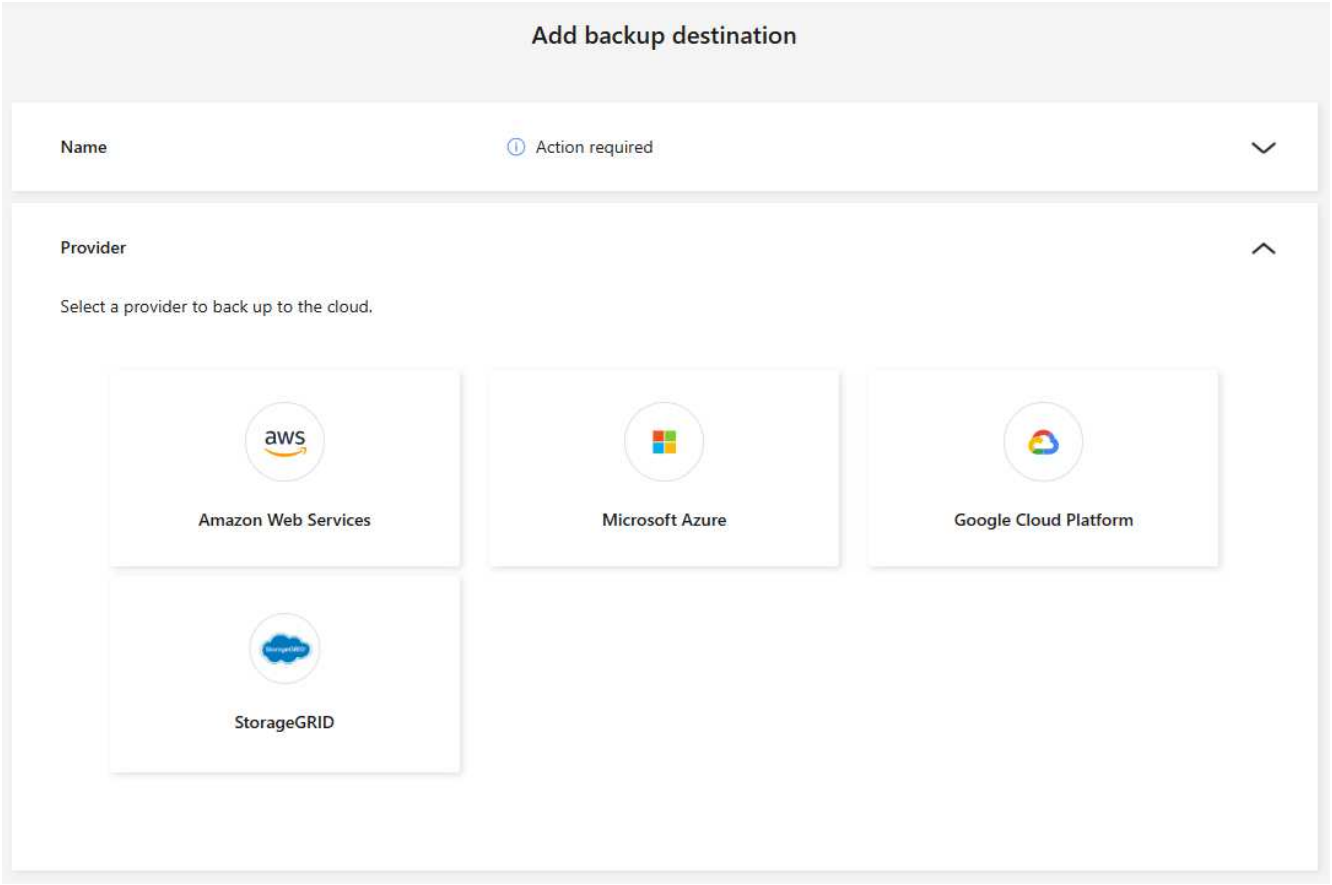
2. Depuis le tableau de bord, sélectionnez **Vérifier et corriger** pour la recommandation « Préparer <fournisseur de sauvegarde> comme destination de sauvegarde ».
3. Continuez avec les instructions en fonction du fournisseur de sauvegarde.

Ajouter StorageGRID comme destination de sauvegarde

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

Étapes

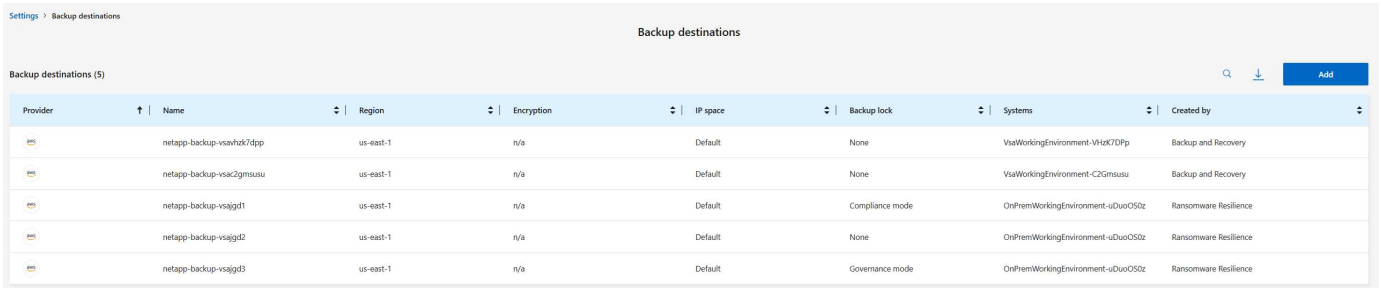
1. Dans la page **Paramètres > Destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.



3. Sélectionnez * StorageGRID*.
4. Sélectionnez la flèche vers le bas à côté de chaque paramètre et saisissez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur**:
     - Créez un nouveau bucket ou apportez votre propre bucket qui stockera les sauvegardes.
     - Nom de domaine complet du nœud de passerelle StorageGRID , port, clé d'accès StorageGRID et informations d'identification de la 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.
5. Sélectionnez **Ajouter**.

Résultat

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



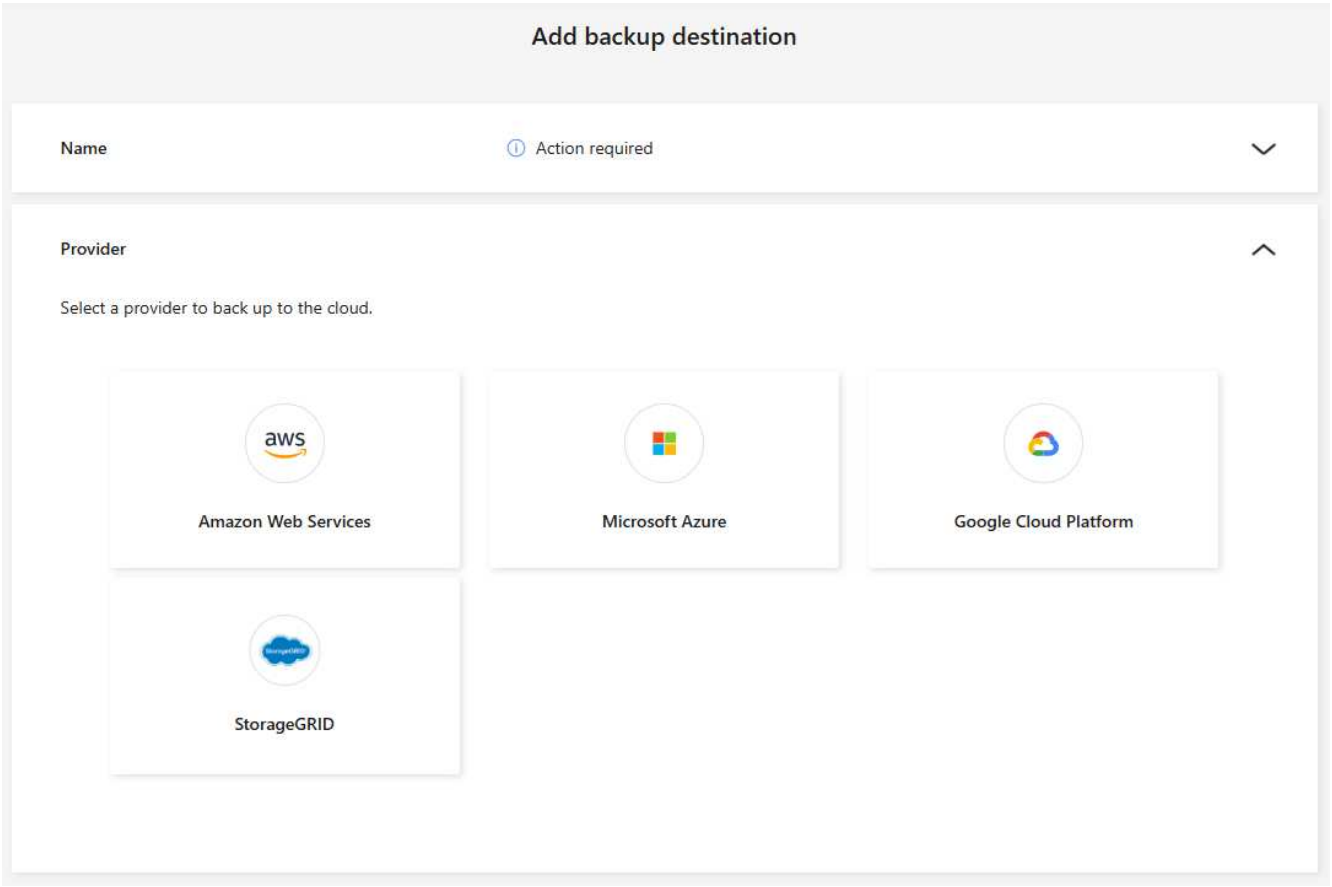
Ajouter Amazon Web Services comme destination de sauvegarde

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

Pour plus de détails sur la gestion de votre stockage AWS dans la console, reportez-vous à "Gérez vos buckets Amazon S3" .

Étapes

1. Dans la page **Paramètres > Destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.



3. Sélectionnez **Amazon Web Services**.
4. 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.

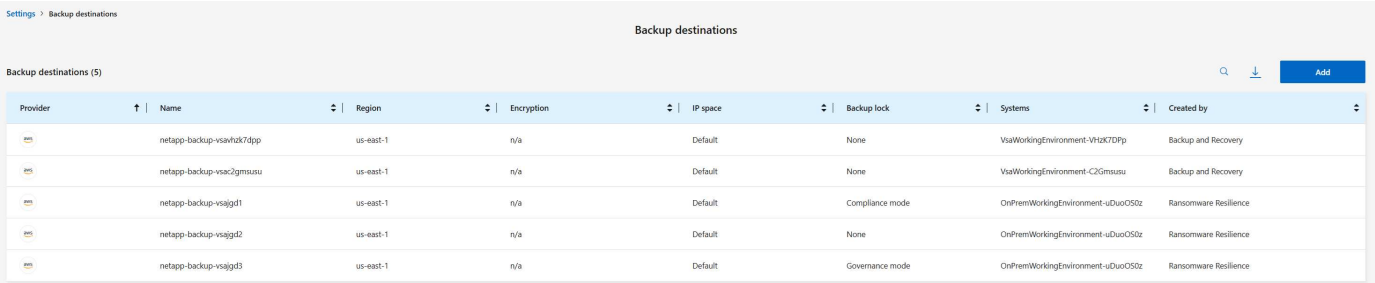
  Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pourrez pas modifier le paramètre ultérieurement une fois la destination de sauvegarde configurée.

  - **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.

5. Sélectionnez **Ajouter**.

Résultat

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



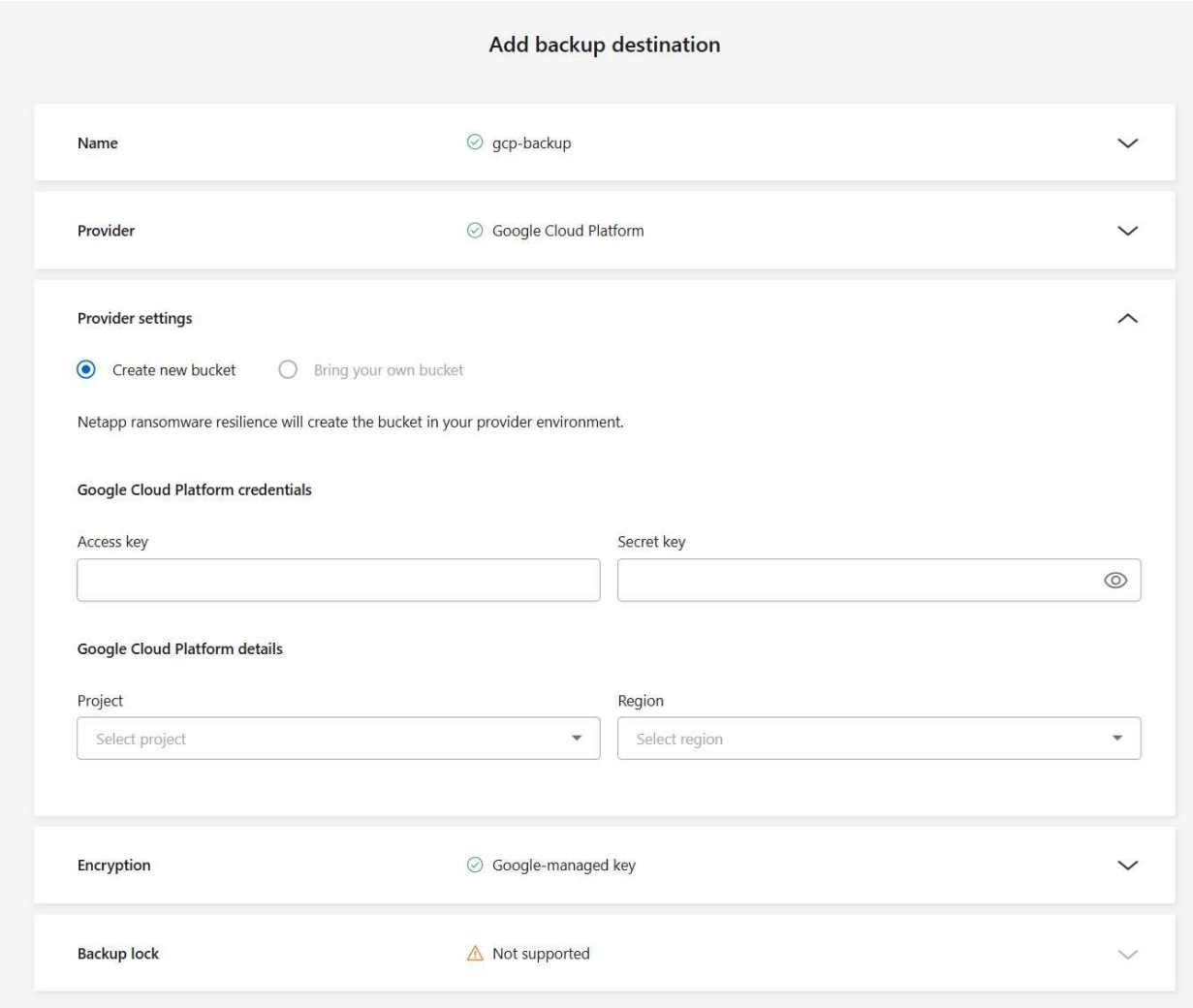
Ajouter Google Cloud Platform comme destination de sauvegarde

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

Pour plus de détails sur la gestion de votre stockage GCP dans la console, reportez-vous à "Options d'installation de l'agent de console dans Google Cloud" .

Étapes

1. Dans la page **Paramètres > Destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.
3. Sélectionnez **Google Cloud Platform**.
4. Sélectionnez la flèche vers le bas à côté de chaque paramètre et saisissez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur**:
     - Créer un nouveau bucket. Entrez la clé d'accès et la clé secrète.
     - Saisissez ou sélectionnez votre projet et votre région Google Cloud Platform.



   - **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 continuer à utiliser les clés gérées par Google.

   - **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 GCP (PrivateLink) que vous avez précédemment configuré.

5. Sélectionnez **Ajouter**.

Résultat

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

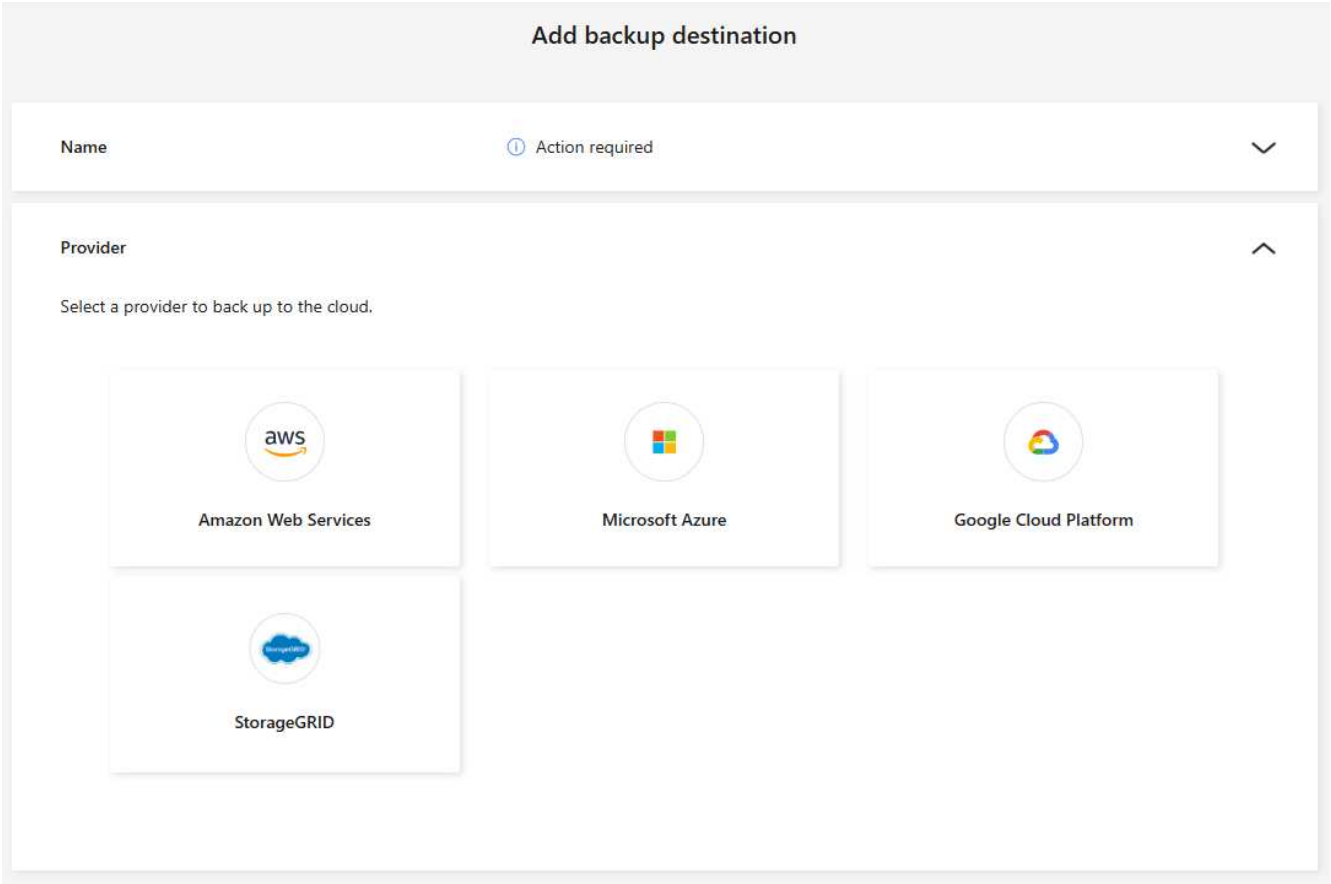
Ajouter Microsoft Azure comme destination de sauvegarde

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 la page **Paramètres > Destinations de sauvegarde**, sélectionnez **Ajouter**.
2. Entrez un nom pour la destination de sauvegarde.



3. Sélectionnez **Azure**.
4. 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.
- Abonnement Azure, région et groupe de ressources pour les informations d'identification Azure

  "Si vous souhaitez utiliser votre propre compte de stockage, reportez-vous à la section Ajouter des comptes de stockage Azure Blob." .

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

Les données du compte sont chiffrées par défaut avec des clés gérées par Microsoft. Vous pouvez continuer à utiliser les clés gérées par Microsoft 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.

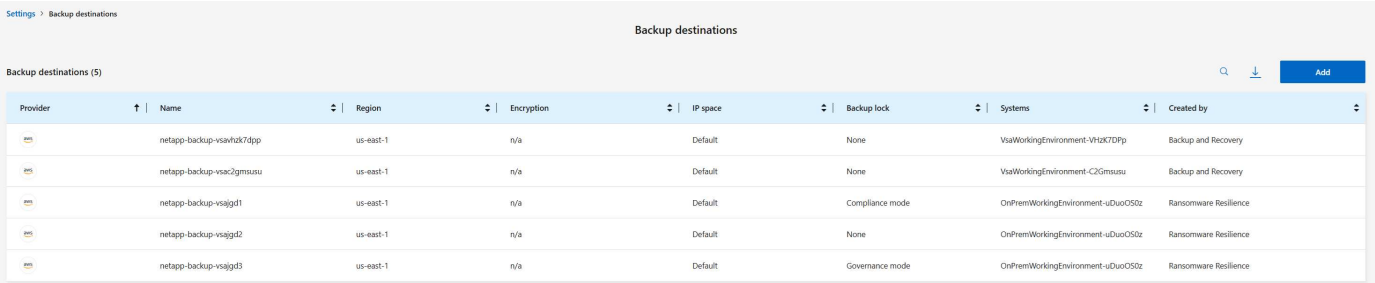
- L'espace IP est le cluster dans lequel résident les volumes que vous souhaitez sauvegarder. Les LIF intercluster pour cet espace IP doivent disposer d'un accès Internet sortant.
- Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré.

  Si vous souhaitez utiliser Azure PrivateLink, reportez-vous à "Azure PrivateLink" .

5. Sélectionnez **Ajouter**.

Résultat

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



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

Vous pouvez envoyer automatiquement des données de NetApp Ransomware Resilience à votre système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces.

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. Cliquez sur **Authentifier**.

   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.

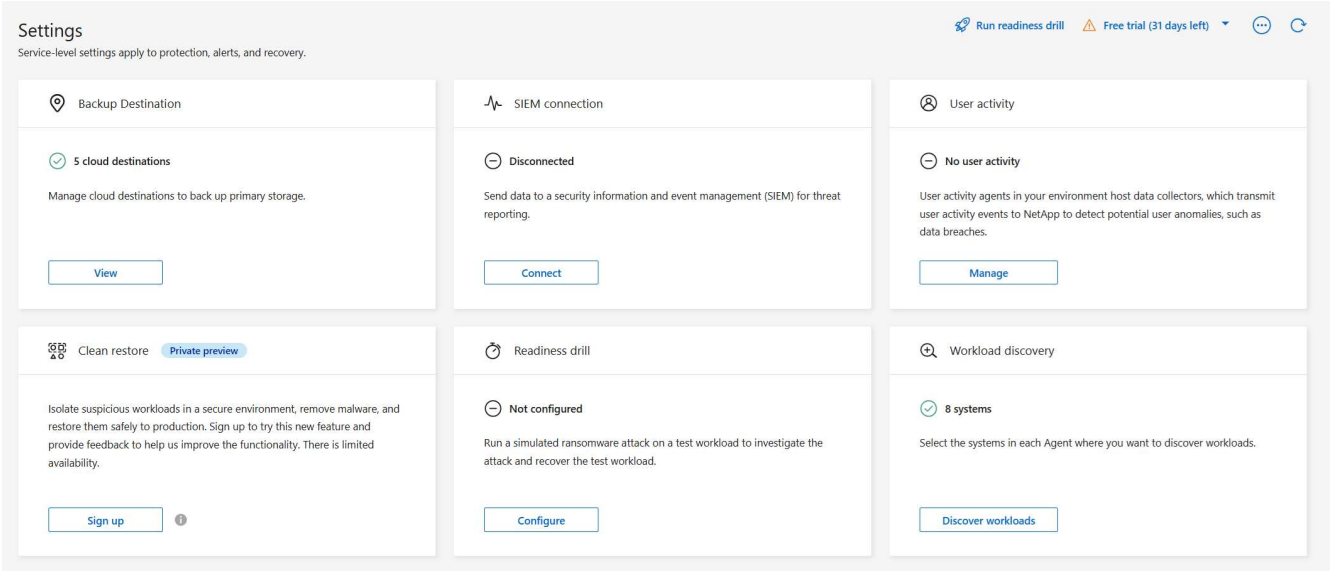
Connecter SIEM dans Ransomware Resilience

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

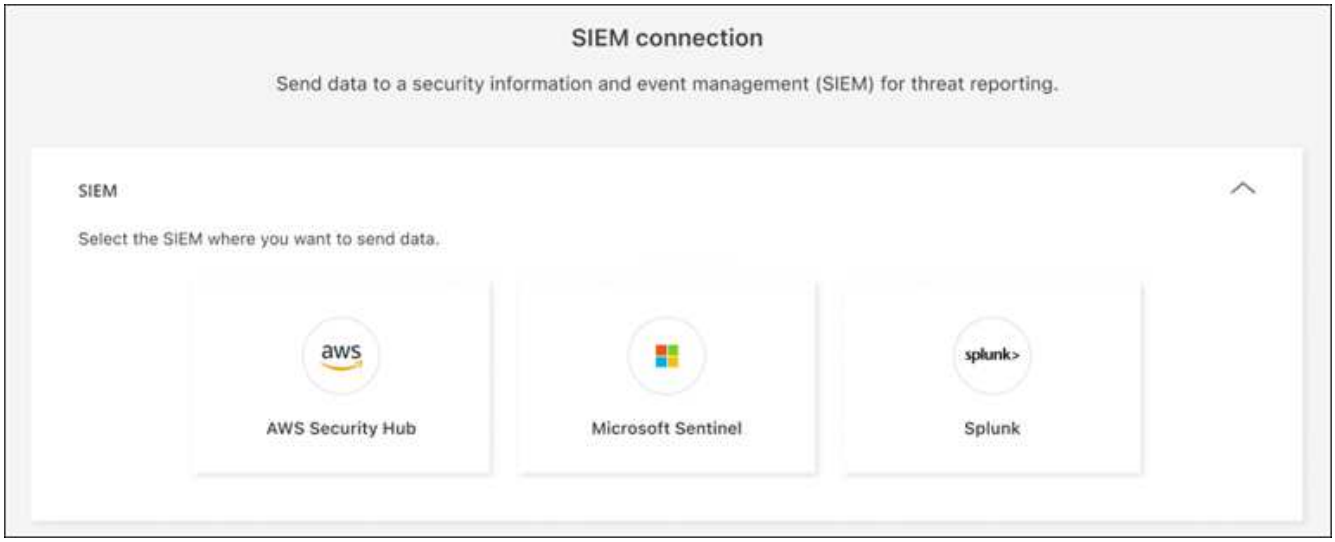
Étapes

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 ».

Configurer la détection de l'activité de l'utilisateur

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

NetApp Ransomware Resilience prend en charge la détection des comportements suspects des utilisateurs, vous permettant de traiter les incidents de ransomware au niveau de l'utilisateur.

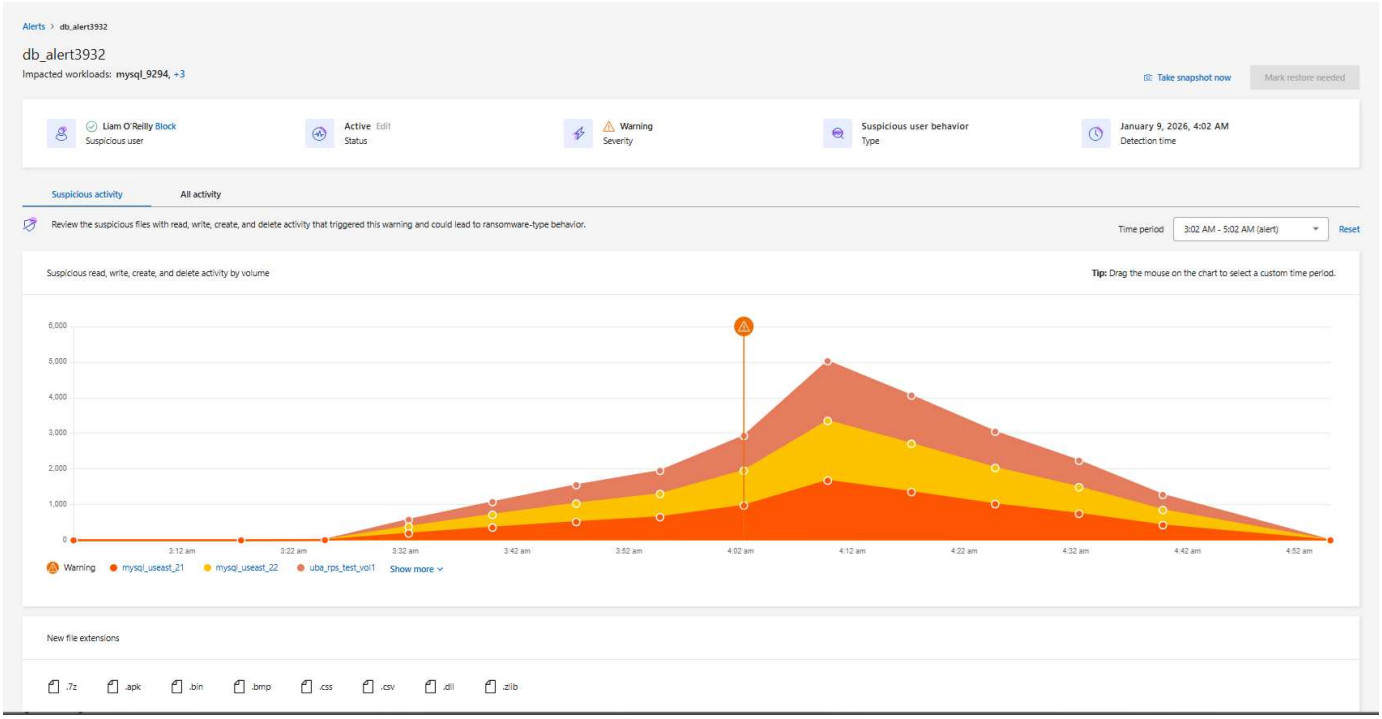
NetApp Ransomware Resilience fournit une détection de violation de données basée sur l'IA en surveillant l'activité utilisateur suspecte. Des augmentations soudaines de l'activité de lecture et des schémas d'accès à l'activité de lecture sont utilisées pour déterminer une intention malveillante. Une 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.

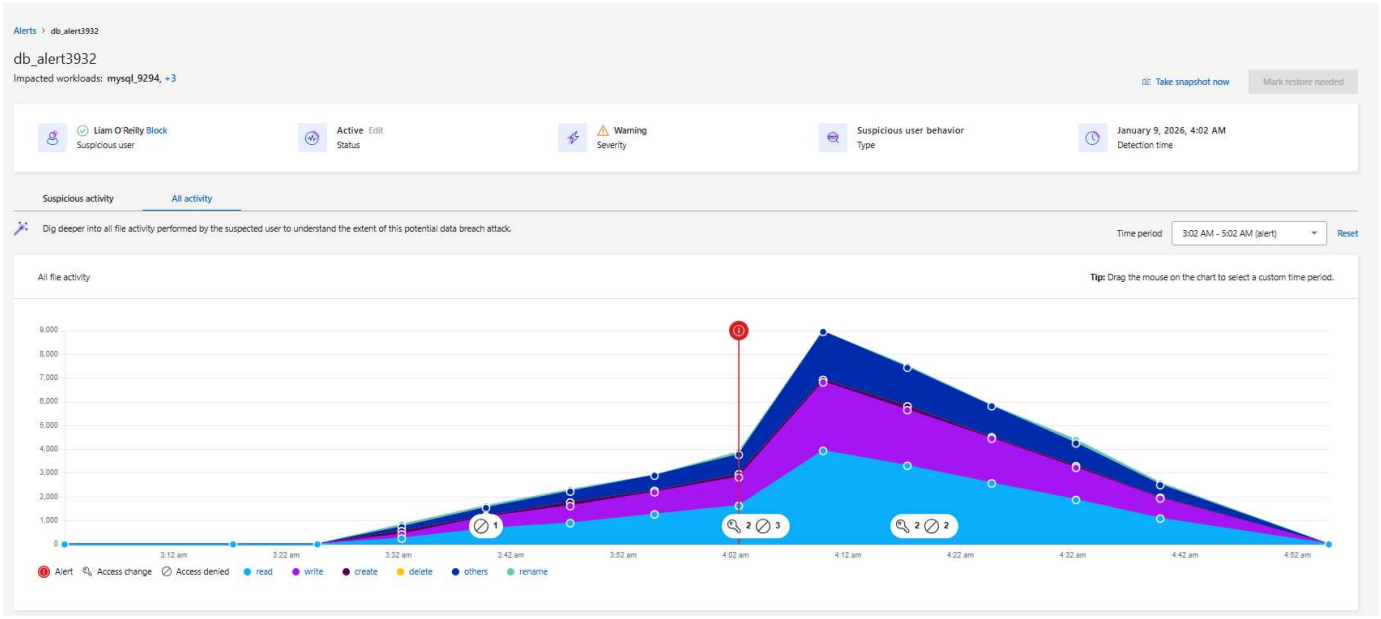
Analyse forensique des activités suspectes des utilisateurs

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

Avant de créer un agent d'activité utilisateur et d'autres collecteurs, vous devez vous assurer de répondre aux exigences décrites concernant le système d'exploitation, le serveur et le réseau.

Prise en charge du fournisseur de cloud

Prise en charge des fournisseurs de services 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

Pour activer la détection des comportements suspects des utilisateurs dans NetApp Ransomware Resilience, vous devez installer au moins un agent d'activité utilisateur. Lorsque vous activez la fonctionnalité de détection d'activité utilisateur suspecte depuis le tableau de bord de Ransomware Resilience, vous devez fournir les informations d'hôte de l'agent d'activité utilisateur.

Un agent peut héberger plusieurs collecteurs de données. Les collecteurs de données envoient les données à

un emplacement SaaS pour analyse. Il existe deux types de collectionneurs :

- Le **collecteur de données** collecte les données d'activité des utilisateurs à partir d' ONTAP.
- Le **connecteur d'annuaire utilisateur** se connecte à votre annuaire pour mapper les identifiants utilisateur aux noms d'utilisateur.

Les collecteurs sont configurés dans les paramètres de résilience aux ransomwares.

> 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 déjà 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.

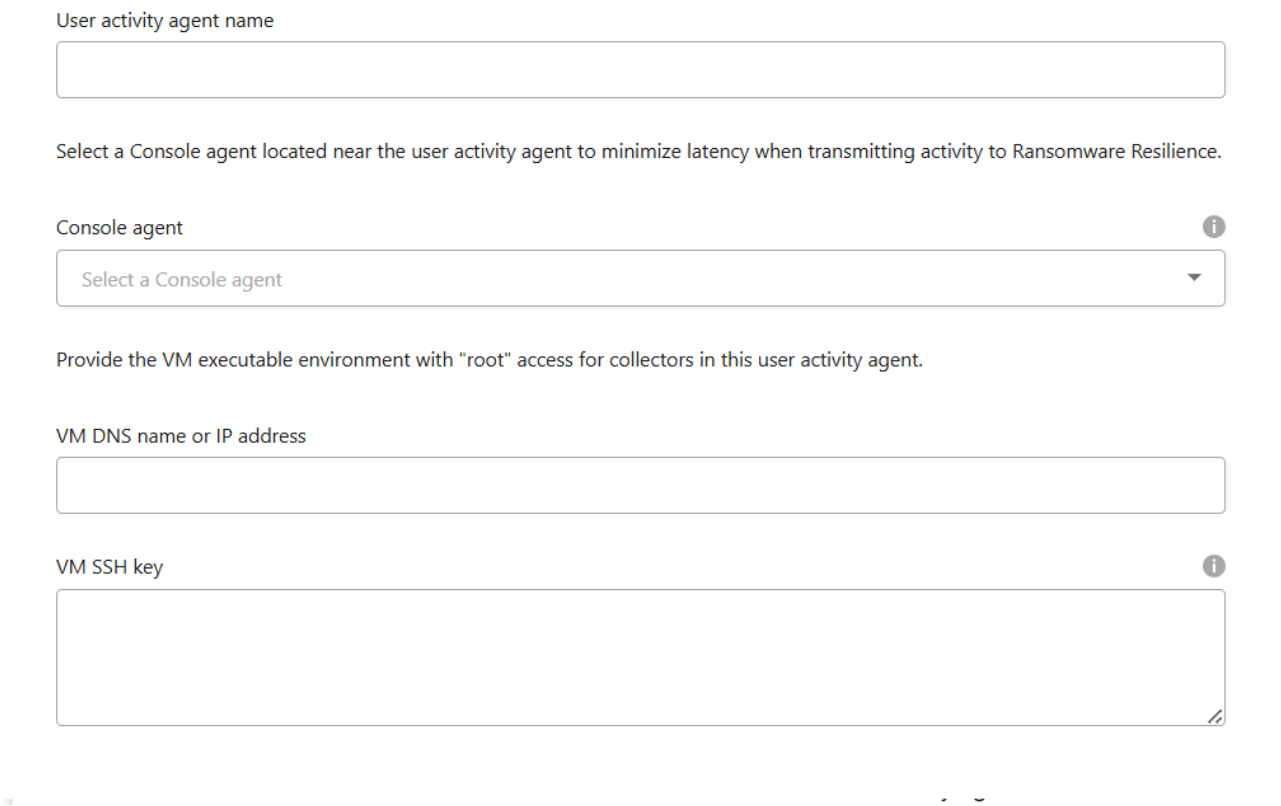
Étapes

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**.

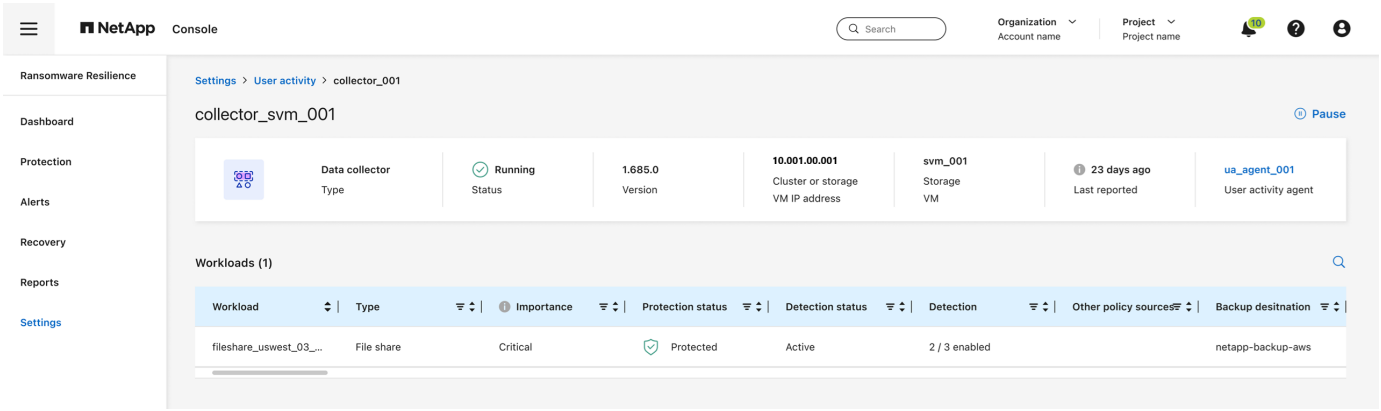
Résultat

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

Les collecteurs de données sont créés automatiquement lorsque vous activez une stratégie de protection contre les ransomwares avec détection d'activité utilisateur suspecte. Pour plus d'informations, voir 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.



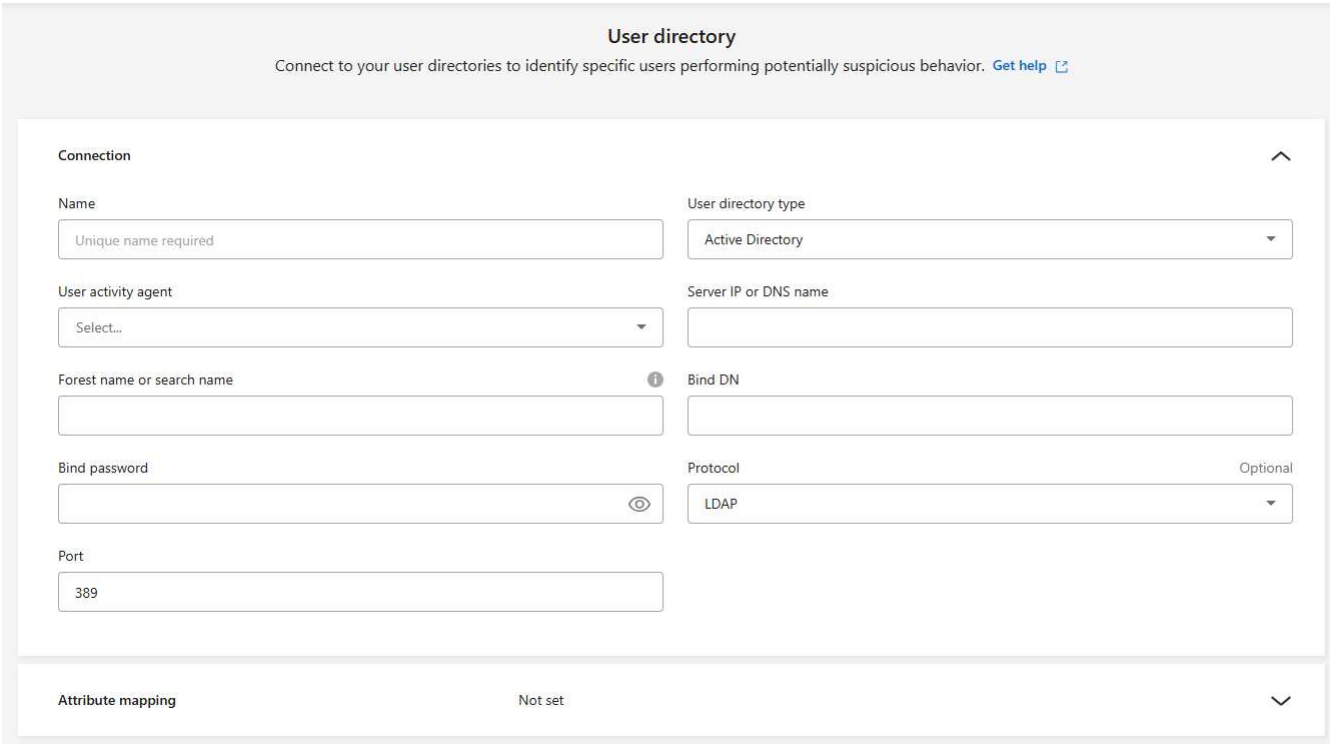
Créer un connecteur d'annuaire utilisateur

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".

Utiliser la résilience aux ransomwares

Surveiller l’état de la charge de travail à l’aide du tableau de bord de NetApp Ransomware Resilience

Le tableau de bord de NetApp Ransomware Resilience fournit des informations rapides sur l’état de protection de vos charges de travail. Vous pouvez rapidement déterminer les charges de travail qui sont à risque ou protégées, identifier les charges de travail affectées par un incident ou en cours de récupération, et évaluer l’étendue de la protection en examinant la quantité de stockage protégée ou à risque.

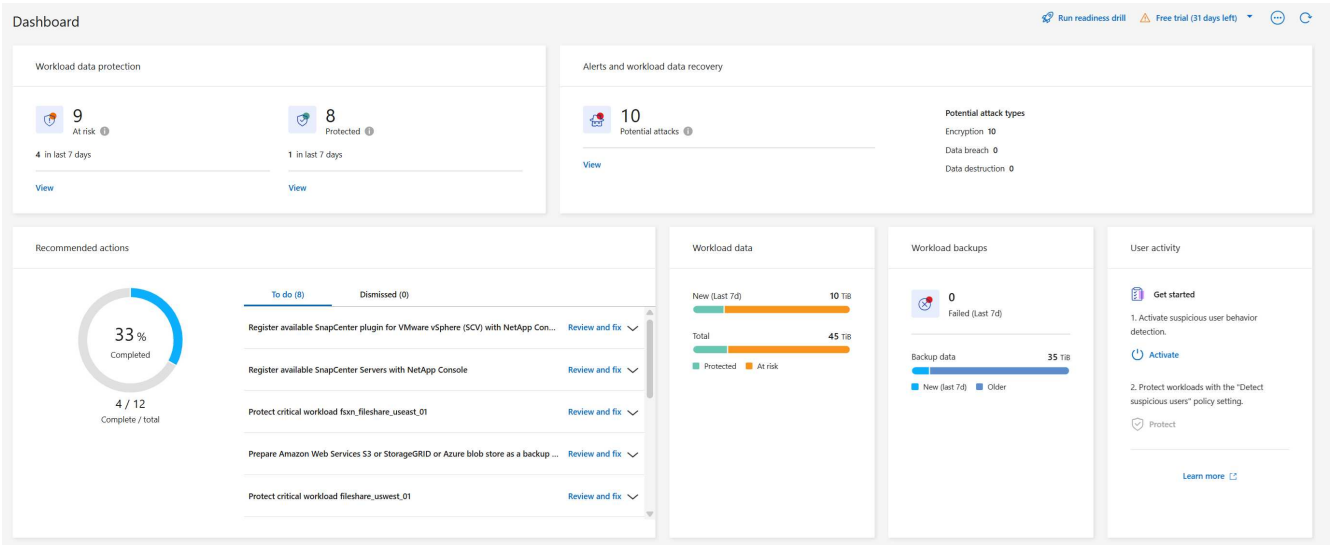
Utilisez le tableau de bord pour consulter les suggestions de protection, modifier les paramètres et télécharger les rapports.

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" .

Examiner l’état 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 les nouvelles recommandations depuis votre dernière visite sur le tableau de bord avec la balise « Nouveau » pendant 24 heures. Les actions apparaissent par ordre de priorité, la plus importante en haut. Examinez, appliquez ou rejetez 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 détails du serveur SIEM/XDR pour activer la détection des menaces. "Configurer les paramètres de protection" .
Activez la protection cohérente de la charge de travail pour les applications ou VMware.	Ces charges de travail ne sont pas gérées par le logiciel SnapCenter ou le SnapCenter Plug-in for VMware vSphere.	Pour qu'ils soient gérés par SnapCenter, activez la protection cohérente avec la charge de travail. "Protégez la charge de travail contre les attaques de ransomware" .
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" .
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. "Configurer les paramètres de protection" .
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 politique à chacune des charges de travail. "Protégez les charges de travail contre les attaques de ransomware" .

Recommandation	Description	Comment résoudre
Enregistrez le plug-in SnapCenter disponible pour VMware vSphere (SCV) avec la console	Une charge de travail VM n'est pas protégée.	Affectez une protection cohérente avec la machine virtuelle à la charge de travail de la machine virtuelle en activant le plug-in SnapCenter pour VMware vSphere. "Protégez les charges de travail contre les attaques de ransomware" .
Enregistrer le serveur SnapCenter disponible avec la console	Une application n'est pas protégée.	Affectez une protection cohérente avec les applications à la charge de travail en activant SnapCenter Server. "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 les charges de travail

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

Vous pouvez protéger les charges de travail contre les attaques de ransomware en activant une protection cohérente avec la charge de travail ou en créant des stratégies de protection contre les ransomwares dans NetApp Ransomware Resilience.

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 parc de données, vous pouvez créer"partages de fichiers de groupe" 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, les services suivants peuvent être utilisés pour gérer la protection :

- NetApp Backup and Recovery pour les partages de fichiers, les partages de fichiers de machines virtuelles
- SnapCenter pour VMware pour les magasins de données VM
- SnapCenter pour Oracle

Les informations de protection de ces services apparaissent dans Ransomware Resilience. Vous pouvez ajouter des politiques de détection à ces services avec Ransomware Resilience. L'ajout d'une politique de protection avec Ransomware Resilience remplace les politiques de protection existantes.

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, Ransomware Resilience, SnapCenter ou SnapCenter Plug-in for VMware vSphere, des instantanés peuvent être pris dans le cadre d' ONTAP ou d'autres produits. Si la protection FPolicy ONTAP est en place, vous pouvez modifier la protection FPolicy à l'aide ONTAP.

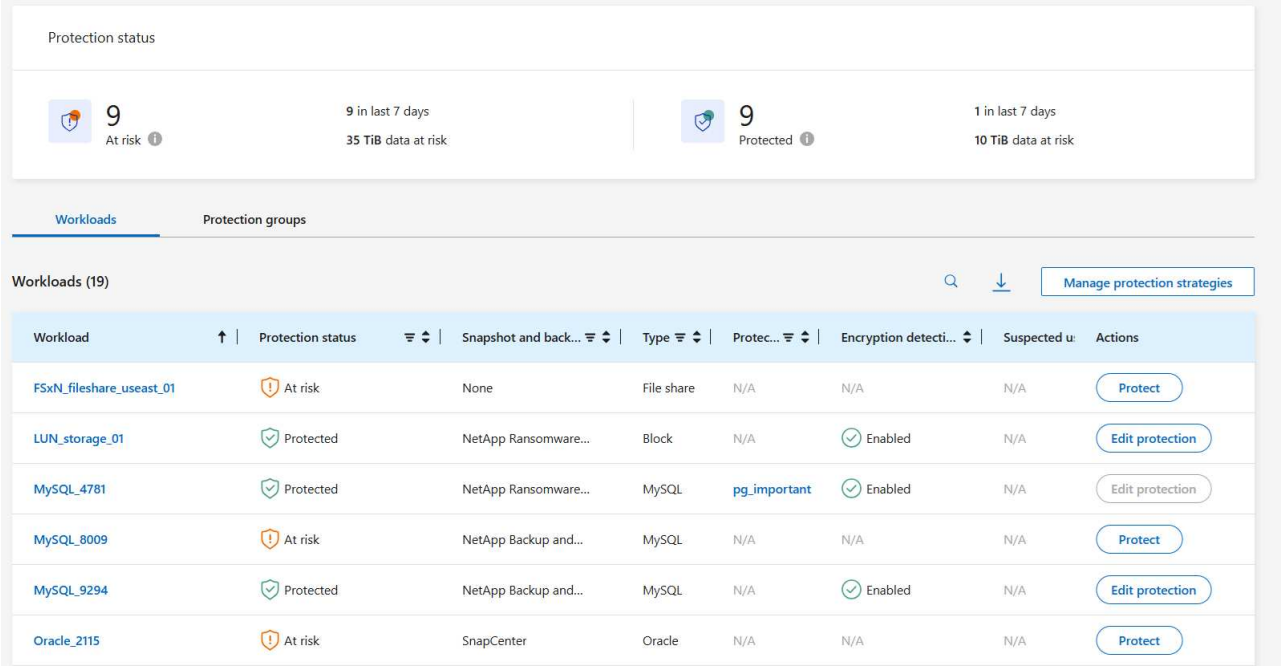
Afficher la protection contre les ransomwares sur une charge de travail

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.

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

Comprendre la page Protection

La page Protection affiche les informations suivantes sur la protection de la charge de travail :

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.

Statut de détection : Une charge de travail peut avoir l'un des statuts de détection de ransomware suivants :

- **Apprentissage** : Une politique de détection de ransomware a récemment été attribuée à la charge de travail et Ransomware Resilience analyse les charges de travail.
- **Actif** : une politique de protection contre la détection de ransomware est attribuée.
- **Non défini** : aucune politique de protection contre la détection de ransomware n'est attribuée.
- **Erreur** : Une stratégie de détection de ransomware a été attribuée, mais Ransomware Resilience a rencontré une erreur.

Lorsque la protection est activée dans Ransomware Resilience, la détection et la création de rapports d'alertes commencent après que l'état de la politique de détection des ransomwares passe du mode d'apprentissage au mode actif.

Les activités liées aux comportements suspects des utilisateurs et à l'activité FPolicy (extension de fichier suspecte) sont répertoriées séparément de l'état de détection.

Politique de détection : Le nom de la politique de détection des ransomwares apparaît, si elle a été attribuée. Si la politique de détection n'a pas été attribuée, « N/A » s'affiche.

Destination de réplication : Si vous avez configuré la réplication par instantané, les noms des machines virtuelles et des systèmes de stockage de destination sont indiqués. En l'absence de réplication, ce champ affiche « Aucune ».

- Politiques de capture instantanée et de sauvegarde * : cette colonne affiche les politiques de capture instantanée et de sauvegarde appliquées à la charge de travail et au produit ou service qui gère ces politiques.
- Géré par SnapCenter
- Géré par SnapCenter Plug-in for VMware vSphere
- Géré par Backup and Recovery
- Nom de la politique de protection contre les ransomwares qui régit les instantanés et les sauvegardes
- Aucune

Importance de la charge de travail

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.

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
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

Niveau politique	Instantané	Fréquence	Rétention (jours)	Nombre de copies d'instantané	Nombre maximal de copies d'instantané
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
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

Activez la protection cohérente des applications ou des machines virtuelles avec SnapCenter

L'activation d'une protection cohérente au niveau des applications ou des machines virtuelles vous aide à protéger vos charges de travail d'application ou de machine virtuelle de manière cohérente, en obtenant un état de repos et cohérent pour éviter toute perte de données potentielle ultérieure si une récupération est nécessaire.

Ce processus lance l'enregistrement du serveur logiciel SnapCenter pour les applications ou du SnapCenter Plug-in for VMware vSphere pour les machines virtuelles à l'aide de la sauvegarde et de la récupération.

Après avoir activé la protection cohérente avec la charge de travail, vous pouvez gérer les stratégies de protection dans Ransomware Resilience. La stratégie de protection comprend les politiques de capture instantanée et de sauvegarde gérées ailleurs ainsi qu'une politique de détection de ransomware gérée dans Ransomware Resilience.

Pour en savoir plus sur l'enregistrement de SnapCenter ou du SnapCenter Plug-in for VMware vSphere à l'aide de Backup and Recovery, reportez-vous aux informations suivantes :

- "Enregistrer le logiciel SnapCenter Server"
- "Enregistrer le SnapCenter Plug-in for VMware vSphere"

Étapes

1. Dans le menu Résilience aux ransomwares, sélectionnez **Tableau de bord**.
2. Dans le volet Recommandations, recherchez l'une des recommandations suivantes et sélectionnez **Réviser et corriger** :
   - Enregistrez le serveur SnapCenter disponible avec la NetApp Console
   - Enregistrez le SnapCenter Plug-in for VMware vSphere (SCV) avec la NetApp Console
3. Suivez les informations pour enregistrer le SnapCenter Plug-in for VMware vSphere-in SnapCenter ou SnapCenter pour l'hôte VMware vSphere à l'aide de Backup and Recovery.
4. Retour à la résilience aux ransomwares.
5. Depuis Ransomware Resilience, accédez au tableau de bord et relancez le processus de découverte.
6. Depuis Ransomware Resilience, sélectionnez **Protection** pour afficher la page Protection.
7. Consultez les détails dans la colonne des stratégies de capture instantanée et de sauvegarde sur la page Protection pour voir que les stratégies sont gérées ailleurs.

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 stratégies de capture instantanée ou de sauvegarde existantes de SnapCenter ou de protection de sauvegarde et de récupération 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)

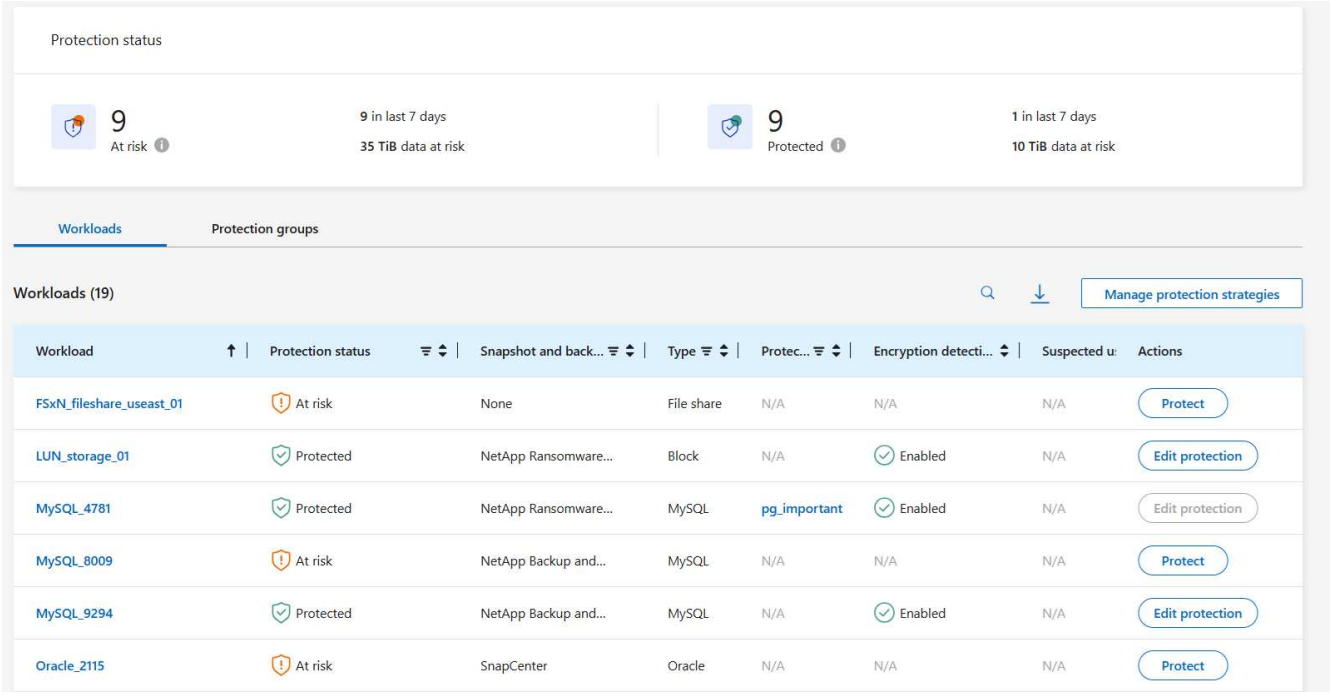
Si les stratégies de capture instantanée ou de sauvegarde n'existent pas sur la charge de travail, vous pouvez

créer une stratégie de protection contre les ransomwares, qui peut inclure les stratégies suivantes que vous créez dans Ransomware Resilience :

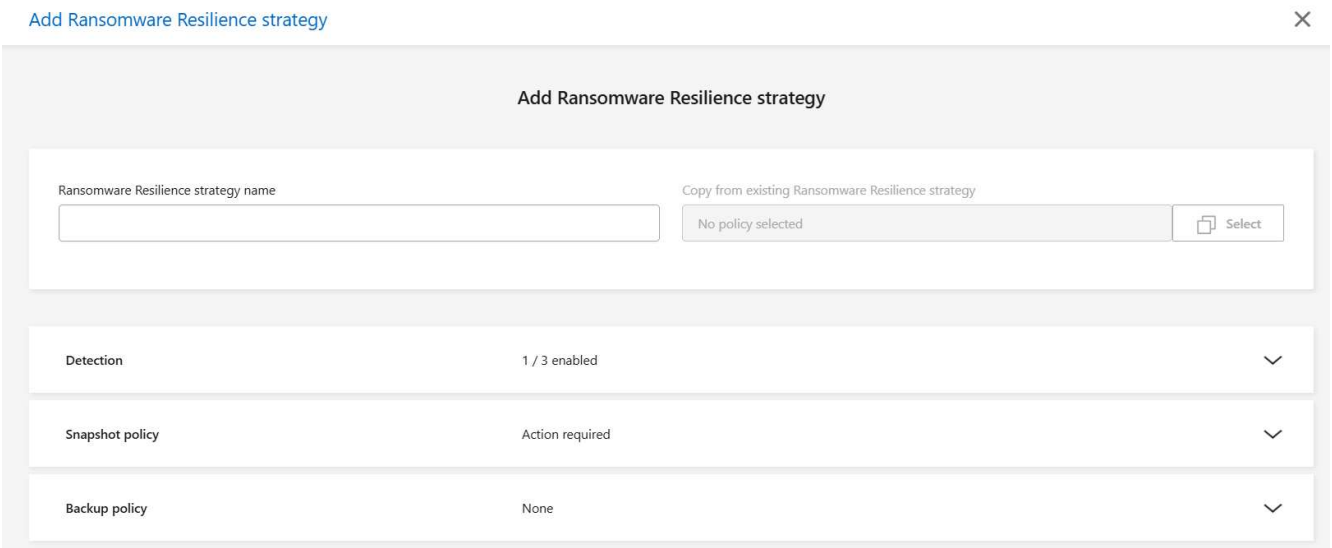
- Politique d'instantané
- Politique de sauvegarde
- Politique de détection des ransomwares
- Réplication secondaire vers ONTAP

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

6. Sélectionnez **Ajouter**.

Ajoutez une politique de détection aux charges de travail avec des politiques de snapshot et de sauvegarde existantes gérées par SnapCenter ou Backup and Recovery

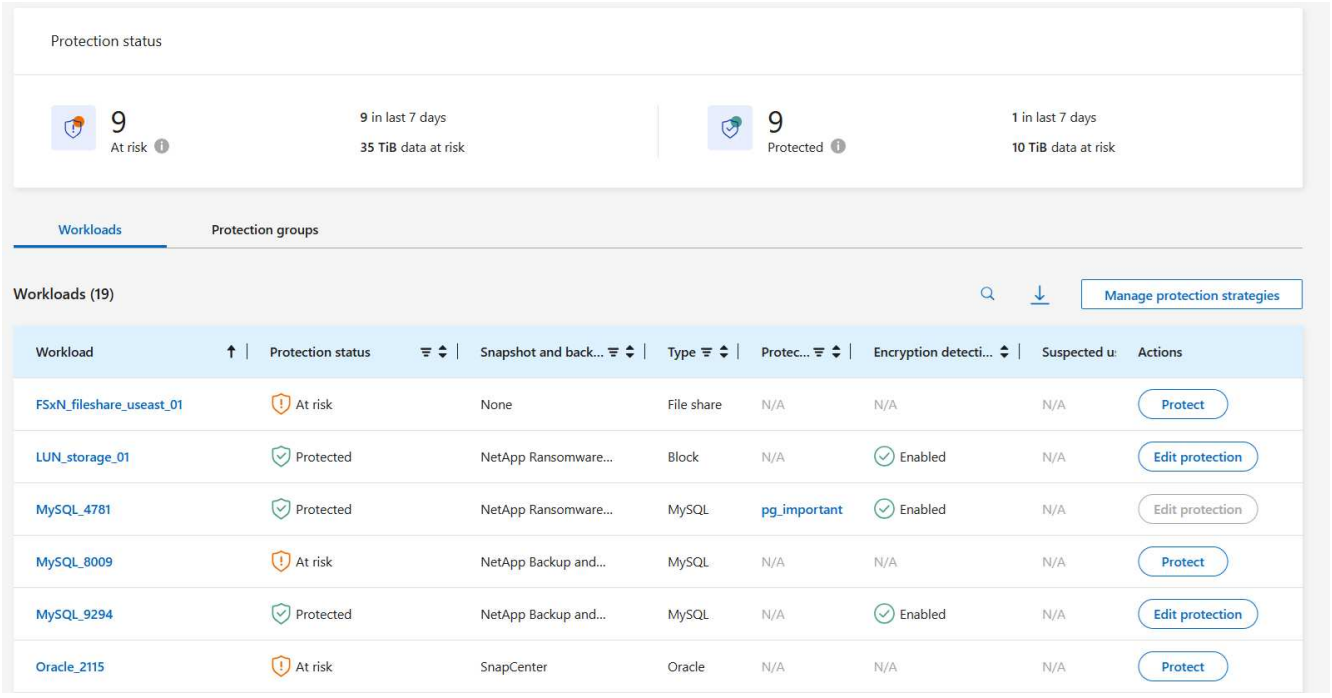
Ransomware Resilience vous permet d'attribuer une politique de détection ou une politique de protection aux charges de travail avec une protection de snapshot et de sauvegarde existante gérée dans d'autres produits ou services NetApp . D'autres services, tels que Backup and Recovery et SnapCenter, utilisent des stratégies qui régissent les snapshots, la réplication vers un stockage secondaire ou les sauvegardes vers un stockage d'objets.

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

Si vous disposez de stratégies de capture instantanée ou de sauvegarde existantes avec Backup and Recovery ou SnapCenter, vous pouvez ajouter une stratégie pour détecter les attaques de ransomware. Pour gérer la protection et la détection avec Ransomware Resilience, voirProtégez-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 SnapCenter ou de sauvegarde et de récupération actives.

4. Pour conserver vos politiques de sauvegarde et de récupération ou SnapCenter existantes et appliquer uniquement une politique de *détection*, laissez la case **Remplacer les politiques existantes** décochée.
5. Pour voir les détails des politiques SnapCenter , sélectionnez la **flèche vers le bas**.
6. Sélectionnez les paramètres de détection que vous souhaitez :

```
*Encryption detection*
*Suspicious user behavior detection*
*Block suspicious file extensions*
```

7. Sélectionnez **Suivant**.
8. 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.

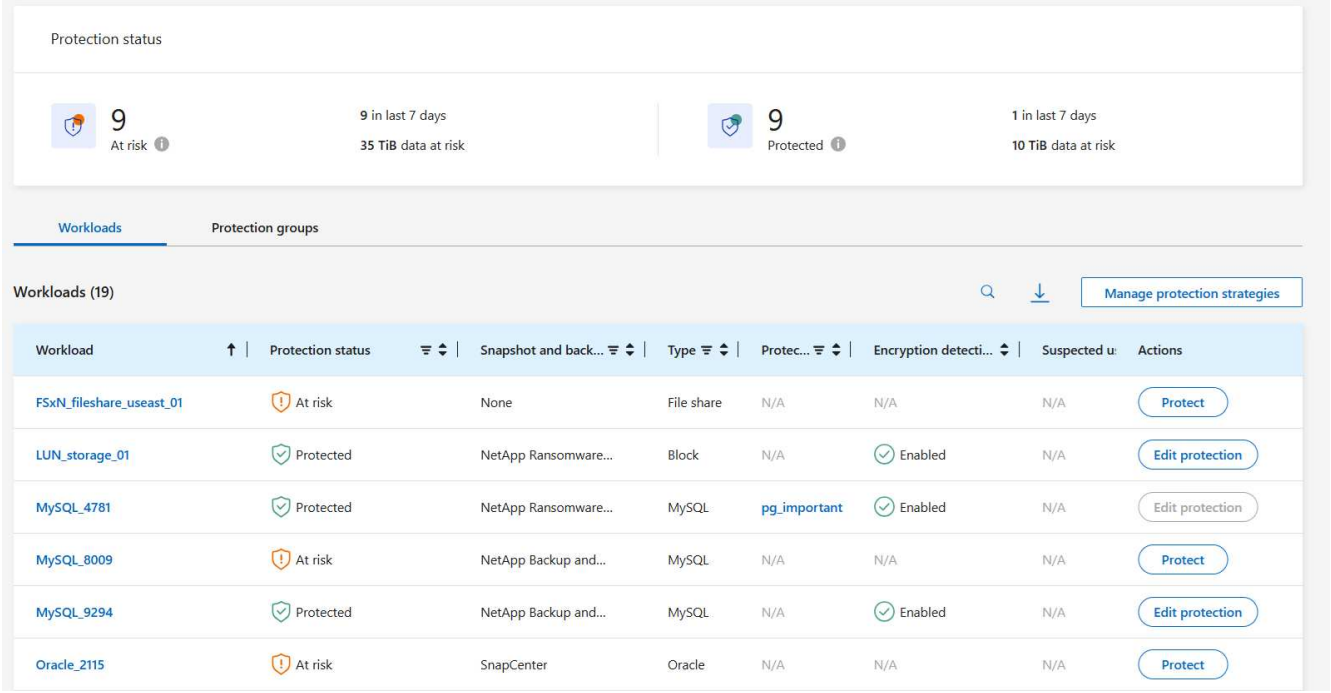
9. Sélectionnez **Suivant**.
10. Revoyez vos choix. Sélectionnez **Créer** pour activer la détection.
11. Sur la page Protection, vérifiez l'**état de détection** pour confirmer que la détection est active.

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 sauvegarde et de récupération ou SnapCenter actives. Pour remplacer les stratégies de sauvegarde et de récupération ou SnapCenter existantes, sélectionnez la case **Remplacer les stratégies existantes**. Lorsque vous sélectionnez la case, Ransomware Resilience remplace la liste des stratégies de détection par des stratégies 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 dispose d'une stratégie de sauvegarde et de récupération ou de SnapCenter existante que vous souhaitez conserver, décochez **Remplacer les stratégies existantes**. Pour remplacer les politiques existantes, cochez **Remplacer les politiques 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.

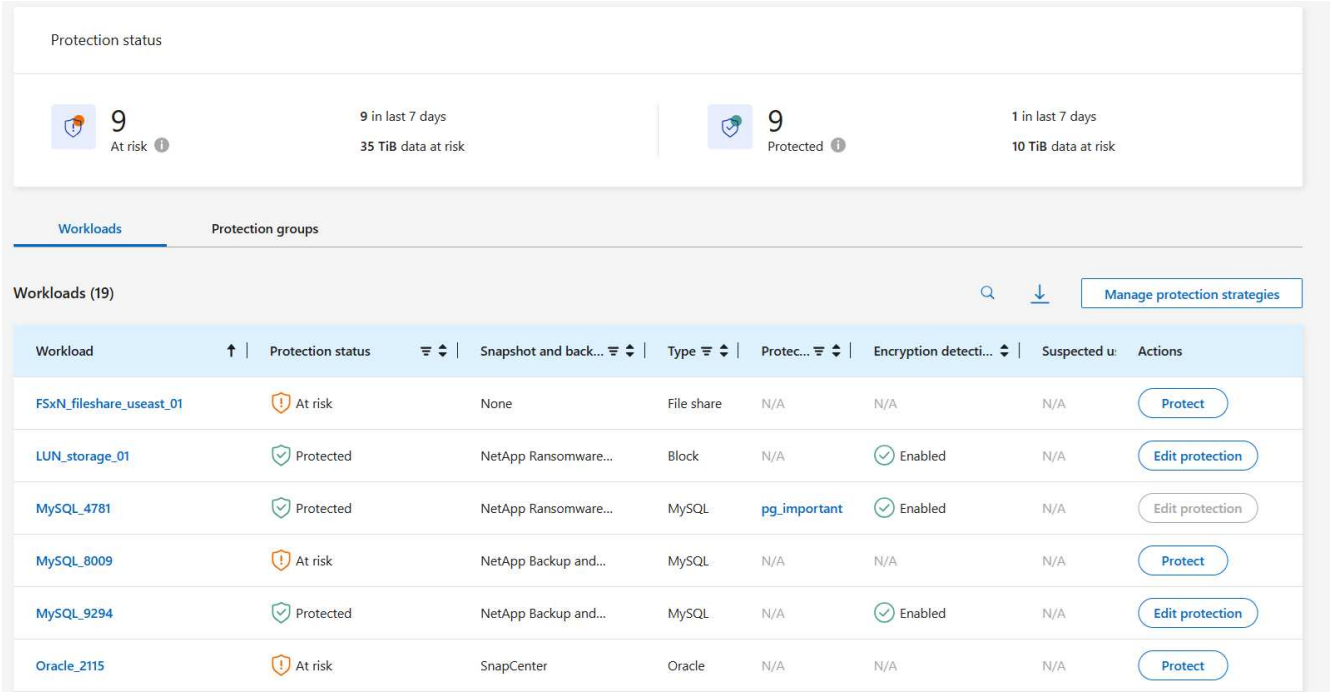
Créer un groupe de protection

Le regroupement des partages de fichiers dans un groupe de protection facilite la protection de votre parc de données. Ransomware Resilience peut protéger tous les volumes d'un groupe en même temps plutôt que de protéger chaque volume séparément.

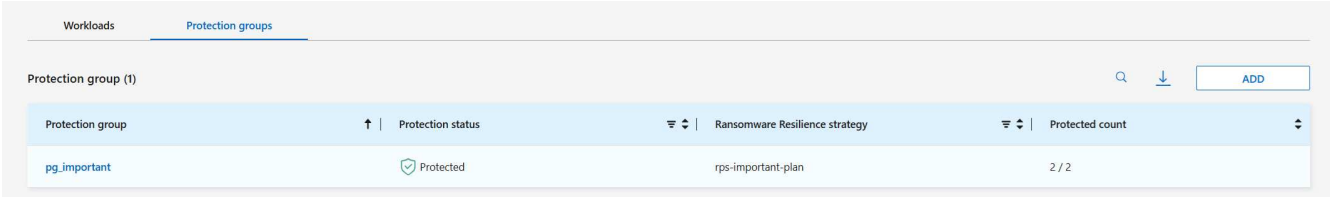
Vous pouvez créer des groupes quel que soit leur état de protection (c'est-à-dire des groupes non protégés et des groupes protégés). Lorsque vous ajoutez une politique de protection à un groupe de protection, la nouvelle politique de protection remplace toute politique existante, y compris les politiques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

Étapes

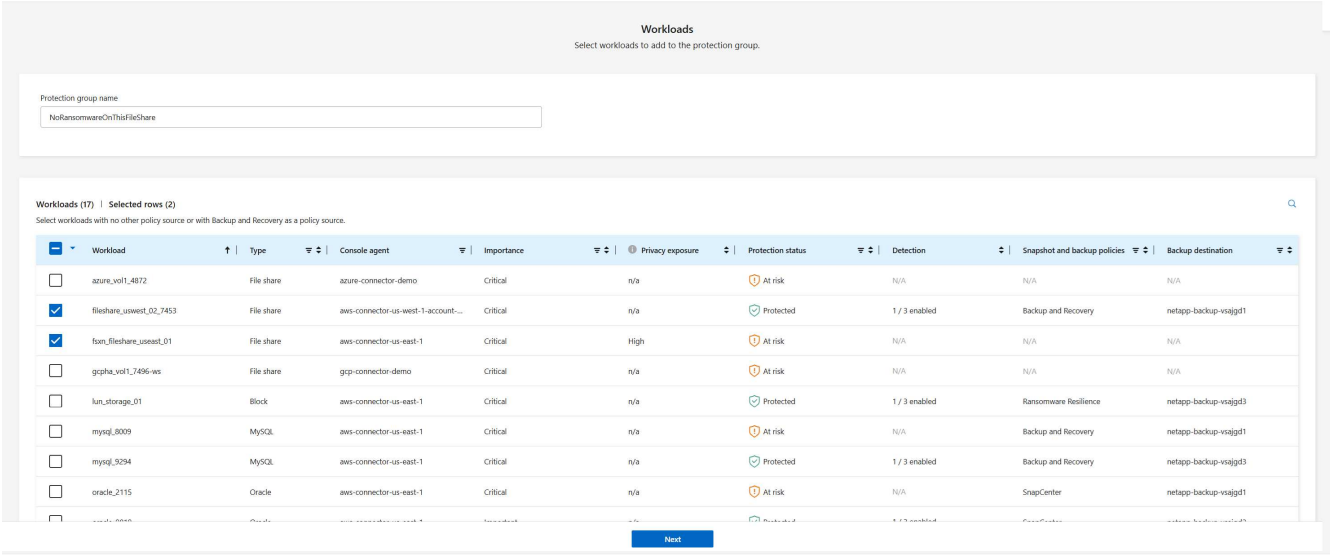
1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.



2. Depuis la page Protection, sélectionnez l'onglet **Groupes de protection**.



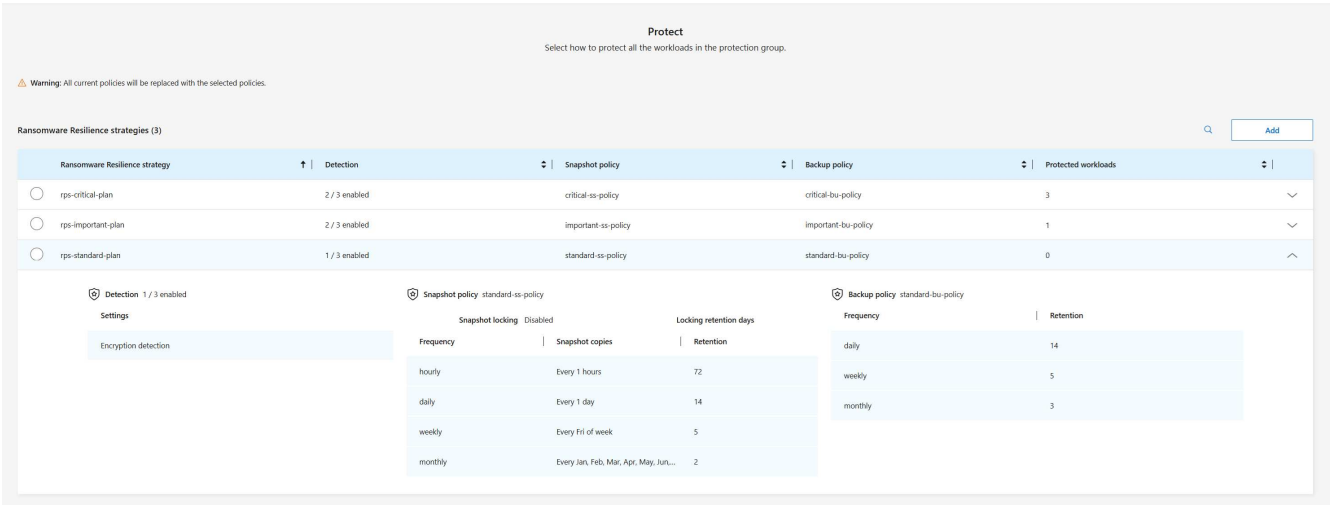
3. Sélectionnez **Ajouter**.



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. Sélectionnez la stratégie pour régir la protection de ce 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 la création du groupe de protection, sélectionnez **Ajouter**.

Modifier la protection du groupe

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

Étapes

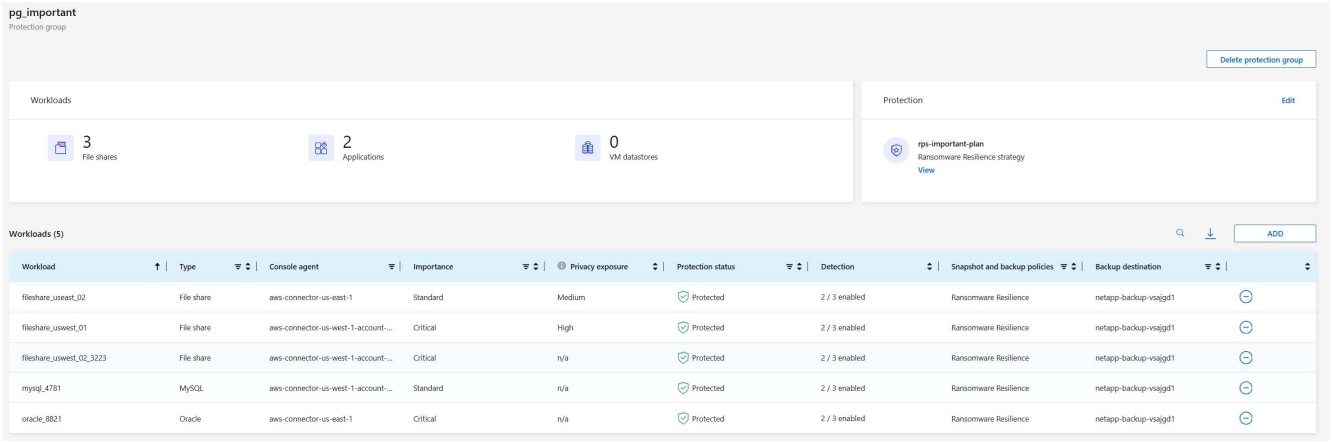
1. Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
2. Depuis la page Protection, sélectionnez l'onglet **Groupes de protection** puis sélectionnez le groupe dont vous souhaitez modifier la politique.
3. Depuis la page d'aperçu du groupe de protection, sélectionnez **Modifier la 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

Vous devrez peut-être ultérieurement supprimer des charges de travail d'un groupe 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.



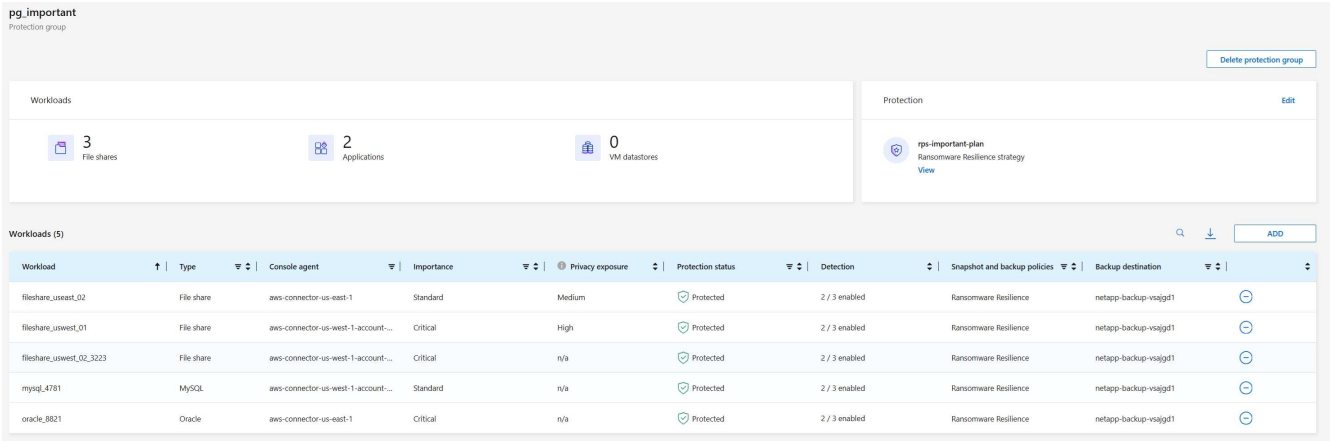
4. À partir de la page du groupe de protection sélectionné, sélectionnez la charge de travail que vous souhaitez supprimer du groupe et sélectionnez *Actions* option.
5. Dans le menu Actions, sélectionnez **Supprimer la charge de travail**.
6. Confirmez que vous souhaitez supprimer la charge de travail et sélectionnez **Supprimer**.

Supprimer le groupe de protection

La suppression du groupe de protection supprime le groupe et sa protection, mais 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**.

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

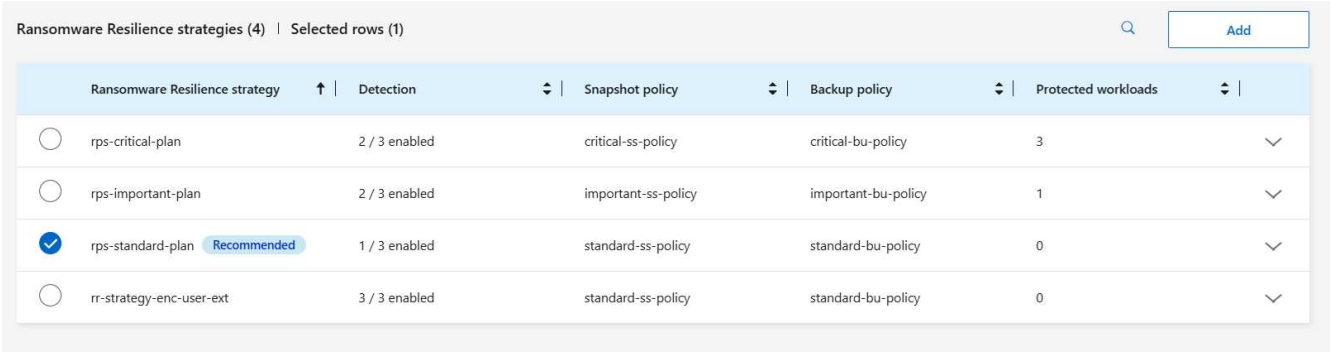
Avant de supprimer une stratégie de protection contre les ransomwares, vous souhaiterez peut-être afficher les charges de travail protégées par cette stratégie.

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**.

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 :

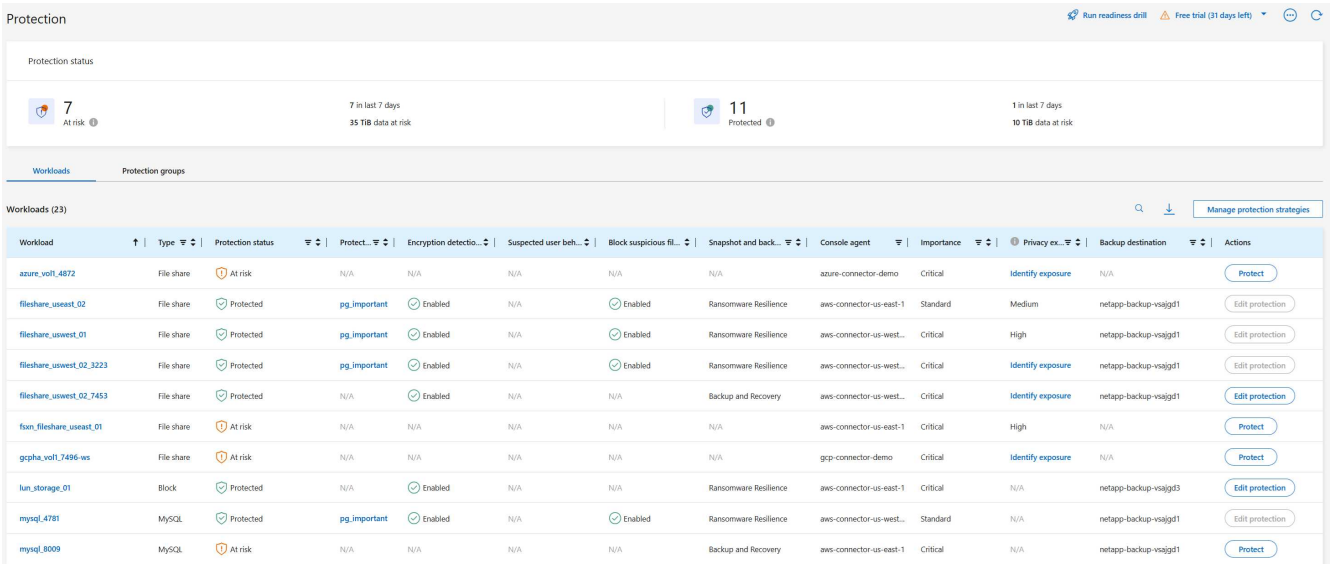
- "En savoir plus sur la classification des données"
- "Catégories de données privées"
- "Examinez les données stockées dans votre organisation"

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

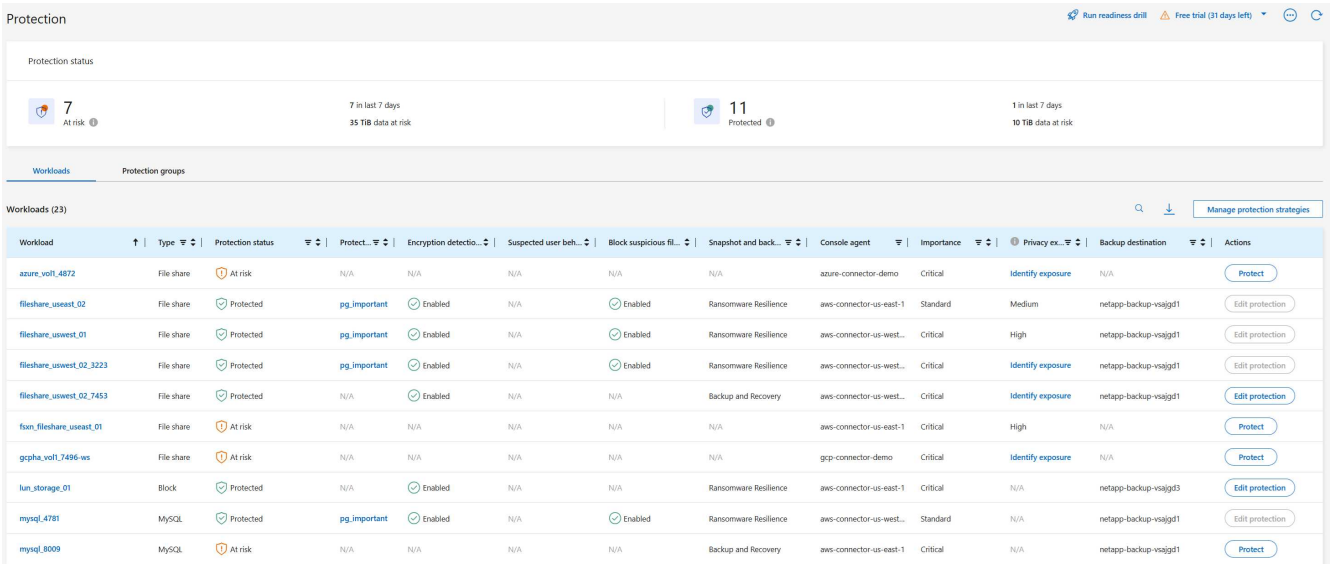
Après avoir analysé les données de classification pour les informations personnelles identifiables, évaluez le risque.

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

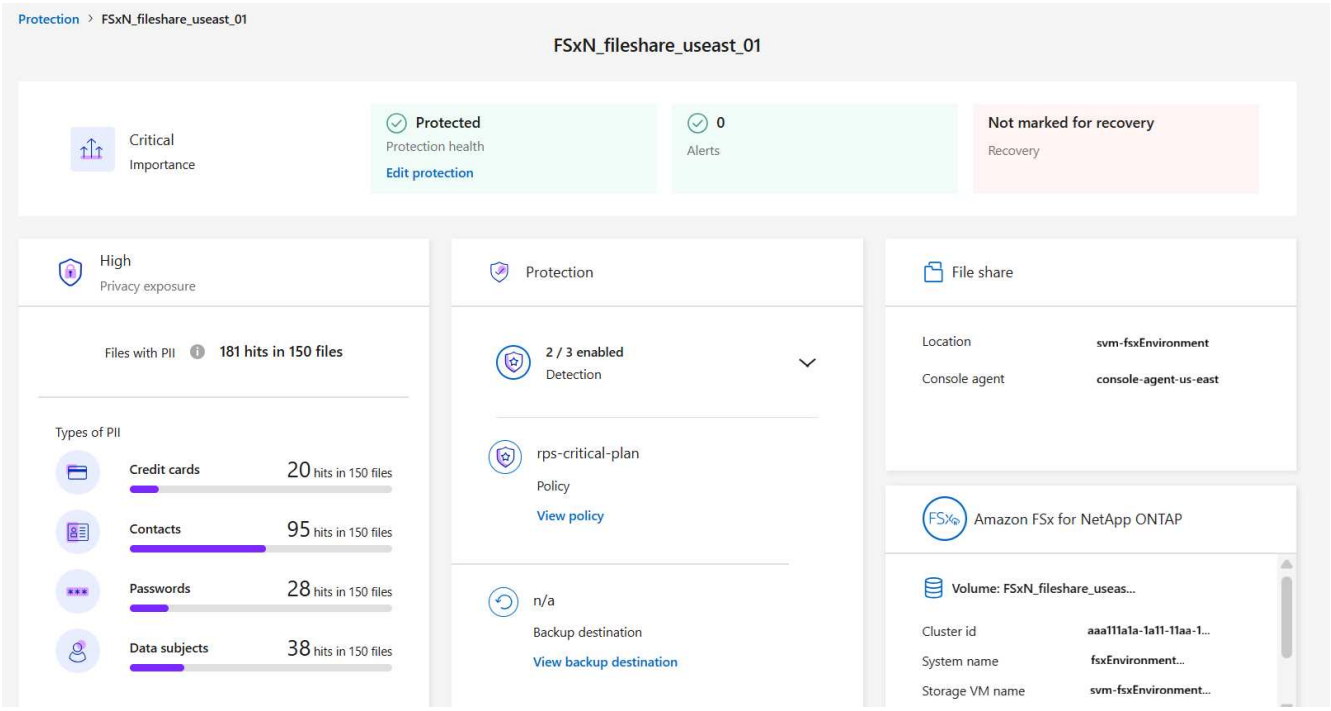
- **Élevé** : Plus de 70 % des fichiers contiennent des informations personnelles identifiables
- **Moyen** : Plus de 30 % et moins de 70 % des fichiers contiennent des informations personnelles identifiables
- **Faible** : Plus de 0 % et moins de 30 % des fichiers contiennent des informations personnelles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

Gérer les alertes dans NetApp Ransomware Resilience

Lorsque NetApp Ransomware Resilience détecte une attaque potentielle, il affiche une alerte sur le tableau de bord et dans la zone de notifications. Ransomware Resilience prend immédiatement un instantané. Consultez le risque potentiel dans l'onglet **Alertes** de résilience aux ransomwares.

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.

Ransomware Resilience fournit des informations appelées *preuves* sur la cause de l'émission de l'alerte, telles que les suivantes :

- 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
- Lorsque le cryptage est élevé, sans modification de l'extension de fichier

Une alerte est classée comme l'une des suivantes :

- **Attaque potentielle** : une alerte se produit lorsque Autonomous Ransomware Protection détecte une nouvelle extension et que l'occurrence se répète plus de 20 fois au cours des dernières 24 heures (comportement par défaut).
- **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" .

Une alerte peut avoir l'un des statuts suivants :

- **Nouveau**
- **Inactif**

Un incident d'alerte peut présenter les états suivants :

- **Nouveau** : Tous les incidents sont marqués « nouveaux » lorsqu'ils sont identifiés pour la première fois.
- **En cours d'examen** : Vous pouvez marquer un incident comme étant en cours d'examen pendant que vous l'évaluez.
- **Rejeté** : Si vous pensez que l'activité n'est pas une attaque de ransomware, vous pouvez modifier le statut sur « Rejeté ».

> Une fois une attaque rejetée, son statut ne peut être modifié. Si vous supprimez une charge de travail, toutes les copies d'instantané prises automatiquement en réponse à une potentielle attaque de ransomware seront définitivement supprimées.

- **Rejet** : L'incident est en cours de rejet.
- **Résolu** : L'incident a été résolu.
- **Résolution automatique** : pour les alertes de faible priorité, l'incident est automatiquement résolu si aucune mesure n'a été prise à ce sujet dans les cinq jours.

> Si vous avez configuré un système de gestion de la sécurité et des événements (SIEM) dans Ransomware Resilience dans la page Paramètres, Ransomware Resilience envoie les détails de l'alerte à votre système SIEM.

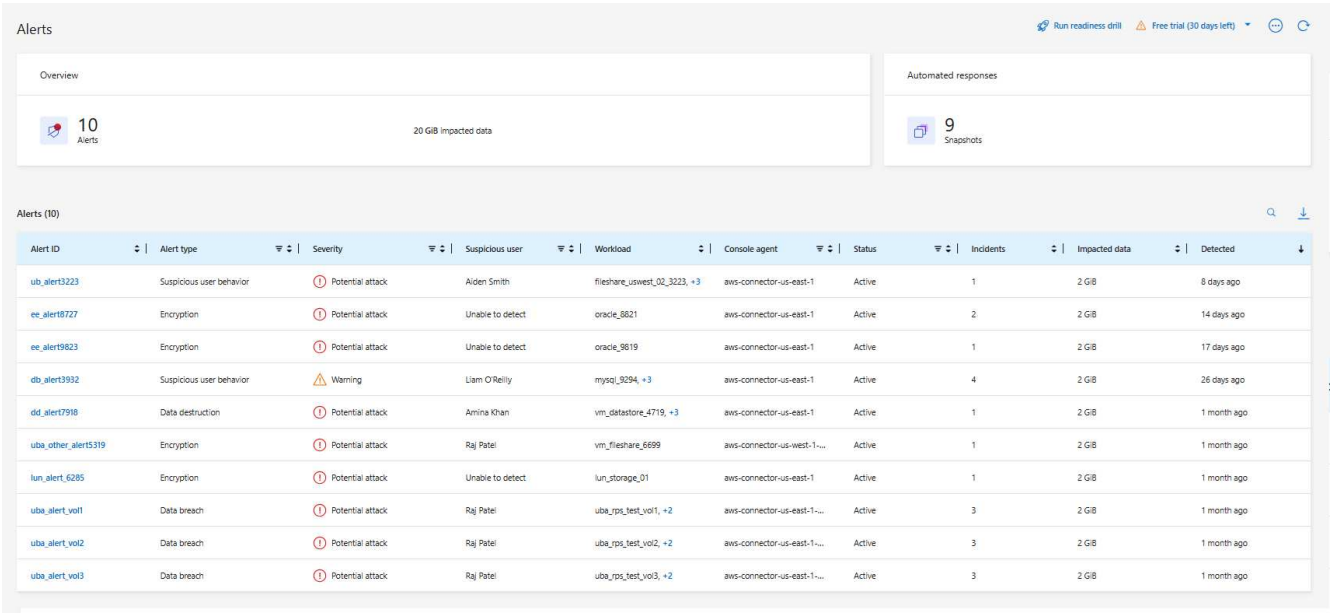
Afficher les alertes

Vous pouvez accéder aux alertes depuis le tableau de bord de résilience aux ransomwares ou depuis l'onglet **Alertes**.

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 de résilience aux ransomwares, examinez 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 **Afficher l'alerte** 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, cliquez sur **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

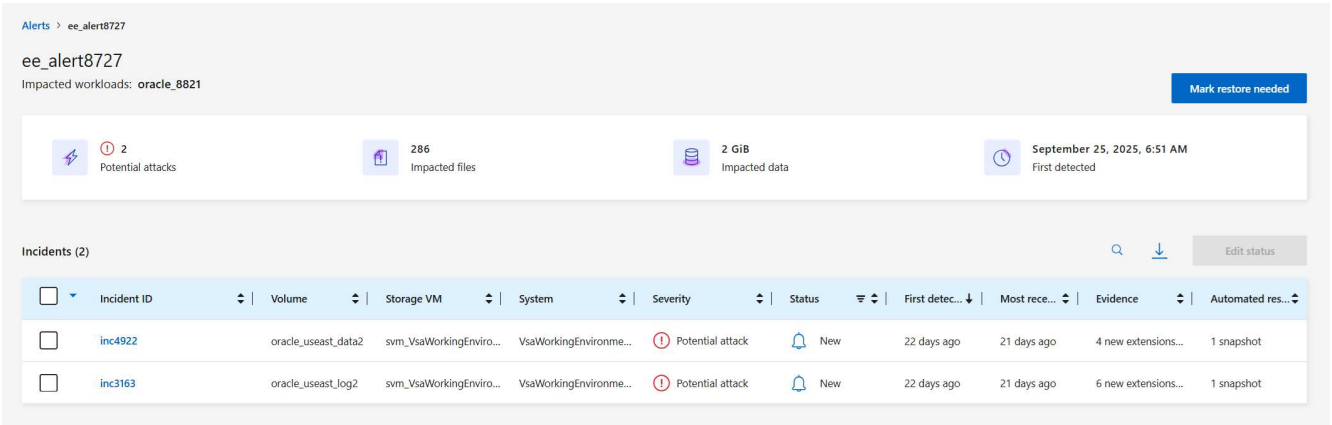
Lorsque la protection autonome contre les ransomwares déclenche une alerte dans Ransomware Resilience, vous pouvez afficher les détails suivants :

- 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
- 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 afficher le comportement anormal des utilisateurs, vous pouvez afficher les données au niveau de l'utilisateur et bloquer des utilisateurs spécifiques. Pour activer les paramètres utilisateur suspects, voir"Configurer les paramètres de résilience aux ransomwares" .

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 **Bloquer** 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.

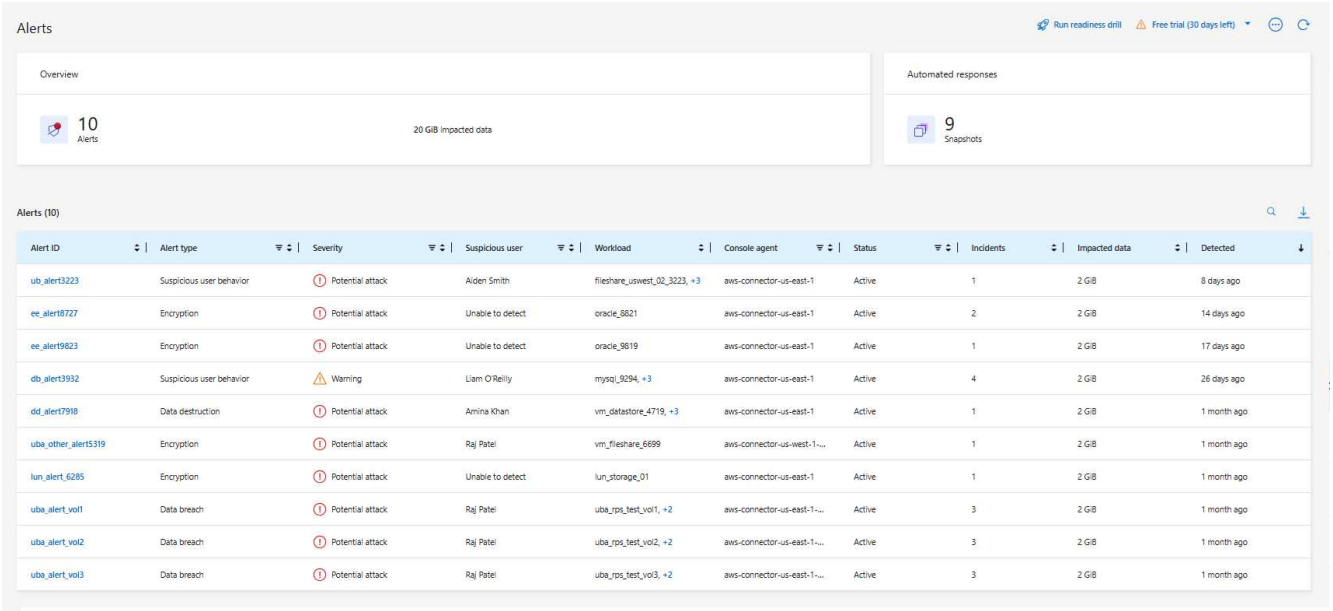
Marquer les incidents de ransomware comme prêts à être récupérés (une fois les incidents neutralisés)

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

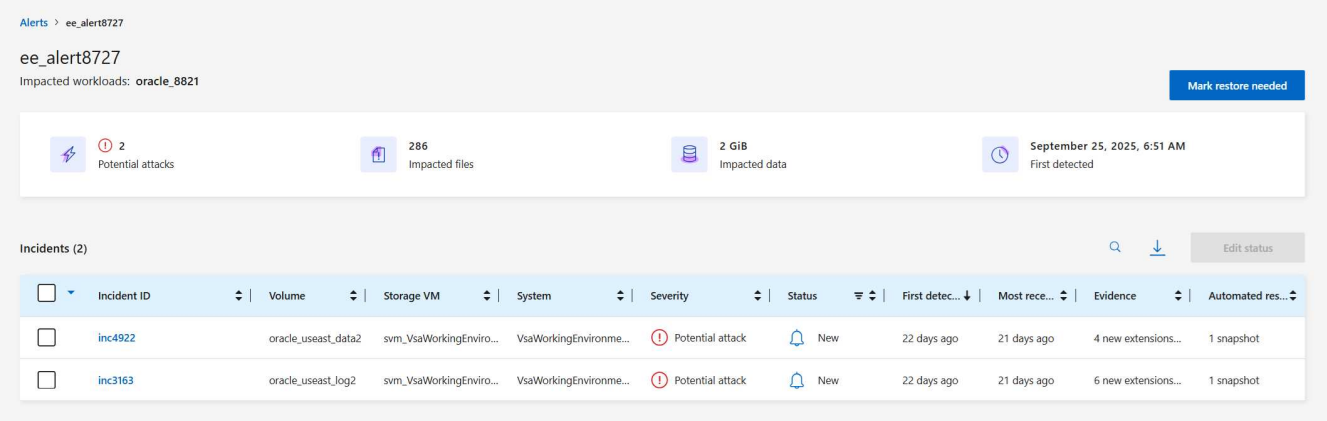
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

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.

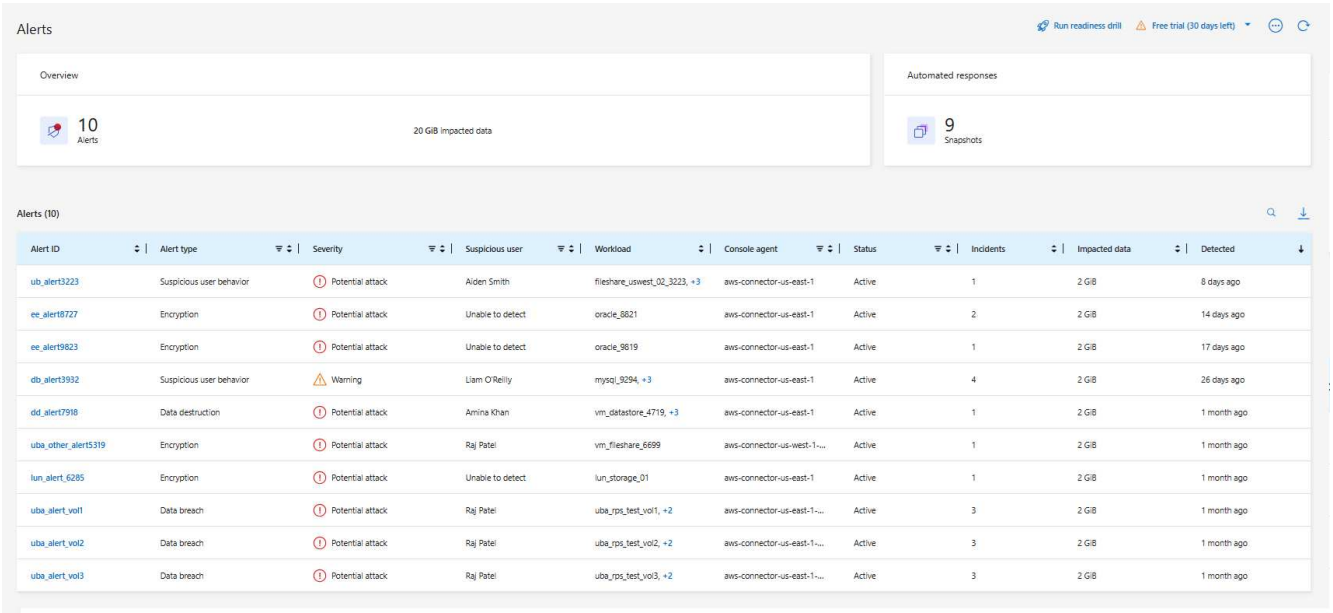
Si vous supprimez une charge de travail, toutes les copies instantanées prises automatiquement en réponse à une attaque potentielle de ransomware sont définitivement supprimées.

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

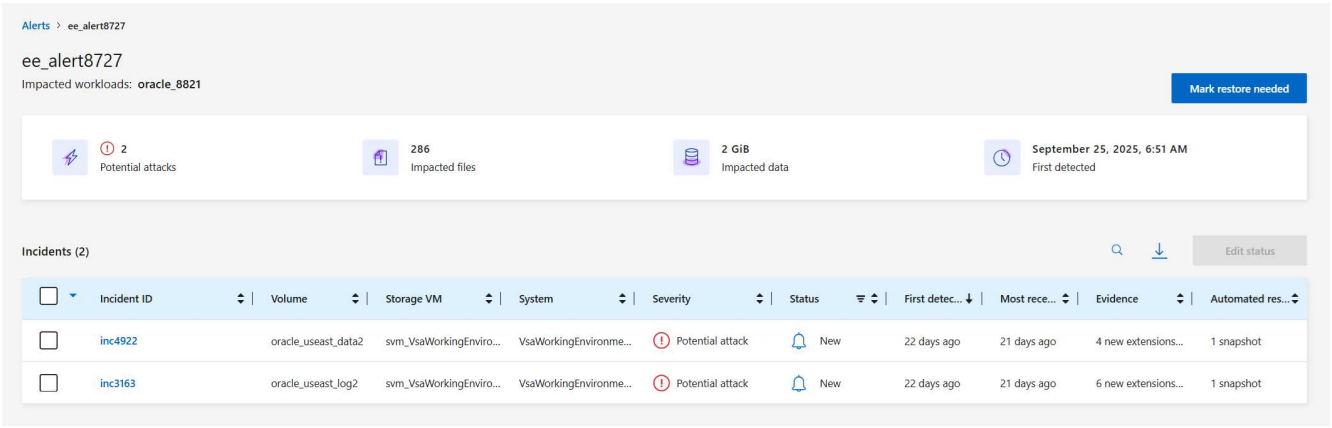
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

Étapes

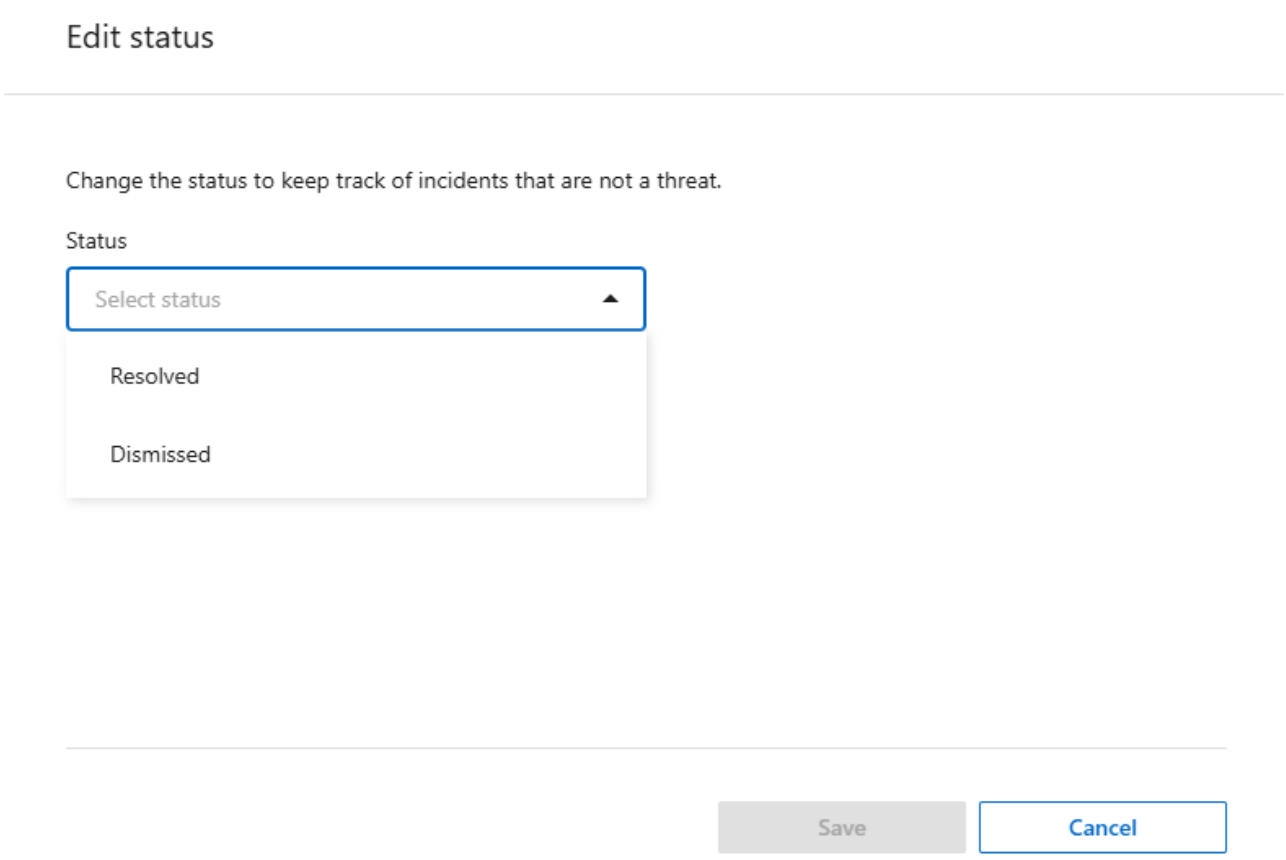
1. Dans le menu Résilience aux ransomwares, sélectionnez **Alertes**.



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.

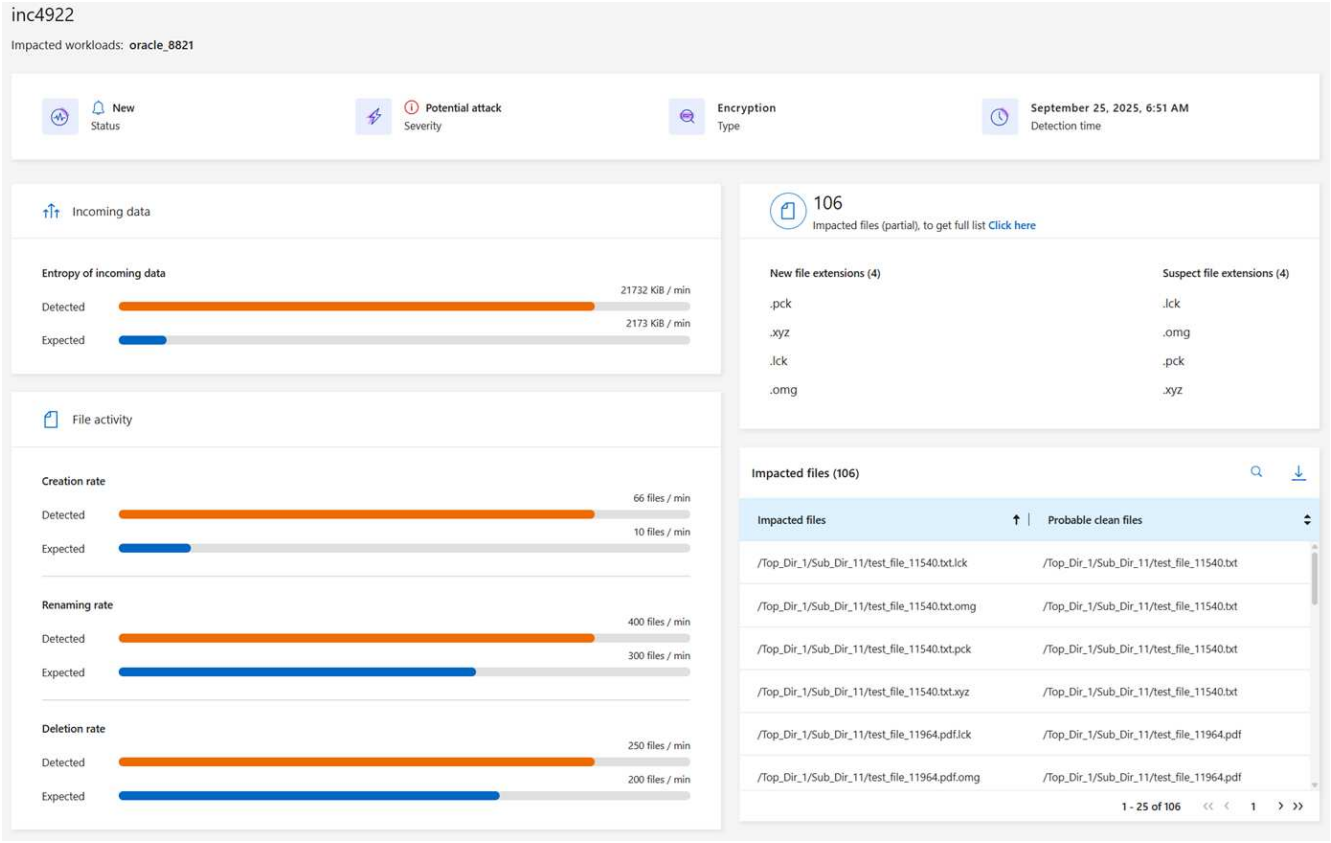
Rôle de console requis Pour effectuer cette tâche, vous devez disposer du rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de résilience aux ransomwares. "En savoir plus sur les rôles de résilience aux ransomwares pour la NetApp Console" .

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 machine virtuelle est gérée par SnapCenter, Ransomware Resilience restaure l'application ou la machine virtuelle à son état précédent et à la dernière transaction à l'aide du processus cohérent avec l'application ou la machine virtuelle. La restauration cohérente avec l'application ou la machine virtuelle ajoute toutes les données qui n'ont pas été stockées, par exemple les données en cache ou dans une opération d'E/S, aux données du volume.
- Si l'application ou la machine virtuelle n'est pas gérée par SnapCenter et 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 tombe en panne.

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 :

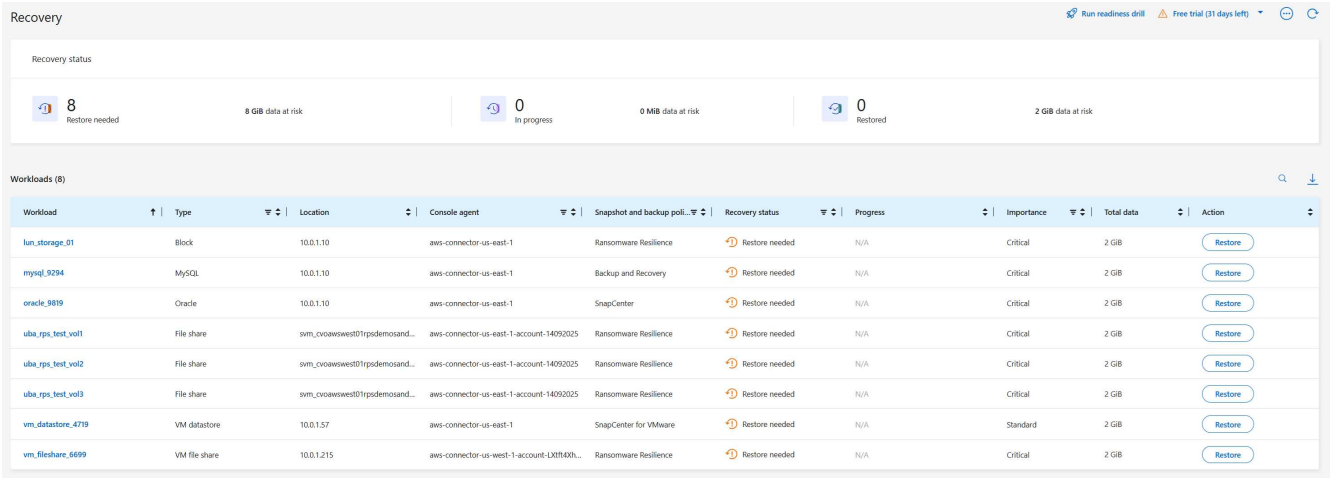
- **Restauration nécessaire** : La charge de travail doit être restaurée.
- **En cours** : L'opération de restauration est actuellement en cours.
- **Restauré** : La charge de travail a été restaurée.
- **Échec** : le processus de restauration de la charge de travail n'a pas pu être terminé.

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, vérifiez les totaux « Restauration nécessaire » dans le volet Alertes et sélectionnez **Afficher tout**.
   - Dans le menu, sélectionnez **Récupération**.
2. Consultez les informations sur la charge de travail dans la page **Récupération**.



Restaurer une charge de travail gérée par SnapCenter

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.

L'état de l'application changera si nécessaire pour la restauration. L'application sera restaurée à son état précédent à partir des fichiers de contrôle, s'ils sont inclus dans la sauvegarde. Une fois la restauration terminée, l'application s'ouvre en mode LECTURE-ÉCRITURE.

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 Ransomware Resilience, 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** : Cohérence avec l'application (ou pour SnapCenter pour machines virtuelles, l'étendue de la restauration est « Par machine virtuelle »)
6. **Source** : Sélectionnez la flèche vers le bas à côté de Source pour voir les détails. 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 l'emplacement d'origine ou alternatif.
   b. Sélectionnez le système.
   c. Sélectionnez la machine virtuelle de stockage.
8. Si la destination d'origine ne dispose pas de suffisamment d'espace pour restaurer la charge de travail, une ligne « Stockage temporaire » apparaît. Vous pouvez sélectionner le stockage temporaire pour restaurer les données de charge de travail. Les données restaurées seront copiées du stockage temporaire vers l'emplacement d'origine. Cliquez sur la **flèche vers le bas** dans la ligne Stockage temporaire et définissez le cluster de destination, la machine virtuelle de stockage et le niveau local.
9. Sélectionnez **Enregistrer**.
10. Sélectionnez **Suivant**.
11. Revoyez vos sélections.
12. Sélectionnez **Restaurer**.
13. 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 non gérée par SnapCenter

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

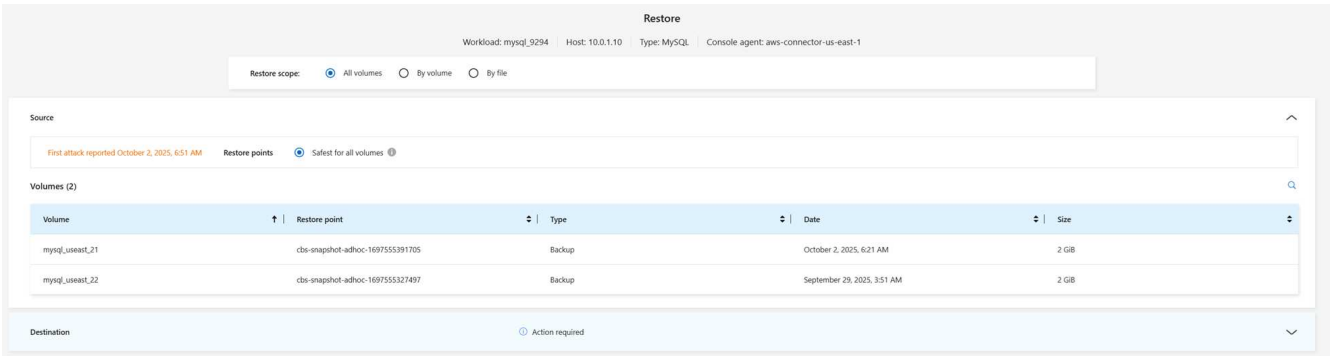
1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Consultez les informations sur la charge de travail dans la page **Récupération**.
3. Sélectionnez une charge de travail qui est dans l'état « Restauration nécessaire ».
4. Pour restaurer, sélectionnez **Restaurer**.
5. **Étendue 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.

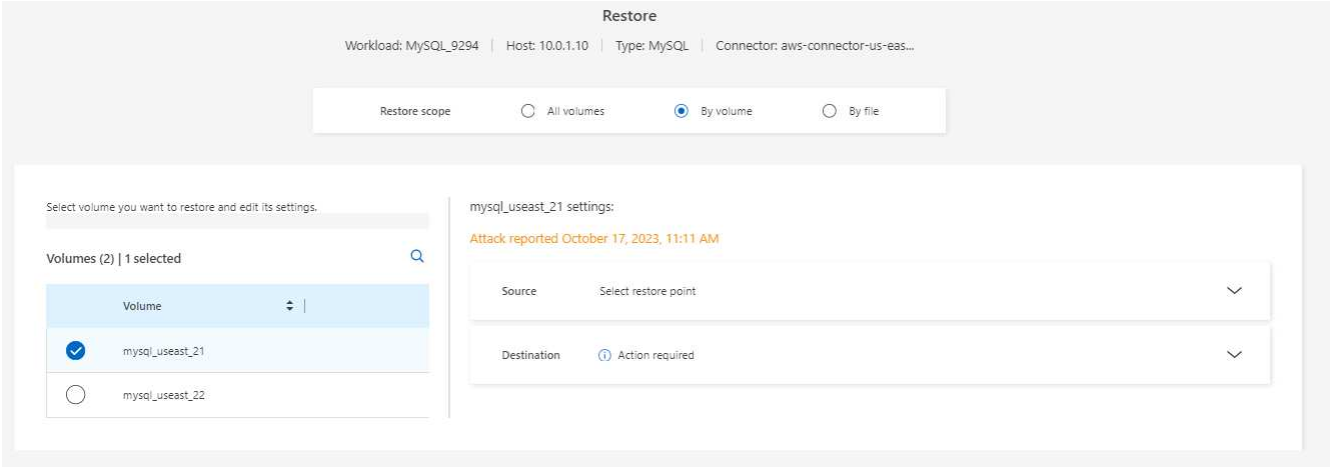
6. **Destination** : Sélectionnez la flèche vers le bas à côté de Destination pour voir les détails.
   a. Sélectionnez le système.
   b. Sélectionnez la machine virtuelle de stockage.
   c. Sélectionnez l'agrégat.
   d. Modifiez le préfixe de volume qui sera ajouté à tous les nouveaux volumes.

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.

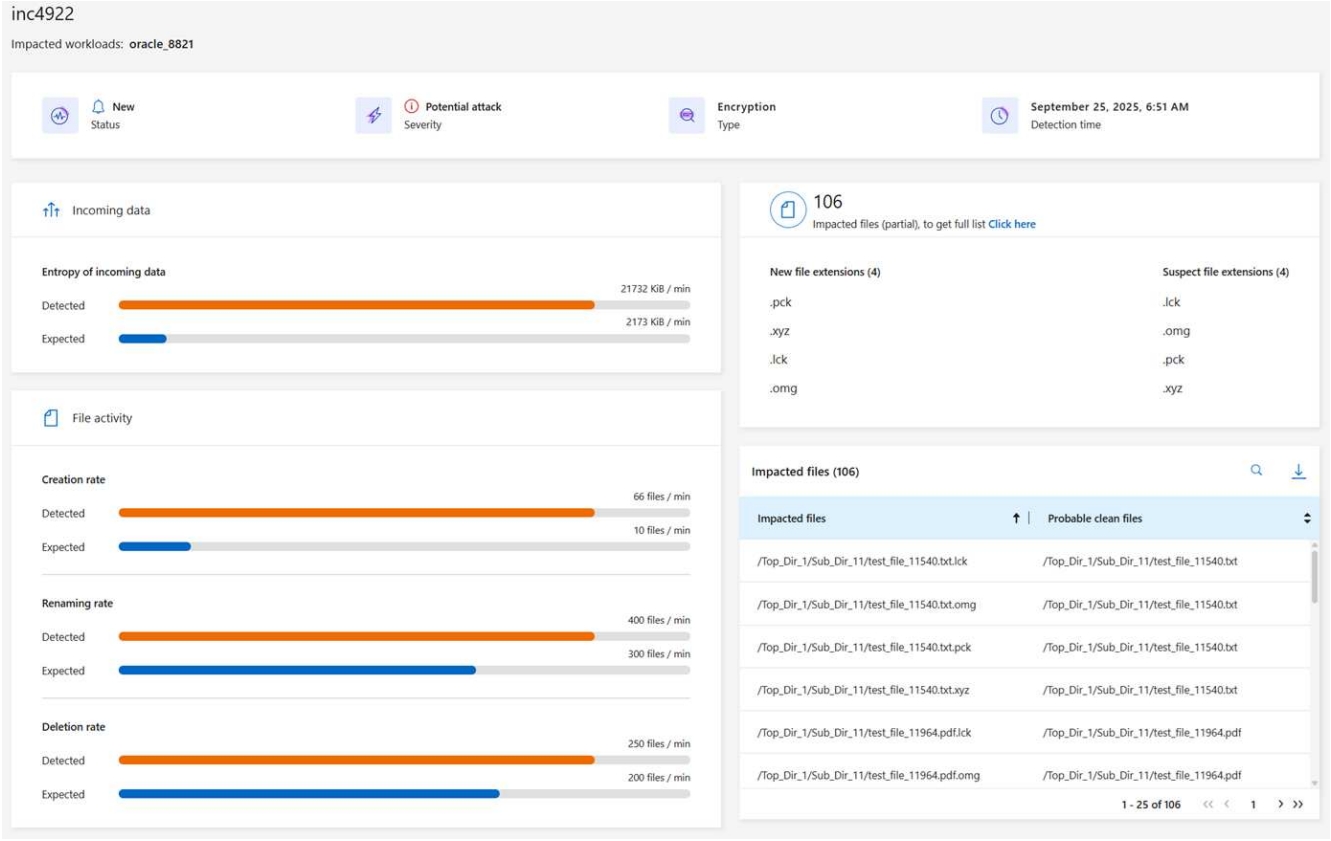
Vous pouvez restaurer une charge de travail d'application au niveau du fichier sur le même système ou sur un système différent.

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.



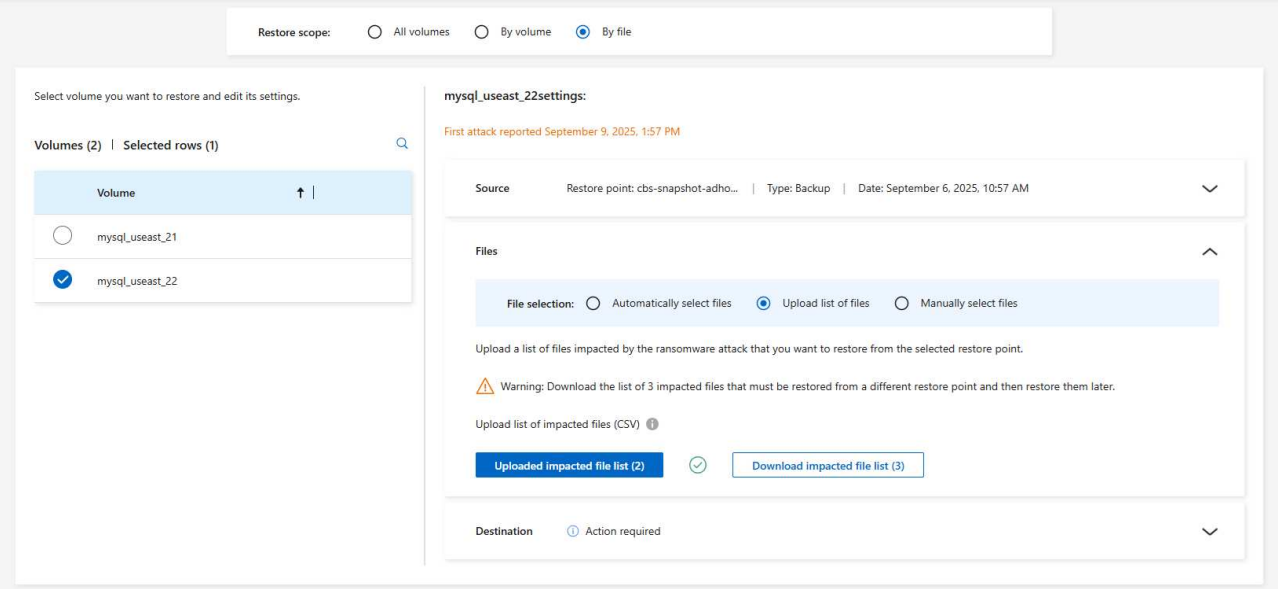
5. Pour voir la liste complète des fichiers, sélectionnez **Cliquez ici** en haut du volet Fichiers concernés.
6. Pour cet incident, sélectionnez l'icône de téléchargement et téléchargez la liste des fichiers impactés au format CSV.

Étapes pour restaurer ces fichiers

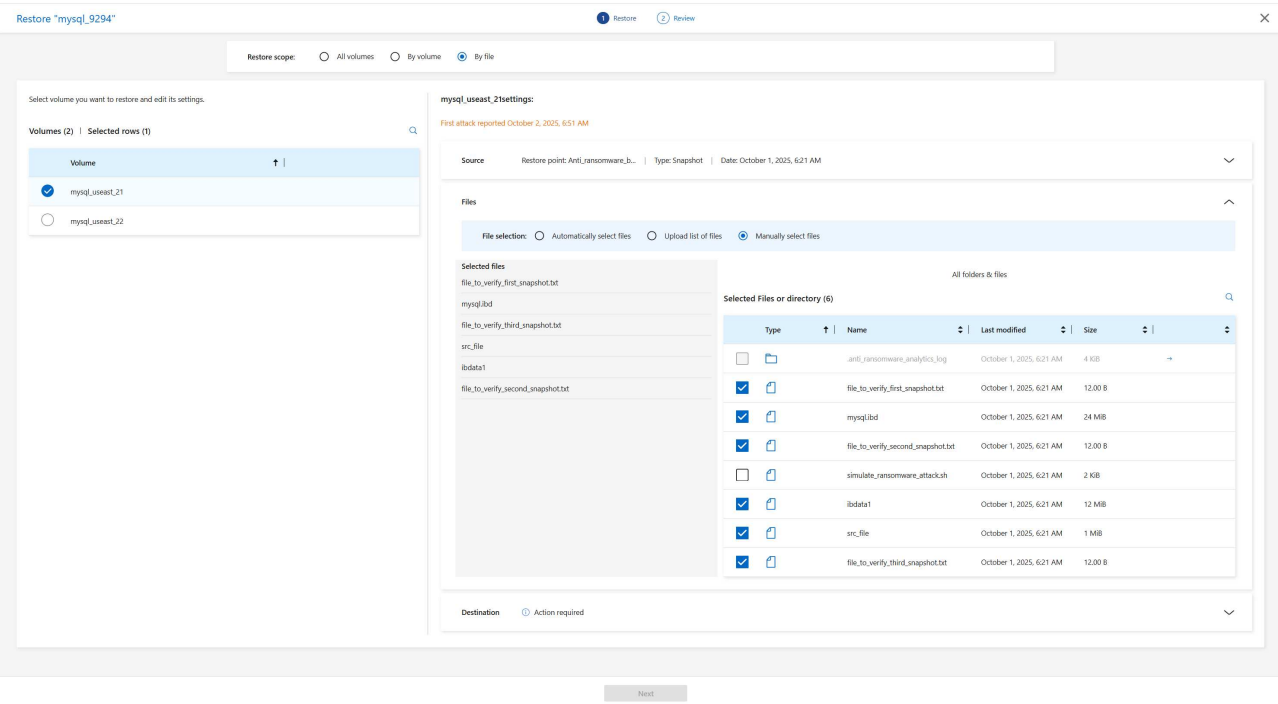
1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Sélectionnez une charge de travail d'application qui est dans l'état « Restauration nécessaire ».
3. Pour restaurer, sélectionnez **Restaurer**.
4. Sur la page Restaurer, dans l'étendue Restaurer, sélectionnez **Par fichier**.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

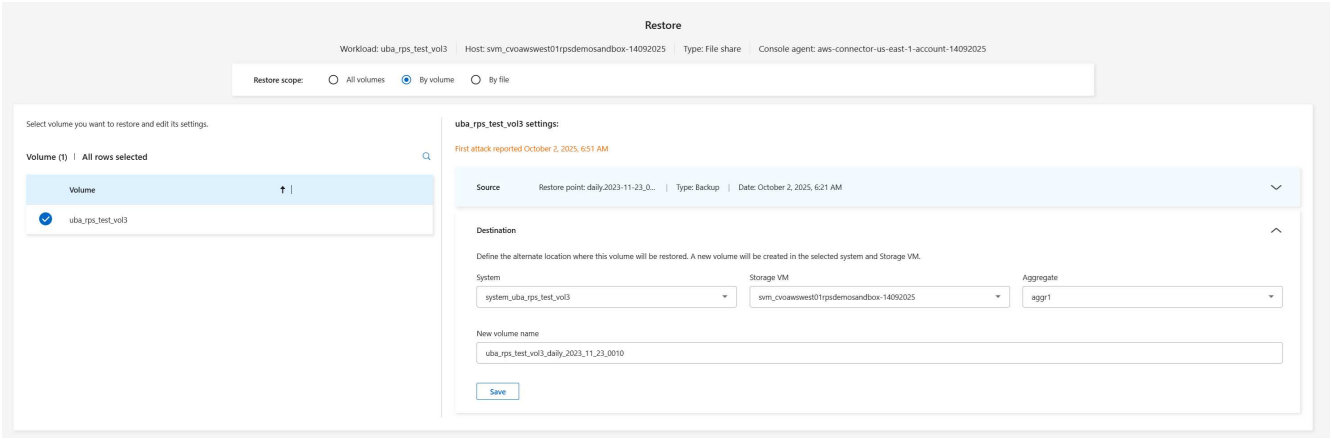
Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

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.

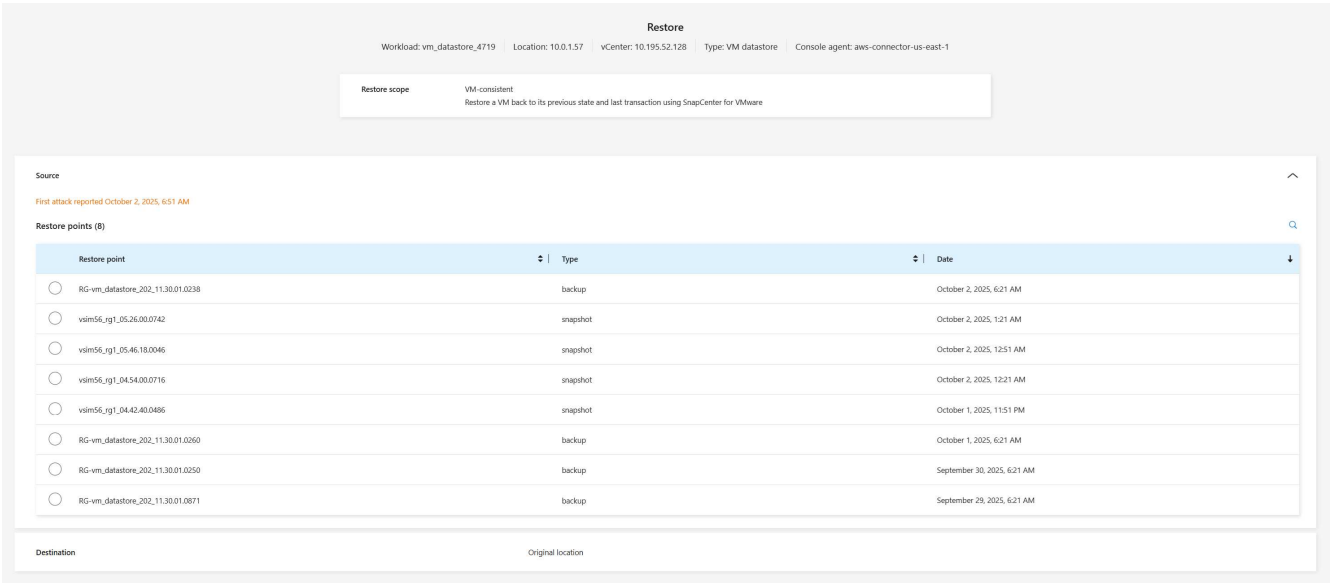
Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

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.

Télécharger les rapports sur la NetApp Ransomware Resilience

Vous pouvez exporter des données de protection et télécharger les fichiers CSV ou JSON qui affichent les détails des exercices de préparation aux attaques, de la protection, des alertes et de la 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.

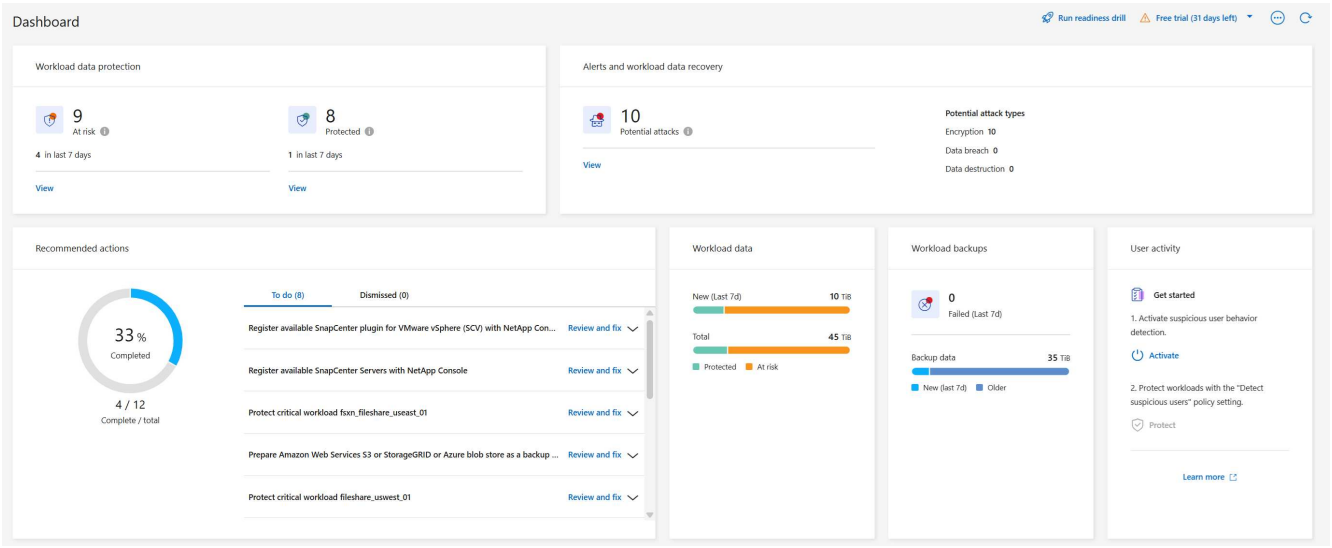
Vous pouvez télécharger les rapports d'exercice de préparation uniquement à partir de la page **Rapports**.

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.

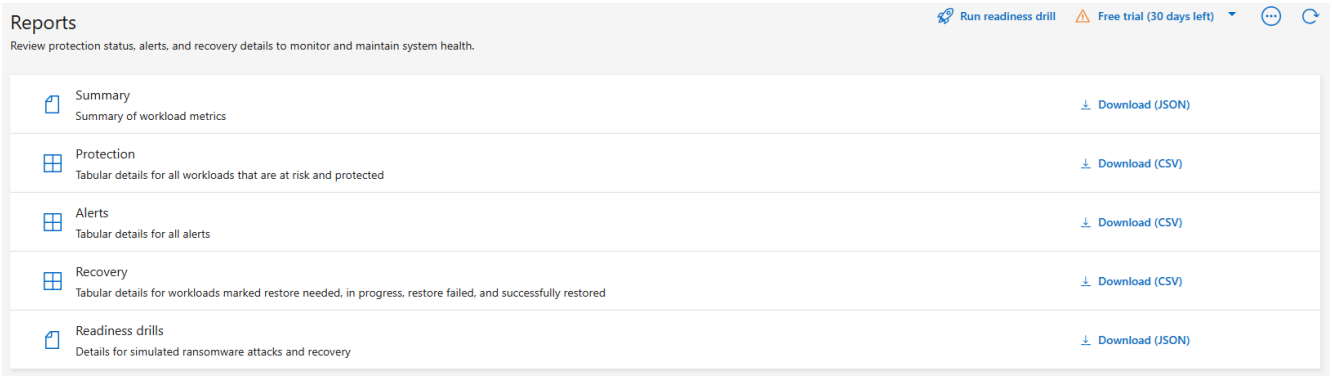
Les fichiers CSV ou JSON incluent des données pour toutes les charges de travail sur tous les systèmes de console.

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 *Actualiser* option 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**.



Connaissances et soutien

Inscrivez-vous pour obtenir de l'aide

L'enregistrement du support est requis pour bénéficier d'un support technique spécifique à la NetApp Console et à ses solutions de stockage et services de données. L'enregistrement du support est également requis pour activer les flux de travail clés pour les systèmes Cloud Volumes ONTAP .

L'inscription au support n'active pas la prise en charge NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à « Obtenir de l'aide » dans la documentation de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Présentation de l'enregistrement de l'assistance

Il existe deux formes d'inscription pour activer le droit au support :

- Enregistrement du numéro de série de votre compte NetApp Console (votre numéro de série 960xxxxxxxxx à 20 chiffres situé sur la page Ressources de support de la console).

  Il s'agit de votre identifiant d'abonnement d'assistance unique pour tout service au sein de la console. Chaque compte de console doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur la place de marché de votre fournisseur de cloud (il s'agit de numéros de série 909201xxxxxxxx à 20 chiffres).

  Ces numéros de série sont communément appelés *numéros de série PAYGO* et sont générés par la NetApp Console au moment du déploiement de Cloud Volumes ONTAP .

L'enregistrement des deux types de numéros de série permet des fonctionnalités telles que l'ouverture de tickets d'assistance et la génération automatique de dossiers. L'enregistrement est terminé en ajoutant des comptes NetApp Support Site (NSS) à la console comme décrit ci-dessous.

Enregistrez la NetApp Console pour le support NetApp

Pour vous inscrire au support et activer le droit de support, un utilisateur de votre compte NetApp Console doit associer un compte de site de support NetApp à sa connexion à la console. La manière dont vous vous inscrivez au support NetApp dépend du fait que vous possédez déjà ou non un compte NetApp Support Site (NSS).

Client existant avec un compte NSS

Si vous êtes un client NetApp avec un compte NSS, il vous suffit de vous inscrire pour bénéficier de l'assistance via la console.

Étapes

1. Sélectionnez **Administration** > **Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite d'authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'inscription a réussi, sélectionnez l'icône Aide, puis sélectionnez **Assistance**.

   La page **Ressources** devrait indiquer que votre compte Console est enregistré pour l'assistance.

   Notez que les autres utilisateurs de la console ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé un compte de site de support NetApp à leur connexion. Cependant, cela ne signifie pas que votre compte n'est pas enregistré pour bénéficier de l'assistance. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre compte a été enregistré.

Client existant mais pas de compte NSS

Si vous êtes un client NetApp existant avec des licences et des numéros de série existants mais *pas* de compte NSS, vous devez créer un compte NSS et l'associer à votre connexion à la console.

Étapes

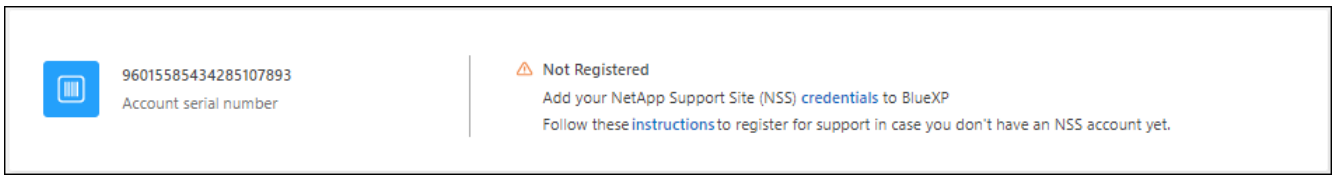
1. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte de console (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement du compte.
2. Associez votre nouveau compte NSS à votre connexion à la console en suivant les étapes ci-dessousClient existant avec un compte NSS .

Tout nouveau chez NetApp

Si vous êtes nouveau sur NetApp et que vous n'avez pas de compte NSS, suivez chaque étape ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console, sélectionnez l'icône Aide, puis sélectionnez **Support**.
2. Recherchez le numéro de série de votre identifiant de compte sur la page d'inscription au support.



3. Accéder à "Site d'inscription au support de NetApp" et sélectionnez **Je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Gamme de produits**, sélectionnez **Cloud Manager**, puis sélectionnez votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, effectuez la vérification de sécurité, puis

confirmez que vous avez lu la politique de confidentialité des données mondiales de NetApp.

Un email est immédiatement envoyé à la boîte mail prévue à cet effet pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers spam si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action depuis l'e-mail.

   La confirmation soumet votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp .

8. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement.

Après avoir terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous avez votre compte de site de support NetApp , associez le compte à votre connexion à la console en suivant les étapes ci-dessousClient existant avec un compte NSS .

Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre compte de console est requise pour activer les workflows clés suivants pour Cloud Volumes ONTAP:

- Enregistrement des systèmes Cloud Volumes ONTAP prépayés pour le support

  Fournir votre compte NSS est nécessaire pour activer le support de votre système et pour accéder aux ressources de support technique NetApp .

- Déploiement de Cloud Volumes ONTAP lorsque vous apportez votre propre licence (BYOL)

  Il est nécessaire de fournir votre compte NSS pour que la console puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut les mises à jour automatiques pour les renouvellements de mandat.

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

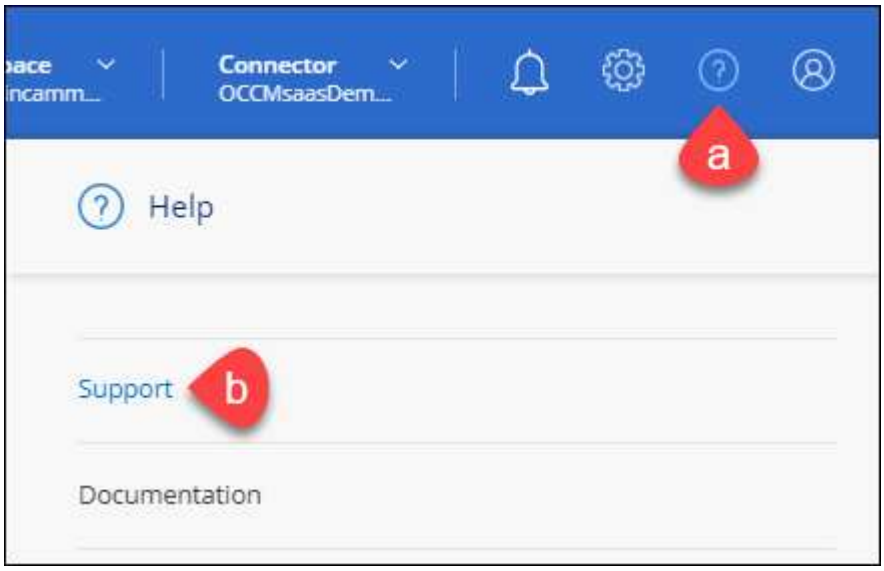
L'association des informations d'identification NSS à votre compte de NetApp Console est différente du compte NSS associé à une connexion utilisateur de console.

Ces informations d'identification NSS sont associées à votre ID de compte de console spécifique. Les utilisateurs appartenant à l'organisation Console peuvent accéder à ces informations d'identification depuis **Support > Gestion NSS**.

- Si vous disposez d'un compte client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous disposez d'un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés aux côtés des comptes de niveau client.

Étapes

1. Dans le coin supérieur droit de la console, sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Sélectionnez **Gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

   NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp pour effectuer le processus d'authentification.

   Ces actions permettent à la console d'utiliser votre compte NSS pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau de logiciels et les futures inscriptions au support.

   Notez ce qui suit :

   - Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS au niveau client.
   - Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS au niveau client et qu'un compte au niveau partenaire existe, vous obtiendrez le message d'erreur suivant :

     « Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de types différents. »

   Il en va de même si vous disposez de comptes NSS préexistants au niveau client et que vous essayez d'ajouter un compte au niveau partenaire.

   - Une fois la connexion réussie, NetApp stockera le nom d'utilisateur NSS.

     Il s'agit d'un identifiant généré par le système qui correspond à votre e-mail. Sur la page **Gestion NSS**, vous pouvez afficher votre e-mail à partir du ••• menu.

- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **Mettre à jour les informations d'identification** dans le ••• menu.

  L'utilisation de cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Obtenir de l'aide

NetApp fournit un support pour NetApp Console et ses services cloud de diverses manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut une assistance technique à distance via un ticket web.

Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud

Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à la documentation de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Pour bénéficier d'un support technique spécifique à NetApp et à ses solutions de stockage et services de données, utilisez les options de support décrites ci-dessous.

Utiliser les options d'auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

  La documentation de la NetApp Console que vous consultez actuellement.

- "Base de connaissances"

  Recherchez dans la base de connaissances NetApp pour trouver des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté NetApp Console pour suivre les discussions en cours ou en créer de nouvelles.

Créer un dossier auprès du support NetApp

En plus des options d'auto-assistance ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tout problème après avoir activé le support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un dossier**, vous devez d'abord associer vos informations

d’identification du site de support NetApp à votre connexion à la console. "Découvrez comment gérer les informations d’identification associées à votre connexion à la console" .

- Si vous ouvrez un dossier pour un système ONTAP doté d’un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans la NetApp Console, sélectionnez **Aide > Support**.
2. Sur la page **Ressources**, choisissez l’une des options disponibles sous Support technique :

   a. Sélectionnez **Appelez-nous** si vous souhaitez parler à quelqu’un au téléphone. Vous serez redirigé vers une page sur netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un dossier** pour ouvrir un ticket avec un spécialiste du support NetApp :

      - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, * NetApp Console* lorsqu’il s’agit d’un problème de support technique lié aux flux de travail ou aux fonctionnalités de la console.
      - **Système** : Si applicable au stockage, sélectionnez * Cloud Volumes ONTAP* ou **On-Prem**, puis l’environnement de travail associé.

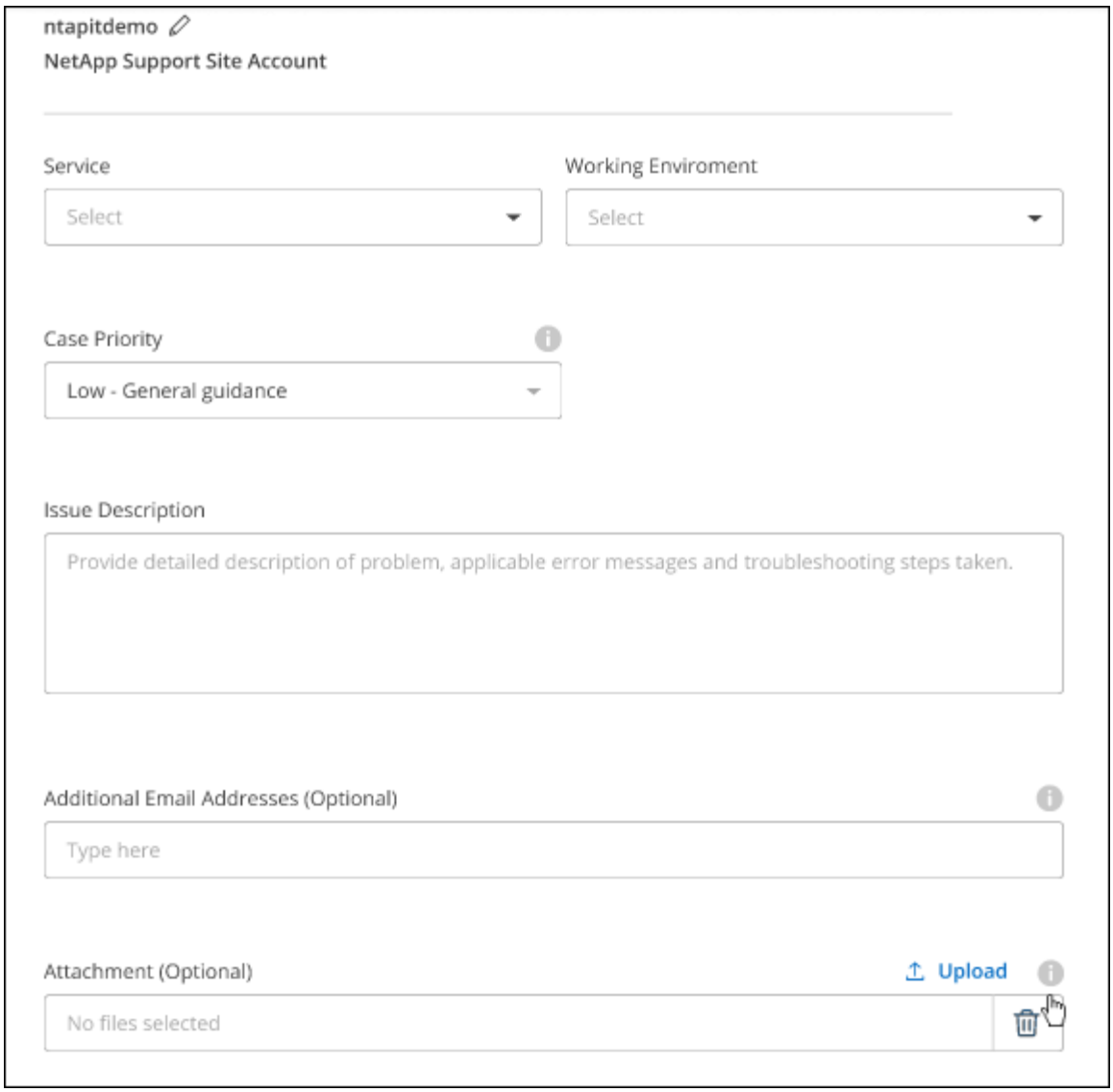
        La liste des systèmes est dans le périmètre de l’organisation de la console et de l’agent de console que vous avez sélectionné dans la bannière supérieure.

      - **Priorité du cas** : Choisissez la priorité du cas, qui peut être Faible, Moyenne, Élevée ou Critique.

        Pour en savoir plus sur ces priorités, passez votre souris sur l’icône d’information à côté du nom du champ.

      - **Description du problème** : Fournissez une description détaillée de votre problème, y compris tous les messages d’erreur applicables ou les étapes de dépannage que vous avez effectuées.
      - **Adresses e-mail supplémentaires** : saisissez des adresses e-mail supplémentaires si vous souhaitez informer quelqu’un d’autre de ce problème.
      - **Pièce jointe (facultatif)** : Téléchargez jusqu’à cinq pièces jointes, une à la fois.

        Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.



Après avoir terminé

Une fenêtre contextuelle apparaîtra avec votre numéro de dossier d'assistance. Un spécialiste du support NetApp examinera votre cas et vous répondra dans les plus brefs délais.

Pour un historique de vos demandes d'assistance, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées « créer une demande d'assistance ». Un bouton à l'extrême droite vous permet de développer l'action pour voir les détails.

Il est possible que vous rencontriez le message d'erreur suivant lorsque vous essayez de créer un dossier :

« Vous n'êtes pas autorisé à créer un dossier contre le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement à laquelle il est associé ne sont pas la même société d'enregistrement pour le numéro de série du compte NetApp Console (c'est-à-dire. 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Soumettez un cas non technique à https://mysupport.netapp.com/site/help

Gérez vos cas d’assistance

Vous pouvez afficher et gérer les cas d’assistance actifs et résolus directement depuis la console. Vous pouvez gérer les cas associés à votre compte NSS et à votre entreprise.

Notez ce qui suit :

- Le tableau de bord de gestion des cas en haut de la page offre deux vues :
  - La vue de gauche montre le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte utilisateur NSS que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte utilisateur NSS.

  Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.
- Vous pouvez ajouter ou supprimer des colonnes d’intérêt et filtrer le contenu des colonnes telles que Priorité et Statut. D’autres colonnes fournissent simplement des capacités de tri.

  Consultez les étapes ci-dessous pour plus de détails.
- Au niveau de chaque cas, nous offrons la possibilité de mettre à jour les notes du cas ou de fermer un cas qui n’est pas déjà au statut Fermé ou En attente de fermeture.

Étapes

1. Dans la NetApp Console, sélectionnez **Aide > Support**.
2. Sélectionnez **Gestion des cas** et si vous y êtes invité, ajoutez votre compte NSS à la console.

   La page **Gestion des cas** affiche les cas ouverts liés au compte NSS associé à votre compte utilisateur de la console. Il s’agit du même compte NSS qui apparaît en haut de la page **Gestion NSS**.
3. Modifiez éventuellement les informations qui s’affichent dans le tableau :
   - Sous **Cas de l’organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre entreprise.
   - Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une période différente.
   - Filtrer le contenu des colonnes.
   - Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant et ensuite choisir les colonnes que vous souhaitez afficher.
4. Gérer un dossier existant en sélectionnant et en sélectionnant l’une des options disponibles :
   - **Voir le cas** : Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes du cas** : fournissez des détails supplémentaires sur votre problème ou sélectionnez **Télécharger des fichiers** pour joindre jusqu’à un maximum de cinq fichiers.

     Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.
   - **Fermer le dossier** : Fournissez des détails sur les raisons pour lesquelles vous fermez le dossier et sélectionnez **Fermer le dossier**.

Questions fréquemment posées sur la NetApp Ransomware Resilience

Cette FAQ peut vous aider si vous recherchez simplement une réponse rapide à une question sur NetApp Ransomware Resilience.

Déploiement

Avez-vous besoin d'une licence pour utiliser Ransomware Resilience ?

Vous pouvez utiliser les types de licences suivants :

- Inscrivez-vous pour un essai gratuit de 30 jours.
- Achetez un abonnement à la carte (PAYGO) à NetApp Intelligent Services et Ransomware Resilience avec Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace et Microsoft Azure Marketplace.
- Apportez votre propre licence (BYOL), qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp . Vous pouvez utiliser le numéro de série de la licence pour activer le BYOL dans la section Licenses and subscriptions de la console.

Comment activer la résilience aux ransomwares ?

Vous pouvez accéder à Ransomware Resilience depuis la NetApp Console. Assurez-vous d'avoir "rôles d'accès" et "prérequis". Si vous avez correctement configuré un agent de console, vous pouvez alors : "découvrir les charges de travail".

Pour plus d'informations, voir"Accéder à la résilience des ransomwares" et"Guide de démarrage rapide de Ransomware Resilience" .

La solution Ransomware Resilience est-elle disponible en modes standard, restreint et privé ?

Ransomware Resilience n'est actuellement disponible qu'en mode standard.

Pour une explication sur ces modes dans tous les services de données NetApp , reportez-vous à "Modes de déploiement de la NetApp Console" .

Accéder

Quelle est l'URL de résilience face aux ransomwares ?

Dans un navigateur, saisissez "https://console.netapp.com/ransomware-resilience" pour accéder à la console.

Comment les autorisations d'accès sont-elles gérées ?

"En savoir plus sur les rôles d'accès à la console pour tous les services". Ransomware Resilience possède également "rôles d'accès dédiés".

Quelle est la meilleure résolution d'écran ?

La résolution d'appareil recommandée pour Ransomware Resilience est de 1920 x 1080 ou supérieure.

Quel navigateur dois-je utiliser ?

Vous pouvez accéder à la NetApp Console avec n'importe quel navigateur Web moderne.

Interopérabilité

La résilience face aux ransomwares est-elle consciente des paramètres de protection dans ONTAP?

Oui, Ransomware Resilience découvre les planifications de snapshots définies dans ONTAP.

Comment Ransomware Resilience interagit-il avec NetApp Backup and Recovery et SnapCenter?

Ransomware Resilience fonctionne avec Backup and Recovery pour découvrir et définir des politiques de capture instantanée et de sauvegarde pour les charges de travail de partage de fichiers.

Ransomware Resilience fonctionne avec SnapCenter ou SnapCenter pour VMware afin de découvrir et de définir des politiques de snapshot et de sauvegarde pour les charges de travail des applications et des machines virtuelles.

Ransomware Resilience fonctionne également avec Backup and Recovery et SnapCenter (y compris SnapCenter pour VMware) pour effectuer une récupération cohérente des fichiers et des charges de travail.

Pour la gestion des licences et la facturation, Ransomware Resilience peut s'intégrer à Backup and Recovery même si vous ne disposez pas d'une licence distincte pour Backup and Recovery. Si vous disposez à la fois de Backup and Recovery et de Ransomware Resilience, toutes les données communes protégées par les deux produits sont facturées uniquement par Ransomware Resilience.

Charges de travail

Qu'est-ce qu'une charge de travail dans le contexte de la résilience aux ransomwares ?

Une charge de travail est une application, une machine virtuelle ou un partage de fichiers. Une charge de travail inclut tous les volumes utilisés par une seule instance d'application.

Par exemple, prenons le cas d'une base de données Oracle déployée sur ora3.host.com avec `vol1` contenant des données et `vol2` contenant des journaux. Les deux volumes constituent la charge de travail de cette instance de base de données Oracle.

Comment Ransomware Resilience priorise-t-il les données de charge de travail ?

La priorité de la charge de travail (critique, standard, importante) est déterminée par les fréquences de snapshots déjà appliquées à chaque volume associé à la charge de travail et aux sauvegardes planifiées.

"En savoir plus sur la priorité ou l'importance de la charge de travail" .

Quelles charges de travail la résilience face aux ransomwares prend-elle en charge ?

Ransomware Resilience peut identifier les charges de travail suivantes : Oracle, partages de fichiers, stockage par blocs, machines virtuelles et banques de données de machines virtuelles.

Si vous utilisez SnapCenter ou SnapCenter pour VMware, toutes les charges de travail prises en charge par ces produits sont également identifiées dans Ransomware Resilience. Ransomware Resilience peut protéger et récupérer SnapCenter et les charges de travail SnapCenter de manière cohérente.

Comment associer des données à une charge de travail ?

Ransomware Resilience détecte les volumes et les extensions de fichiers et les associe à la charge de travail appropriée.

Si vous utilisez SnapCenter ou SnapCenter pour VMware et que vous avez configuré des charges de travail dans Backup and Recovery, Ransomware Resilience détecte les charges de travail gérées par SnapCenter et SnapCenter pour VMware ainsi que leurs volumes associés.

Qu’est-ce qu’une charge de travail protégée ?

Dans Ransomware Resilience, une charge de travail affiche l’état **protégé** lorsqu’une stratégie de *détection* principale est activée, ce qui signifie "Protection autonome contre les ransomwares (ARP)" est activé sur tous les volumes liés à la charge de travail.

Qu’est-ce qu’une charge de travail « à risque » ?

Si une charge de travail ne dispose pas d’une stratégie de détection principale activée, elle est considérée comme « à risque », même si une stratégie de sauvegarde et de capture instantanée est activée. Pour vous protéger contre les ransomwares, vous devez activer un "politique de détection".

J’ai ajouté un nouveau volume, mais il n’est pas encore apparu. Que dois-je faire?

Si vous avez ajouté un nouveau volume à votre environnement, relancez la découverte de la charge de travail. Une fois le volume découvert, "appliquer des politiques de protection pour protéger le nouveau volume".

Politiques de protection

Les politiques de résilience aux ransomwares peuvent-elles coexister avec d’autres types de politiques de charge de travail ?

À l’heure actuelle, la sauvegarde et la récupération (Cloud Backup) prennent en charge une politique de sauvegarde par volume. Si vous configurez la protection de sauvegarde avec Backup and Recovery, celle-ci partage les mêmes politiques de sauvegarde avec Ransomware Resilience.

Les copies instantanées ne sont pas limitées et peuvent être ajoutées séparément de chaque service.

Quelles sont les politiques requises dans une stratégie de protection contre les ransomwares ?

UN "stratégie de protection contre les ransomwares" nécessite :

- une politique de détection des ransomwares, et
- une politique d’instantané

Une politique de sauvegarde n’est pas requise dans la stratégie de résilience aux ransomwares.

La résilience face aux ransomwares est-elle consciente des paramètres de protection dans ONTAP?

Oui, Ransomware Resilience découvre les planifications de snapshots définies dans ONTAP. Il permet également de déterminer si ARP et FPolicy sont activés sur tous les volumes d’une charge de travail détectée. Les informations affichées dans le tableau de bord de résilience aux ransomwares proviennent d’autres solutions et produits NetApp .

La solution Ransomware Resilience prend-elle en compte les politiques déjà définies dans Backup and Recovery et SnapCenter?

Oui, si vous avez des charges de travail gérées dans Backup and Recovery ou SnapCenter, les politiques gérées par ces produits sont intégrées dans Ransomware Resilience.

Est-il possible de modifier les politiques transférées depuis NetApp Backup and Recovery et/ou SnapCenter?

Non, vous ne pouvez pas modifier les politiques gérées par Backup and Recovery ou SnapCenter à partir de Ransomware Resilience. Vous gérez toutes les modifications apportées à ces politiques dans Backup and Recovery ou SnapCenter.

Si des politiques existent depuis ONTAP (telles que ARP, FPolicy et les instantanés), sont-elles modifiées dans Ransomware Resilience ?

Non. Ransomware Resilience ne modifie aucune politique de détection existante (paramètres ARP, FPolicy) d'

ONTAP.

Que se passe-t-il si vous ajoutez de nouvelles politiques dans Backup and Recovery ou SnapCenter après avoir souscrit à Ransomware Resilience ?

Ransomware Resilience reconnaît les politiques nouvellement créées et les modifications de politiques dans Backup and Recovery ou SnapCenter.

Est-il possible de modifier les politiques depuis ONTAP?

Oui, vous pouvez modifier les politiques d' ONTAP dans Ransomware Resilience. Vous pouvez également créer de nouvelles politiques dans Ransomware Resilience et les appliquer aux charges de travail. Cette action remplace les politiques ONTAP existantes par les politiques créées dans Ransomware Resilience.

Est-il possible de désactiver les politiques dans ONTAP?

Vous pouvez désactiver ARP dans les politiques de détection à l'aide de l'interface utilisateur, des API ou de l'interface de ligne de commande du gestionnaire système dans ONTAP.

Vous pouvez désactiver FPolicy et les stratégies de sauvegarde en appliquant une stratégie différente qui ne les inclut pas.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

- "Avis concernant la NetApp Console"