



# **Documentation sur la résilience aux ransomwares de NetApp**

## **NetApp Ransomware Resilience**

NetApp  
October 06, 2025

# Sommaire

Documentation sur la résilience aux ransomwares de NetApp	1
Notes de version	2
Nouveautés de NetApp Ransomware Resilience	2
06 octobre 2025	2
15 juillet 2025	2
9 juin 2025	3
13 mai 2025	3
29 avril 2025	4
14 avril 2025	4
10 mars 2025	5
16 décembre 2024	6
7 novembre 2024	6
30 septembre 2024	7
2 septembre 2024	7
5 août 2024	8
1 juillet 2024	8
10 juin 2024	9
14 mai 2024	10
5 mars 2024	11
6 octobre 2023	12
Limitations connues de NetApp Ransomware Resilience	12
Problème d'option de réinitialisation de l'exercice de préparation	13
Limitations Amazon FSx for NetApp ONTAP	13
Commencer	14
En savoir plus sur la résilience aux ransomwares de NetApp	14
Résilience aux ransomwares au niveau des données	14
Ce que vous pouvez faire avec Ransomware Resilience	15
Avantages de l'utilisation de Ransomware Resilience	16
Coût	16
Licences	17
Console NetApp	17
Comment fonctionne la résilience aux ransomwares	17
Cibles de sauvegarde, systèmes et sources de données de charge de travail pris en charge	20
Termes qui pourraient vous aider à vous protéger contre les ransomwares	21
Conditions préalables à la résilience aux ransomwares NetApp	21
Dans la console NetApp	21
Dans ONTAP 9.11.1 et versions ultérieures	22
Pour les sauvegardes de données	22
Mettre à jour les autorisations des utilisateurs non administrateurs dans un système ONTAP	22
Démarrage rapide pour NetApp Ransomware Resilience	23
Configurer la résilience NetApp Ransomware	24
Préparer la destination de sauvegarde	24
Configurer la console NetApp	24

Accéder à la résilience des ransomwares NetApp	25
Configurer les licences pour NetApp Ransomware Resilience	26
Autres licences	27
Essayez-le en utilisant un essai gratuit de 30 jours	27
Abonnez-vous via AWS Marketplace	28
Abonnez-vous via Microsoft Azure Marketplace	31
Abonnez-vous via Google Cloud Platform Marketplace	33
Apportez votre propre permis de conduire (BYOL)	36
Mettez à jour votre licence de console lorsqu'elle expire	37
Mettre fin à l'abonnement PAYGO	37
Découvrez les charges de travail dans NetApp Ransomware Resilience	38
Sélectionnez les charges de travail à découvrir et à protéger	38
Découvrez les charges de travail nouvellement créées pour les systèmes précédemment sélectionnés	40
Découvrez de nouveaux systèmes	40
Effectuez un exercice de préparation aux attaques de ransomware dans NetApp Ransomware Resilience	41
Configurer un exercice de préparation aux attaques de ransomware	41
Démarrer un exercice de préparation	44
Répondre à une alerte d'exercice de préparation	44
Restaurer la charge de travail du test	46
Modifier le statut des alertes après l'exercice de préparation	47
Rapports d'examen sur l'exercice de préparation	48
Configurer les paramètres de protection dans NetApp Ransomware Resilience	48
Accéder directement à la page Paramètres	49
Simuler une attaque de ransomware	49
Configurer la découverte de la charge de travail	49
Identifiez les comportements utilisateur suspectés d'anomalie en vous connectant à Data Infrastructure Insights Sécurité de la charge de travail	49
Ajouter une destination de sauvegarde	50
Connectez-vous à un système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces	57
Utiliser la résilience aux ransomwares	63
Utiliser la résilience aux ransomwares NetApp	63
Surveiller l'état de la charge de travail à l'aide du tableau de bord de résilience NetApp Ransomware	63
Examiner l'état de la charge de travail à l'aide du tableau de bord	63
Consultez les recommandations de protection sur le tableau de bord	65
Exporter les données de protection vers des fichiers CSV	67
Accéder à la documentation technique	67
Protéger les charges de travail	68
Protégez les charges de travail avec les stratégies de protection NetApp Ransomware Resilience	68
Recherchez des informations personnelles identifiables avec la classification des données NetApp dans Ransomware Resilience	83
Gérez les alertes de ransomware détectées avec NetApp Ransomware Resilience	87
Afficher les alertes	89
Répondre à un e-mail d'alerte	89

Détecter les activités malveillantes et les comportements anormaux des utilisateurs	90
Marquer les incidents de ransomware comme prêts à être récupérés (une fois les incidents neutralisés)	93
Ignorer les incidents qui ne sont pas des attaques potentielles	94
Afficher la liste des fichiers concernés	96
Récupérez après une attaque de ransomware (après neutralisation des incidents) avec NetApp	
Ransomware Resilience	97
Afficher les charges de travail prêtes à être restaurées	98
Restaurer une charge de travail gérée par SnapCenter	98
Restaurer une charge de travail non gérée par SnapCenter	99
Télécharger les rapports sur la résilience aux ransomwares NetApp	107
Connaissances et soutien	109
Inscrivez-vous pour obtenir de l'aide	109
Présentation de l'enregistrement de l'assistance	109
Enregistrez BlueXP pour le support NetApp	109
Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP	112
Obtenir de l'aide	113
Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud	113
Utiliser les options d'auto-assistance	114
Créer un dossier auprès du support NetApp	114
Gérez vos demandes d'assistance (Aperçu)	116
Questions fréquemment posées sur la résilience aux ransomwares NetApp	119
Déploiement	119
Accéder	119
Interaction avec d'autres services	120
Charges de travail	120
Politiques de protection	121

# Documentation sur la résilience aux ransomwares de NetApp

# Notes de version

## Nouveautés de NetApp Ransomware Resilience

Découvrez les nouveautés de NetApp Ransomware Resilience.

### 06 octobre 2025

#### La BlueXP ransomware protection est désormais NetApp Ransomware Resilience

La réplication du ransomware BlueXP a été renommée NetApp Ransomware Resilience.

#### BlueXP est désormais NetApp Console

BlueXP a été renommé et repensé pour mieux refléter son rôle dans la gestion de votre infrastructure de données.

La console NetApp 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 console NetApp"](#) .

### 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](#)".

## **1 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 d'aperçu, le service protège les charges de travail basées sur les applications des magasins de données Oracle, MySQL, VM et des partages de fichiers sur le stockage NAS sur site ainsi que Cloud Volumes ONTAP sur AWS (à l'aide du protocole NFS) dans les 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 ce système :

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

# Commencer

## En savoir plus sur la résilience aux ransomwares de NetApp

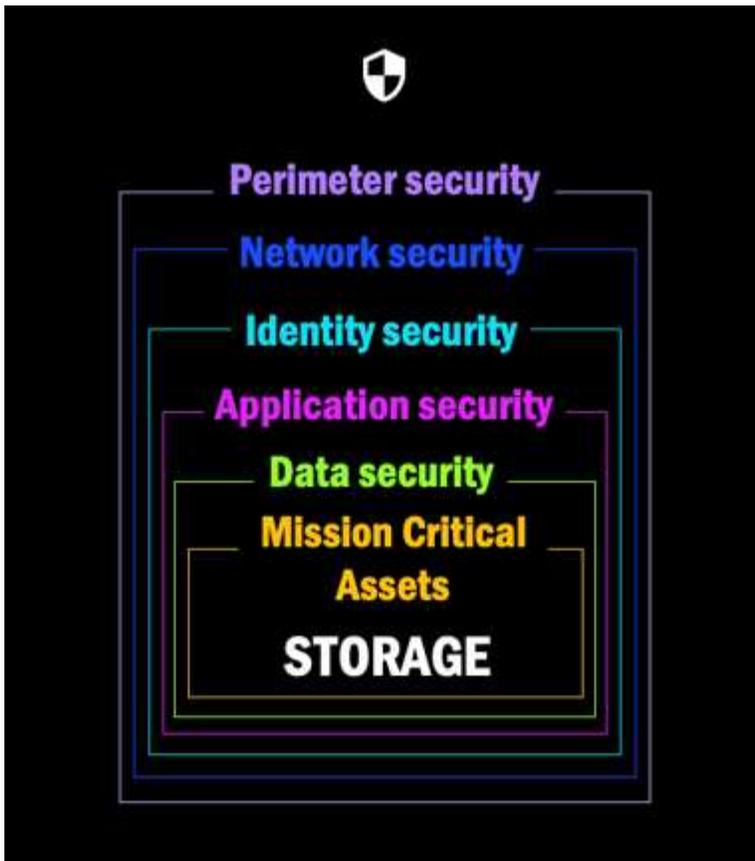
Les attaques de ransomware peuvent bloquer l'accès à vos données et les attaquants peuvent demander une rançon en échange de la divulgation des données ou de leur décryptage. Selon l'IDC, il n'est pas rare que les victimes de ransomware subissent plusieurs attaques de ransomware. L'attaque peut perturber 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 basées sur les applications d'Oracle, MySQL, les banques de données VM et les partages de fichiers sur le stockage NAS sur site (à l'aide des protocoles NFS et CIFS) et le stockage SAN (FC, iSCSI et NVMe) ainsi que 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 sur la console NetApp . Vous pouvez sauvegarder des données sur Amazon Web Services, Google Cloud, le stockage cloud Microsoft Azure et NetApp StorageGRID.

### Résilience aux ransomwares au niveau des données

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

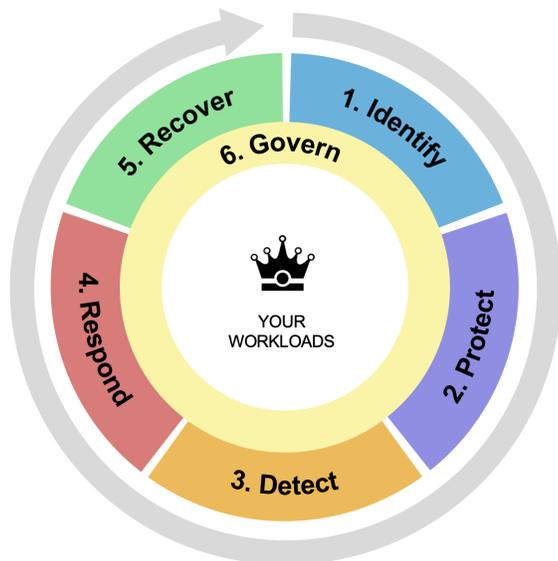
- **Couche la plus externe** : il s'agit de votre première ligne de défense utilisant des pare-feu, des systèmes de détection d'intrusion et des réseaux privés virtuels pour protéger les limites du réseau.
- **Sécurité du réseau** : Cette couche s'appuie sur la base de la segmentation du réseau, de la 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 :

- **Identifiez** toutes les charges de travail basées sur des applications, de partage de fichiers ou gérées par VMware dans les systèmes NAS (NFS ou CIFS) et SAN (FC, iSCSI et NVMe) sur site NetApp dans la console NetApp, les projets et les agents de la 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.
- **Détectez** 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.]
- **Répondez** aux attaques potentielles de ransomware en lançant automatiquement un instantané NetApp ONTAP inviolable qui est verrouillé afin que la copie ne puisse pas être supprimée accidentellement ou de manière malveillante. Vos données de sauvegarde resteront immuables et protégées de bout en bout contre les attaques de ransomware à la source et à la 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.



1. Automatically **discovers** and prioritizes data in NetApp storage **with a focus on top application-based workloads**

2. **One-click protection** of top workload data (backup, immutable/indelible snapshots, secure configuration, different security domain)

3. **Accurately detects** ransomware as **quickly** as possible using **next-generation AI-based anomaly detection**

4. Automated response to secure safe recovery point, attack alerting, and integration with top **SIEM and XDR solutions**

5. Rapidly restores data via simplified **orchestrated recovery** to accelerate application uptime

6. Implement your ransomware protection **strategy and policies**, and **monitor outcomes**

## 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 principales charges de travail basées sur les applications, telles que les banques de données MySQL, Oracle, VMware et 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

NetApp ne vous facture pas l'utilisation de la version d'essai de Ransomware Resilience.



Avec la sortie d'octobre 2024, les nouveaux déploiements de Ransomware Resilience offrent un essai gratuit de 30 jours. Auparavant, Ransomware Resilience proposait un essai gratuit de 90 jours. Si vous êtes déjà inscrit à l'essai gratuit de 90 jours, cet essai est valable pendant 90 jours.

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. Vous pouvez également utiliser Data Infrastructure Insights (anciennement Cloud Insights) Workload Security (licence requise) pour étudier le comportement des utilisateurs et empêcher des utilisateurs spécifiques d'effectuer d'autres activités.

Pour plus de détails, consultez la section "[Configurer les licences](#)".

## Console NetApp

La résilience aux ransomwares est accessible via la console NetApp.

La console NetApp 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 pas besoin de licence ni d'abonnement pour commencer à utiliser NetApp Console et vous n'encourez des frais que lorsque vous devez déployer des agents de console dans votre cloud pour garantir la connectivité à vos systèmes de stockage ou à vos services de données NetApp. Cependant, certains services de données NetApp accessibles depuis la console sont sous licence ou basés sur un abonnement.

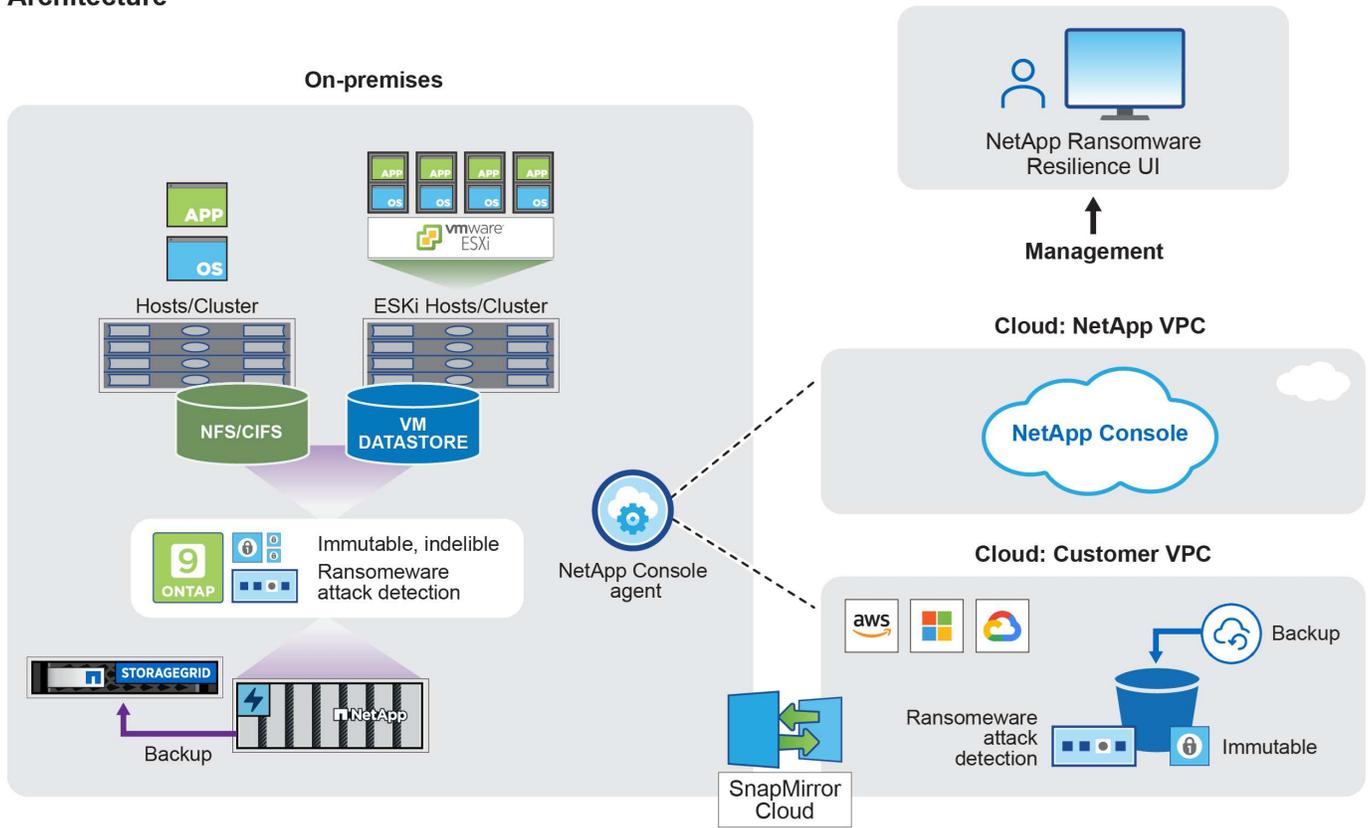
En savoir plus sur le "[Console NetApp](#)".

## 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
<b>IDENTIFIER</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Identifie les données client des API de service ONTAP et SnapCenter et les associe aux charges de travail. En savoir plus sur <a href="#">"ONTAP"</a> et <a href="#">"Logiciel SnapCenter"</a> .</li> <li>• 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 la sauvegarde et la récupération, 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. En savoir plus sur <a href="#">"Protection autonome contre les ransomwares"</a> , <a href="#">"Sauvegarde et récupération NetApp"</a> , et <a href="#">"Politique ONTAP"</a> .</li> <li>• 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.</li> </ul>
<b>PROTÉGER</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>DÉTECTER</b>	<ul style="list-style-type: none"> <li>• Détecte les attaques potentielles avec un modèle d'apprentissage automatique (ML) intégré qui détecte le cryptage et les activités potentiellement anormaux.</li> <li>• 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.</li> <li>• 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 ), Data Infrastructure Insights (anciennement Cloud Insights), Workload Security et FPolicy.</li> </ul>
<b>RÉPONDRE</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>

Fonctionnalité	Description
<b>RÉCUPÉRER</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
<b>GOUVERNER</b>	<ul style="list-style-type: none"> <li>• Affecte les stratégies de protection contre les ransomwares</li> <li>• Vous aide à surveiller les résultats.</li> </ul>

## 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

- NAS ONTAP sur site (utilisant les protocoles NFS et CIFS) avec ONTAP version 9.11.1 et supérieure
- SAN ONTAP sur site (utilisant les protocoles FC, iSCSI et NVMe) avec ONTAP version 9.17.1 et supérieure
- Cloud Volumes ONTAP 9.11.1 ou supérieur pour AWS (utilisant les protocoles NFS et CIFS)
- Cloud Volumes ONTAP 9.11.1 ou supérieur pour Google Cloud Platform (utilisant les protocoles NFS et CIFS)
- Cloud Volumes ONTAP 9.12.1 ou supérieur pour Microsoft Azure (utilisant les protocoles NFS et CIFS)
- Cloud Volumes ONTAP 9.17.1 ou supérieur pour AWS, Google Cloud Platform et Microsoft Azure (à l'aide des protocoles FC, iSCSI et NVMe)
- Amazon FSx for NetApp ONTAP, qui utilise la protection autonome contre les ransomwares (ARP et non ARP/AI)



ARP/AI nécessite ONTAP 9.16 ou supérieur.



Les éléments suivants ne sont pas pris en charge : les volumes FlexGroup , les versions ONTAP antérieures à 9.11.1, les volumes de point de montage, les volumes de chemin de montage, les volumes hors ligne et les volumes de protection des données (DP).

## 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 :

- Partages de fichiers NetApp
- Stockage en bloc
- Banques de données VMware
- Bases de données (MySQL et Oracle)
- Plus à venir bientôt

De plus, 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 qui pourraient vous aider à vous protéger contre les ransomwares

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 MySQL ou Oracle, des banques de données VMware ou des partages de fichiers.

## Conditions préalables à la résilience aux ransomwares NetApp

Commencez à utiliser NetApp Ransomware Resilience en vérifiant l'état de préparation de votre environnement opérationnel, de votre connexion, de votre accès réseau et de votre navigateur Web.

Pour utiliser Ransomware Resilience, vous aurez besoin des prérequis.

### Dans la console NetApp

- Un compte utilisateur de la console NetApp avec des privilèges d'administrateur d'organisation pour la découverte des ressources.
- Une organisation de console avec au moins un agent de console actif se connectant à des clusters ONTAP locaux ou à Cloud Volumes ONTAP dans AWS ou dans Azure.
- 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).
  - Les clusters ONTAP ou Cloud Volumes ONTAP avec la version 9.11.1 ou supérieure du système d'exploitation ONTAP sont pris en charge.



Les charges de travail SAN sont prises en charge uniquement dans ONTAP 9.17.1 et versions ultérieures.

- Si vos clusters ONTAP locaux ou Cloud Volumes ONTAP dans AWS ou dans le cloud Azure ne sont pas déjà intégrés dans la console, vous avez besoin d'un agent de console.

Se référer à "[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.

## Dans ONTAP 9.11.1 et versions ultérieures

- Une licence ONTAP One est activée sur l'instance ONTAP locale.
- Une licence pour NetApp Autonomous Ransomware Protection, utilisée par Ransomware Resilience, activée sur l'instance ONTAP locale, selon la version d' ONTAP que vous utilisez. Se référer à "[Présentation de la protection autonome contre les ransomwares](#)".



La version générale de Ransomware Resilience, contrairement à la version Preview, inclut une licence pour la technologie NetApp Autonomous Ransomware Protection. Se référer à "[Présentation de la protection autonome contre les ransomwares](#)" pour plus de détails.

Pour plus de détails sur les licences, reportez-vous à "[En savoir plus sur la résilience aux ransomwares](#)".

- Pour appliquer des configurations de protection (telles que l'activation de la protection autonome contre les ransomwares et autres), Ransomware Resilience a besoin d'autorisations 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 le cluster ONTAP est déjà intégré dans la console à l'aide d'informations d'identification d'utilisateur non administrateur, les autorisations d'utilisateur non administrateur doivent être mises à jour avec les autorisations nécessaires en se connectant au cluster ONTAP , décrites sur cette page.

## Pour les sauvegardes de données

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

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](#)".

## 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, procédez comme suit.

1. Connectez-vous à la console et recherchez le système dont les autorisations utilisateur ONTAP doivent être mises à jour.
2. Sélectionnez le système pour voir les 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 à l'aide de l'utilisateur administrateur.
5. Afficher les rôles existants pour cet utilisateur. Entrer:

```
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. Revenez à l'interface utilisateur de Ransomware Resilience pour l'utiliser.

## Démarrage rapide pour NetApp Ransomware Resilience

Voici un aperçu des étapes nécessaires pour démarrer avec NetApp Ransomware Resilience. Les liens à l'intérieur de chaque étape vous mènent à une page qui fournit plus de détails.

1

### Réviser les prérequis

["Assurez-vous que votre système répond à ces exigences"](#) .

2

### Configurer la résilience aux ransomwares

- ["Préparez NetApp StorageGRID, Amazon Web Services, Google Cloud Platform ou Microsoft Azure comme destination de sauvegarde"](#) .
- ["Configurer un agent de console"](#) .
- ["Configurer les licences"](#) .
- ["Découvrir les charges de travail dans la console"](#) .
- ["Configurer les destinations de sauvegarde"](#) .
- ["Activer éventuellement la détection des menaces"](#) .
- ["En option, effectuez un exercice de préparation aux attaques de ransomware"](#) .

3

### Quelle est la prochaine étape ?

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

- ["Afficher l'état de protection de la charge de travail sur le tableau de bord"](#) .
- ["Protéger les charges de travail"](#) .
- ["Répondre à la détection d'attaques potentielles de ransomware"](#) .
- ["Se remettre d'une attaque \(après neutralisation des incidents\)"](#) .

## Configurer la résilience NetApp Ransomware

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

- Configurer 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 console NetApp

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 résilience des ransomwares NetApp

Connectez-vous à NetApp Ransomware Resilience via la console NetApp .

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 d'accès BlueXP pour tous les services"](#) .

### 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"](#) .

# Ransomware Resilience

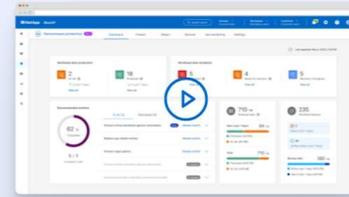
## Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get full access to ransomware resilience with a 30-day free trial.

Start 30-day free trial

We won't read the contents of your data or change existing protection.



### Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click



### Detect and respond

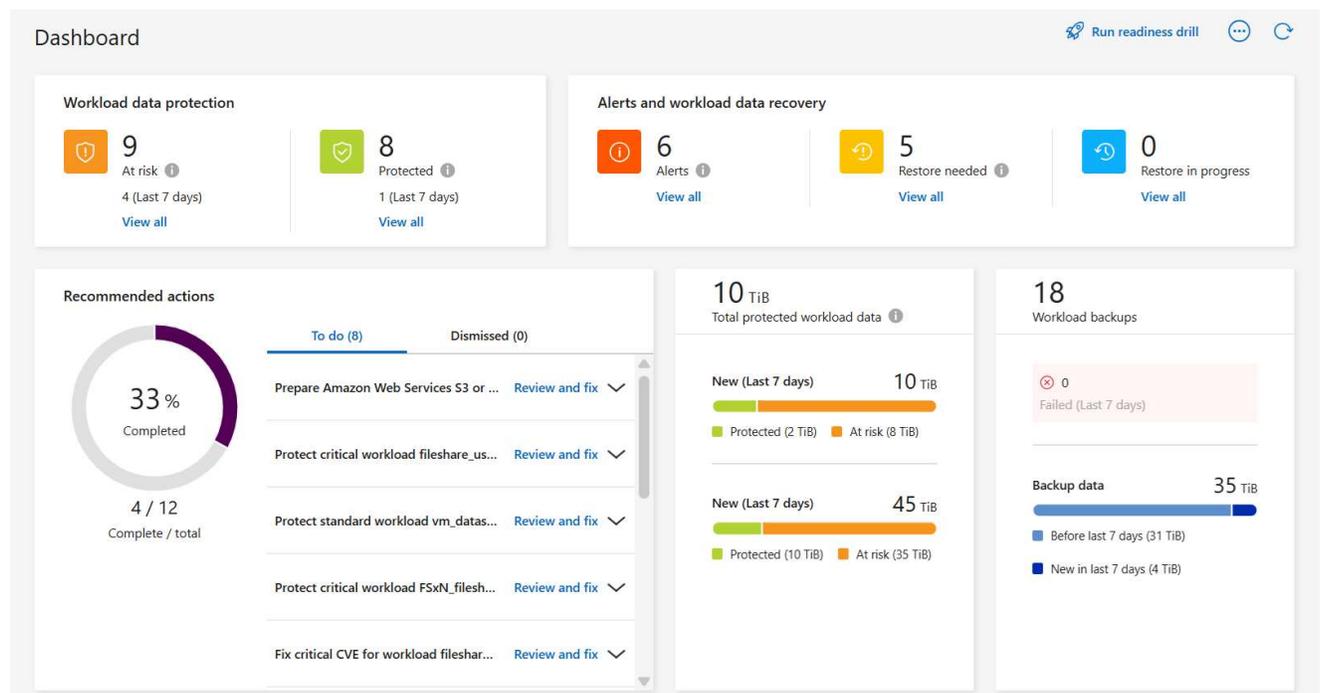
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point



### Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

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** Vous pouvez utiliser les types de licences suivants :

- Inscrivez-vous pour un 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), 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 console.

Après avoir configuré votre BYOL ou acheté un abonnement PAYGO, vous pouvez voir la licence dans la section Licences et abonnements de la console.

Une fois l'essai gratuit terminé ou la licence ou l'abonnement expiré, vous pouvez toujours effectuer les opérations suivantes dans Ransomware Resilience :

- Afficher les charges de travail et l'état de la charge de travail.
- Supprimez toute ressource, telle qu'une politique.
- Exécutez toutes les opérations planifiées qui ont été créées pendant la période d'essai ou sous la licence.

## Autres licences

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



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.

Vous pouvez visualiser le comportement anormal des utilisateurs avec Data Infrastructure Insights Workload Security. Cela nécessite une licence pour Data Infrastructure Insights Workload Security et que vous l'activez dans Ransomware Resilience. Pour un aperçu de la sécurité des charges de travail de Data Infrastructure Insights, consultez ["À propos de la sécurité de la charge de travail"](#)



Si vous ne disposez pas d'une licence pour Data Infrastructure Insights Workload Security et que vous ne l'activez pas dans Ransomware Resilience, vous ne verrez pas les informations sur le comportement anormal des utilisateurs.

## Essayez-le en utilisant un essai gratuit de 30 jours

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



Avec la sortie d'octobre 2024, les nouveaux déploiements de Ransomware Resilience bénéficient désormais de 30 jours d'essai gratuit. Auparavant, Ransomware Resilience proposait 90 jours d'essai gratuit. Si vous bénéficiez déjà de l'essai gratuit de 90 jours, cette offre se poursuit pendant 90 jours.

Aucune limite de capacité n'est appliquée pendant le procès.

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 console NetApp , sélectionnez **Protection > Résilience aux ransomwares**.

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

**Ransomware Resilience**  
Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

[Start 30-day free trial](#)

We won't read the contents of your data or change existing protection.

**Identify and protect**  
Automatically identifies workloads at risk, recommends fixes, and protects with one-click.

**Detect and respond**  
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point.

**Recover**  
Restores workloads in minutes through simplified, orchestrated workload-consistent recovery.

4. Si vous n'avez pas déjà ajouté de connecteur pour d'autres services, ajoutez-en un.

Pour ajouter un agent de console, reportez-vous à ["En savoir plus sur les agents de console"](#) .

5. Après avoir configuré un agent de console, dans la page de destination de Ransomware Resilience, le bouton permettant d'ajouter un agent de console se transforme en bouton permettant de découvrir les charges de travail. Sélectionnez **Commencer par découvrir les charges de travail**.
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.

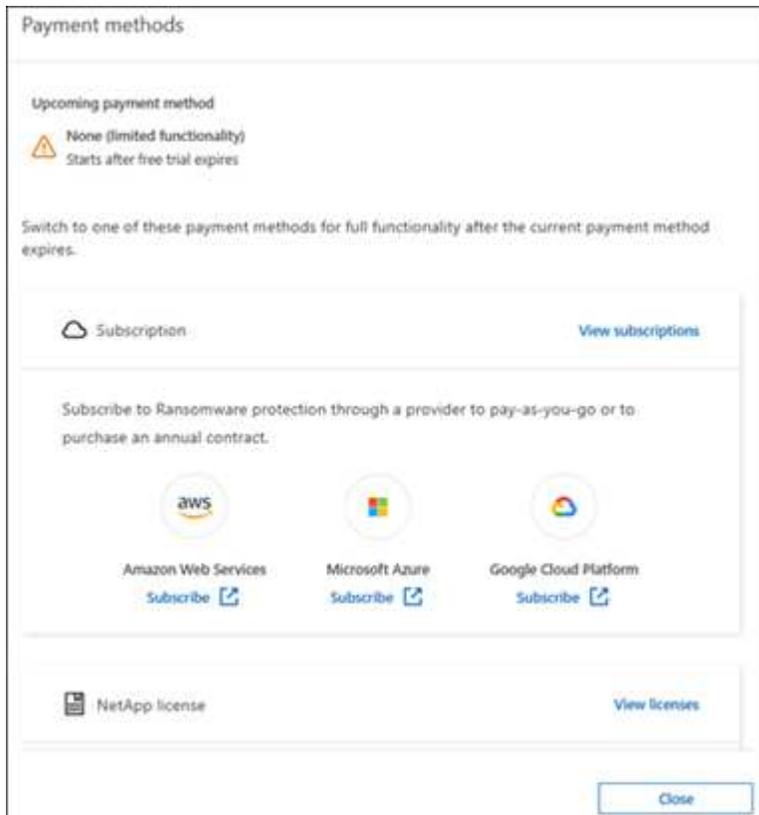
[Abonnez-vous via AWS Marketplace](#) [Abonnez-vous via Microsoft Azure Marketplace](#) [Abonnez-vous via Google Cloud Platform Marketplace](#) Apportez votre propre permis de conduire (BYOL)

## 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**.

## Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number   
  Upload License File

---

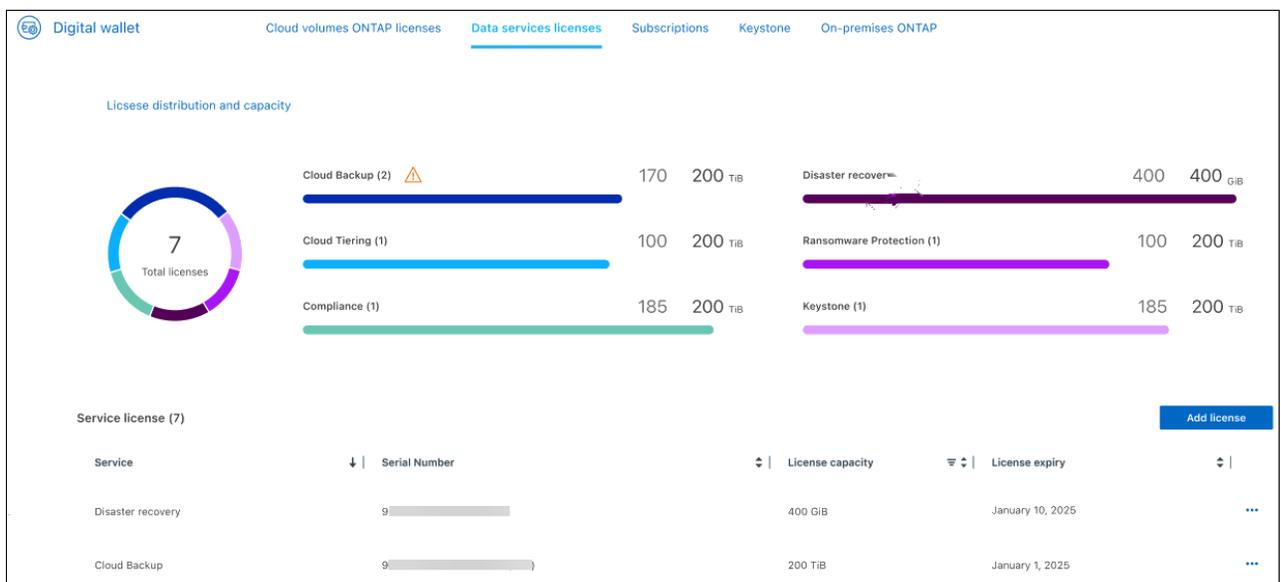
Serial Number

Enter Serial Number

**Notice:** You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

Add License
Cancel

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 et sélectionnez **Ajouter une licence**.
9. Pour afficher les détails de la licence, dans la navigation de gauche de la console, sélectionnez **Administration > Licences et abonnements**.
  - 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**.

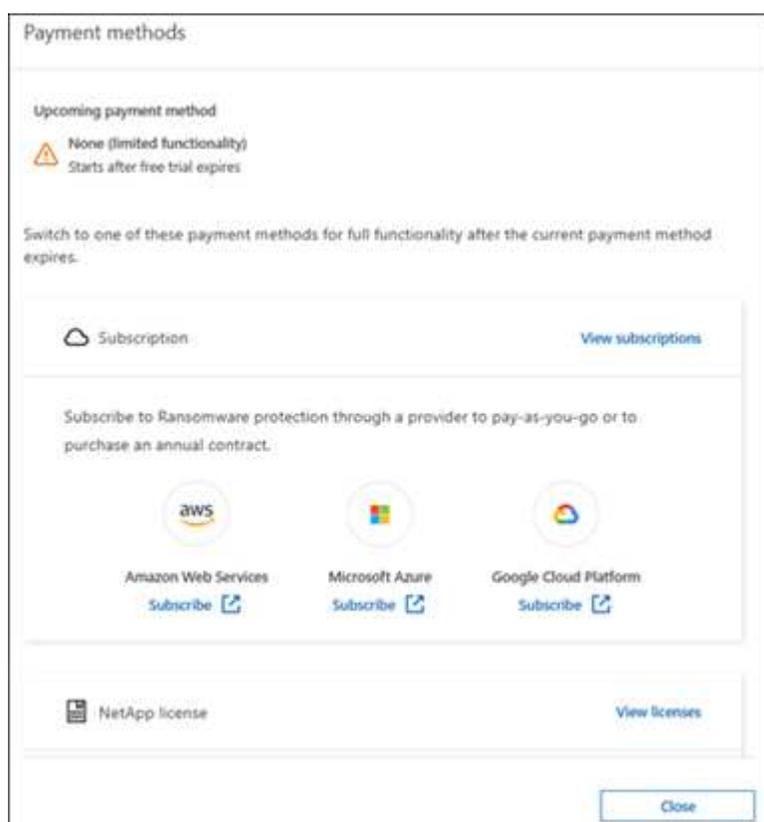
Un message apparaît indiquant qu'une licence a été ajoutée.

## Abonnez-vous via 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**.

## Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number   
  Upload License File

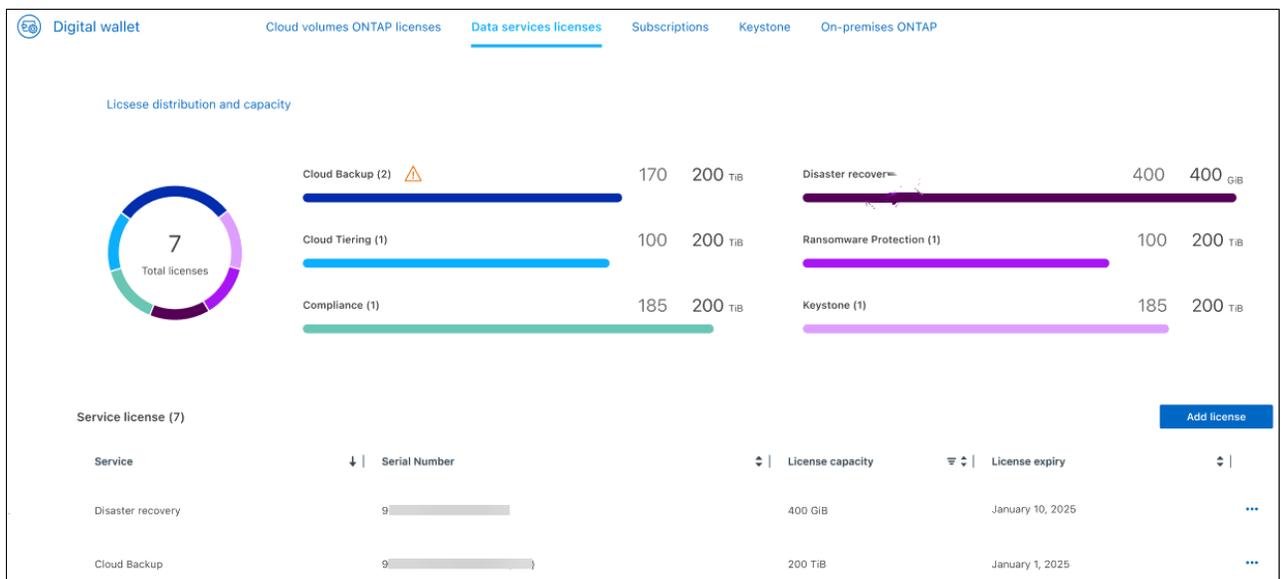
Serial Number

Enter Serial Number

**Notice:** You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

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 Licences et abonnements, dans la navigation de gauche de la console, sélectionnez **Gouvernance > Licences et abonnements**.
  - 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**.

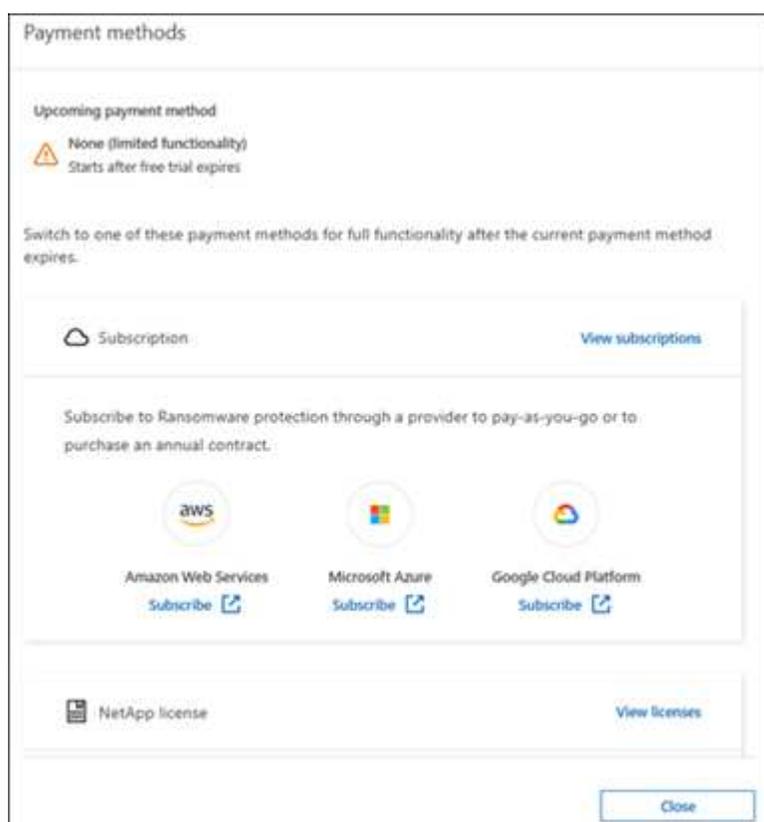
Un message apparaît indiquant qu'une licence a été ajoutée.

## 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 à **Ransomware Resilience**

Google Cloud

Product details



## NetApp Intelligent Services

[NetApp, Inc.](#)

Get best-in-class data protection and security for your workloads running on NetApp® ONTAP® storage.

[Subscribe](#)

[Overview](#) [Pricing](#) [Documentation](#) [Support](#) [Related Products](#)

### Overview

NetApp offers a comprehensive suite of intelligent services for your ONTAP systems. They proactively protect critical workloads against evolving cyberthreats, detect and respond to ransomware attacks in real time, eliminate backup windows, and orchestrate a quick recovery in minutes when disaster strikes. NetApp intelligent services and Cloud Volumes ONTAP® solution are fully integrated into the NetApp BlueXP™ control plane, providing centralized management of ONTAP storage and services.

This listing replaces the NetApp BlueXP listing.

Click the Subscribe button to use the following NetApp intelligent data services through your Google Cloud account.

**Ransomware Protection:** [🔗](#) Protect your most critical data by orchestrating a comprehensive ransomware defense for your ONTAP workloads. Prepare for an attack by intelligently identifying and protecting critical workload data with a single click. AI-powered anomaly detection uncovers and responds to potential attacks

### Additional details

Type: [SaaS & APIs](#)

Last product update: 5/12/25

Category: [Analytics](#), [DevOps](#), [Storage](#), [Security](#)

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**.

## Add License

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

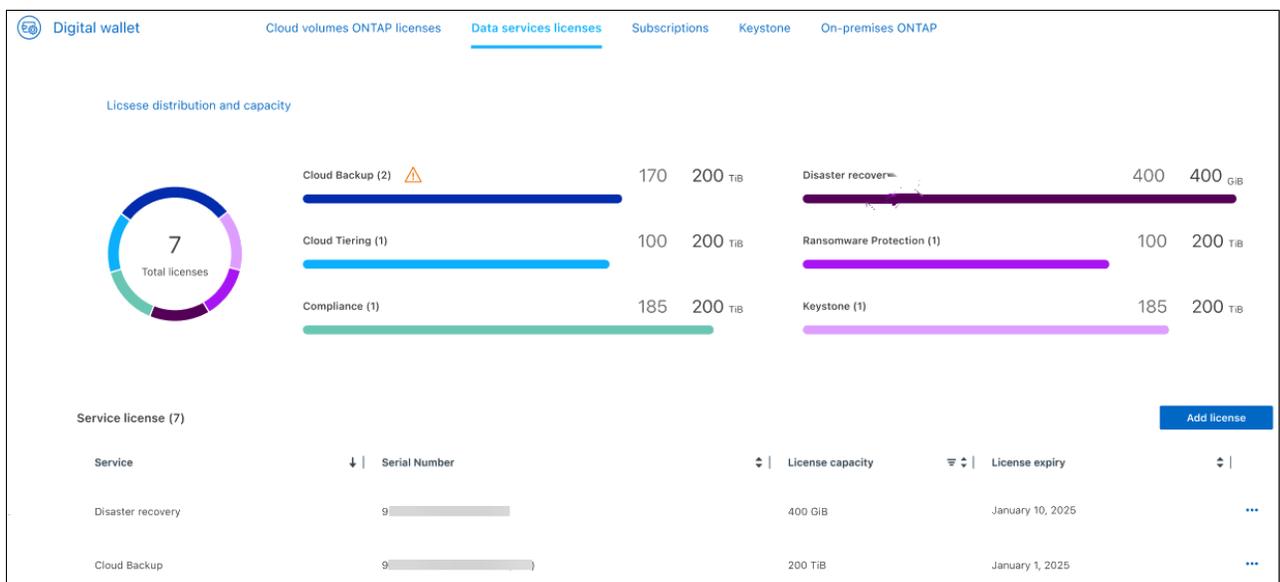
Enter Serial Number
  Upload License File

Serial Number

Enter Serial Number

**Notice:** You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

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 > Licences et abonnements**.
  - 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**.

**Add License**

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

Enter Serial Number     Upload License File

Serial Number

Enter Serial Number

**Notice:** You can't enter a serial number because you haven't added the NetApp Support Site account that's authorized to access the serial number. To add the account to BlueXP, click Help > Support > NSS Management. Otherwise, use the Upload License File option.

Add License    Cancel

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 Licences et abonnements 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 Licences et abonnements 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 > Licences et abonnements**.
  - 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**.

# Découvrez les charges de travail dans NetApp Ransomware Resilience

Avant de pouvoir utiliser NetApp Ransomware Resilience, il doit d'abord découvrir les données. 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.

**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 d'accès à la console pour tous les services"](#) .

**Que découvre Ransomware Resilience ?** Ransomware Resilience évalue les applications MySQL, les applications Oracle, les banques de données VMware, les partages de fichiers et le stockage en blocs.



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

Ransomware Resilience découvre et affiche les configurations système prises en charge et non prises en charge dans le tableau de bord.

Ransomware Resilience vérifie votre protection de sauvegarde actuelle, vos copies instantanées et vos options de protection autonome contre les ransomwares NetApp . Il recommande ensuite des moyens d'améliorer votre protection contre les ransomwares.

**Comment pouvez-vous découvrir les charges de travail ?** Vous pouvez faire ce qui suit :

- Dans chaque agent de console, sélectionnez les systèmes sur 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.
- Découvrez les charges de travail nouvellement créées pour les systèmes précédemment sélectionnés.
- Découvrez de nouveaux systèmes.

## 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 console NetApp , sélectionnez **Protection > Protection contre les ransomwares**.

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

# Ransomware Resilience

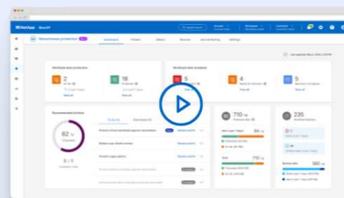
## Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

Start 30-day free trial

 We won't read the contents of your data or change existing protection.



### Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click



### Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point



### Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery



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.

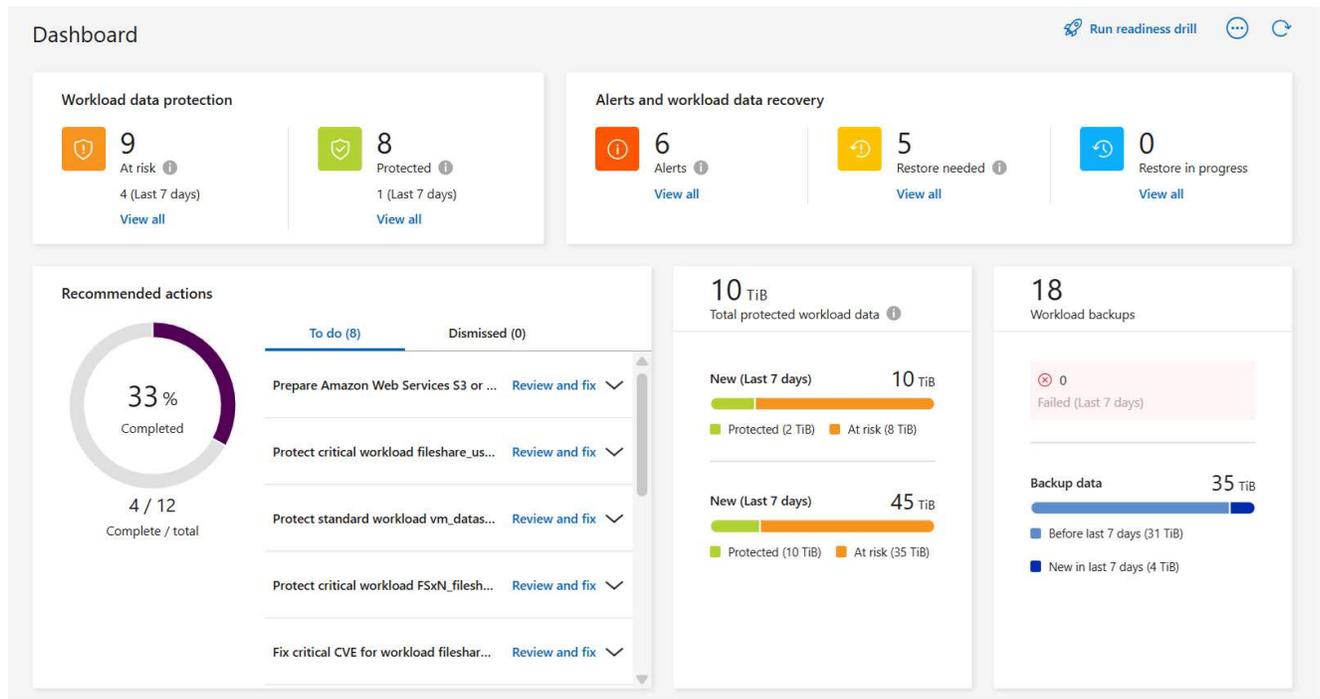
[Capture d'écran de la découverte des charges de travail]

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 découvre les données de charge de travail uniquement pour les agents de console avec les systèmes sélectionnés. Ce processus peut prendre quelques 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 déjà sélectionné des systèmes à découvrir, vous pouvez découvrir les charges de travail nouvellement créées pour ces environnements à partir du tableau de bord.

### Étapes

1. Pour identifier la date de la dernière découverte, regardez l'horodatage 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 rechercher de nouvelles charges de travail.

## 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 la verticale  ... option 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**.



Ce processus peut prendre quelques minutes et une icône de chargement indique la progression.

3. Ransomware Resilience détecte les systèmes pris en charge et non pris en charge. Ransomware Resilience 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**.

## 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.

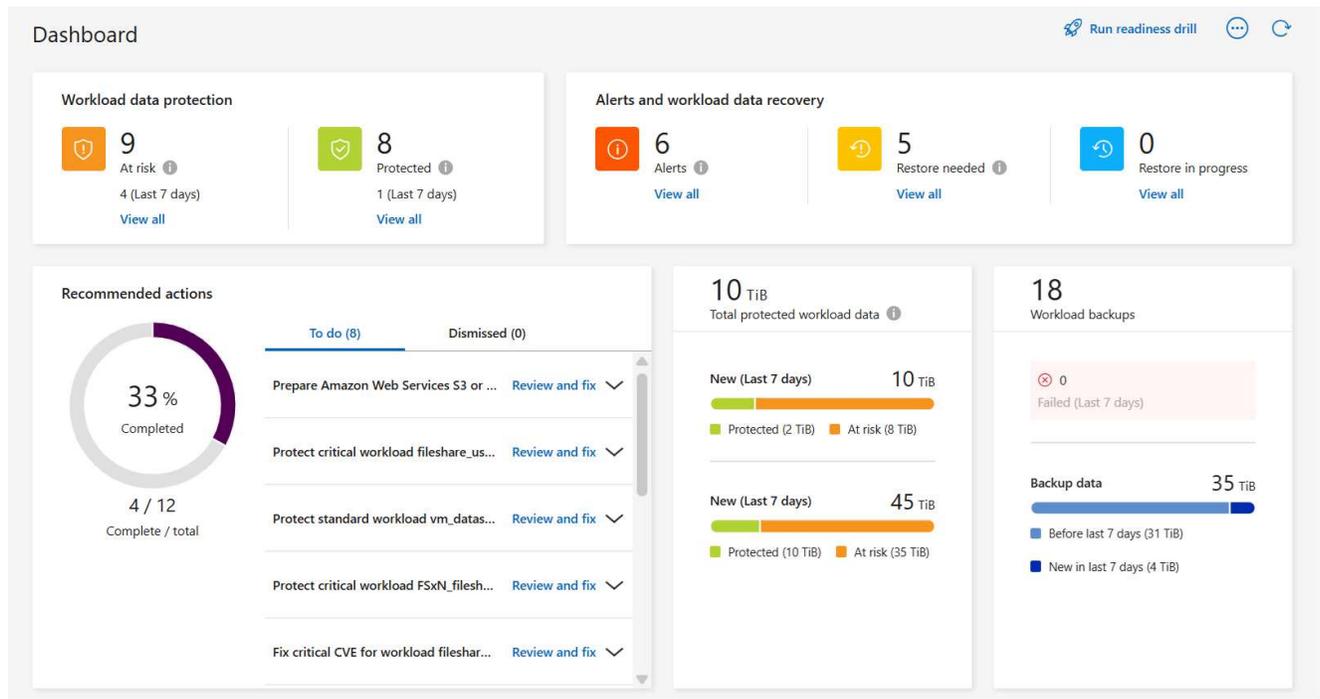
Vous devez saisir un nom d'utilisateur et un mot de passe dans les situations suivantes :

- 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 d'accès à la console pour tous les services](#)".

### 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.

## Readiness drill

Run a simulated ransomware attack on a new test workload that will be saved in the selected system. Then, investigate the simulated attack and recover the test workload. You can run a readiness drill multiple times.

 Your real workload data will not be impacted.

Select a readiness drill test environment where the new test workload will be created.

Console agent

System

Storage VM

New test workload

 Requires 10 GiB of storage

Save

Cancel

3. Procédez comme suit :

- Sélectionnez l'agent de console que vous souhaitez utiliser pour l'exercice de préparation.
- Sélectionnez un système de test.
- Sélectionnez un SVM de stockage de test.
- 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.
- 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 d'accès à la console pour tous les services](#)".

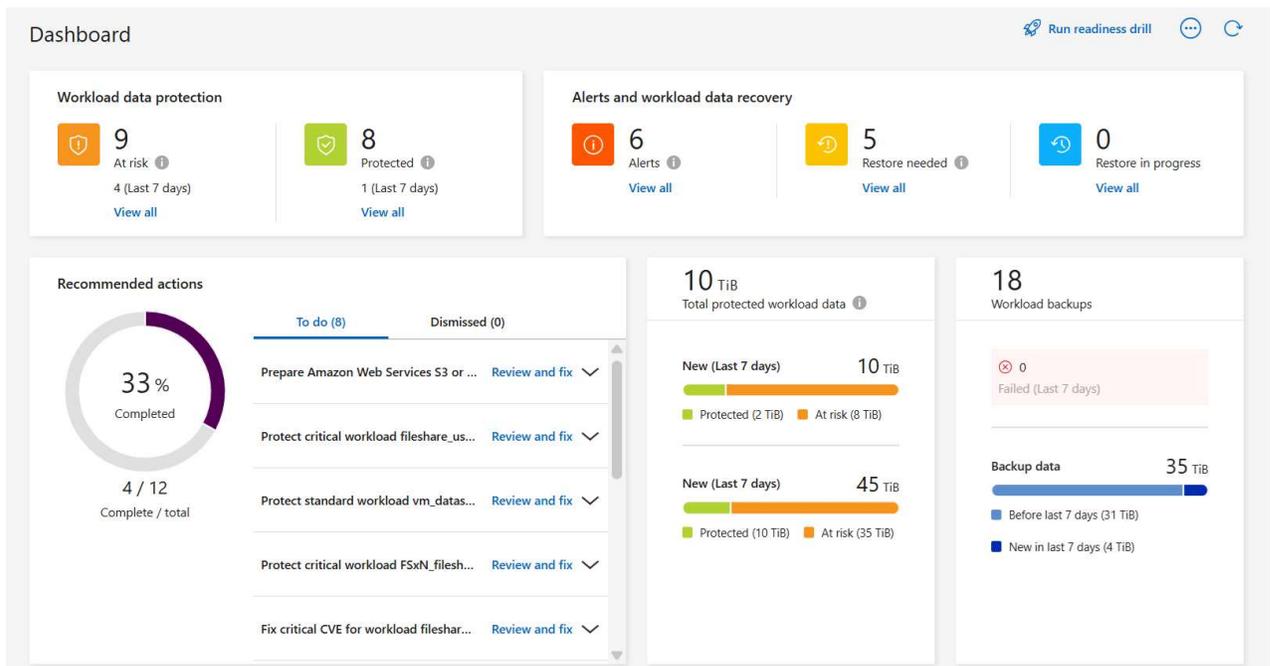
Lorsque vous démarrez l'exercice de préparation, Ransomware Resilience ignore le mode d'apprentissage et démarre l'exercice en mode actif. L'état de détection de la charge de travail est Actif.



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**.

2. Si vous avez déjà configuré l'exercice de préparation, après avoir sélectionné **Démarrer**, l'exercice de préparation commence.



Une fois l'exercice démarré, vous ne pouvez pas modifier la configuration de l'exercice de préparation. Vous pouvez le réinitialiser pour recommencer.

## 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 d'accès à la console pour tous les services".

## 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.

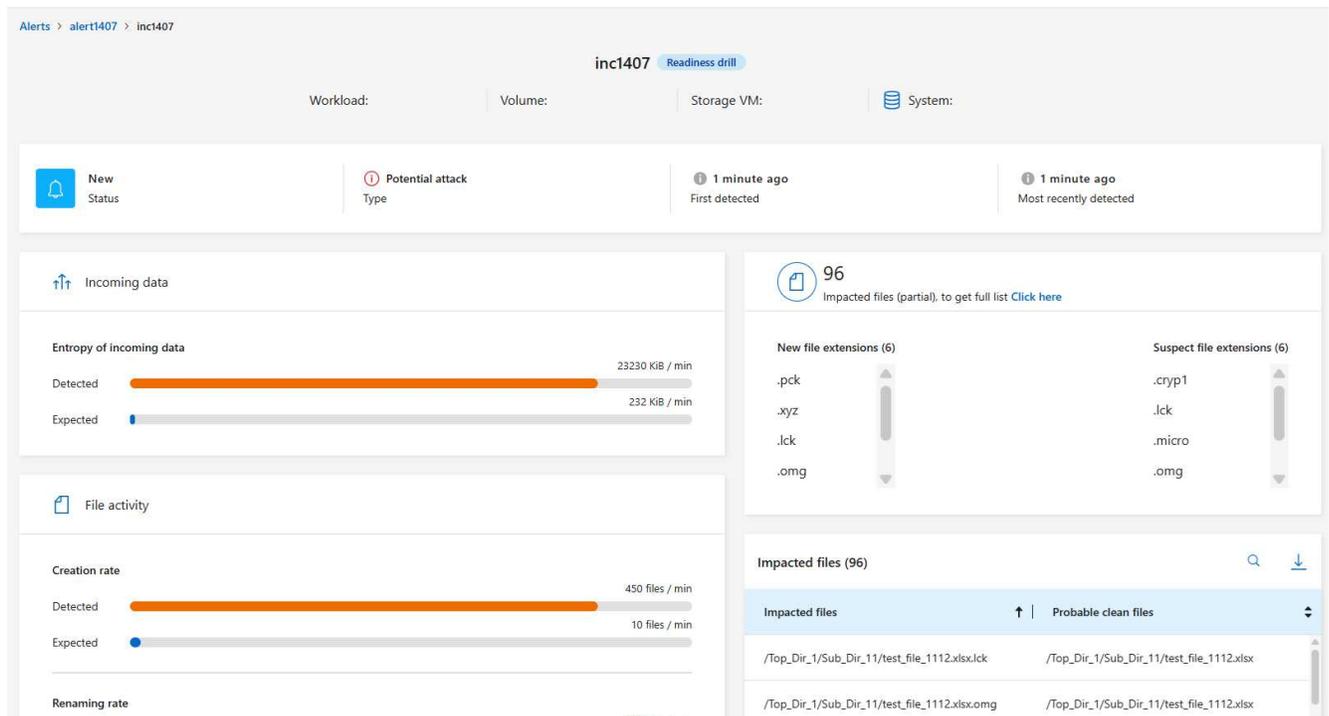
Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
alert8727	Oracle_8821	10.0.1.193	Oracle	New	aws-connector-us-east-1	2	2 GiB	23 days ago
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	New	aws-connector-us-east-1	1	2 GiB	23 days ago
alert3932	MySQL_9294	10.0.1.10	MySQL	New	aws-connector-us-east-1	2	2 GiB	23 days ago
alert7918	vm_datastore_202_735...	10.195.52.126	VM datastore	New	onprem-connector	1	2 GiB	23 days ago
alert5319	vm_datastore_uswest_...	10.0.1.215	VM file share	New	aws-connector-us-west-1-account-LXtff4X...	1	2 GiB	23 days ago
alert1407 <b>Readiness drill</b>	rps_test_gri	rps_test_readiness_drill_svm	File share	New	aws-connector-us-east-1	1	2 GiB	1 minute ago

Workload rps\_test\_readiness-drill-workload-test, marked restore needed. [Restore workload](#)

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

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data	First detected	Most rec
alert1407 <b>Readiness drill</b>	rps_test_awsSystemTest	svm_rps_test_readi...	File share	Active	aws-connector-us-east-1	1	2 GiB	Just now	Just now

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



Voici quelques éléments à rechercher :

- Regardez le type d'attaque potentiel.

Si le type indique qu'un utilisateur est suspecté d'activité malveillante, vérifiez le nom d'utilisateur. Vous souhaitez peut-être examiner plus en détail l'utilisateur dans la sécurité de la charge de travail de Data Infrastructure Insights en sélectionnant **Enquêter dans la sécurité de la charge de travail**.

- 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 d'accès à la console pour tous les services](#)".

### 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.

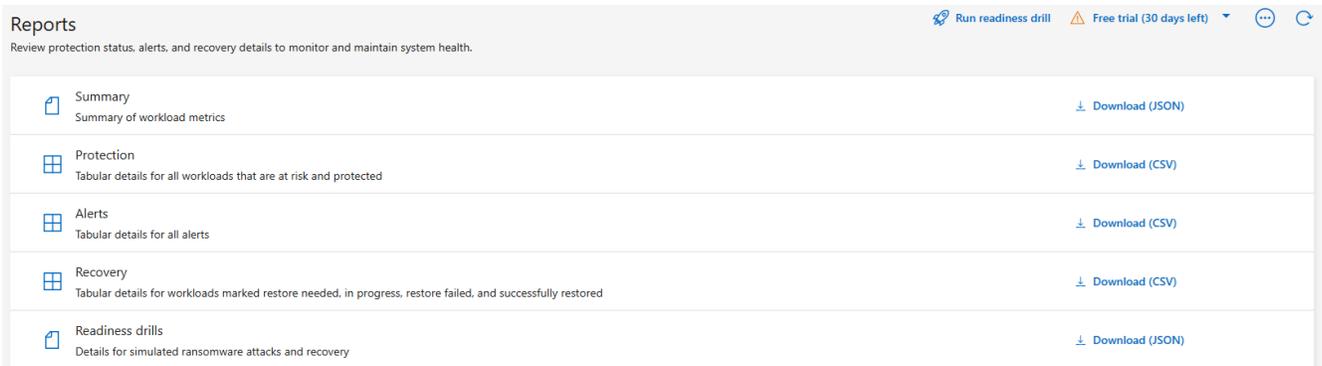
## Rapports d'examen sur l'exercice de préparation

Une fois l'exercice de préparation terminé, vous souhaitez 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 d'accès BlueXP pour tous les services"](#) .

### 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

Vous pouvez configurer des destinations de sauvegarde, envoyer des données à un système externe de gestion de la sécurité et des événements (SIEM), effectuer un exercice de préparation aux attaques, configurer la découverte de charges de travail ou configurer la connexion à la sécurité de la charge de travail Data Infrastructure Insights en accédant à l'option **Paramètres**.

**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 d'accès à la console pour tous les services"](#) .

**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 la connexion à la sécurité de la charge de travail Data Infrastructure Insights pour voir les informations sur les utilisateurs suspects dans les alertes de ransomware.
- Ajouter une destination de sauvegarde.

- Connectez votre système de gestion de la sécurité et des événements (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.

## 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.

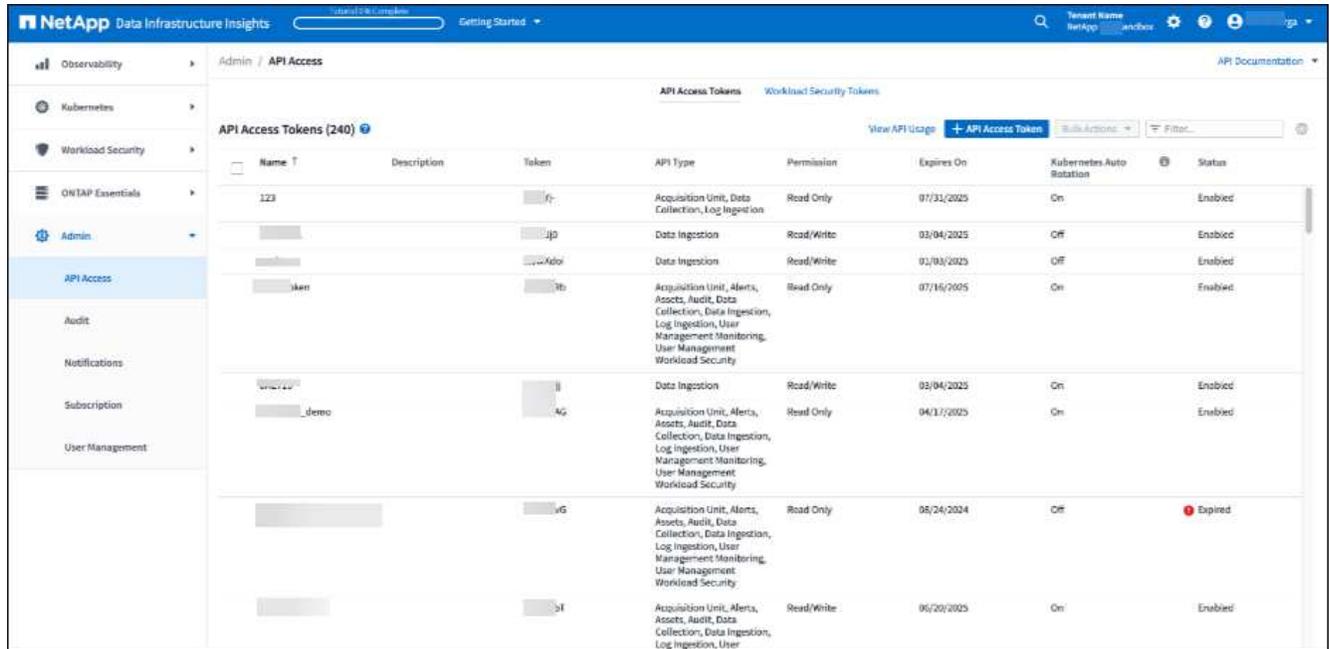
## Identifiez les comportements utilisateur suspectés d'anomalie en vous connectant à Data Infrastructure Insights Sécurité de la charge de travail

Avant de pouvoir afficher les détails du comportement utilisateur suspecté d'anomalie dans Ransomware Resilience, vous devez configurer la connexion au système de sécurité Data Infrastructure Insights Workload.

## Obtenir un jeton d'accès API auprès du système de sécurité Data Infrastructure Insights Workload

Obtenez un jeton d'accès API auprès du système de sécurité Data Infrastructure Insights Workload.

1. Connectez-vous au système de sécurité de la charge de travail Data Infrastructure Insights .
2. Dans la navigation de gauche, sélectionnez **Admin > Accès API**.



Name	Description	Token	API Type	Permission	Expires On	Kubernetes Auto Rotation	Status
123		[redacted]	Acquisition Unit, Data Collection, Log Ingestion	Read Only	07/31/2025	On	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	03/04/2025	Off	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	01/03/2025	Off	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management, Workload Security	Read Only	07/16/2025	On	Enabled
[redacted]		[redacted]	Data Ingestion	Read/Write	03/04/2025	On	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management, Workload Security	Read Only	04/17/2025	On	Enabled
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management, Workload Security	Read Only	05/24/2024	Off	Expired
[redacted]		[redacted]	Acquisition Unit, Alerts, Assets, Audit, Data Collection, Data Ingestion, Log Ingestion, User Management Monitoring, User Management, Workload Security	Read/Write	05/20/2025	On	Enabled

3. Créez un jeton d'accès API ou utilisez-en un existant.
4. Copiez le jeton d'accès API.

## Se connecter à Data Infrastructure Insights Sécurité de la charge de travail

1. Dans le menu Paramètres de résilience aux ransomwares, recherchez la vignette **Connexion de sécurité de la charge de travail**.
2. Sélectionnez **Connecter**.
3. Saisissez l'URL de l'interface utilisateur de sécurité de la charge de travail de l'infrastructure de données.
4. Saisissez le jeton d'accès API qui donne accès à la sécurité de la charge de travail.
5. Sélectionnez **Connecter**.

## 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. Effectuez des opérations de sauvegarde à l'aide du service de sauvegarde FSx for ONTAP .

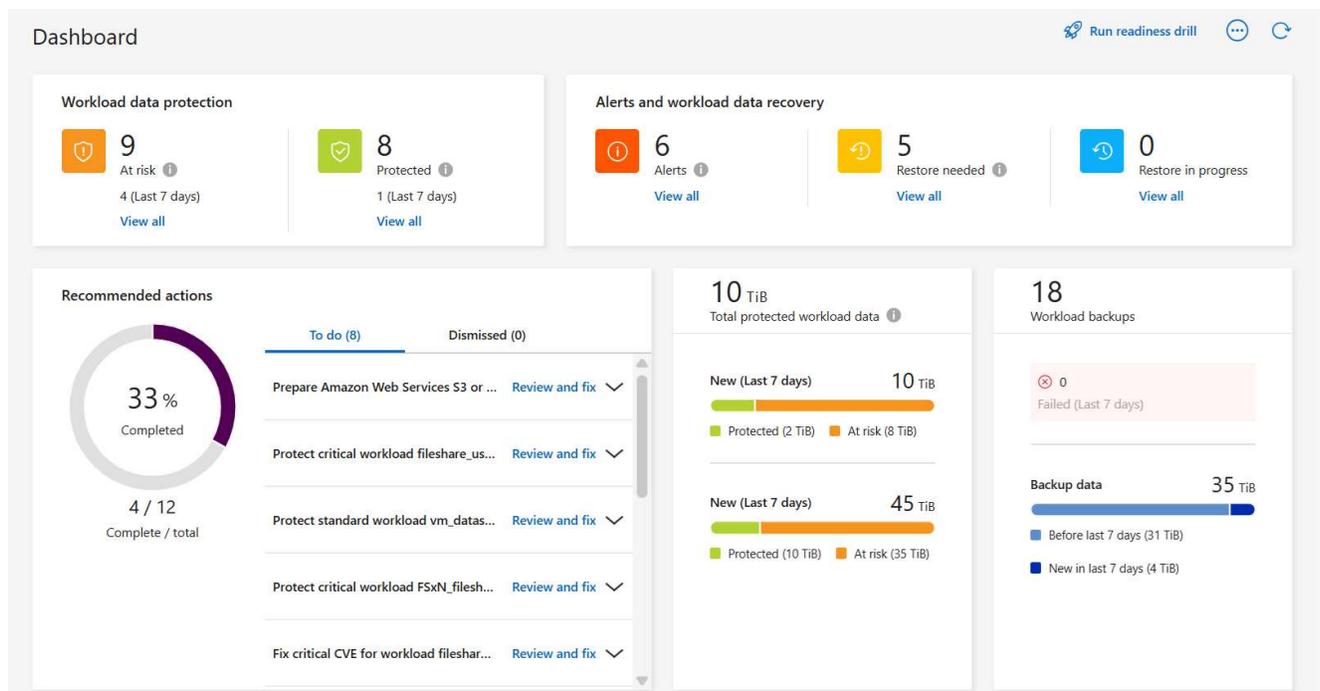
Vous pouvez ajouter une destination de sauvegarde en fonction d'une action recommandée à partir du tableau de bord ou en accédant à l'option Paramètres du menu.

## 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.



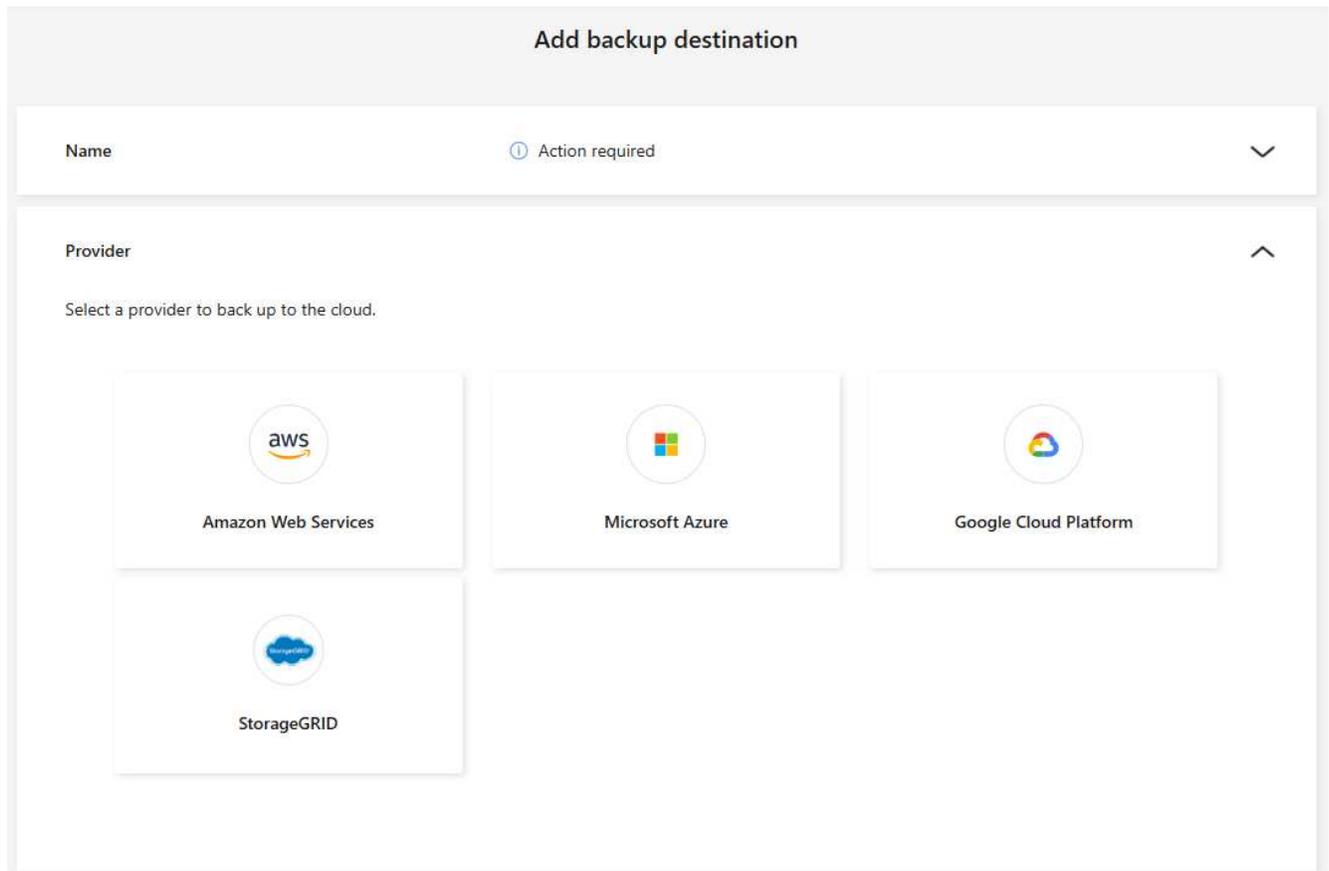
2. Depuis le tableau de bord, sélectionnez **Vérifier et corriger** pour la recommandation « Préparer <fournisseur de sauvegarde> comme destination de sauvegarde ».
3. Continuez avec les instructions en fonction du fournisseur de sauvegarde.

## 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.

Settings > Backup destinations

Backup destinations

Backup destinations (5) 🔍 ⬇️ ➕

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsahzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHhK7Dpp	NetApp Backup and Recovery

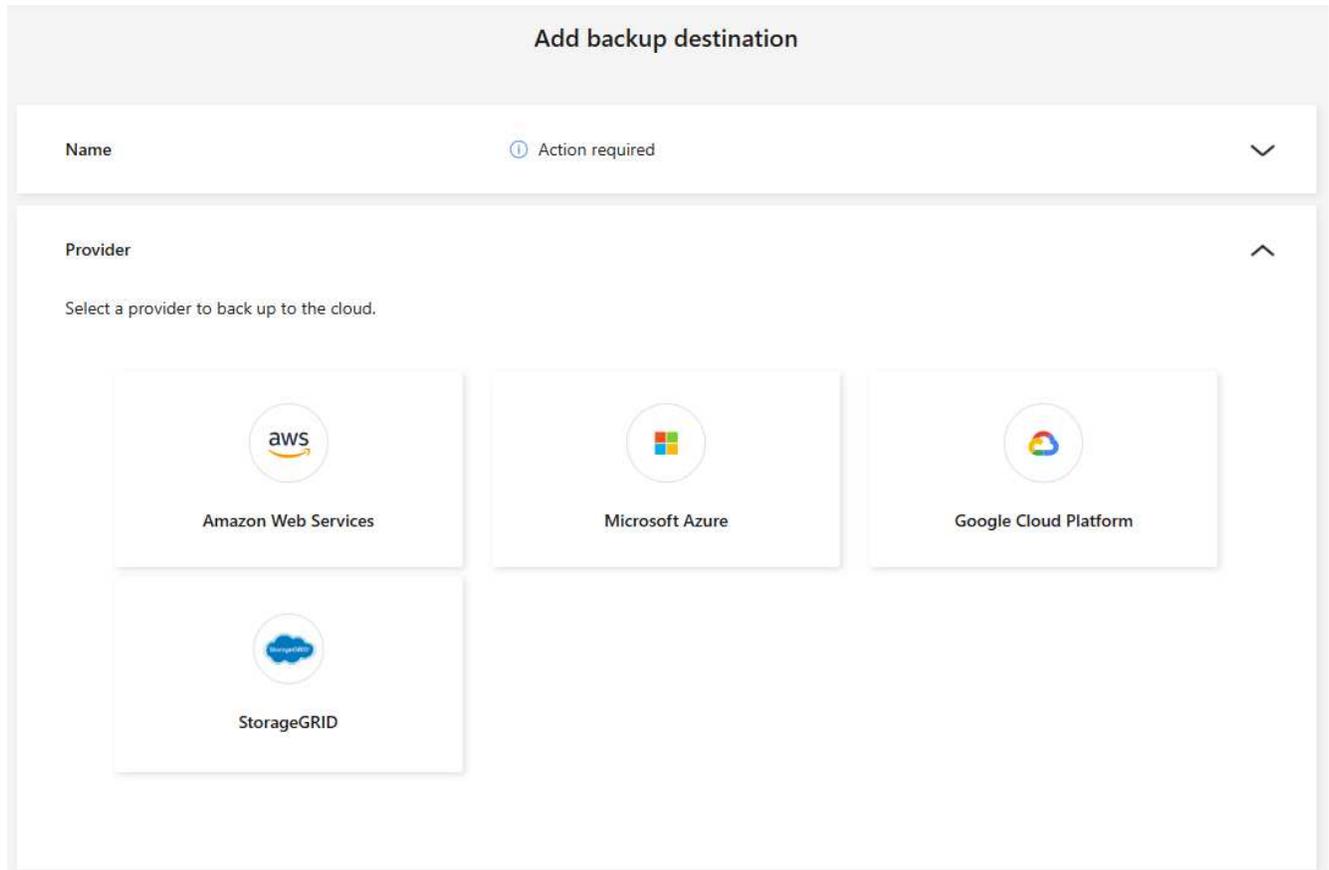
## Ajouter Amazon Web Services comme destination de sauvegarde

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
  - **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.

"Si vous souhaitez apporter votre propre seu, reportez-vous à [Ajouter des seaux S3](#)".

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.

Settings > Backup destinations

Backup destinations

Backup destinations (5)

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsahzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VhtzK7Dpp	NetApp Backup and Recovery

### 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.

Name	aws-backup	▼
Provider	Select a provider to back up to the cloud.	
	 Amazon Web Services	 Microsoft Azure
	 StorageGRID	 Google Cloud Platform
Provider settings	ⓘ Action required	▼
Encryption	✔ AWS managed key   Name: AWS SSE-S3	▼
Networking	✔ IPspace: default	▼
Backup lock	✔ None	▼

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.

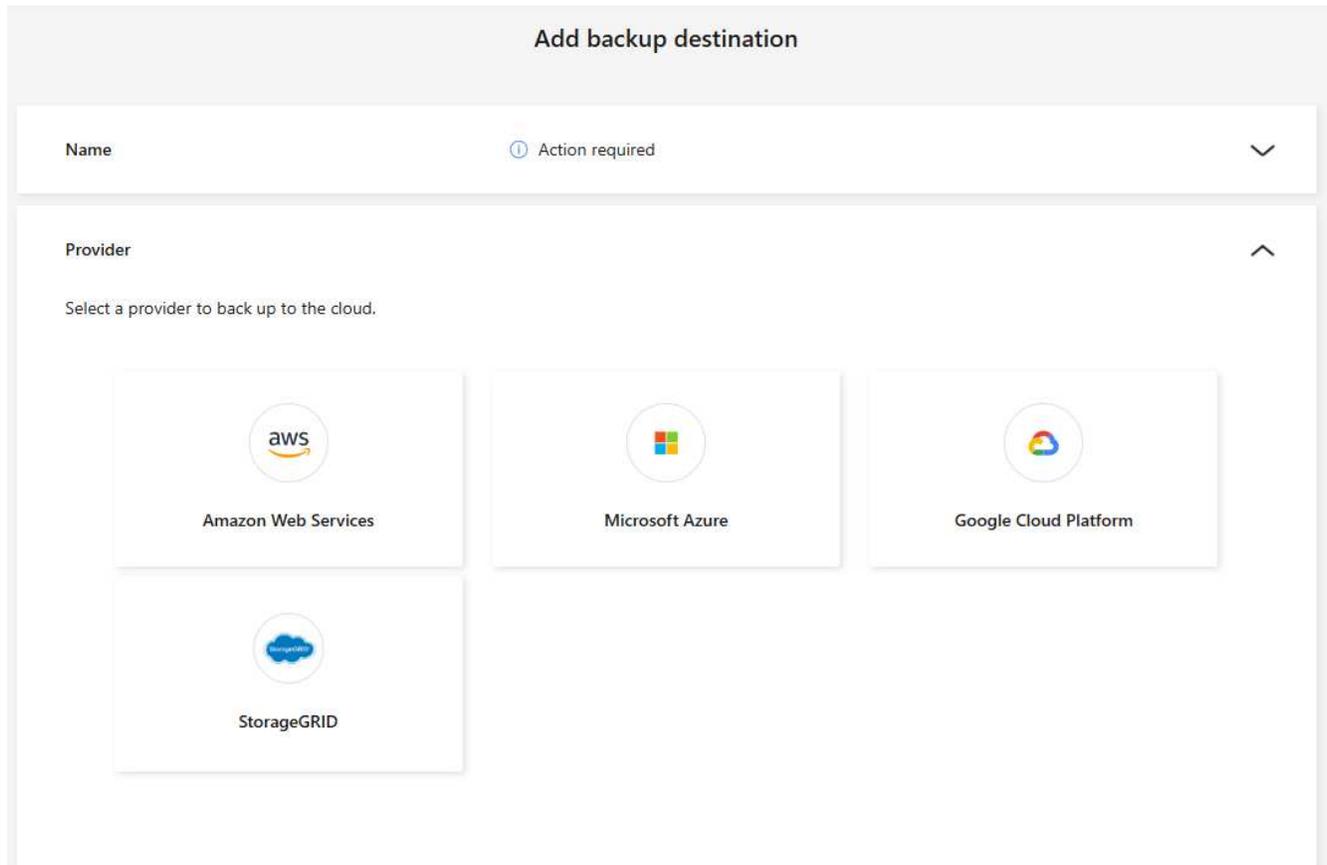
## Ajouter Microsoft Azure comme destination de sauvegarde

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.



The screenshot shows a dialog box titled "Add backup destination". At the top, there is a "Name" field with a dropdown arrow and a status indicator "Action required". Below this, there is a "Provider" section with a dropdown arrow and the text "Select a provider to back up to the cloud." Underneath, there are four provider cards: "Amazon Web Services" (AWS logo), "Microsoft Azure" (Azure logo), "Google Cloud Platform" (GCP logo), and "StorageGRID" (StorageGRID logo).

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.

Name	Provider	Region	Encryption	IP space	Backup lock	Systems	Created by
netapp-backup-vsac2gmsusu	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsusu	NetApp Backup and Recovery
netapp-backup-vsajgd1	AWS	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd2	AWS	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsajgd3	AWS	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoOS0z	NetApp Ransomware Resilience
netapp-backup-vsavhzk7dpp	AWS	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHzk7Dp	NetApp Backup and Recovery

## Connectez-vous à un système de gestion de la sécurité et des événements (SIEM) pour l'analyse et la détection des menaces

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. Vous pouvez sélectionner AWS Security Hub, Microsoft Sentinel ou Splunk Cloud comme SIEM.

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

### À propos des données d'événement 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 Ransomware Resilience, vous devez effectuer les étapes de haut niveau 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 Ransomware Resilience, vous devez effectuer les étapes de haut niveau 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 votre secret d'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.

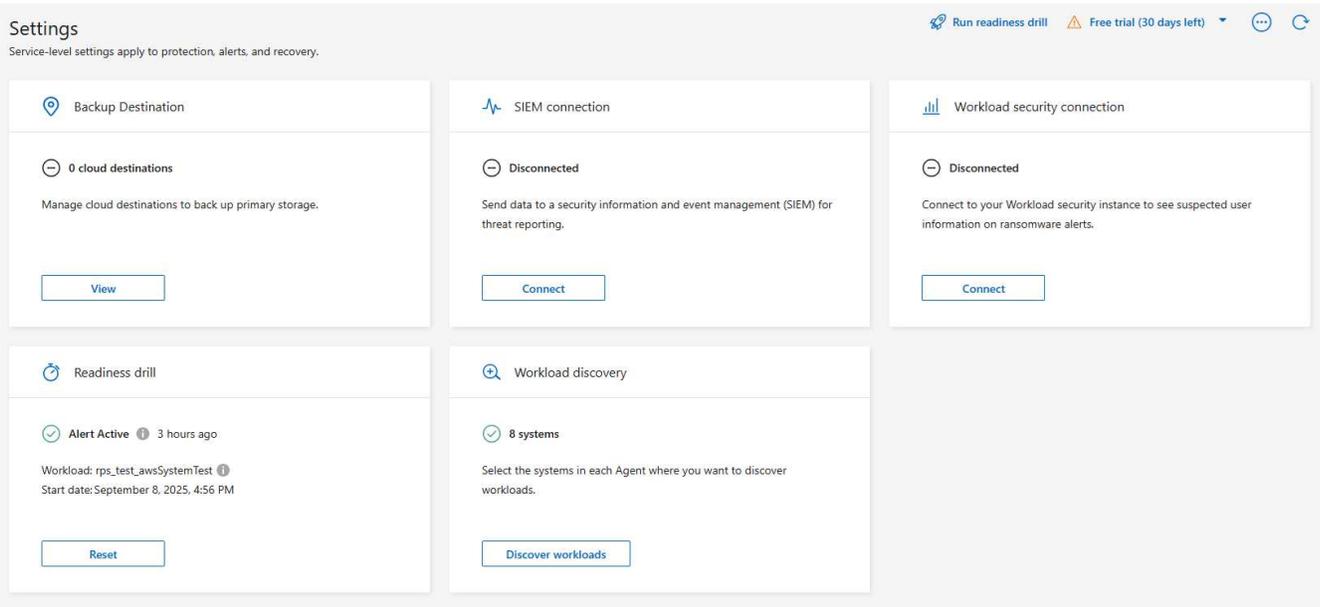
### Connecter SIEM dans Ransomware Resilience

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

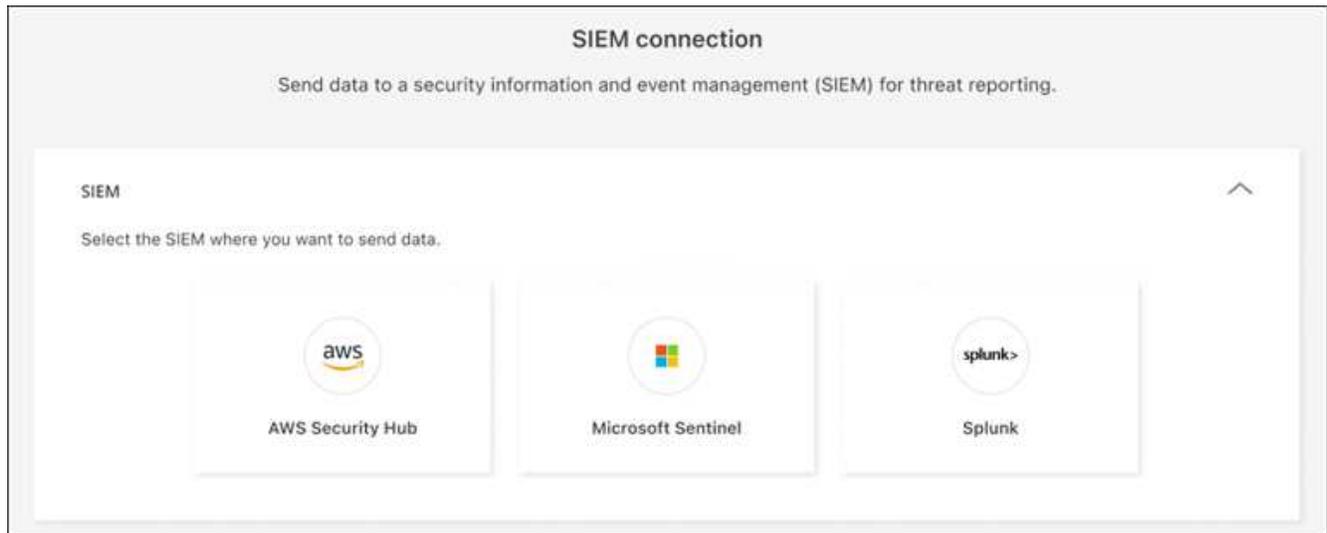
#### Étapes

1. Dans le menu de la console, sélectionnez **Protection > Résilience aux ransomwares**.
2.
  1. 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 ».

# Utiliser la résilience aux ransomwares

## Utiliser la résilience aux ransomwares NetApp

Avec NetApp Ransomware Resilience, vous pouvez afficher l'état de la charge de travail et protéger les charges de travail.

- ["Découvrez les charges de travail dans Ransomware Resilience"](#) .
- ["Afficher la protection et l'état de la charge de travail à partir du tableau de bord"](#) .
  - Examinez et appliquez les recommandations de protection contre les ransomwares.
- ["Protéger les charges de travail"](#):
  - Attribuez une stratégie de protection contre les ransomwares aux charges de travail.
  - Augmentez la protection des applications pour prévenir de futures attaques de ransomware.
  - Créer, modifier ou supprimer une stratégie de protection.
- ["Répondre à la détection d'attaques potentielles de ransomware"](#) .
- ["Se remettre d'une attaque"](#)(après que les incidents soient neutralisés).
- ["Configurer les paramètres de protection"](#) .

## Surveiller l'état de la charge de travail à l'aide du tableau de bord de résilience NetApp Ransomware

Le tableau de bord de résilience NetApp Ransomware 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.

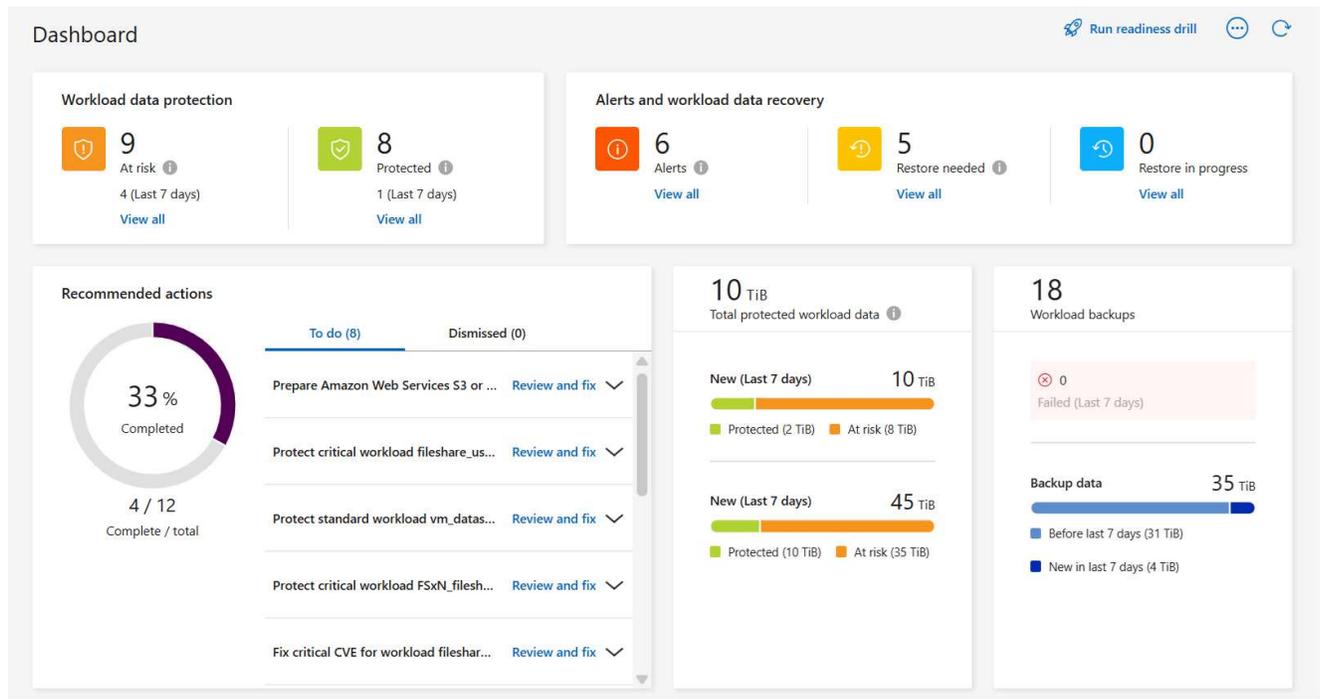
Utilisez le tableau de bord pour examiner les suggestions de protection, modifier les paramètres, télécharger des rapports et afficher la documentation.

**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 d'accès BlueXP pour tous les services"](#) .

## 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. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
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. " <a href="#">Configurer les paramètres de protection</a> ".
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. " <a href="#">Protégez la charge de travail contre les attaques de ransomware</a> ".
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 " <a href="#">Documentation du Digital Advisor</a> ".

Recommandation	Description	Comment résoudre
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 suspects, activez la détection sur le stockage secondaire et bien plus encore. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
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. " <a href="#">Configurer les paramètres de protection</a> ".
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. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
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. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
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. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
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. " <a href="#">Protégez les charges de travail contre les attaques de ransomware</a> ".
Consultez les nouvelles alertes.	De nouvelles alertes existent.	Consultez les nouvelles alertes. " <a href="#">Répondre à une alerte de ransomware détectée</a> ".

## 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\*  option en haut à droite pour rafraîchir les données qui apparaîtront dans les fichiers.
2. Effectuez l'une des opérations suivantes :
  - Depuis 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](https://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 d'accès à la console pour tous les services](#)".

### Comprendre les stratégies de protection contre les ransomwares

Les stratégies de protection contre les ransomwares englobent à la fois des politiques de *détection* et de *protection*.

- **Les politiques de détection** détectent les menaces de ransomware et bloquent éventuellement les extensions de fichiers suspects.
- **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.



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 :

- Sauvegarde et récupération NetApp pour les partages de fichiers, les partages de fichiers de machines virtuelles
- SnapCenter pour VMware pour les banques de données VM
- SnapCenter pour Oracle et MySQL

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. Effectuez des opérations de sauvegarde à l'aide du service de sauvegarde FSx for ONTAP . Vous définissez des politiques de sauvegarde pour les charges de travail dans FSx pour ONTAP dans AWS, pas dans Ransomware Resilience. Les politiques 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 la 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**.

Protection status



**9**  
At risk ⓘ

9 in last 7 days  
35 TiB data at risk



**9**  
Protected ⓘ

1 in last 7 days  
10 TiB data at risk

**Workloads**      Protection groups

Workloads (19) Manage protection strategies

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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.

**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.

- 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** : Copies instantanées prises plus d'une fois par heure (programme de protection très agressif)
- **Important** : Copies instantanées prises moins d'une fois par heure mais plus d'une fois par jour
- **Standard** : Copies instantanées prises plus d'une 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 :

Niveau politique	Instantané	Fréquence	Rétention (jours)	nombre de copies instantanées	Nombre total maximal de copies d'instantanés
<b>Politique de charge de travail critique</b>	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

Niveau politique	Instantané	Fréquence	Rétention (jours)	nombre de copies instantanées	Nombre total maximal de copies d'instantanés
<b>Politique importante relative à la charge de travail</b>	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
<b>Politique de charge de travail standard</b>	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

### 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 console NetApp
  - Enregistrez le SnapCenter Plug-in for VMware vSphere (SCV) avec la console NetApp

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 :

- **Créer 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

- **Créer 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

## Étapes pour créer une stratégie de protection contre les ransomwares

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

The screenshot shows a dashboard titled "Protection status". It features two summary cards: "At risk" with a value of 9 and "Protected" with a value of 9. Below these are two tabs: "Workloads" (selected) and "Protection groups". The "Workloads" tab displays a table with 19 items, showing details for six workloads.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. Depuis la page Protection, sélectionnez une charge de travail, puis **Protéger**.

The screenshot shows a table titled "Ransomware Resilience strategies (4) | Selected rows (1)". The table lists four strategies with their respective detection, snapshot, backup policies, and the number of protected workloads.

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input checked="" type="radio"/> rps-standard-plan <b>Recommended</b>	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0
<input type="radio"/> rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0

3. Depuis la page Stratégies de protection contre les ransomwares, sélectionnez **Ajouter**.

**Add Ransomware Resilience strategy**

Ransomware Resilience strategy name <input style="width: 95%; border: none; border-bottom: 1px solid #ccc;" type="text"/>	Copy from existing Ransomware Resilience strategy <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center; justify-content: space-between;"> <span>No policy selected</span> <span style="font-size: 0.8em;">Select</span> </div>
--	---

Detection	1 / 3 enabled	▼
Snapshot policy	Action required	▼
Backup policy	None	▼

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 principale** : activez la détection de ransomware pour que Ransomware Resilience détecte 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 cette option pour que Ransomware Resilience bloque 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 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, voir [Protégez-vous grâce à la résilience contre les ransomwares](#).

#### **Étapes**

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

Protection status

9 At risk 9 in last 7 days 35 TiB data at risk

9 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (19) Manage protection strategies

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

- Depuis la page Protection, sélectionnez une charge de travail, puis sélectionnez **Protéger**.
- Ransomware Resilience détecte s'il existe des politiques SnapCenter ou de sauvegarde et de récupération actives.
- 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.
- Pour voir les détails des politiques SnapCenter , sélectionnez la **flèche vers le bas**.

Sélectionnez une politique de détection puis sélectionnez **Protéger**.

- 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

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

Protection status



**9**  
At risk ⓘ

9 in last 7 days  
35 TiB data at risk



**9**  
Protected ⓘ

1 in last 7 days  
10 TiB data at risk

[Workloads](#)    Protection groups

Workloads (19) 🔍 ⬇️ [Manage protection strategies](#)

Workload	↑	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01		At risk	None	File share	N/A	N/A	N/A	<a href="#">Protect</a>
LUN_storage_01		Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	<a href="#">Edit protection</a>
MySQL_4781		Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	<a href="#">Edit protection</a>
MySQL_8009		At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	<a href="#">Protect</a>
MySQL_9294		Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	<a href="#">Edit protection</a>
Oracle_2115		At risk	SnapCenter	Oracle	N/A	N/A	N/A	<a href="#">Protect</a>

- Depuis la page Protection, sélectionnez une charge de travail, puis sélectionnez **Protéger**.
- 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.
- 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, voir [Créer une politique de protection](#) . Sélectionnez **Suivant**.
- Sélectionnez une destination de sauvegarde ou créez-en une nouvelle. Sélectionnez **Suivant**.
- Passez en revue la nouvelle stratégie de protection, puis sélectionnez **Protéger** pour l'appliquer.
- 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

- Dans le menu Résilience aux ransomwares, sélectionnez **Protection**.
- Depuis la page Protection, sur la ligne de charge de travail, sélectionnez **Modifier la protection**.
- 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**.
- Dans la page Politiques, sélectionnez la flèche vers le bas correspondant à la politique que vous souhaitez attribuer pour consulter les détails.
- Sélectionnez la politique que vous souhaitez attribuer.
- Sélectionnez **Protéger** pour terminer la modification.

## Partages de fichiers de groupe pour une protection plus facile

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 qui ne sont pas protégés et des groupes qui sont 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**.

Protection status

9 At risk 9 in last 7 days 35 TiB data at risk

9 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (19) [Manage protection strategies](#)

Workload	↑	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01		At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01		Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781		Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009		At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294		Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115		At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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

Workloads Protection groups

Protection group (1) [ADD](#)

Protection group	↑	Protection status	Ransomware resilience strategy	Protected count
pg_important		Protected	rps-important-plan	2 / 2

3. Sélectionnez **Ajouter**.

**Workloads**  
Select workloads to add to the protection group.

Protection group name

**Workloads (16)** Q  
Select workloads with no other policy source or with NetApp Backup and Recovery as a policy source.

<input type="checkbox"/>	Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection status
<input type="checkbox"/>	FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	None
<input type="checkbox"/>	LUN_storage_01	Block	aws-connector-us-east-1	Critical	n/a	Protected	Active
<input type="checkbox"/>	MySQL_8009	MySQL	aws-connector-us-east-1	Critical	n/a	At risk	None
<input type="checkbox"/>	MySQL_9294	MySQL	aws-connector-us-east-1	Critical	n/a	Protected	Active
<input type="checkbox"/>	Oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	At risk	None

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



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

- Sélectionnez **Suivant**.

**Protect**  
Select how to protect all the workloads in the protection group.

**Warning:** All current policies will be replaced with the selected policies.

**Ransomware resilience strategies (3)** Q Add

<input type="radio"/>	Ransomware resilience strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads
<input type="radio"/>	rps-critical-plan	critical-ss-policy	critical-bu-policy	rps-policy-all	3
<input type="radio"/>	rps-important-plan	important-ss-policy	important-bu-policy	rps-policy-all	1
<input type="radio"/>	rps-standard-plan	standard-ss-policy	standard-bu-policy	rps-policy-primary	0

- Sélectionnez la politique qui régira la protection de ce groupe.
- Sélectionnez **Suivant**.
- Passer en revue les sélections pour le groupe de protection.
- Sélectionnez **Ajouter**.

### Modifier la protection du groupe

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

### Étapes

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

The screenshot shows the 'pg\_important' protection group page. It includes a 'Delete protection group' button and a 'Workloads' section with icons for File shares (0), Applications (2), and VM datastores (0). A table titled 'Workloads (2)' lists the following items:

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection status
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	n/a	Protected	Learning mode
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	Active

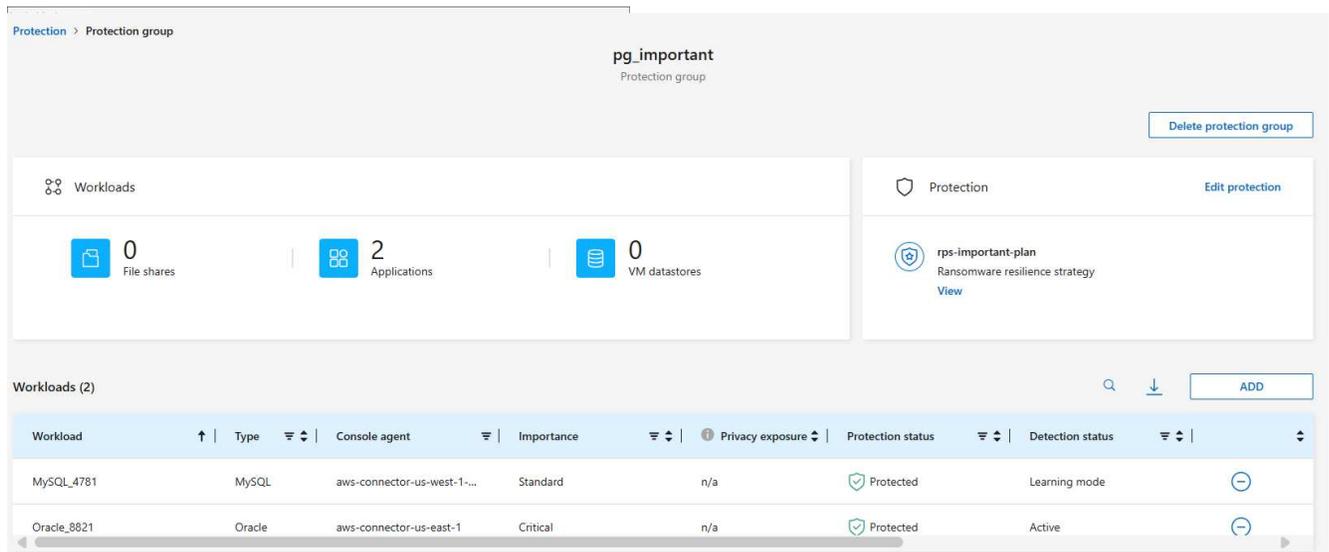
4. À partir de la page du groupe de protection sélectionné, sélectionnez la charge de travail que vous souhaitez supprimer du groupe et sélectionnez **\*Actions\*** option.
5. Dans le menu Actions, sélectionnez **Supprimer la charge de travail**.
6. Confirmez que vous souhaitez supprimer la charge de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



- Depuis la page du groupe de protection sélectionné, en haut à droite, sélectionnez **Supprimer le groupe de protection**.
- 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

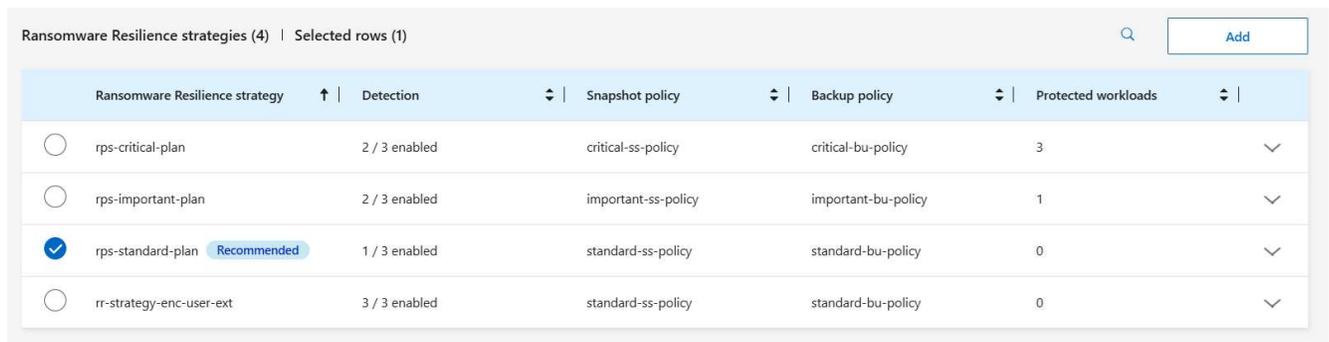
Avant de supprimer une stratégie de protection contre les ransomwares, vous souhaitez peut-être afficher les charges de travail protégées par cette stratégie.

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

### Étapes à suivre pour consulter la liste des stratégies

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

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



- 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 classification des données NetApp 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 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.



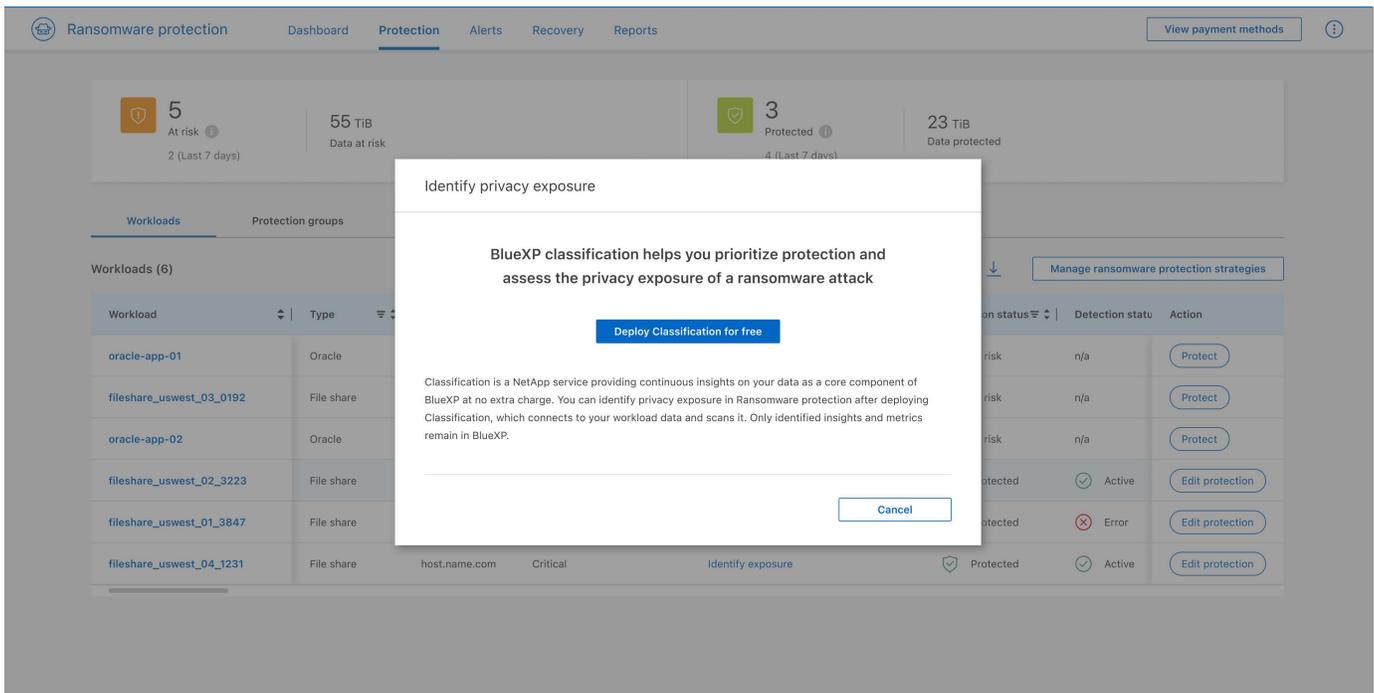
Ce processus peut avoir un impact sur l'importance de la charge de travail pour vous aider à garantir que vous disposez de la protection appropriée.

**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 d'accès à la console pour tous les services](#)".

### 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.

Protection Run readiness drill ⚠ Free trial (30 days left) ⋮ ↻

**9**  
At risk  ⓘ  
4 (Last 7 days)

**35** TiB  
Data at risk

**9**  
Protected  ⓘ  
1 (Last 7 days)

**10** TiB  
Data protected

Workloads Protection groups

Workloads (19) 🔍 ⏴ Manage protection strategies

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Protection grc	Actions
FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	<span style="color: orange;">⚠</span> At risk	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Protect</span>
LUN_storage_01	Block	aws-connector-us-east-1	Critical	N/A	<span style="color: green;">✔</span> Protected	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Edit Protection</span>
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	N/A	<span style="color: green;">✔</span> Protected	pg_important	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Edit Protection</span>
MySQL_8009	MySQL	aws-connector-us-east-1	Critical	Identify exposure	<span style="color: orange;">⚠</span> At risk	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Protect</span>
MySQL_9294	MySQL	aws-connector-us-east-1	Critical	N/A	<span style="color: green;">✔</span> Protected	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Edit Protection</span>
Oracle_2115	Oracle	aws-connector-us-east-1	Critical	N/A	<span style="color: orange;">⚠</span> At risk	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Protect</span>
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	N/A	<span style="color: green;">✔</span> Protected	pg_important	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Edit Protection</span>
Oracle_9819	Oracle	aws-connector-us-east-1	Important	N/A	<span style="color: green;">✔</span> Protected	N/A	<span style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;">Edit Protection</span>

- 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 Classification, 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

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

Protection Run readiness drill Free trial (30 days left)

**9**  
At risk  
4 (Last 7 days)

**35 TiB**  
Data at risk

**9**  
Protected  
1 (Last 7 days)

**10 TiB**  
Data protected

Workloads Protection groups

Workloads (19) Manage protection strategies

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Protection grc	Actions
FSxN_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	<a href="#">Protect</a>
LUN_storage_01	Block	aws-connector-us-east-1	Critical	N/A	Protected	N/A	<a href="#">Edit Protection</a>
MySQL_4781	MySQL	aws-connector-us-west-1-...	Standard	N/A	Protected	pg_important	<a href="#">Edit Protection</a>
MySQL_8009	MySQL	aws-connector-us-east-1	Critical	Identify exposure	At risk	N/A	<a href="#">Protect</a>
MySQL_9294	MySQL	aws-connector-us-east-1	Critical	N/A	Protected	N/A	<a href="#">Edit Protection</a>
Oracle_2115	Oracle	aws-connector-us-east-1	Critical	N/A	At risk	N/A	<a href="#">Protect</a>
Oracle_8821	Oracle	aws-connector-us-east-1	Critical	N/A	Protected	pg_important	<a href="#">Edit Protection</a>
Oracle_9819	Oracle	aws-connector-us-east-1	Important	N/A	Protected	N/A	<a href="#">Edit Protection</a>

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

Protection > FSxN\_fileshare\_useast\_01

### FSxN\_fileshare\_useast\_01

**Critical Importance**

**Protected**  
Protection health  
[Edit protection](#)

**0**  
Alerts

**Not marked for recovery**  
Recovery

**High** Privacy exposure

Files with PII **181 hits in 150 files**

Types of PII

- Credit cards** 20 hits in 150 files
- Contacts** 95 hits in 150 files
- Passwords** 28 hits in 150 files
- Data subjects** 38 hits in 150 files

**Protection**

**2 / 3 enabled** Detection

rps-critical-plan Policy  
[View policy](#)

n/a Backup destination  
[View backup destination](#)

**File share**

Location: svm-fsxEnvironment  
Console agent: console-agent-us-east

Amazon FSx for NetApp ONTAP

Volume: FSxN\_fileshare\_useas...

Cluster id: aaa111a1a-1a11-11aa-1-...  
System name: fsxEnvironment...  
Storage VM name: svm-fsxEnvironment...

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"](#)

## Gérez les alertes de ransomware détectées avec NetApp Ransomware Resilience

Lorsque NetApp Ransomware Resilience détecte une attaque possible, il affiche une alerte sur le tableau de bord et dans la zone 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 possible, une notification apparaît dans les paramètres de notification de la console et un e-mail est envoyé à l'adresse 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 résilience aux ransomwares.

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 uniquement basés 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 avoir l'un des états suivants :

- **Nouveau** : Tous les incidents sont marqués « nouveaux » lorsqu'ils sont identifiés pour la première fois.
- **Rejeté** : Si vous pensez que l'activité n'est pas une attaque de ransomware, vous pouvez modifier le statut sur « Rejeté ».



Après avoir rejeté une attaque, vous ne pouvez pas revenir en arrière. Si vous supprimez une charge de travail, toutes les copies instantanées prises automatiquement en réponse à l'attaque potentielle du 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.

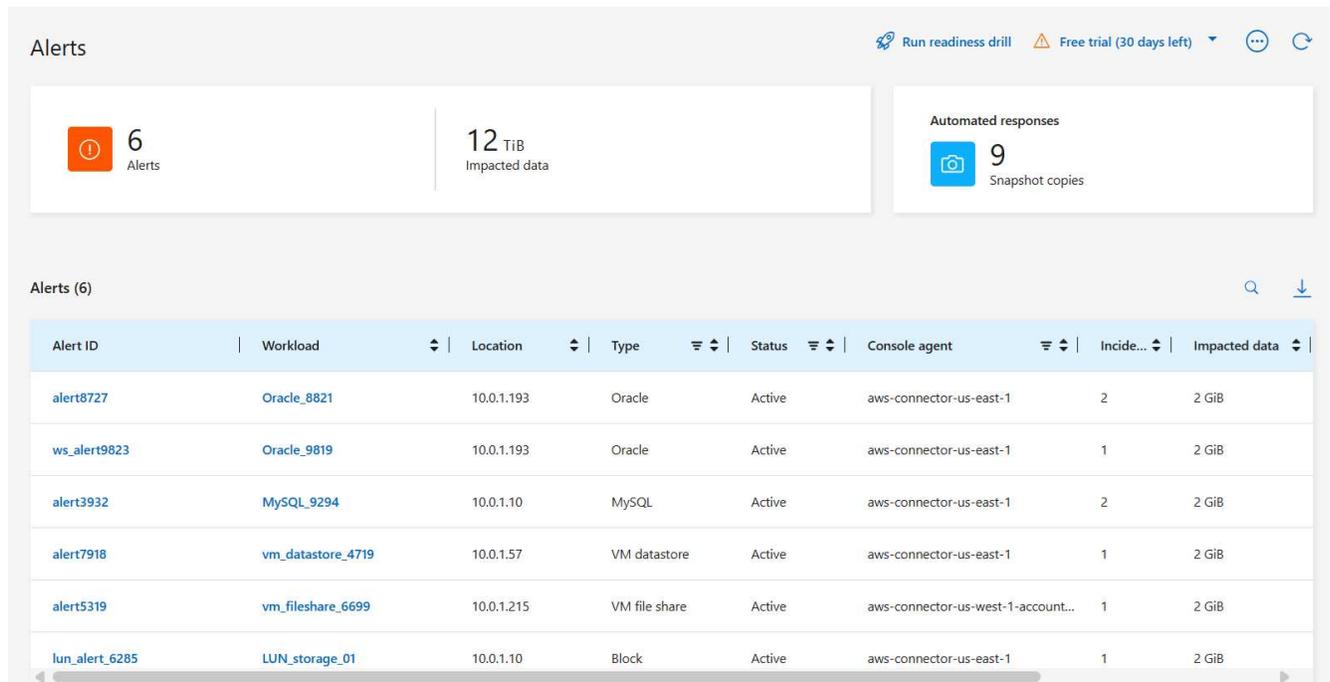
## Afficher les alertes

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 d'accès BlueXP pour tous les services](#)".

### 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**.



The screenshot shows the 'Alerts' page in the console. At the top, there are two summary cards: one for '6 Alerts' and another for '12 TiB Impacted data'. To the right, there is a card for 'Automated responses' showing '9 Snapshot copies'. Below these is a table with 6 alerts. The table has columns for Alert ID, Workload, Location, Type, Status, Console agent, Incidents, and Impacted data.

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

6. Continuez avec l'une des options suivantes :
  - [Détecer 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 en fonction de leurs préférences de notification d'abonnement. L'e-mail contient des informations sur l'alerte, notamment la gravité et les ressources concernées.

Vous pouvez recevoir des notifications par e-mail pour les alertes de résilience aux ransomwares. Cette

fonctionnalité vous aide à rester informé des alertes, de leur gravité et des ressources impactées.



Pour vous abonner aux notifications par e-mail, reportez-vous à ["Définir les paramètres de notification par e-mail"](#) .

1. Dans Ransomware Resilience, accédez à la page **Paramètres**.
2. Sous **Notifications**, recherchez les paramètres de notification par e-mail.
3. Saisissez l'adresse e-mail à laquelle vous souhaitez recevoir des alertes.
4. Enregistrez vos modifications.

Vous recevrez désormais des notifications par e-mail lorsque de nouvelles alertes seront générées.

**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 d'accès BlueXP pour tous les services"](#) .

### 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 :
  - [Détection des activités malveillantes et des 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 existe une activité malveillante.

**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 d'accès à la console pour tous les services"](#) .

**Quels détails apparaissent ?** Les détails qui s'affichent dépendent de la manière dont l'alerte a été déclenchée :

- Déclenché par la fonctionnalité de protection autonome contre les ransomwares dans ONTAP. Cela détecte les activités malveillantes en fonction du comportement des fichiers dans le volume.
- Déclenché par Data Infrastructure Insights Sécurité de la charge de travail. Cela nécessite une licence pour la sécurité de la charge de travail Data Infrastructure Insights et que vous l'activiez dans Ransomware Resilience. Cette fonctionnalité détecte les comportements anormaux des utilisateurs dans vos charges de travail de stockage et vous permet de bloquer tout accès ultérieur de cet utilisateur.

Pour activer la sécurité de la charge de travail dans Ransomware Resilience, accédez à la page **Paramètres** et sélectionnez l'option **Connexion de sécurité de la charge de travail**.

Pour un aperçu de la sécurité des charges de travail de Data Infrastructure Insights, consultez "[À propos de la sécurité des charges de travail](#)".



Si vous ne disposez pas d'une licence pour la sécurité de la charge de travail de l'infrastructure de données et que vous ne l'activez pas dans Ransomware Resilience, vous ne verrez pas les informations sur le comportement anormal des utilisateurs.

Lorsqu'une activité malveillante se produit, une alerte est générée et un instantané automatisé est pris.

### Afficher l'activité malveillante uniquement à partir de la protection autonome contre les ransomwares

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.

Incident ID	Volume	Storage VM	System	Type	Status	First detected	Most recent	Evidence	Automated re...
inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copy

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

## Afficher le comportement anormal des utilisateurs dans Data Infrastructure Insights Sécurité de la charge de travail

Lorsque la sécurité de la charge de travail Data Infrastructure Insights déclenche une alerte dans Ransomware Resilience, vous pouvez afficher l'utilisateur suspect, bloquer l'utilisateur et enquêter sur l'activité de l'utilisateur directement dans la sécurité de la charge de travail Data Infrastructure Insights .



Ces fonctionnalités s'ajoutent aux détails disponibles uniquement auprès d'Autonomous Ransomware Protection.

### Avant de commencer

Cette option nécessite une licence pour la sécurité de la charge de travail Data Infrastructure Insights et que vous l'activiez dans Ransomware Resilience.

Pour activer la sécurité de la charge de travail dans Ransomware Resilience, procédez comme suit :

1. Accédez à la page **Paramètres**.
2. Sélectionnez l'option **Connexion Workload Security**.

Pour plus de détails, consultez la section "[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.

Alerts > alert8727

alert8727

Impacted workloads: Oracle\_8821 Mark restore needed

⚡ 2 Potential attacks

📁 286 Impacted files

💾 2 GiB Impacted data

🕒 September 2, 2025, 1:57 PM First detected

Incidents (2) 🔍 ⬇️ Edit status

Incident ID	Volume	Storage VM	System	Severity	Status	First detected	Most recently de...	Evidence	Au
inc4922	oracle_usea...	svm_VsaWorki...	VsaWorking...	Potential attack	New	13 days ago	12 days ago	4 new extensions detected	1 S
inc3163	oracle_usea...	svm_VsaWorki...	VsaWorking...	Potential attack	New	13 days ago	12 days ago	6 new extensions detected	1 S

4. Pour empêcher un utilisateur suspect d'accéder à votre environnement surveillé par la console, sélectionnez le lien **Bloquer l'utilisateur**.
5. Recherchez l'alerte ou un incident dans l'alerte :
  - a. Pour rechercher plus en détail l'alerte dans la sécurité de la charge de travail de Data Infrastructure Insights , sélectionnez le lien **Enquêter sur la sécurité de la charge de travail**.
  - b. Sélectionnez un incident pour consulter les détails de l'incident.

Data Infrastructure Insights La sécurité de la charge de travail s'ouvre dans un nouvel onglet.

The screenshot shows the NetApp Cloud Insights interface for a Ransomware Attack. The main alert area displays the attack name, detection time, and status. Below this, there are buttons for 'Block User', 'Restore Entities', and 'Re Take Snapshots'. The 'Total Attack Results' section provides a summary of affected volumes, deleted files, and encrypted files. A line graph shows the activity of encrypted files over time, with a significant spike at 8:50 PM. The 'Related Users' section identifies the user 'Heri' and the number of files encrypted.

## 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 démarrer la 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 d'accès à la console pour tous les services"](#) .

### Étapes

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

Alerts

Run readiness drill Free trial (30 days left)

6 Alerts | 12 TiB Impacted data | 9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

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

Alerts > alert3932

alert3932

Workload: MySQL\_9294 | Location: | Type: MySQL | Console agent: aws-con... | Mark restore needed

2 Potential attacks | 19 days ago First detected | 2 GiB Impacted data | 286 Impacted files

Incidents (2)

Incident ID	Volume	Storage VM	System	Type	Status	First detec...	Most rece...	Evidence	Automated re...
inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copy

- Si vous déterminez que les incidents sont prêts à être récupérés, sélectionnez **Marquer comme restauration nécessaire**.
- Confirmez l'action et sélectionnez **Marquer comme restauration nécessaire**.
- 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 la condition précédente n'est pas remplie, ils peuvent être licenciés.

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 sur 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 ce statut en un autre statut et vous ne pouvez pas 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 d'accès à la console pour tous les services](#)".

## Étapes

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

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data
alert8727	Oracle_8821	10.0.1.193	Oracle	Active	aws-connector-us-east-1	2	2 GiB
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	Active	aws-connector-us-east-1	1	2 GiB
alert3932	MySQL_9294	10.0.1.10	MySQL	Active	aws-connector-us-east-1	2	2 GiB
alert7918	vm_datastore_4719	10.0.1.57	VM datastore	Active	aws-connector-us-east-1	1	2 GiB
alert5319	vm_fileshare_6699	10.0.1.215	VM file share	Active	aws-connector-us-west-1-account...	1	2 GiB
lun_alert_6285	LUN_storage_01	10.0.1.10	Block	Active	aws-connector-us-east-1	1	2 GiB

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

Incident ID	Volume	Storage VM	System	Type	Status	First detec...	Most rece...	Evidence	Automated re...
inc3444	mysql_useast_21	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	2 Snapshot copi
inc7792	mysql_useast_22	svm_VsaWorkingEnvir...	VsaWorkingEnvironme...	Potential attack	New	19 days ago	18 days ago	4 new extensions...	1 Snapshot copi

3. Sélectionnez un ou plusieurs incidents. Ou sélectionnez tous les incidents en sélectionnant la case ID d'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.

## Edit status

---

Change the status to keep track of incidents that are not a threat.

Status

Select status ▲

Resolved

Dismissed

---

Save

Cancel

5. Dans la boîte Modifier le statut, sélectionnez le statut « **Rejeté** ».

Des informations supplémentaires sur la charge de travail et sur le fait que les copies instantanées sont supprimées s'affichent.

6. Sélectionnez **Enregistrer**.

Le statut de l'incident ou des incidents passe à « Ignoré ».

## 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 d'accès à la console pour tous les services"](#) .

## 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.

The screenshot shows the NetApp Ransomware Resilience interface for workload MySQL\_9294. It displays a 'Potential attack' alert detected 19 days ago. Key metrics include 'Entropy of incoming data' (Detected: 25156 KIB/min, Expected: 2510 KIB/min) and 'File activity' (Creation rate: Detected 65 files/min, Expected 6 files/min). A table lists impacted files (109 total) with columns for 'Impacted files' and 'Probable clean files'. The table shows file paths and their original and suspect extensions.

Impacted files	Probable clean files
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.lck	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt
/Top_Dir_1/Sub_Dir_11/test_file_10386.txt.omg	/Top_Dir_1/Sub_Dir_11/test_file_10386.txt

5. Pour cet incident, sélectionnez l'icône de téléchargement et téléchargez 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**.

[Page de 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 d'accès à la console pour tous les services"](#) .

### 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 d'accès à la console pour tous les services](#)".

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**.

Restore "MySQL\_9294" 1 Restore 2 Review

**Restore**

Workload: MySQL\_9294 Host: 10.0.1.10 Type: MySQL Console agent: aws-connector-us-east-1

Restore scope:  All volumes  By volume  By file

Source ^

First attack reported September 9, 2025, 1:57 PM Restore points  Safest for all volumes ⓘ

Volumes (2) 🔍

Volume	Restore point	Type	Date	Size
mysql_useast_21	cbs-snapshot-adhoc-1697555391705	Backup	September 9, 2025, 1:27 PM	2 GiB
mysql_useast_22	cbs-snapshot-adhoc-1697555327497	Backup	September 6, 2025, 10:57 AM	2 GiB

Destination v

Action required

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.

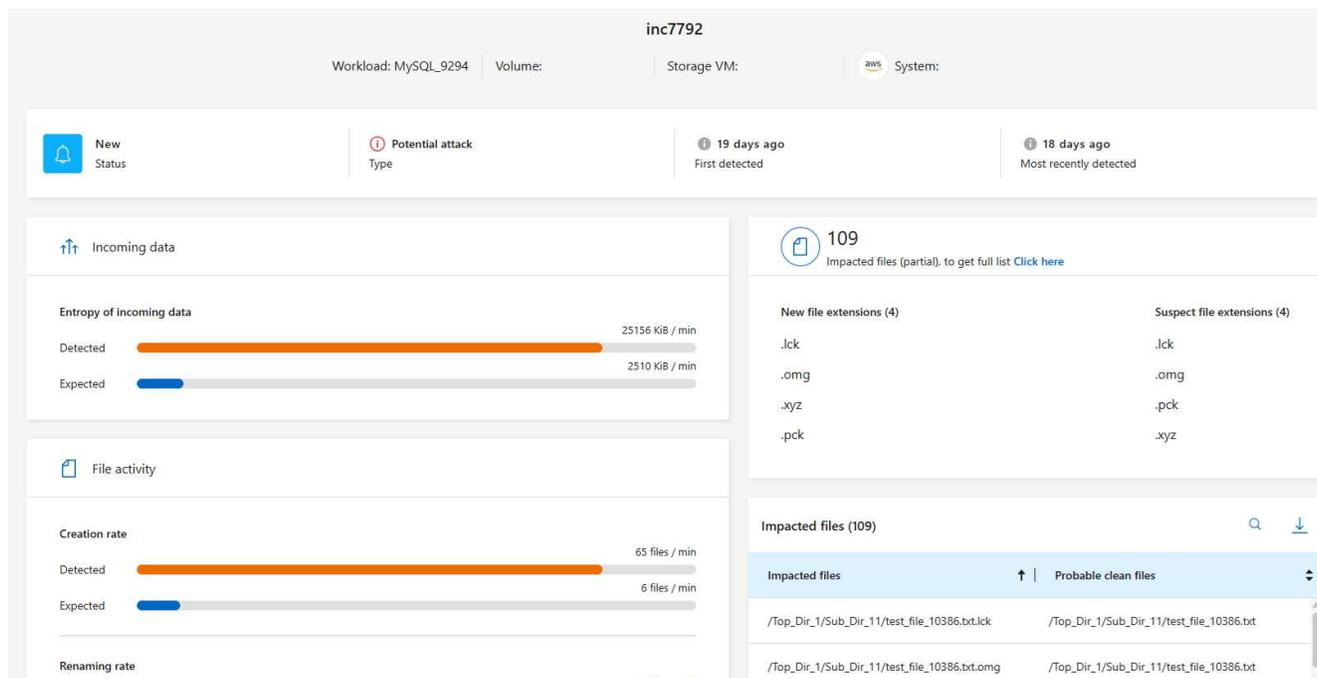
### Étapes pour obtenir la liste des fichiers impactés

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

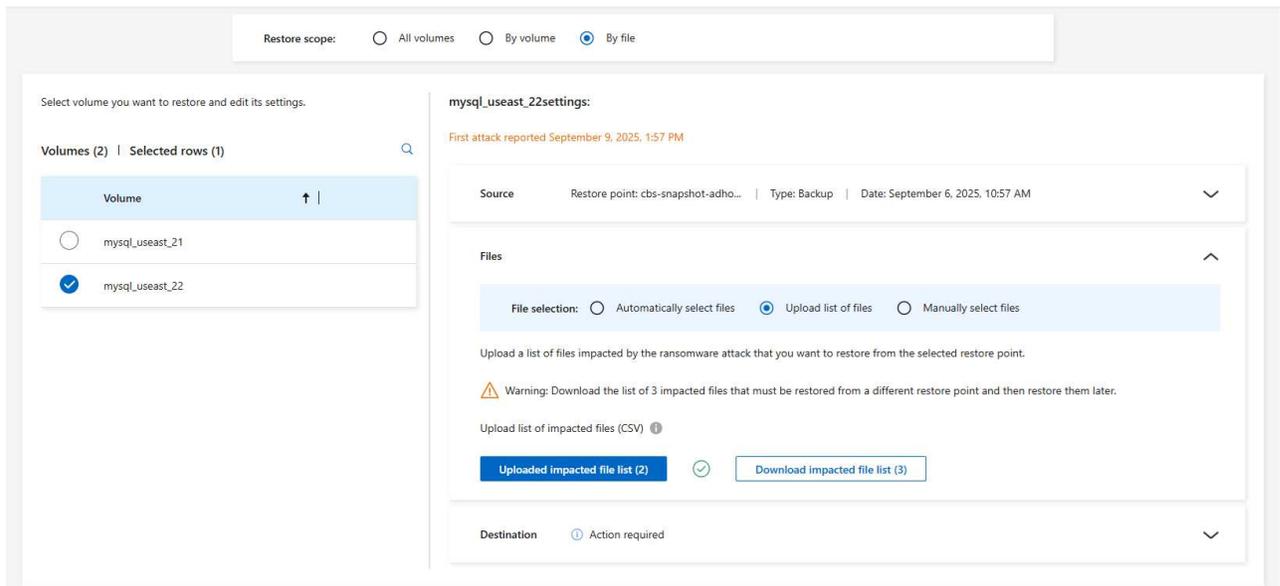
1. Dans le menu Résilience aux ransomwares, sélectionnez **Récupération**.
2. Sélectionnez une charge de travail d'application qui est dans l'état « Restauration nécessaire ».
3. Pour restaurer, sélectionnez **Restaurer**.
4. Sur la page Restaurer, dans l'étendue Restaurer, sélectionnez **Par fichier**.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



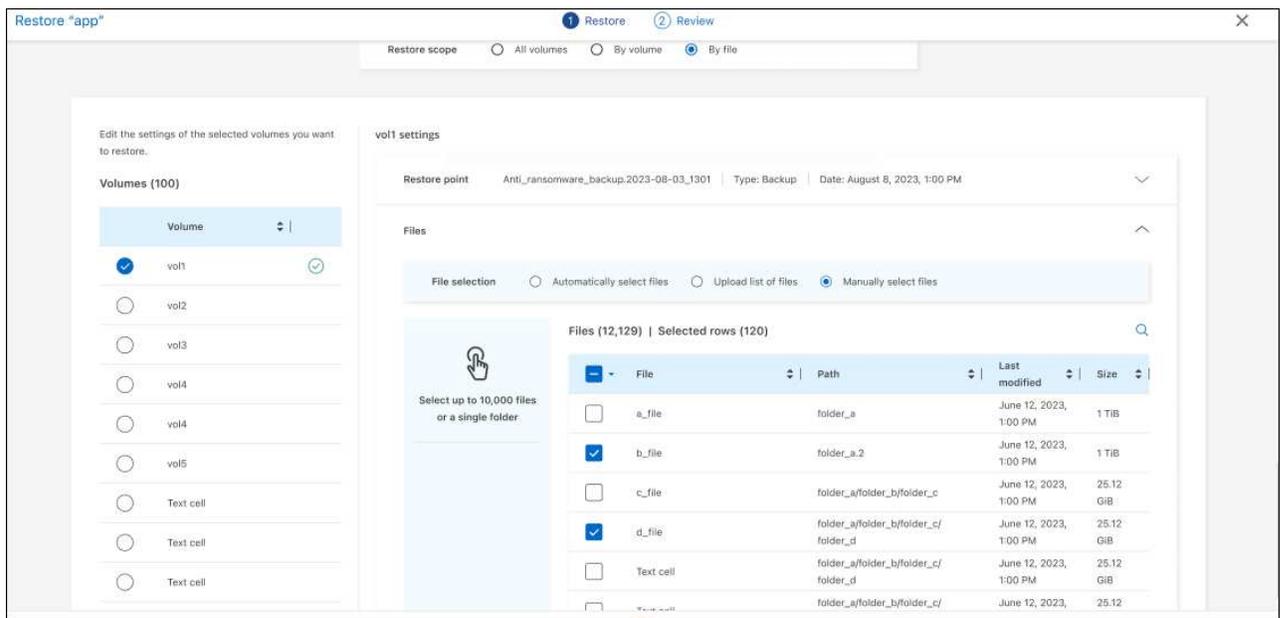
La colonne Raison du volet Points de restauration indique la raison de l'instantané ou de la sauvegarde comme étant « Planifiée » ou « Réponse automatisée à un incident de ransomware ».

### 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**.

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

Restore "vm\_datastore\_202\_7359" 1 Restore 2 Review

Restore

Workload: vm\_datastore\_202\_735... | Location: 10.195.52.126 | vCenter: 10.195.52.128 | Type: VM datastore | Connector: onprem-connector-account-LXtf4X...

Restore scope  By VM

Source

Restore points attack time: October 17, 2023, 11:27 AM

Restore points (4)

Restore point	Provider	Date
<input type="radio"/> RG-vm_datastore_202_11-21-2023_20.30.01.0238	AWS	November 21, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-20-2023_20.30.01.0260	AWS	November 20, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-19-2023_20.30.01.0250	AWS	November 19, 2023, 8:30 PM
<input type="radio"/> RG-vm_datastore_202_11-18-2023_20.30.01.0871	AWS	November 18, 2023, 8:30 PM

Destination Original location

Next

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 résilience aux ransomwares NetApp

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, vous devez actualiser les données, ce qui actualise également les données qui apparaîtront dans les fichiers.

**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 d'accès BlueXP pour tous les services"](#) .

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

- **Protection** : Contient l'état et les détails de toutes les charges de travail, y compris le nombre total de charges 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.



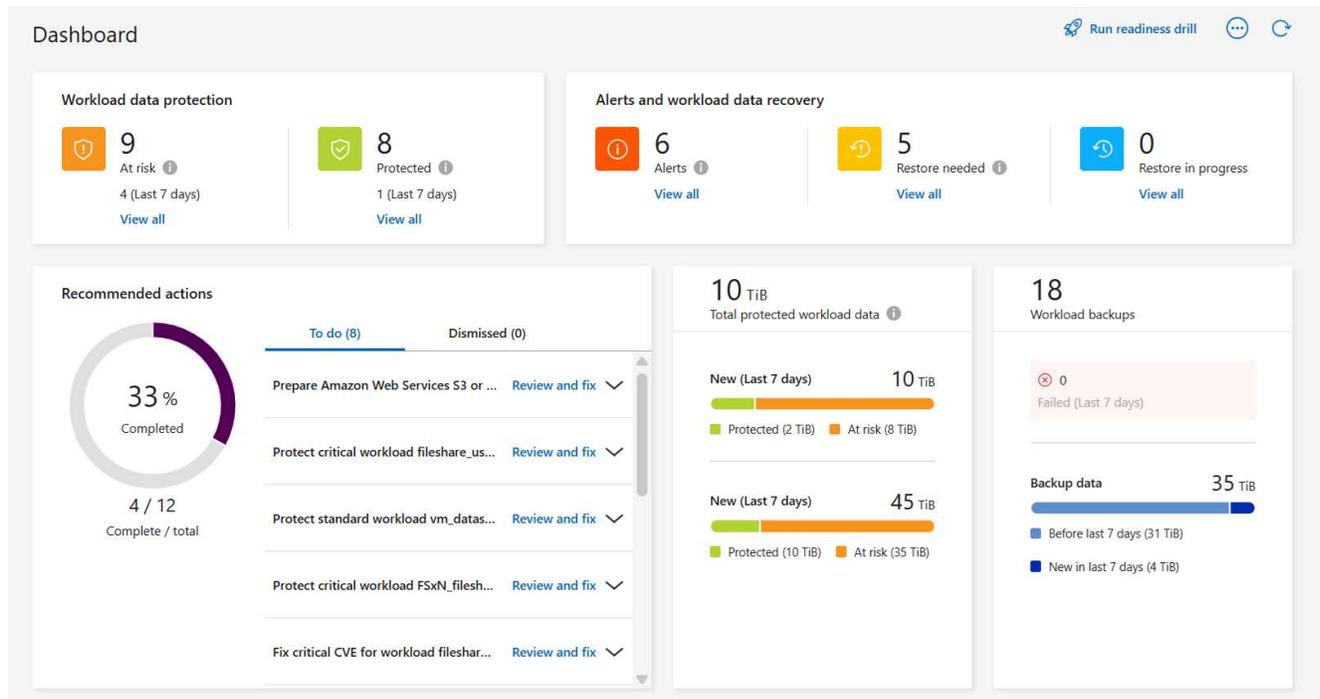
Vous pouvez télécharger les rapports d'exercice de préparation uniquement à partir de la page **Rapports**.

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.

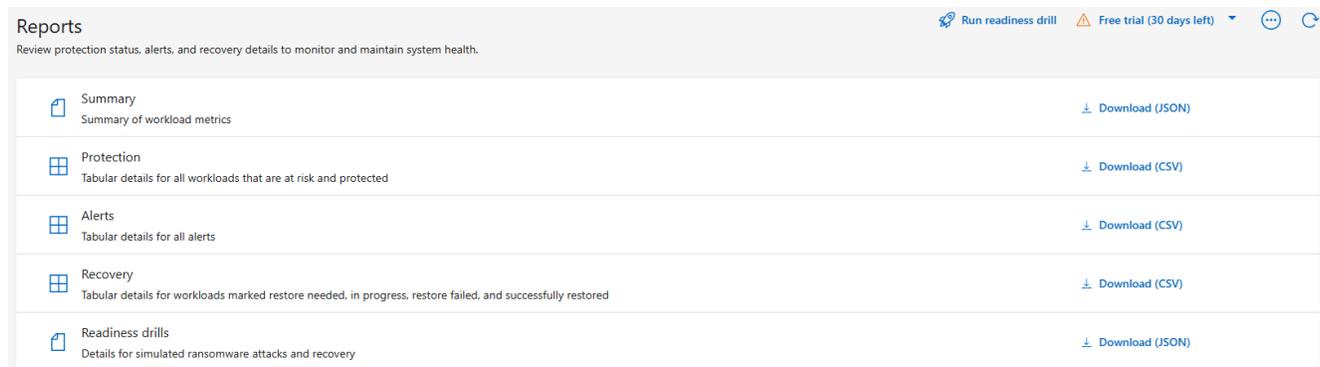
Les fichiers CSV ou JSON incluent des données pour toutes les charges de travail sur tous les systèmes de console.

### 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 recevoir un support technique spécifique à BlueXP et à ses solutions et services de stockage. 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 BlueXP 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 BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxxx situé sur la page Ressources d'assistance dans BlueXP).

Il s'agit de votre identifiant d'abonnement d'assistance unique pour tout service au sein de BlueXP. Chaque abonnement de support au niveau du compte BlueXP 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 BlueXP 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 BlueXP comme décrit ci-dessous.

## Enregistrez BlueXP pour le support NetApp

Pour vous inscrire au support et activer le droit de support, un utilisateur de votre organisation (ou compte) BlueXP doit associer un compte de site de support NetApp à sa connexion BlueXP . 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 du support via BlueXP.

### Étapes

1. En haut à droite de la console BlueXP , sélectionnez l'icône Paramètres, puis sélectionnez **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 organisation BlueXP est enregistrée pour bénéficier du support.



Notez que les autres utilisateurs BlueXP 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 BlueXP . Cependant, cela ne signifie pas que votre organisation BlueXP n'est pas enregistrée pour bénéficier du support. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre organisation a été enregistrée.

### 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 BlueXP .

#### Étapes

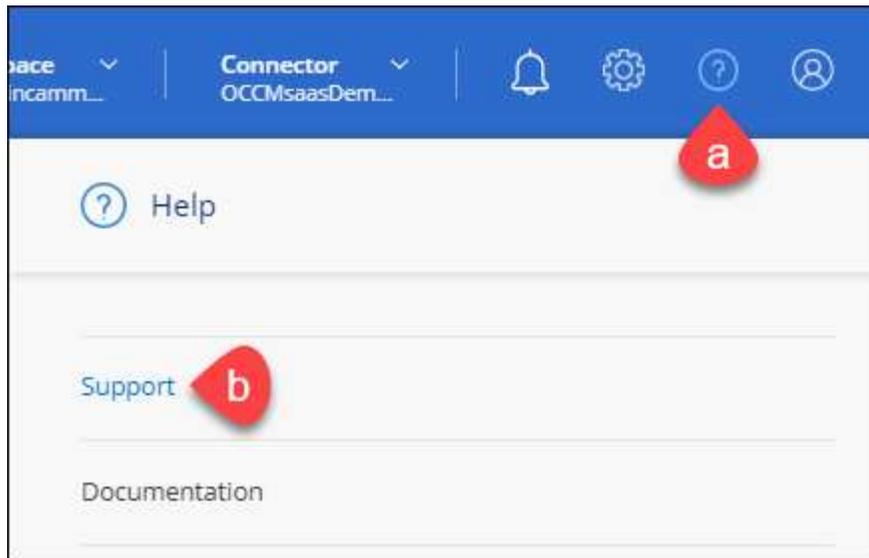
1. Créez un compte sur le site de support NetApp en remplissant le "[Formulaire d'inscription des utilisateurs du site de support NetApp](#)"
  - a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement \* Client/Utilisateur final NetApp \*.
  - b. Assurez-vous de copier le numéro de série du compte BlueXP (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 BlueXP en suivant les étapes ci-dessous [Client existant avec un compte NSS](#) .

### Tout nouveau chez NetApp

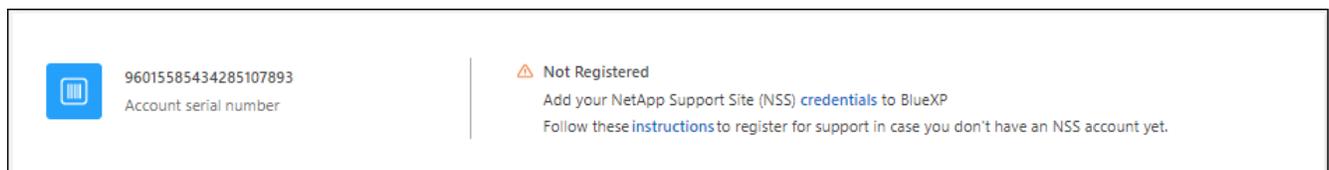
Si vous êtes nouveau sur NetApp et que vous n'avez pas de compte NSS, suivez chaque étape ci-dessous.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP , 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 BlueXP en suivant les étapes ci-dessous [Client 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 organisation BlueXP 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 BlueXP 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

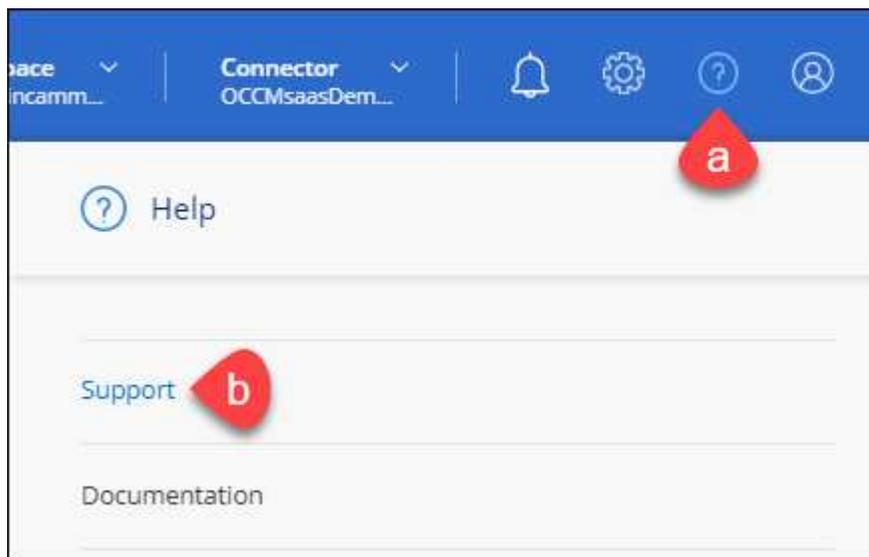
L'association des informations d'identification NSS à votre organisation BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP .

Ces informations d'identification NSS sont associées à votre ID d'organisation BlueXP spécifique. Les utilisateurs appartenant à l'organisation BlueXP 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 BlueXP , 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 BlueXP 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 propose une assistance pour BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances 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 « Obtenir de l'aide » dans la documentation BlueXP de ce produit.

- ["Amazon FSx pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Pour recevoir une assistance technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options d'assistance 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 BlueXP que vous consultez actuellement.

- ["Base de connaissances"](#)

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

- ["Communautés"](#)

Rejoignez la communauté BlueXP 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 BlueXP . ["Découvrez comment gérer les informations d'identification associées à votre connexion BlueXP"](#) .
- 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 BlueXP, 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, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
    - **Environnement de travail** : Si applicable au stockage, sélectionnez \* Cloud Volumes ONTAP\* ou **Sur site**, puis l'environnement de travail associé.

La liste des environnements de travail est comprise dans le champ d'application de l'organisation

BlueXP (ou du compte), du projet (ou de l'espace de travail) et du connecteur que vous avez sélectionnés dans la bannière supérieure du service.

- **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.

The screenshot shows a web form for a NetApp Support Site Account. At the top, it displays the account name 'ntapitdemo' with an edit icon and the text 'NetApp Support Site Account'. Below this, there are two dropdown menus: 'Service' and 'Working Environment', both currently set to 'Select'. The 'Case Priority' dropdown is set to 'Low - General guidance' and has an information icon to its right. The 'Issue Description' field is a large text area with the placeholder text 'Provide detailed description of problem, applicable error messages and troubleshooting steps taken.'. Below that is the 'Additional Email Addresses (Optional)' field, which is currently empty and has an information icon to its right. At the bottom, there is an 'Attachment (Optional)' section with an 'Upload' button and an information icon. The attachment area shows 'No files selected' and a trash icon.

### 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 BlueXP (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 :

- Utilisez le chat intégré au produit
- Soumettez un cas non technique à <https://mysupport.netapp.com/site/help>

## Gérez vos demandes d'assistance (Aperçu)

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

La gestion des cas est disponible en aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Veuillez nous envoyer vos commentaires en utilisant le chat intégré au produit.

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.

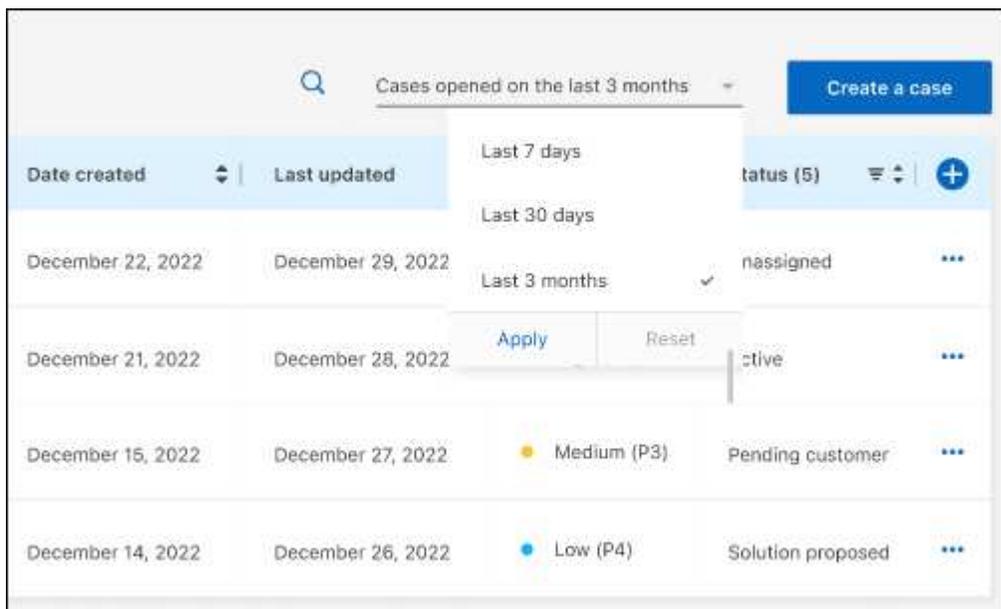
### Étapes

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

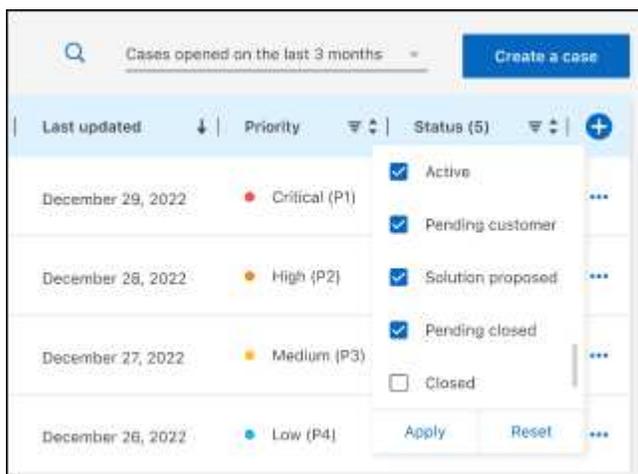
La page **Gestion des cas** affiche les cas ouverts liés au compte NSS associé à votre compte utilisateur BlueXP . Il s'agit du même compte NSS qui apparaît en haut de la page **Gestion NSS**.

3. Modifiez éventuellement les informations qui s'affichent dans le tableau :

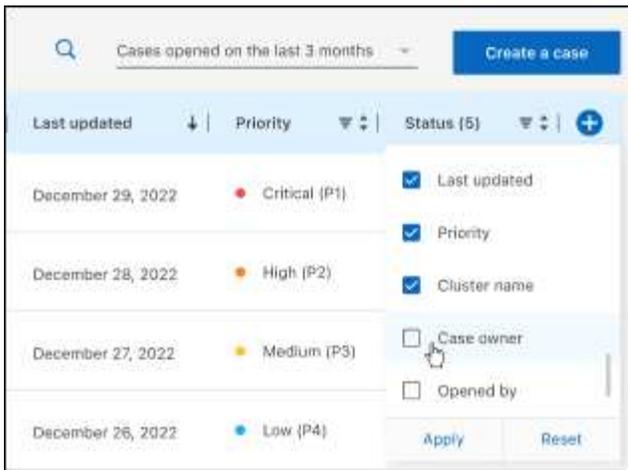
- Sous **Cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre entreprise.
- Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une période différente.



- Filtrer le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant  et ensuite choisir les colonnes que vous souhaitez afficher.

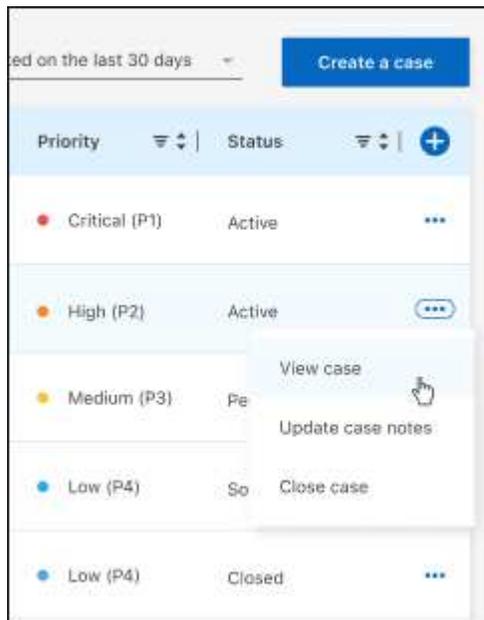


4. Gérer un dossier existant en sélectionnant... et en sélectionnant l'une des options disponibles :

- **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 résilience aux ransomwares NetApp

Cette FAQ peut vous aider si vous recherchez simplement une réponse rapide à une question sur la résilience aux ransomwares de NetApp .

## 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 Licences et abonnements de la console.

**Comment activer la résilience aux ransomwares ?** La résilience aux ransomwares ne nécessite aucune activation. Vous pouvez accéder à Ransomware Resilience depuis la console NetApp .

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

Pour démarrer avec Ransomware Resilience, sélectionnez « Commencer à découvrir les charges de travail » sur sa page d'accueil initiale.

**Ransomware Resilience est-il disponible en modes standard, restreint et privé ?** À l'heure actuelle, Ransomware Resilience n'est disponible qu'en mode standard. Restez à l'écoute pour en savoir plus.

Pour une explication sur ces modes dans tous les services de données NetApp , reportez-vous à "[Modes de déploiement de la console NetApp](#)" .

## Accéder

**Quelle est l'URL de résilience aux ransomwares ?** Dans un navigateur, saisissez "<https://console.netapp.com/ransomware-resilience>" pour accéder à la console.

**Comment sont gérées les autorisations d'accès ?** "[En savoir plus sur les rôles d'accès à la console pour tous les services](#)" .

**Quelle est la meilleure résolution d'appareil ?** La résolution d'appareil recommandée pour Ransomware Resilience est de 1920 x 1080 ou supérieure.

**Quel navigateur dois-je utiliser ?** Tout navigateur moderne.

# Interaction avec d'autres services

## **Ransomware Resilience est-il conscient des paramètres de protection définis dans NetApp ONTAP?**

Oui, Ransomware Resilience découvre les planifications d'instantanés définies dans ONTAP.

**Si vous définissez une politique à l'aide de Ransomware Resilience, devez-vous apporter des modifications futures uniquement dans ce service ?** Nous vous recommandons d'effectuer des modifications de politique à partir de Ransomware Resilience.

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

Ransomware Resilience utilise les produits et services suivants :

- Sauvegarde et récupération pour découvrir et définir des stratégies de capture instantanée et de sauvegarde pour les charges de travail de partage de fichiers
- 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.

# Charges de travail

**Qu'est-ce qui constitue une charge de travail ?** 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, une instance Oracle DB déployée sur ora3.host.com peut avoir vol1 et vol2 pour ses données et ses journaux, respectivement. Ces volumes constituent ensemble la charge de travail pour cette instance spécifique de l'instance Oracle DB.

**Comment Ransomware Resilience priorise-t-il les données de charge de travail ?** La priorité des données est déterminée par les copies instantanées effectuées et les sauvegardes planifiées.

La priorité de la charge de travail (critique, standard, importante) est déterminée par les fréquences d'instantanés déjà appliquées à chaque volume associé à la charge de travail.

["En savoir plus sur la priorité ou l'importance de la charge de travail"](#) .

## **Quelles charges de travail Ransomware Resilience prend-il en charge ?**

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

De plus, 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, et Ransomware Resilience peut les protéger et les récupérer de manière cohérente avec la charge de travail.

## **Comment associez-vous des données à une charge de travail ?**

Ransomware Resilience associe les données à une charge de travail des manières suivantes :

- Ransomware Resilience découvre les volumes et les extensions de fichiers et les associe à la charge de travail appropriée.
- De plus, si vous disposez de SnapCenter ou de SnapCenter pour VMware et que vous avez configuré des

charges de travail dans Sauvegarde et récupération, Ransomware Resilience découvre les charges de travail gérées par SnapCenter et SnapCenter pour VMware et leurs volumes associés.

**Qu'est-ce qu'une charge de travail « protégée » ?** Dans Ransomware Resilience, une charge de travail affiche un statut « protégé » lorsqu'une politique de détection principale est activée. Pour l'instant, cela signifie qu'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 n'a pas de stratégie de détection principale activée, elle est « à risque » même si une stratégie de sauvegarde et de snapshot est activée.

**Nouveau volume ajouté, mais n'apparaît pas encore** Si vous avez ajouté un nouveau volume à votre environnement, relancez la découverte et appliquez des politiques de protection pour protéger ce nouveau volume.

## Politiques de protection

**Les politiques de résilience aux ransomwares coexistent-elles 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. Ainsi, la sauvegarde et la récupération ainsi que la résilience aux ransomwares partagent des politiques de sauvegarde.

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

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

Les politiques suivantes sont requises dans la stratégie de protection contre les ransomwares :

- Politique de détection des ransomwares
- Politique d'instantané

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

**Ransomware Resilience est-il conscient des paramètres de protection définis dans NetApp ONTAP?**

Oui, Ransomware Resilience découvre les planifications de snapshots définies dans ONTAP et si ARP et FPolicy sont activés sur tous les volumes d'une charge de travail découverte. Les informations que vous voyez initialement dans le tableau de bord sont agrégées à partir d'autres solutions et produits NetApp .

**Ransomware Resilience est-il au courant des 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.

**Pouvez-vous 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 à partir d' ONTAP (déjà activées dans System Manager 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 vous être inscrit à Ransomware Resilience ?**

Ransomware Resilience reconnaît toutes les nouvelles politiques créées dans Backup and Recovery ou SnapCenter.

**Pouvez-vous modifier les politiques d' 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.

**Pouvez-vous désactiver les politiques ?**

Vous pouvez désactiver ARP dans les stratégies de détection à l'aide de l'interface utilisateur du gestionnaire système, des API ou de la CLI.

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

## Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.