Documentation sur la protection contre les ransomwares BlueXP

BlueXP ransomware protection

NetApp
March 22, 2024

Sommaire

Documentation sur la protection contre les ransomwares BlueXP

Notes de version : découvrez les nouveautés de la protection contre les ransomwares BlueXP

Découvrez les nouveautés de la présentation de la protection contre les ransomwares BlueXP.

5 mars 2024

Cette version préliminaire de la protection contre les ransomwares BlueXP inclut les mises à jour suivantes :

- **Gestion des stratégies de protection** : outre l'utilisation de stratégies prédéfinies, vous pouvez désormais créer, modifier et supprimer des stratégies. "En savoir plus sur la gestion des règles".
- **Immuabilité sur le stockage secondaire (DataLock)** : vous pouvez maintenant rendre la sauvegarde immuable dans le stockage secondaire en utilisant la technologie NetApp DataLock dans le magasin d'objets. "En savoir plus sur la création de règles de protection".
- **Sauvegarde automatique vers 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".
- **Fonctions supplémentaires pour enquêter sur les attaques potentielles**: Vous pouvez maintenant afficher plus 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. Désormais, vous pouvez restaurer volume par volume, tous les volumes d'une charge de travail, voire quelques fichiers du volume, le tout dans un seul workflow. "En savoir plus sur la restauration suite à une attaque par ransomware (après la neutralisation des incidents)".

"Découvrez la protection contre les ransomwares BlueXP".

6 octobre 2023

Le service de protection contre les ransomwares BlueXP est une solution SaaS qui protège vos données, détecte les attaques et vous permet de restaurer vos données suite à une attaque par ransomware.

Pour la version préliminaire, le service protège les workloads applicatifs d'Oracle, de MySQL, de datastores de machine virtuelle et de partages de fichiers sur un stockage NAS sur site ainsi que Cloud Volumes ONTAP sur AWS (à l'aide du protocole NFS) sur tous les comptes BlueXP et sauvegarde les données dans un stockage cloud Amazon Web Services.

Le service de protection contre les ransomwares BlueXP permet d'exploiter pleinement plusieurs technologies NetApp. Votre administrateur de la sécurité des données ou votre ingénieur en opérations de sécurité peut ainsi atteindre les objectifs suivants :

- Consultez rapidement la protection contre les ransomwares sur tous vos workloads.
- Obtenez des recommandations sur la protection contre les ransomwares
- Améliorez votre protection en vous appuyant sur les recommandations de BlueXP pour la protection contre les ransomwares.
- Appliquez des règles de protection contre les ransomwares pour protéger vos principaux workloads et les données à haut risque contre les attaques par ransomware.

- Surveillez l’état de vos workloads contre les attaques par ransomware à la recherche d’anomalies des données.
- Évaluez rapidement l’impact des incidents de ransomware sur votre workload.
- Restaurez intelligemment les données après des incidents de ransomware en vous assurant qu’elles ne sont pas réinfectées par les données stockées.

"Découvrez la protection contre les ransomwares BlueXP".

Commencez

Découvrez la présentation de la protection contre les ransomwares BlueXP

Les attaques par ransomware peuvent bloquer l'accès à vos systèmes et à vos données, et les pirates peuvent demander une rançon en échange de la publication des données ou du décryptage. Selon l'IDC, il n'est pas rare que les victimes d'un ransomware se trouvent plusieurs attaques. L'attaque peut interrompre l'accès à vos données entre un jour et plusieurs semaines.

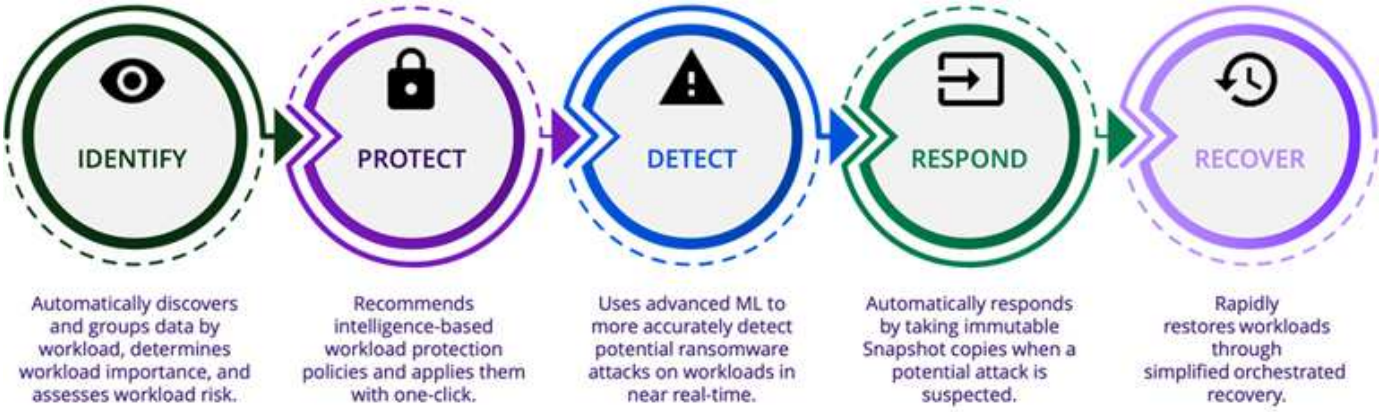
La protection contre les ransomwares BlueXP est un service d'orchestration pour la protection contre les ransomwares, la détection et la restauration. Pour la version de prévisualisation, le service protège les charges de travail basées sur les applications d'Oracle, de MySQL, de datastores de machines virtuelles, et partages de fichiers sur un stockage NAS sur site et sur Cloud Volumes ONTAP dans Amazon Web Services (à l'aide du protocole NFS) dans l'ensemble des comptes BlueXP, et sauvegardes des données dans le stockage cloud Amazon Web Services ou NetApp StorageGRID.

CETTE DOCUMENTATION EST FOURNIE SOUS FORME D'APERÇU TECHNOLOGIQUE. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Les possibilités de la protection BlueXP contre les ransomware

Le service de protection contre les ransomwares BlueXP permet d'exploiter pleinement plusieurs technologies NetApp. Votre administrateur du stockage, votre administrateur de la sécurité des données ou votre ingénieur en opérations de sécurité peuvent ainsi atteindre les objectifs suivants :

- **Identifiez** tous les workloads applicatifs, de partage de fichiers ou gérés par VMware dans NetApp NAS sur site avec les environnements de travail NFS dans BlueXP, entre les comptes BlueXP, les espaces de travail et les connecteurs BlueXP. Il catégorise ensuite la priorité des données et fournit des recommandations d'amélioration de la protection contre les ransomware.
- **Protégez** vos charges de travail en activant les sauvegardes et les copies Snapshot sur vos données.
- **Détectez** anomalies qui pourraient être des attaques par ransomware.
- **Répondre** aux attaques par ransomware potentielles en lançant automatiquement une copie Snapshot NetApp ONTAP.
- **Récupérez** vos charges de travail qui accélèrent la disponibilité des charges de travail grâce à l'orchestration de plusieurs technologies NetApp. Vous pouvez choisir de restaurer des volumes, des dossiers ou des fichiers spécifiques. Le service fournit des recommandations sur les meilleures options.



Avantages de l'utilisation de la protection contre les ransomware BlueXP

La protection contre les ransomwares BlueXP offre les avantages suivants :

- Découvre les workloads et les datasets, analyse la priorité en fonction de l'indice d'utilisation et classe leur importance relative.
- Évaluez votre stratégie de protection contre les ransomwares et affichez-la dans un tableau de bord facile à comprendre.
- Fournit des recommandations sur les étapes suivantes basées sur la découverte et l'analyse des postures de protection.
- Vous pouvez appliquer les recommandations de protection des données basées sur l'IA ou le ML en un clic.
- Protège les données des principaux workloads basés sur les applications, tels que MySQL, Oracle, les datastores VMware et les partages de fichiers.
- Détection des attaques par ransomware visant les données en temps réel sur le stockage primaire à l'aide de la technologie d'IA
- Lancement d'actions automatisées en réponse à des attaques potentielles détectées grâce à la création de copies Snapshot et à l'envoi d'alertes en cas d'activité anormale
- Récupération adaptée pour respecter les politiques de RPO La protection contre les ransomwares BlueXP orchestre la restauration en cas d'incidents de ransomware à l'aide de plusieurs services de restauration NetApp, notamment la sauvegarde et la restauration BlueXP (anciennement Cloud Backup).

Le coût

NetApp ne vous facture pas pour l'utilisation de la version préliminaire de la protection contre les ransomwares BlueXP.

Licences

La préversion de la protection contre les ransomware BlueXP elle-même ne nécessite aucune licence spéciale. Toutes les licences d'aperçu sont des licences d'évaluation.

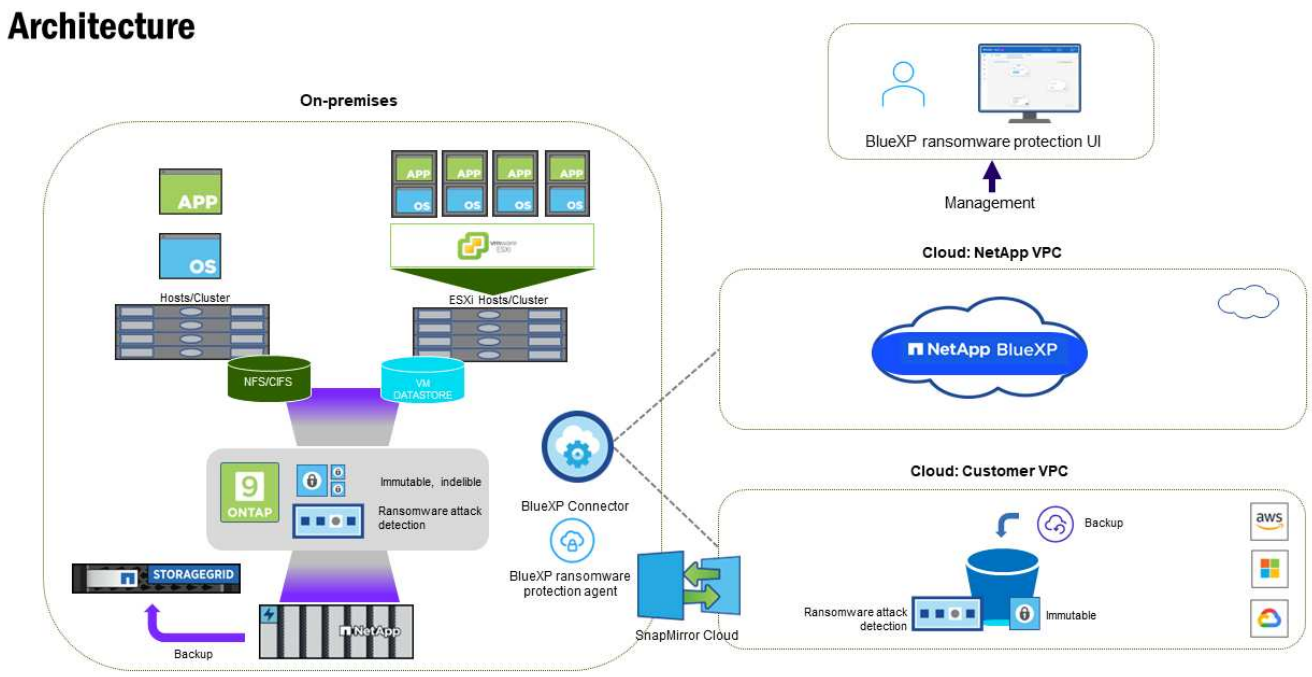
Pour la version de prévisualisation, NetApp vous aide à configurer l'évaluation et les licences requises.

La prévisualisation de la protection contre les ransomware BlueXP nécessite les licences suivantes :

- ONTAP
- Technologie de protection anti-ransomware autonome de NetApp. Reportez-vous à la section "Présentation de la protection autonome contre les ransomwares" pour plus d'informations.
- Service de sauvegarde et de restauration BlueXP

Fonctionnement de la protection BlueXP contre les ransomware

À un niveau élevé, la protection contre les ransomwares BlueXP fonctionne comme ça.



Fonction	Description
IDENTIFIER	• Recherche toutes les données NAS (montages NFS) sur site du client connectées à BlueXP. • Identifie les données des clients à partir des API de service ONTAP et les associe à des workloads. En savoir plus sur "ONTAP" et "Logiciel SnapCenter". • Découvre le niveau de protection actuel de chaque volume des copies Snapshot NetApp, les règles de sauvegarde et les fonctionnalités de détection intégrées. Le service associe ensuite cette stratégie de protection aux workloads à l'aide de la sauvegarde et de la restauration BlueXP, de BlueXP Digital Advisor, des services ONTAP et des technologies NetApp, telles que la protection anti-ransomware autonome, FPolicy, les règles de sauvegarde et les règles Snapshot. En savoir plus sur "Protection autonome contre les ransomwares" et "Sauvegarde et restauration BlueXP", "Conseiller digital BlueXP", et "ONTAP FPolicy". • Attribue une priorité commerciale à chaque charge de travail en fonction des niveaux de protection automatiquement découverts et recommande des règles pour les charges de travail en fonction de leurs priorités. • La protection contre les ransomwares apprend également les associations de règles et recommande vos règles personnalisées pour des charges de travail similaires.
PROTÉGER	• Surveille activement les workloads et orchestre l'utilisation de la sauvegarde et de la restauration BlueXP et des API ONTAP en appliquant des règles à chacun des workloads identifiés.
DÉTECTER	• Détecte les attaques potentielles à l'aide d'un modèle de machine learning intégré qui détecte les activités et le chiffrement potentiellement anormaux. • Cette fonctionnalité propose une détection double couche, qui commence par détecter les attaques par ransomware potentielles dans le stockage primaire et répondre aux activités anormales avec des copies Snapshot automatisées supplémentaires qui créent les points de restauration de données les plus proches. Ce service permet d'approfondir l'identification des attaques potentielles avec plus de précision sans affecter les performances des principaux workloads. • Déterminez les fichiers suspects spécifiques et mappent cette attaque aux workloads associés à l'aide de ONTAP, de la protection anti-ransomware autonome et des technologies FPolicy.
RÉPONDRE	• Affiche les données pertinentes, telles que l'activité des fichiers, l'activité des utilisateurs et l'entropie, pour vous aider à mener à bien les analyses d'attaque. • Initie des copies Snapshot rapides à l'aide des technologies et produits NetApp tels que ONTAP, la protection anti-ransomware autonome et FPolicy.
RÉCUPÉRER	• Détermine le meilleur Snapshot ou sauvegarde et recommande le meilleur point de restauration réel (RPA) à l'aide des technologies de sauvegarde et de restauration BlueXP, de ONTAP, de protection anti-ransomware autonome et des services et technologies FPolicy. • Orchestre la restauration des workloads, y compris les machines virtuelles, les partages de fichiers et les bases de données avec cohérence des applications.

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

Utilisez l'aperçu de la protection contre les ransomwares BlueXP pour découvrir comment vos données sont résilientes face à une cyberattaque sur les types de cibles de sauvegarde, d'environnements de travail et de sources de données suivants :

Cibles de sauvegarde prises en charge

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Environnements de travail pris en charge

- NAS ONTAP sur site (utilisant le protocole NFS)
- ONTAP Select
- Cloud Volumes ONTAP dans AWS (via le protocole NFS)

Sources de données

Pour la version Preview, le service protège les charges de travail basées sur les applications suivantes :

- Partages de fichiers NetApp
- Les datastores VMware
- Bases de données (pour la version preview, Oracle et MySQL)

Des conditions qui peuvent vous aider à protéger vos données contre les ransomwares

Pour en savoir plus sur la terminologie relative à la protection contre les ransomwares,

- **Protection** : la protection dans BlueXP contre les ransomware signifie que les snapshots et les sauvegardes immuables s'effectuent sur une base régulière vers un domaine de sécurité différent à l'aide de politiques de protection.
- **Charge de travail** : dans la version préliminaire de la protection contre les ransomwares BlueXP, une charge de travail peut inclure des bases de données MySQL ou Oracle, des datastores VMware ou des partages de fichiers.

Protection BlueXP contre les ransomware requise

Commencez à utiliser la protection contre les ransomwares BlueXP en vérifiant le niveau de préparation de votre environnement opérationnel, de votre connexion, de votre accès réseau et de votre navigateur Web.

Pour utiliser la version d'aperçu de la protection contre les ransomwares BlueXP, vous devez disposer des conditions préalables suivantes :

- Un compte dans NetApp StorageGRID ou AWS S3 pour les cibles de sauvegarde et les autorisations d'accès définies

  Reportez-vous à la "Liste d'autorisations AWS" pour plus d'informations.

- ONTAP 9.11.1 et versions ultérieures
  - Autorisations ONTAP de l'administrateur du cluster
  - Une licence pour la protection anti-ransomware autonome de NetApp, utilisée par la protection anti-ransomware BlueXP, activée sur l'instance ONTAP sur site, selon la version de ONTAP que vous utilisez. Reportez-vous à la section "Présentation de la protection autonome contre les ransomwares".

    Pour plus d'informations sur les licences, reportez-vous à la section "Découvrez la protection contre les ransomwares BlueXP".

- Dans BlueXP :
  - Un connecteur BlueXP pour chaque cloud privé virtuel (VPC) ou une région sur site doit être configuré dans BlueXP. Reportez-vous à la section "Documentation BlueXP pour configurer le connecteur".

    > Si vous disposez de plusieurs connecteurs BlueXP, le service analyse les données entre tous les connecteurs au-delà de celui qui s'affiche actuellement dans l'interface utilisateur BlueXP.

  - Service de sauvegarde et de restauration BlueXP avec sauvegarde activée dans l'environnement de travail
  - Un environnement de travail BlueXP avec le stockage sur site NetApp NAS
  - Un compte BlueXP avec au moins un connecteur actif connecté aux clusters ONTAP sur site. Tous les environnements source et de travail doivent se trouver sur le même compte BlueXP.
  - Un compte utilisateur BlueXP avec des privilèges d'administrateur de compte pour la découverte des ressources
  - "Exigences standard de BlueXP"

Démarrage rapide de la protection contre les ransomware BlueXP

Voici les étapes à suivre pour démarrer avec la protection BlueXP contre les ransomwares. Les liens de chaque étape vous mènent à une page qui fournit plus de détails.

1 Passer en revue les prérequis

"Assurez-vous que votre environnement répond à ces exigences".

2 Configurez le service de protection contre les ransomwares

- "Préparez NetApp StorageGRID ou Amazon Web Services en tant que destination de sauvegarde".
- "Configurez un connecteur dans BlueXP".
- "Configurer les destinations de sauvegarde".
- "Découvrez les workloads dans BlueXP".

3 Et la suite ?

Après avoir configuré le service, voici ce que vous pourriez faire ensuite.

- "Consultez l'état de la protection des workloads dans le tableau de bord".
- "Protégez les workloads".
- "Répondez à la détection des attaques par ransomware potentielles".
- "Récupérer après une attaque (après neutralisation des incidents)".

Configurez la protection BlueXP contre les ransomware

Pour configurer la protection contre les ransomwares BlueXP, effectuez quelques étapes.

Avant de commencer, consultez "prérequis" pour vous assurer que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez l'une des destinations de sauvegarde suivantes :

- NetApp StorageGRID
- Amazon Web Services

Une fois que vous avez configuré les options de la destination de sauvegarde elle-même, vous la configurez ultérieurement en tant que destination de sauvegarde dans le service de protection contre les ransomwares BlueXP.

Préparez StorageGRID à devenir une destination de sauvegarde

Si vous souhaitez utiliser StorageGRID comme destination de sauvegarde, reportez-vous à la section "Documentation StorageGRID" Pour plus d'informations sur StorageGRID.

Préparez AWS à devenir une destination de sauvegarde

- Configuration d'un compte dans AWS.
- Configurer "Autorisations AWS" Dans AWS.

Pour en savoir plus sur la gestion de votre stockage AWS dans BlueXP, consultez la section "Gestion de vos compartiments Amazon S3".

Configurez BlueXP

L'étape suivante consiste à configurer BlueXP et le service de protection contre les ransomwares BlueXP.

Révision "Exigences standard de BlueXP".

Créez un connecteur dans BlueXP

Contactez votre ingénieur commercial NetApp pour essayer ce service. Ensuite, lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service de protection contre les ransomware.

Pour créer un connecteur dans BlueXP avant d'utiliser le service, reportez-vous à la documentation BlueXP qui décrit "Comment créer un connecteur BlueXP".

Si vous disposez de plusieurs connecteurs BlueXP, le service analyse les données entre tous les connecteurs au-delà de celui qui s'affiche actuellement dans l'interface utilisateur BlueXP. Ce service détecte tous les espaces de travail et tous les connecteurs associés à ce compte.

Accédez à la protection BlueXP contre les ransomware

Vous utilisez NetApp BlueXP pour vous connecter au service de protection contre les ransomwares BlueXP. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

Pour plus de détails, reportez-vous à "Accédez à la protection BlueXP contre les ransomware".

Configurez les destinations de sauvegarde dans la protection contre les ransomwares BlueXP

Utilisez l'option BlueXP ransomware protection backup destinations pour configurer les destinations de sauvegarde. Pour plus de détails, reportez-vous à "Configurer les options de paramètres".

Accédez à la protection BlueXP contre les ransomware

Vous utilisez NetApp BlueXP pour vous connecter au service de protection contre les ransomwares BlueXP.

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

Étapes

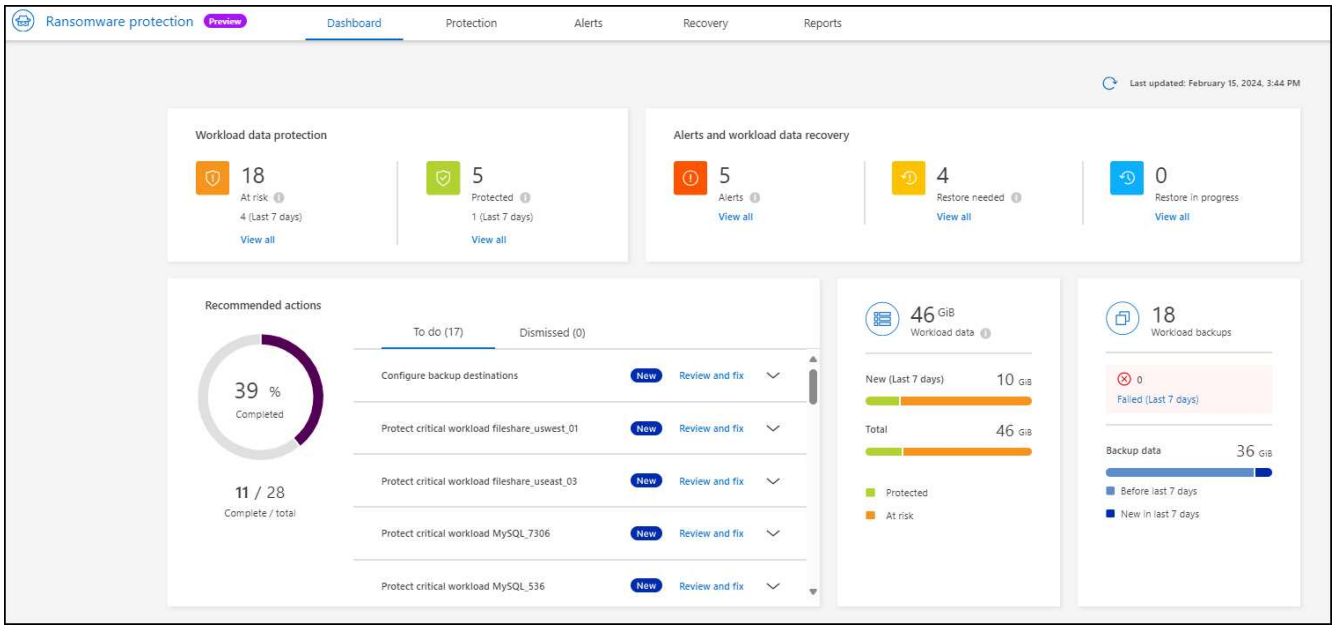
1. Ouvrez un navigateur Web et accédez au "Console BlueXP".

   La page de connexion NetApp BlueXP s'affiche.

2. Connectez-vous à BlueXP.
3. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

   S'il s'agit de votre première connexion à ce service, la page d'accueil s'affiche.

   Sinon, le tableau de bord de protection BlueXP contre les ransomwares s'affiche.



4. Commencez à utiliser le service.
   - Si vous ne disposez pas d'un connecteur BlueXP ou que ce n'est pas le cas pour cette présentation, vous devrez peut-être contacter le support NetApp ou suivre les messages pour vous inscrire à cette présentation.
   - Si vous découvrez BlueXP et n'avez utilisé aucun connecteur, lorsque vous sélectionnez « * protection contre les ransomware * », un message s'affiche pour vous inscrire. Envoyez le formulaire. NetApp vous contactera au sujet de votre demande d'évaluation.
   - Si vous utilisez BlueXP avec un connecteur existant, lorsque vous sélectionnez "**protection contre les ransomware**", un message s'affiche pour vous inscrire.
   - Si vous participez déjà à l'aperçu, lorsque vous sélectionnez "**protection contre les ransomware**", vous pouvez continuer avec le service. Si vous ne l'avez pas déjà fait, vous devez sélectionner l'option **découvrir les charges de travail**.

Découvrez les workloads dans la solution de protection BlueXP contre les ransomwares

Pour utiliser la protection contre les ransomwares BlueXP, le service doit d'abord détecter les données. Pendant la découverte, la protection contre les ransomwares BlueXP analyse tous les volumes et fichiers des environnements de travail sur tous les connecteurs BlueXP et espaces de travail d'un compte.

Pour la version préliminaire, la protection contre les ransomwares BlueXP évalue les applications MySQL, les applications Oracle, les datastores VMware et les partages de fichiers.

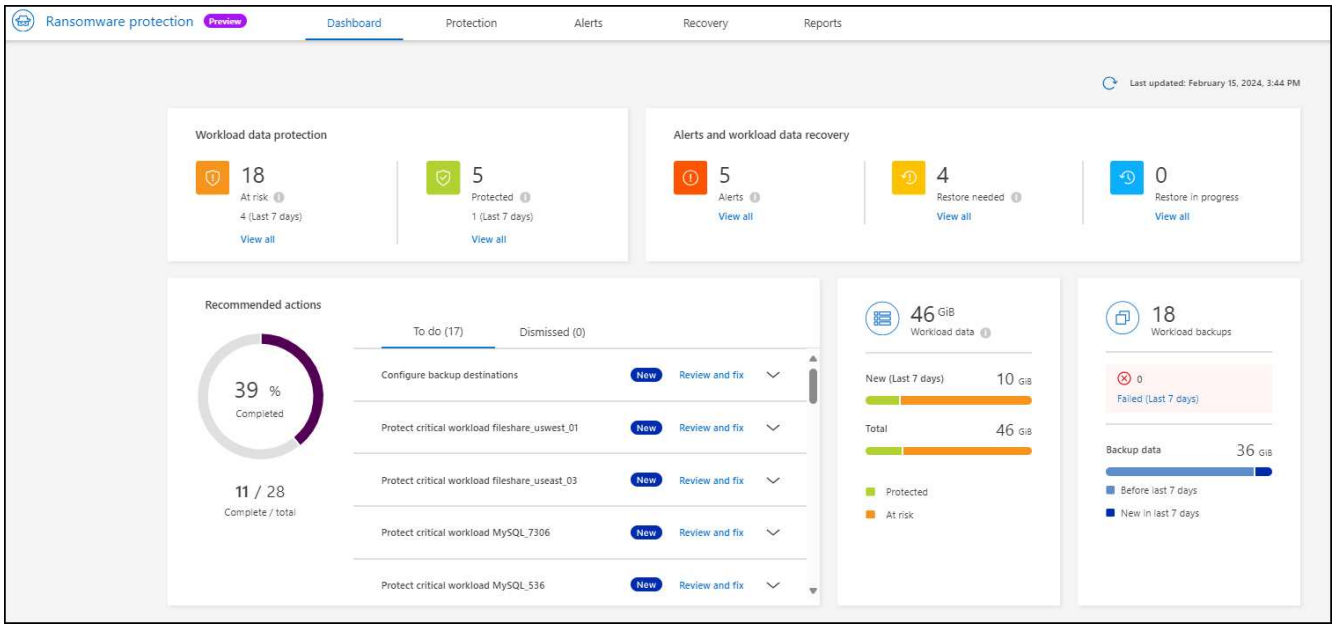
Le service évalue le niveau de protection existant, notamment la protection de sauvegarde actuelle, les copies Snapshot et les options de protection anti-ransomware autonome de NetApp. En fonction de l'évaluation, le service recommande ensuite comment améliorer la protection contre les ransomwares.

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

2. Sélectionnez **découvrir les charges de travail** sur la page d'accueil initiale.

   Le service détecte les données du workload et affiche l'état de santé de la protection des données dans le tableau de bord.



Configurez les paramètres de protection contre les ransomwares BlueXP

Vous pouvez configurer une destination de sauvegarde en consultant les recommandations du tableau de bord.

Ajouter une destination de sauvegarde

La protection contre les ransomwares BlueXP permet d'identifier les workloads qui ne disposent pas encore de sauvegardes, ainsi que les workloads pour lesquels aucune destination de sauvegarde n'est attribuée.

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
- Services Web Amazon (AWS)

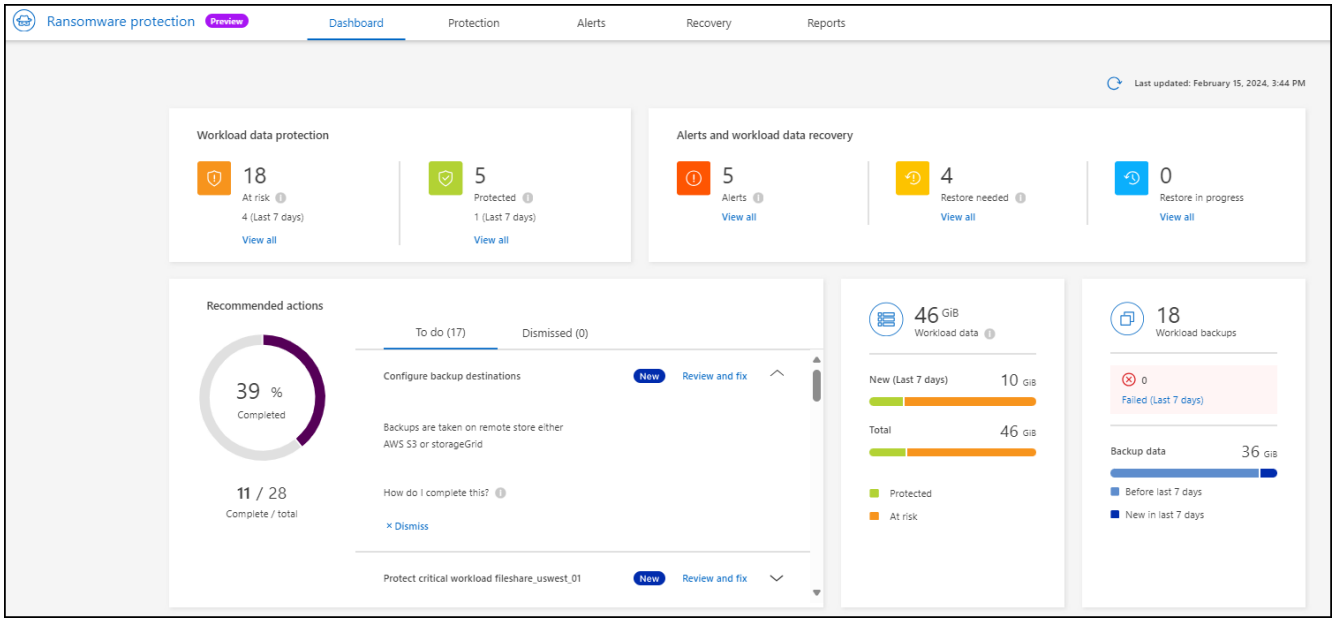
Vous pouvez ajouter une destination de sauvegarde en fonction d'une action recommandée dans le tableau de bord.

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

Le tableau de bord fournit de nombreuses recommandations. Il peut être recommandé de configurer une destination de sauvegarde.

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.
2. Vérifiez le volet actions recommandées du tableau de bord.

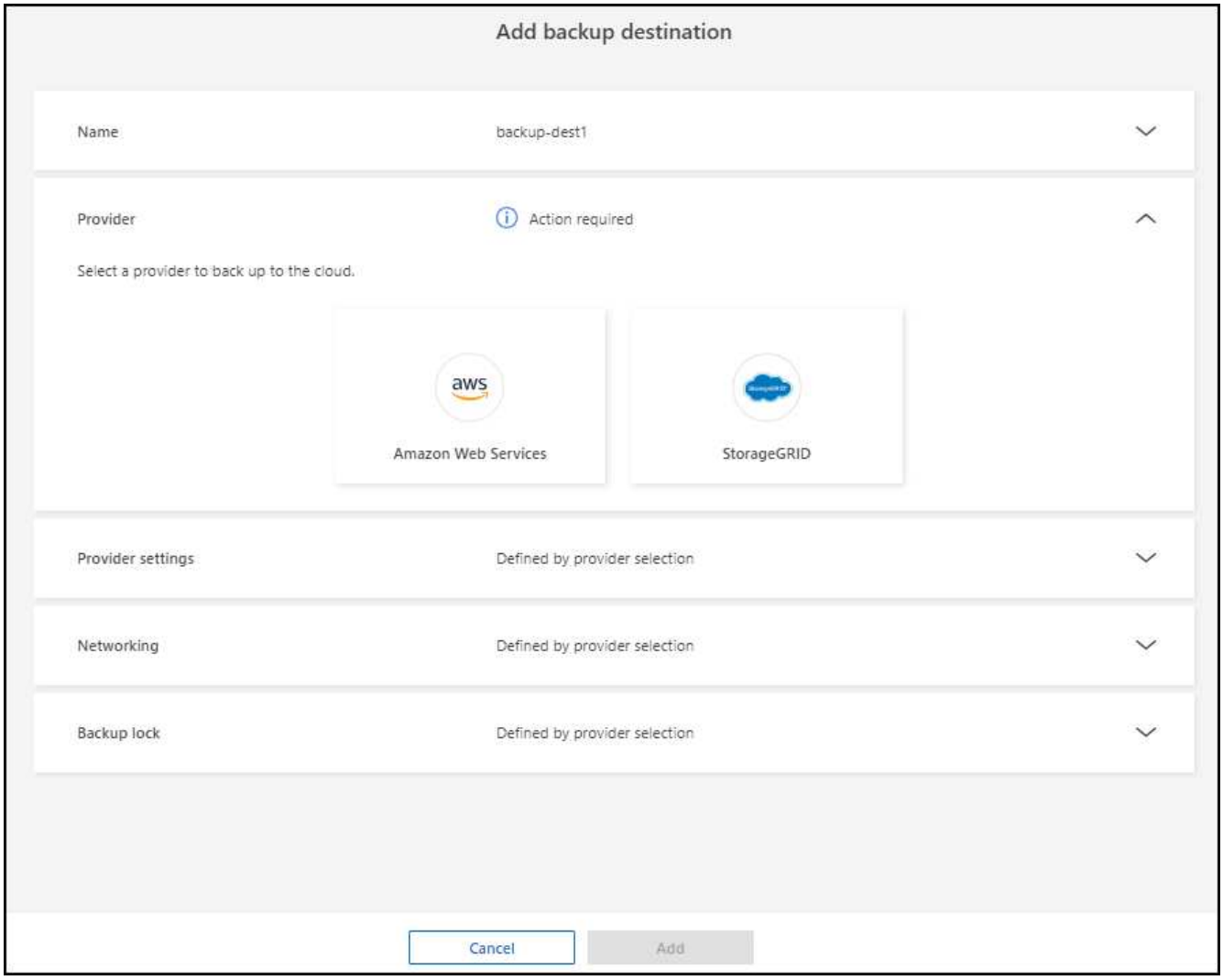


3. Dans le tableau de bord, sélectionnez **revoir et corriger** pour la recommandation de "configurer les destinations de sauvegarde".
4. Suivez les instructions en fonction du fournisseur de sauvegarde.

Ajouter StorageGRID comme destination de sauvegarde

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

1. Sur 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 en regard de chaque paramètre et entrez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur** :
     - Créez un nouveau compartiment ou utilisez votre propre compartiment pour stocker les sauvegardes.
     - Nœud de passerelle StorageGRID Nom de domaine complet, port, clé d'accès StorageGRID et informations d'identification de clé secrète.
   - **Mise en réseau** : choisissez l'IPspace.
     - L'IPspace est le cluster où résident les volumes à sauvegarder. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
   - **Verrou de sauvegarde** : choisissez si vous souhaitez que le service protège les sauvegardes contre la modification ou la 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 de 14 jours maximum.

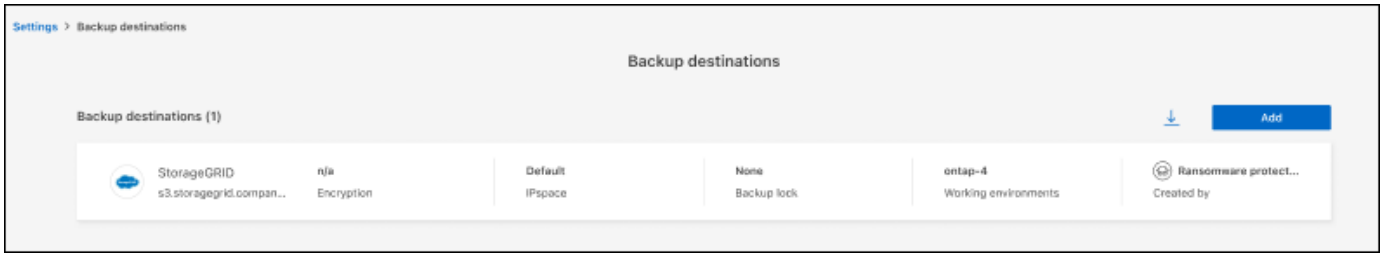
> Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pouvez pas le modifier ultérieurement après la configuration de la destination de sauvegarde.

- **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.

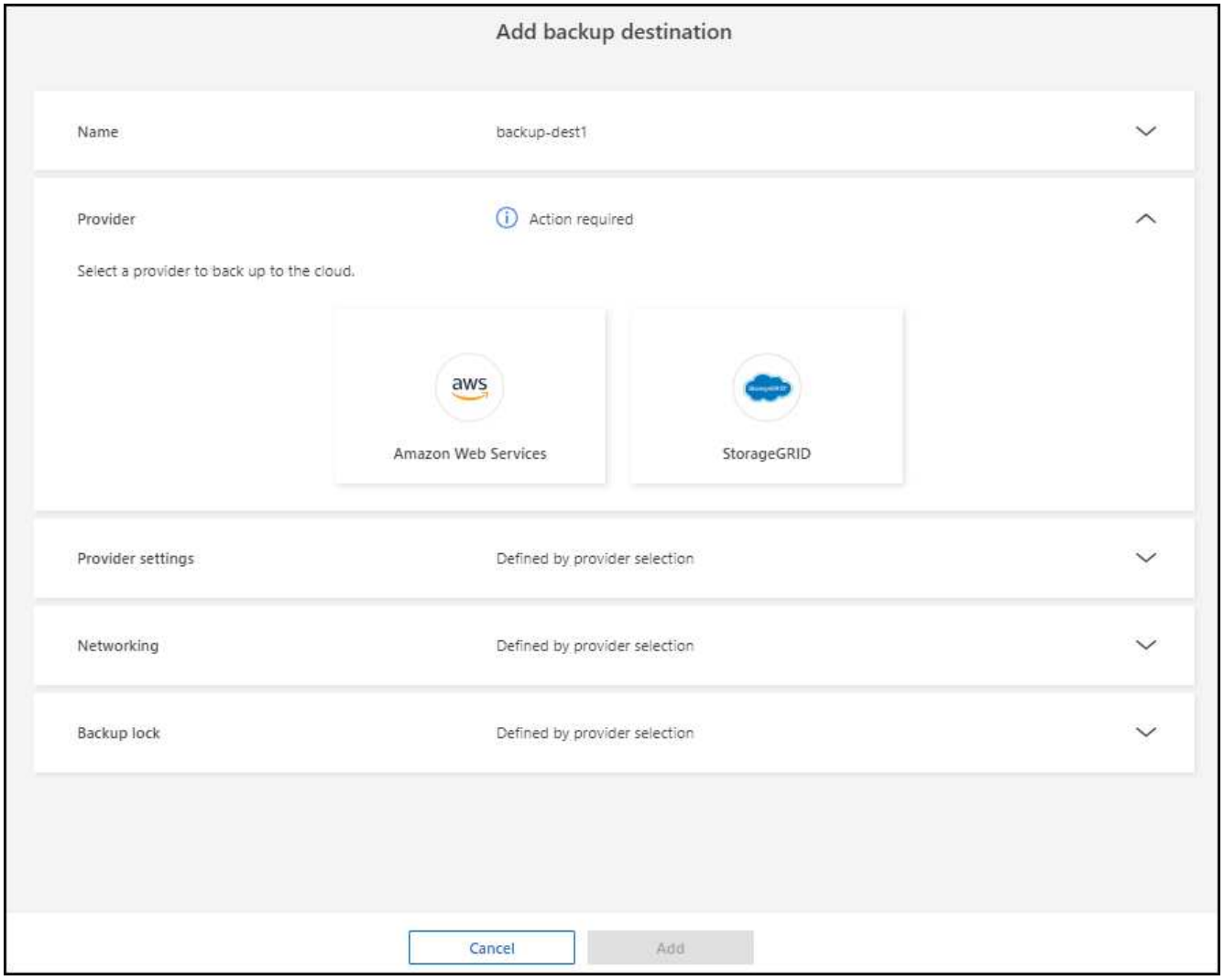


Ajoutez Amazon Web Services comme destination de sauvegarde

Pour configurer AWS en tant que destination de sauvegarde, entrez les informations suivantes.

Pour en savoir plus sur la gestion de votre stockage AWS dans BlueXP, consultez la section "Gestion de vos compartiments Amazon S3".

1. Sur 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 en regard de chaque paramètre et entrez ou sélectionnez des valeurs :
   - **Paramètres du fournisseur** :
     - Créez un nouveau compartiment, sélectionnez un compartiment existant s'il en existe déjà dans BlueXP, ou utilisez votre propre compartiment pour stocker les sauvegardes.
     - Compte AWS, région, clé d'accès et clé secrète pour les identifiants AWS

       "Pour ajouter votre propre compartiment, reportez-vous à la section Ajout de compartiments S3".
   - **Encryption** : si vous créez un nouveau compartiment S3, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Si vous avez choisi un compartiment existant, les informations de chiffrement sont déjà disponibles.

     Les données qui se trouvent dans le compartiment sont chiffrées avec des clés gérées par AWS par défaut. Vous pouvez continuer à utiliser des clés gérées par AWS ou gérer le chiffrement de vos données à l'aide de vos propres clés.
   - **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé.
     - L'IPspace est le cluster où résident les volumes à sauvegarder. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.

- Vous pouvez également choisir d'utiliser un terminal privé AWS (PrivateLink) que vous avez configuré précédemment.

  Pour utiliser AWS PrivateLink, reportez-vous à la section "AWS PrivateLink pour Amazon S3".

- **Verrou de sauvegarde** : choisissez si vous souhaitez que le service protège les sauvegardes contre la modification ou la 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 de 14 jours maximum.

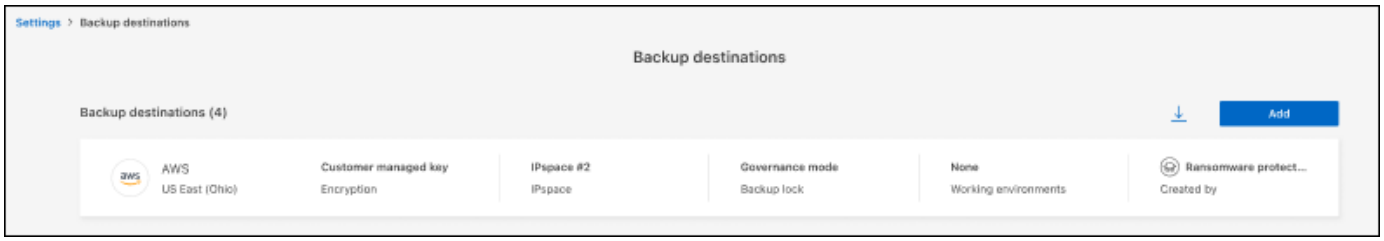
  Si vous configurez le paramètre de verrouillage de sauvegarde maintenant, vous ne pouvez pas le modifier ultérieurement après la configuration de la destination de sauvegarde.

  - **Mode 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.



Forum aux questions sur la protection contre les ransomwares BlueXP

Cette FAQ peut vous aider si vous cherchez juste une réponse rapide à une question.

L'accès

Quelle est l'URL de protection contre les ransomware BlueXP ?
Pour l'URL, dans un navigateur, entrez : "https://console.bluexp.netapp.com/" Pour accéder à la console BlueXP.

Avez-vous besoin d'une licence pour utiliser la protection contre les ransomware BlueXP ?
Aucun fichier de licence NetApp n'est requis. La préversion de la protection contre les ransomware BlueXP elle-même ne nécessite aucune licence spéciale. Toutes les licences d'aperçu sont des licences d'évaluation.

La version préliminaire de ce service nécessite une licence du service de sauvegarde et de restauration BlueXP.

Pour la version de prévisualisation, NetApp vous aide à configurer l'évaluation et les licences requises.

Comment activez-vous la protection contre les ransomware BlueXP ?
La protection contre les ransomwares BlueXP ne nécessite aucune activation. L'option de protection contre les ransomware est automatiquement activée dans le menu de navigation gauche de BlueXP.

Pour obtenir la version préliminaire, vous devez vous inscrire ou contacter votre ingénieur commercial NetApp pour essayer ce service. Ensuite, lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service.

La protection BlueXP contre les ransomware est-elle disponible en modes standard, restreint et privé ?
Pour l'instant, la protection contre les ransomwares BlueXP n'est disponible qu'en mode standard. Restez à l'affût de tout.

Pour plus d'informations sur ces modes dans tous les services BlueXP, reportez-vous à la section "Modes de déploiement BlueXP".

Comment les autorisations d'accès sont-elles gérées?
Seuls les administrateurs de comptes ont la possibilité de lancer le service et de découvrir les workloads (car cela implique de s'engager à utiliser une ressource). Les interactions suivantes peuvent être effectuées par n'importe quel rôle.

Quelle est la meilleure résolution de périphérique?
La résolution recommandée pour la protection contre les ransomwares BlueXP est de 1920 x 1080 ou supérieure.

Quel navigateur dois-je utiliser?
N'importe quel navigateur moderne fonctionnera.

Interaction avec d'autres services

La protection contre les ransomware BlueXP est-elle consciente des paramètres de protection créés dans NetApp ONTAP ?
Oui, la protection contre les ransomware BlueXP découvre les calendriers Snapshot définis dans ONTAP.

Si vous avez défini une stratégie à l'aide de la protection contre les ransomware BlueXP, devez-vous apporter des modifications futures uniquement dans ce service ?
Nous vous recommandons de modifier les règles à partir du service de protection contre les ransomwares BlueXP.

Charges de travail

Qu'est-ce qui constitue une charge de travail?
Une charge de travail inclut tous les volumes utilisés par une seule instance d'application. Par exemple, une instance de base de données Oracle 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 de cette instance spécifique de l'instance Oracle DB.

Comment la protection par ransomware BlueXP hiérarchise-t-elle les données de workload ?
La priorité des données pour la version d'aperçu dépend des copies Snapshot effectuées et des sauvegardes planifiées.

La priorité de la charge de travail est déterminée par les fréquences Snapshot suivantes :

- **Critique** : copies Snapshot prises moins de 1 par heure (planning de protection extrêmement agressif)
- **Important** : copies snapshot prises moins de 1 par jour mais supérieures à 1 par heure
- **Standard**: Copies snapshot prises plus de 1 par jour

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

Le tableau de bord n'affiche pas toutes mes charges de travail. Qu'est-ce qui pourrait se passer?
Actuellement, seuls les volumes NFS sont pris en charge. Les volumes iSCSI, les volumes CIFS et les autres configurations non prises en charge sont filtrés et n'apparaissent pas dans le tableau de bord.

Règles de protection

Les politiques de ransomware de BlueXP coexistent-elles avec les autres types de politiques de workloads ?
À ce stade, la sauvegarde et la restauration BlueXP (Cloud Backup) prennent en charge une règle de sauvegarde par volume. Ainsi, la sauvegarde et la restauration BlueXP ainsi que la protection contre les ransomwares BlueXP partagent les politiques de sauvegarde.

Les copies Snapshot ne sont pas limitées et peuvent être ajoutées séparément pour chaque service.

Utilisez la protection BlueXP contre les ransomwares

Utilisez la protection BlueXP contre les ransomwares

Avec la protection BlueXP contre les ransomwares, vous pouvez consulter l'état des workloads et les protéger.

- "Découvrez les workloads dans la solution de protection BlueXP contre les ransomwares".
- "Affichez la protection et l'état des workloads dans le tableau de bord".
  - Analysez et agissez sur les recommandations de protection contre les ransomware.
- "Protégez les workloads":
  - Attribuez une stratégie de protection contre les ransomwares à vos workloads.
  - Renforcez la protection de vos applications pour prévenir les attaques par ransomware futures.
  - Créez, modifiez ou supprimez une règle de protection.
- "Répondez à la détection des attaques par ransomware potentielles".
- "Récupérer après une attaque" (après neutralisation des incidents).
- "Configurer les paramètres de protection".

Consultez rapidement l'état des workloads à l'aide du tableau de bord

Le tableau de bord de protection contre les ransomwares BlueXP fournit des informations d'un coup d'œil sur l'état de la protection de vos workloads. Vous pouvez identifier rapidement les workloads à risque ou protégés, identifier les workloads impactés par un incident ou par la restauration, et évaluer l'étendue de la protection en examinant la quantité de stockage protégée ou en péril.

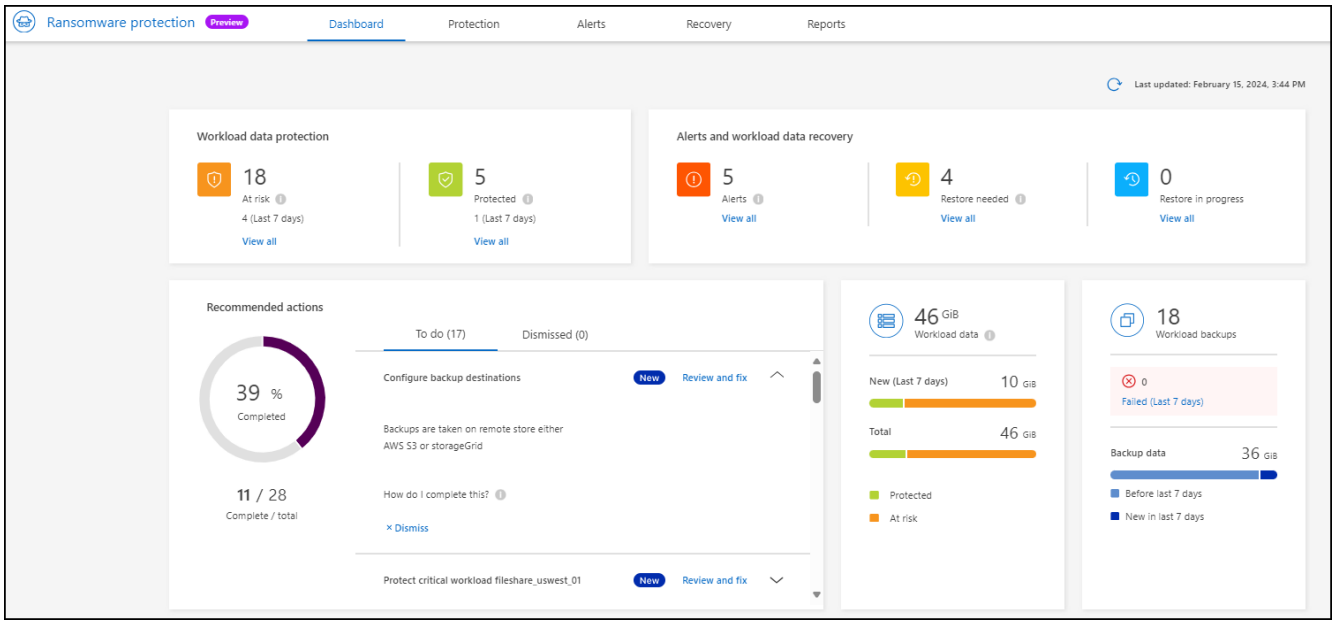
Vous pouvez également utiliser le tableau de bord pour examiner les recommandations de protection et agir en conséquence.

Vérifiez l'état du workload à l'aide du tableau de bord

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.

   Après la découverte, le tableau de bord indique l'état de santé de la protection des données des workloads.



2. Dans chacun de ces volets, vous pouvez afficher et effectuer l'une des opérations suivantes :

   - **Protection des données de charge de travail** : cliquez sur **Afficher tout** pour voir toutes les charges de travail qui sont à risque ou protégées sur la page protection. Les charges de travail sont menacées lorsque les niveaux de protection ne correspondent pas à une règle de protection. Reportez-vous à la section "Protégez les workloads".
   - **Alertes et récupération des données de charge de travail** : cliquez **Afficher tout** pour voir les incidents actifs qui ont affecté votre charge de travail, sont prêts pour la récupération après que les incidents sont neutralisés ou sont en cours de récupération. Reportez-vous à la section "Répondre à une alerte détectée".

     Un incident est classé dans l'un des États suivants :

     - Impacté (s'affiche sur la page alertes)
     - Prêt pour la restauration (voir la page récupération)
     - Récupération (s'affiche sur la page récupération)
     - Échec de la restauration (s'affiche sur la page récupération)
     - Récupéré (affiché sur la page récupération)
   - **Actions recommandées** : pour augmenter la protection, examinez chaque recommandation et cliquez sur **revoir et corriger**.

     Reportez-vous à la section "Passez en revue les recommandations de protection sur le tableau de bord" ou "Protégez les workloads".

     Toutes les recommandations ajoutées depuis la dernière visite du tableau de bord sont indiquées par « Nouveau » pendant au moins 24 heures. Les actions sont répertoriées par ordre de priorité, les plus importantes étant affichées en haut. Vous pouvez examiner et agir sur chacun d'eux ou le rejeter.

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

   - **Données sur la charge de travail** : surveiller les changements dans la couverture de protection au cours des 7 derniers jours.
   - **Sauvegardes de charge de travail** : surveillez les modifications des sauvegardes de charge de travail

créées par le service qui ont échoué ou qui ont réussi au cours des 7 derniers jours.

Passez en revue les recommandations de protection sur le tableau de bord

La protection contre les ransomwares BlueXP évalue la protection de vos workloads et recommande des mesures pour améliorer cette protection.

Vous pouvez revoir une recommandation et agir sur celle-ci, ce qui fait passer l'état de la recommandation sur terminé. Ou, si vous voulez agir plus tard, vous pouvez le rejeter. Le rejet d'une action déplace la recommandation vers une liste d'actions rejetées, que vous pouvez examiner ultérieurement.

Voici un échantillon des recommandations que le service offre.

Recommandation	Description	Comment résoudre le problème
Ajoutez une règle de protection contre les ransomwares	La charge de travail n'est actuellement pas protégée.	Attribuez une stratégie à la charge de travail. Reportez-vous à la section "Protégez vos workloads contre les attaques par ransomware".
Configurer les destinations de sauvegarde	Le workload ne possède actuellement aucune destination de sauvegarde.	Ajoutez des destinations de sauvegarde à ce workload pour le protéger. Reportez-vous à la section "Configurer les paramètres de protection".
Renforcer la politique.	Certaines charges de travail ne bénéficient peut-être pas d'une protection suffisante. Renforcer la protection des charges de travail à l'aide d'une règle	Augmentez la conservation, ajoutez des sauvegardes, appliquez des sauvegardes immuables, bloquez les extensions de fichiers suspectes, activez la détection sur le stockage secondaire et plus encore. Reportez-vous à la section "Protégez vos workloads contre les attaques par ransomware".
Protégez les workloads applicatifs stratégiques ou importants contre les ransomwares.	La page protéger affiche les charges de travail d'application critiques ou importantes (selon le niveau de priorité attribué) qui ne sont pas protégées.	Attribuez une règle à ces charges de travail. Reportez-vous à la section "Protégez vos workloads contre les attaques par ransomware".
Protégez les workloads stratégiques ou importants de partage de fichiers contre les ransomwares.	La page protection affiche les charges de travail critiques ou importantes de type partage de fichiers ou datastore qui ne sont pas protégées.	Attribuez une stratégie à chacun des workloads. Reportez-vous à la section "Protégez vos workloads contre les attaques par ransomware".
Passez en revue les nouvelles alertes	De nouvelles alertes existent.	Passez en revue les nouvelles alertes. Reportez-vous à la section "Répondez à la détection d'une alerte par ransomware".

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.
2. Dans le volet actions recommandées, sélectionnez une recommandation et sélectionnez **revoir et corriger**.
3. Pour annuler l'action jusqu'à plus tard, sélectionnez **rejeter**.

   La recommandation disparaît de la liste des tâches et apparaît sur la liste des tâches rejetées.

   Vous pouvez ensuite modifier un élément rejeté en un élément à faire. Lorsque vous marquez un élément terminé ou que vous modifiez un élément rejeté en une action à faire, le nombre total d'actions augmente de 1.

4. Pour revoir les informations sur la façon d'agir sur les recommandations, sélectionnez l'icône **information**.

Protégez vos workloads contre les attaques par ransomware

Vous pouvez protéger vos workloads contre les attaques par ransomware en effectuant les actions suivantes à l'aide de la protection BlueXP.

- Afficher la protection des charges de travail existantes.
- Attribuez une stratégie à une charge de travail.
  - Renforcez la protection des applications pour éviter les attaques de réinscriptibles futures.
  - Modifier la protection d'une charge de travail précédemment protégée dans le service RW.
- Gérer les stratégies (uniquement celles que vous avez créées).

La protection contre les ransomwares BlueXP attribue une priorité à chaque workload lors de la découverte. La priorité de la charge de travail est déterminée par les fréquences Snapshot suivantes :

- **Critique** : copies Snapshot prises moins de 1 par heure (planning de protection extrêmement agressif)
- **Important** : copies snapshot prises moins de 1 par jour mais supérieures à 1 par heure
- **Standard**: Copies snapshot prises plus de 1 par jour

Etat de protection : une charge de travail peut afficher l'un des États de protection suivants pour indiquer si une règle est appliquée ou non :

- **Protégé** : une politique est appliquée.
- **À risque**: Aucune politique n'est appliquée.
- **En cours**: Une politique est appliquée mais pas encore terminée.
- **Échec** : une politique est appliquée mais ne fonctionne pas.

Protection de la santé : une charge de travail peut avoir l'un des États de protection de la santé suivants :

- **Healthy** : la protection est activée pour la charge de travail et des sauvegardes et des copies Snapshot ont été effectuées.
- **En cours** : des sauvegardes ou des copies Snapshot sont en cours.

- **Échec** : les sauvegardes ou les copies Snapshot ne se sont pas terminées avec succès.
- **N/A** : la protection n'est pas activée ou suffisante sur la charge de travail.

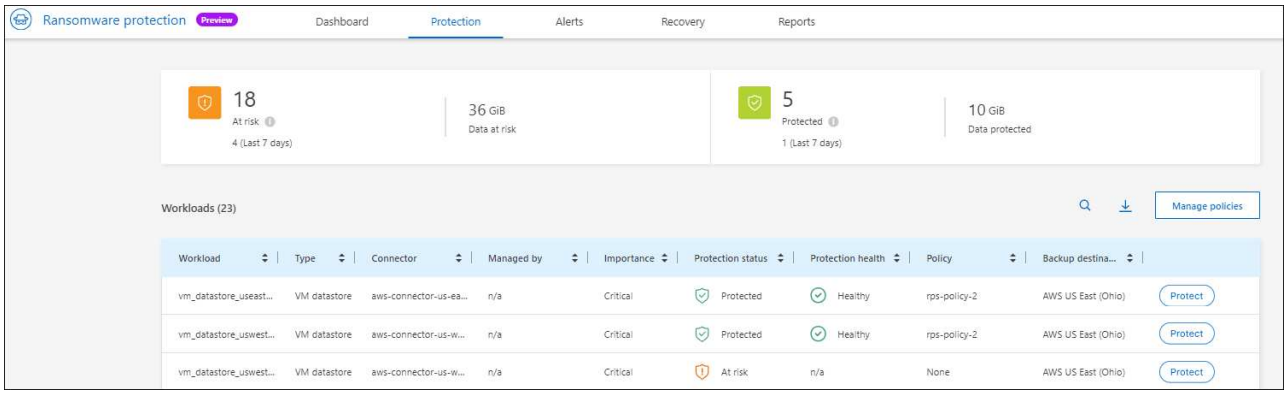
Découvrir la protection des workloads contre les ransomwares

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

- Workloads de VM
- Workloads de partage de fichiers

Étapes

1. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection** > **protection contre les ransomware**.
2. Effectuez l'une des opérations suivantes :
   - Dans le volet protection des données du tableau de bord, sélectionnez **Afficher tout**.
   - Dans le menu, sélectionnez **protection**.



3. À partir de cette page, vous pouvez attribuer une stratégie à une charge de travail.

Attribuez une règle de protection prédéfinie aux charges de travail

Pour vous aider à protéger vos données, vous pouvez attribuer une stratégie de protection contre les ransomwares à un ou plusieurs workloads. Vous pouvez également attribuer une stratégie différente à une charge de travail qui possède déjà une stratégie.

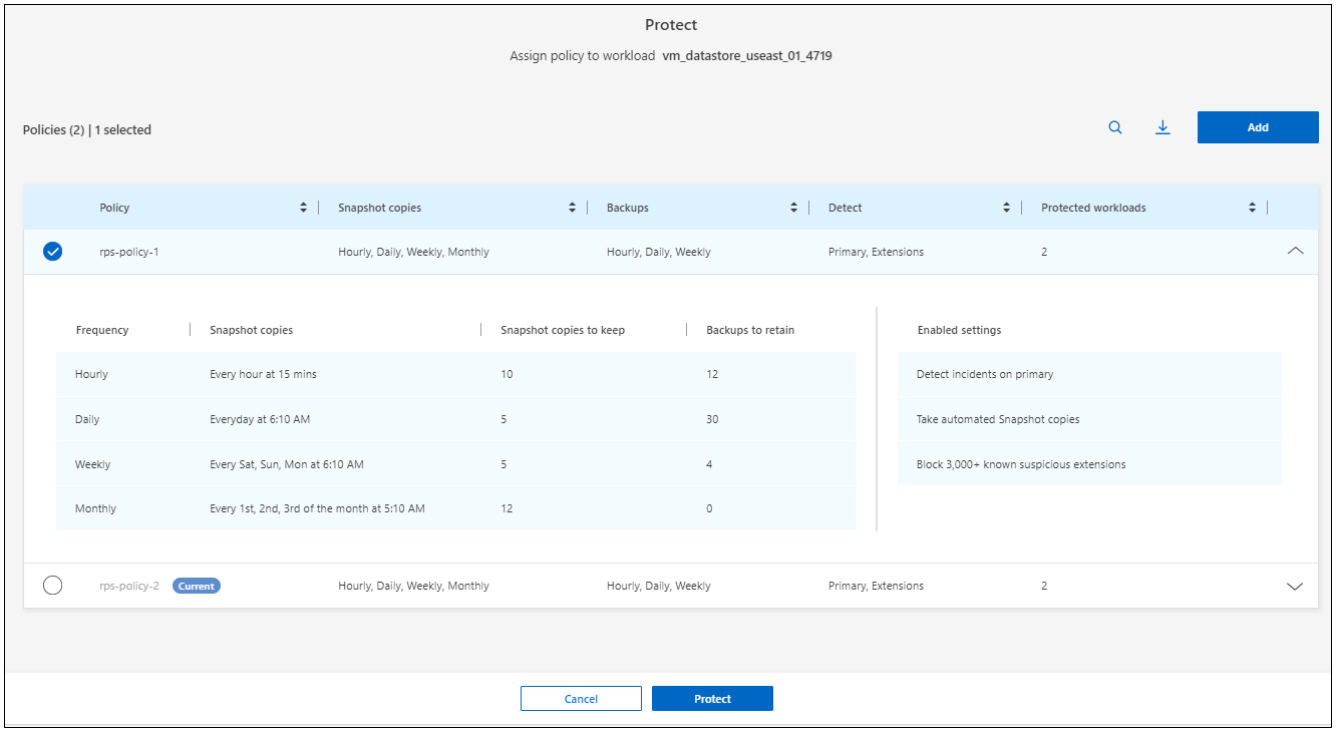
La protection contre les ransomwares BlueXP inclut les règles prédéfinies suivantes qui correspondent à la priorité des workloads :

Niveau des règles	Snapshot	Fréquence	Conservation (jours)	Nombre de copies Snapshot	Nombre maximal de copies Snapshot
Politique de la charge de travail critique	Quart horaire	Toutes les 15 minutes	3	288	309
	Tous les jours	Tous les jours	14	14	309
	Hebdomadaire	Toutes les 1 semaine	35	5	309
	Tous les mois	Tous les 30 jours	60	2	309
Politique importante de la charge de travail	Quart horaire	Toutes les 30 minutes	3	144	165
	Tous les jours	Tous les jours	14	14	165
	Hebdomadaire	Toutes les 1 semaine	35	5	165
	Tous les mois	Tous les 30 jours	60	2	165
Politique standard de la charge de travail	Quart horaire	Toutes les 60 minutes	3	72	93
	Tous les jours	Tous les jours	14	14	93
	Hebdomadaire	Toutes les 1 semaine	35	5	93
	Tous les mois	Tous les 30 jours	60	2	93

Étapes

1. À partir de la protection contre les ransomwares BlueXP, effectuez l'une des opérations suivantes :
   - Dans le volet protection des données du tableau de bord, sélectionnez **Afficher tout**.
   - Dans le volet recommandations du tableau de bord, sélectionnez une recommandation concernant l'attribution d'une stratégie et sélectionnez **revoir et corriger**.
   - Dans le menu, sélectionnez **protection**.
2. Dans la page protection, examinez les charges de travail et sélectionnez **Protect** en regard de la charge de travail.

   Une liste de stratégies s'affiche.



3. Pour afficher les détails, cliquez sur la flèche vers le bas d'une stratégie.
4. Sélectionnez une stratégie à affecter à la charge de travail.
5. Sélectionnez **protéger**.
6. Consultez le volet actions recommandées du tableau de bord, qui affiche l'action comme « terminée ».

Créer une règle de protection

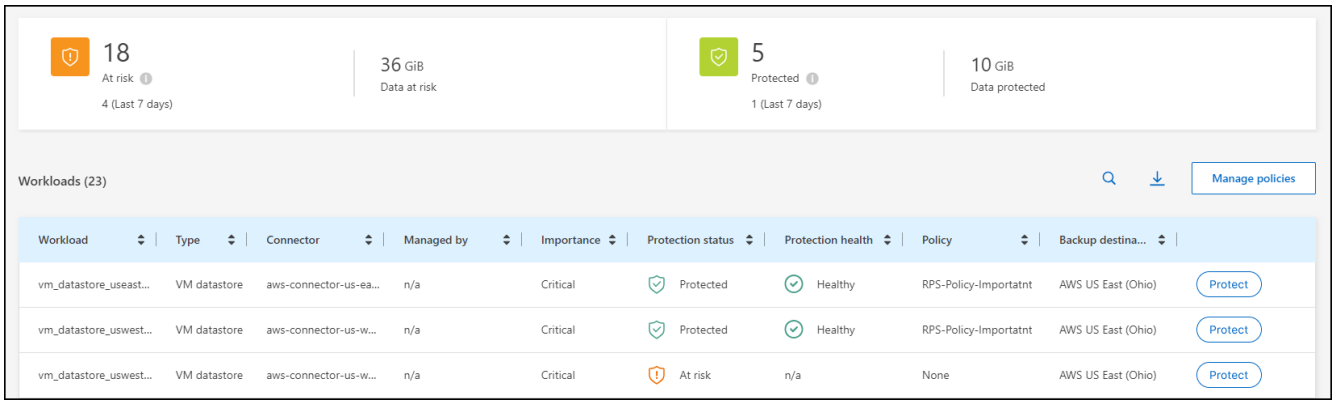
Si les règles existantes ne répondent pas aux besoins de votre entreprise, vous pouvez créer une nouvelle règle de protection. Vous pouvez créer votre propre stratégie à partir de zéro ou utiliser une stratégie existante et modifier ses paramètres.

Vous pouvez créer des règles qui régissent le stockage primaire et secondaire et traiter le stockage primaire et secondaire de la même manière ou différemment.

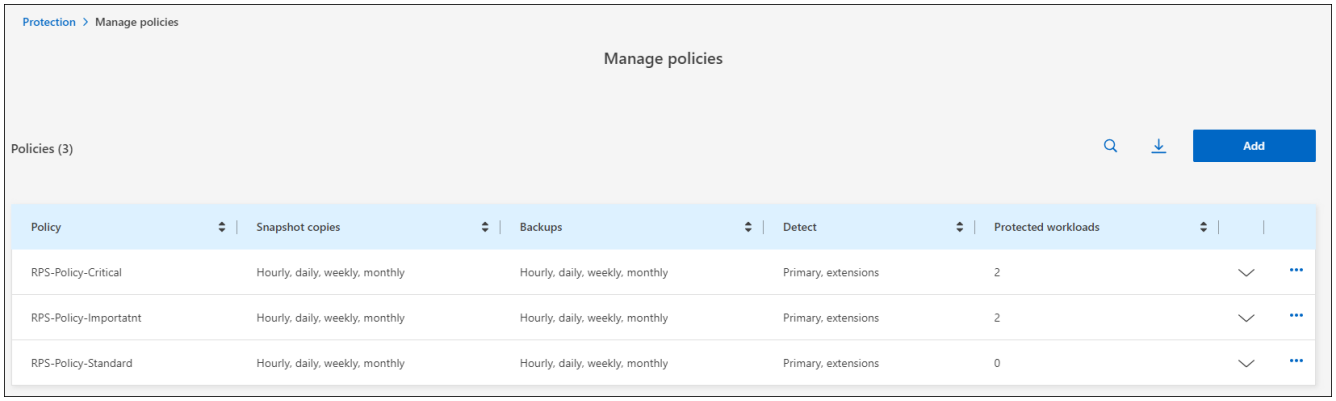
Vous pouvez créer une règle lorsque vous les gérez ou lors du processus d'attribution d'une règle à une charge de travail.

Étapes de création d'une stratégie pendant la gestion des règles

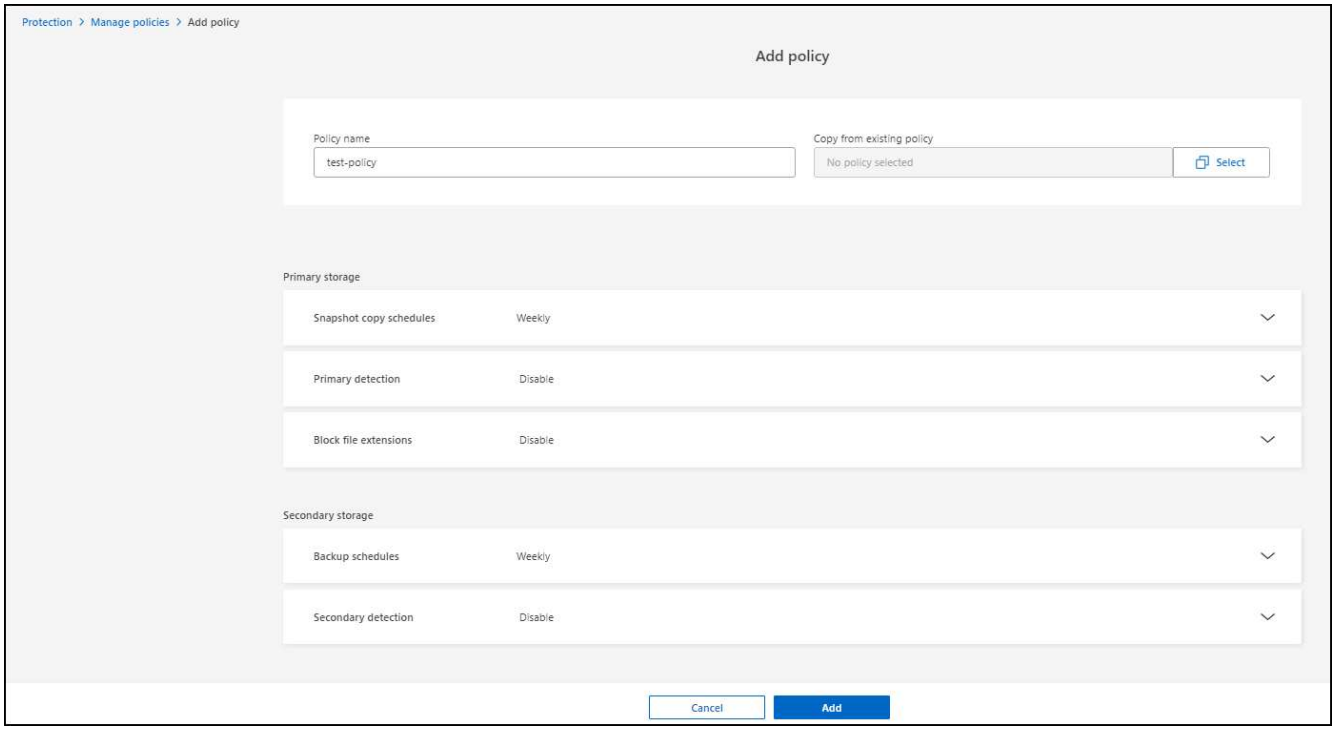
1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.



2. Dans la page protection, sélectionnez **gérer les stratégies**.



3. Sur la page gérer les stratégies, sélectionnez **Ajouter**.



4. Entrez un nouveau nom de stratégie ou un nom de stratégie existant pour le copier. Si vous entrez un nom de stratégie existant, choisissez la stratégie à copier.

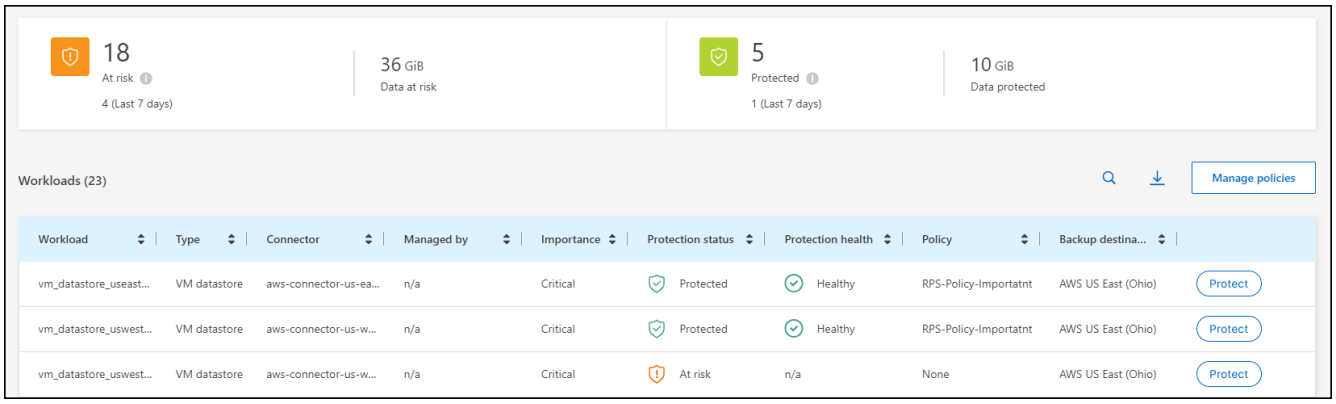
Si vous choisissez de copier et de modifier une stratégie existante, vous devez modifier au moins un paramètre pour la rendre unique.

5. Pour chaque élément, sélectionnez la flèche vers le bas.
   - **Stockage primaire** :
     - **Plannings de copie Snapshot** : choisissez les options de planification, le nombre de copies Snapshot à conserver et sélectionnez pour activer la planification.
     - **Détection primaire** : permet au service de détecter les incidents de ransomware sur le stockage primaire.
     - **Bloquer les extensions de fichier** : activez cette option pour que le bloc de service ait des extensions de fichier suspectes connues. Le service effectue des copies Snapshot automatisées lorsque la détection primaire est activée.
   - **Stockage secondaire** :
     - **Plannings de sauvegarde** : choisissez des options de planification pour le stockage secondaire et activez le planning.
     - **Détection secondaire** : activez le service pour détecter les incidents de ransomware sur le stockage secondaire.
     - **Verrouiller les sauvegardes** : choisissez cette option pour empêcher la modification ou la suppression des sauvegardes sur le stockage secondaire pendant une certaine période. On parle également de *stockage immuable*.

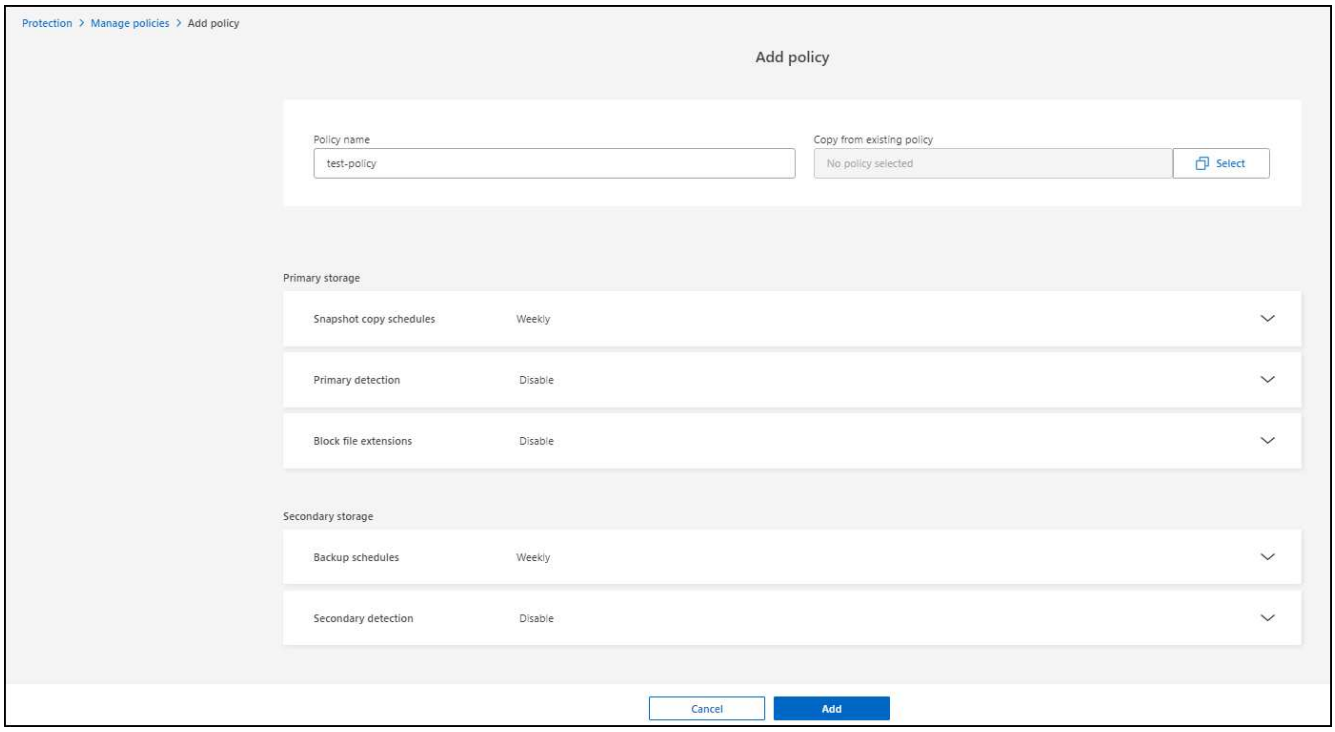
       Cette option utilise la technologie NetApp DataLock, qui verrouille les sauvegardes sur le stockage secondaire. La période pendant laquelle le fichier de sauvegarde est verrouillé (et conservé) est appelée période de rétention de DataLock. Elle est basée sur la planification de la stratégie de sauvegarde et le paramètre de conservation que vous avez définis, ainsi qu'une mémoire tampon de 14 jours. Toute stratégie de rétention DataLock inférieure à 30 jours est arrondie à 30 jours minimum.
6. Sélectionnez **Ajouter**.

Étapes de création d'une règle pendant l'affectation de la règle de protection

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.



2. Dans la page protection, sélectionnez **protéger**.
3. Dans la page protéger, sélectionnez **Ajouter**.



4. Terminez le processus, qui est identique à la création d'une stratégie à partir de la page gérer les stratégies.

Attribuez une autre stratégie de protection

Vous pouvez choisir une autre règle de protection pour une charge de travail.
Il est préférable d'augmenter la protection pour prévenir les attaques par ransomware à venir en modifiant la règle de protection.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protéger, sélectionnez une charge de travail et sélectionnez **protéger**.
3. Dans la page protéger, sélectionnez une stratégie différente pour la charge de travail.
4. Pour modifier les détails de la police, sélectionnez la flèche vers le bas à droite et modifiez les détails.
5. Sélectionnez **Enregistrer** pour terminer la modification.

Modifier une stratégie existante

Vous ne pouvez modifier les détails d'une règle que si elle n'est pas associée à une charge de travail.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez **gérer les stratégies**.
3. Dans la page gérer les stratégies, sélectionnez l'option **actions** pour la stratégie que vous souhaitez modifier.
4. Dans le menu actions, sélectionnez **Modifier la stratégie**.
5. Modifiez les détails.

6. Sélectionnez **Enregistrer** pour terminer la modification.

Supprimer une règle

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

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez **gérer les stratégies**.
3. Dans la page gérer les stratégies, sélectionnez l'option **actions** de la stratégie que vous souhaitez supprimer.
4. Dans le menu actions, sélectionnez **Supprimer la stratégie**.

Répondez à la détection d'une alerte par ransomware

Si la protection contre les ransomwares BlueXP détecte une attaque, une alerte s'affiche dans le tableau de bord de protection contre les ransomwares BlueXP et dans les notifications BlueXP en haut à droite indiquant une attaque potentielle par ransomware. Par ailleurs, le service initie immédiatement la création d'une copie Snapshot. À ce stade, vous devez examiner le risque potentiel dans l'onglet * alertes * de la protection contre les ransomwares BlueXP.

Pour commencer à restaurer vos données, cochez l'alerte comme étant prête pour la restauration afin que votre administrateur de stockage puisse commencer le processus de restauration.

Chaque alerte peut avoir plusieurs incidents sur des volumes différents avec des États différents. Veillez donc à examiner tous les incidents.

Le service fournit des informations appelées *Evidence* sur ce qui a provoqué l'émission de l'alerte, telles que :

- Les extensions de fichier ont été créées ou modifiées
- La création du fichier s'est produite et a augmenté d'un pourcentage répertorié
- La suppression du fichier s'est produite et a augmenté d'un pourcentage répertorié

Une alerte est basée sur les types de comportement suivants :

- **Attaque potentielle** : une alerte se produit lorsque la protection anti-ransomware autonome détecte une nouvelle extension et que l'occurrence est répétée plus de 20 fois au cours des 24 dernières 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 la déclarer comme une attaque.
  - Une entropie élevée est observée.
  - Les opérations de lecture/écriture/renommage/suppression de fichiers ont généré une augmentation de 100 % de l'activité au-delà de la base de données.

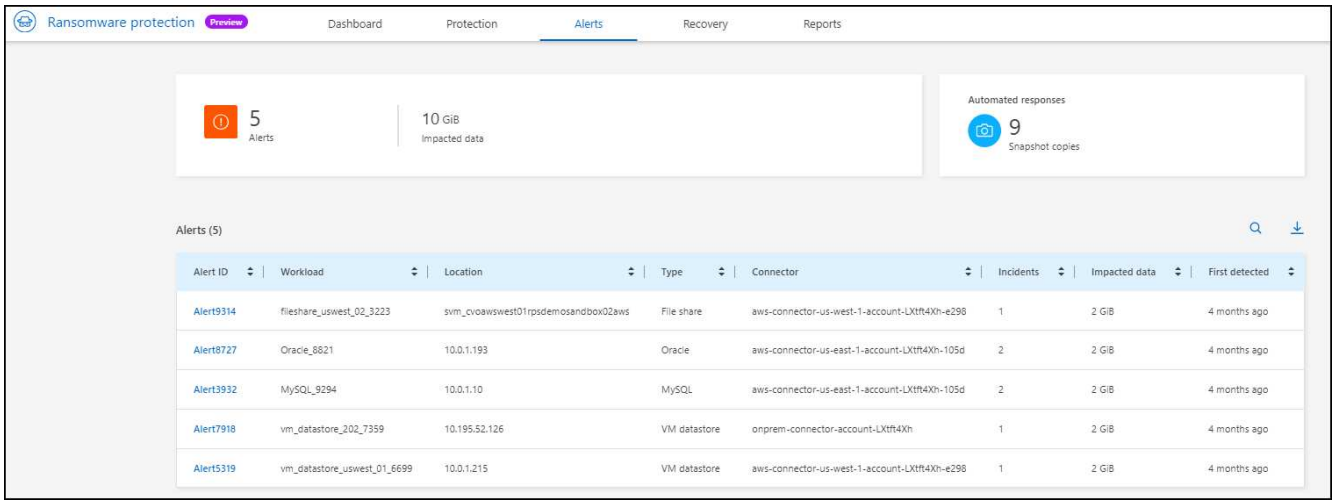
La preuve est basée sur des informations issues de la protection anti-ransomware autonome en ONTAP. Pour plus de détails, reportez-vous à "Présentation de la protection autonome contre les ransomwares".

Afficher les alertes

Vous pouvez accéder aux alertes à partir du tableau de bord de protection BlueXP contre les ransomware ou de l'onglet **alertes**.

Étapes

1. Dans le tableau de bord de protection contre les ransomwares BlueXP, consultez le volet alertes.
2. Sélectionnez **Afficher tout** sous l'une des statues.
3. Cliquez sur une alerte pour examiner tous les incidents sur chaque volume pour chaque alerte.
4. Pour consulter d'autres alertes, cliquez sur **Alert** dans le fil d'Ariane en haut à gauche.
5. Consultez les alertes sur la page alertes.



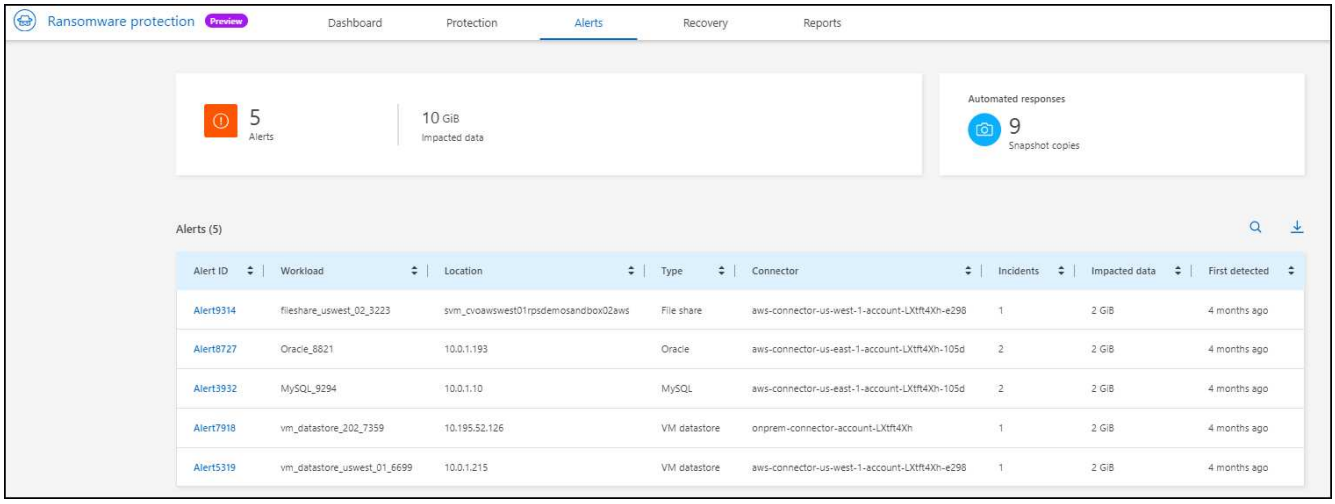
6. Passez à Marquer les incidents de ransomware comme prêts pour la restauration (après neutralisation des incidents).

Marquer les incidents de ransomware comme prêts pour la restauration (après neutralisation des incidents)

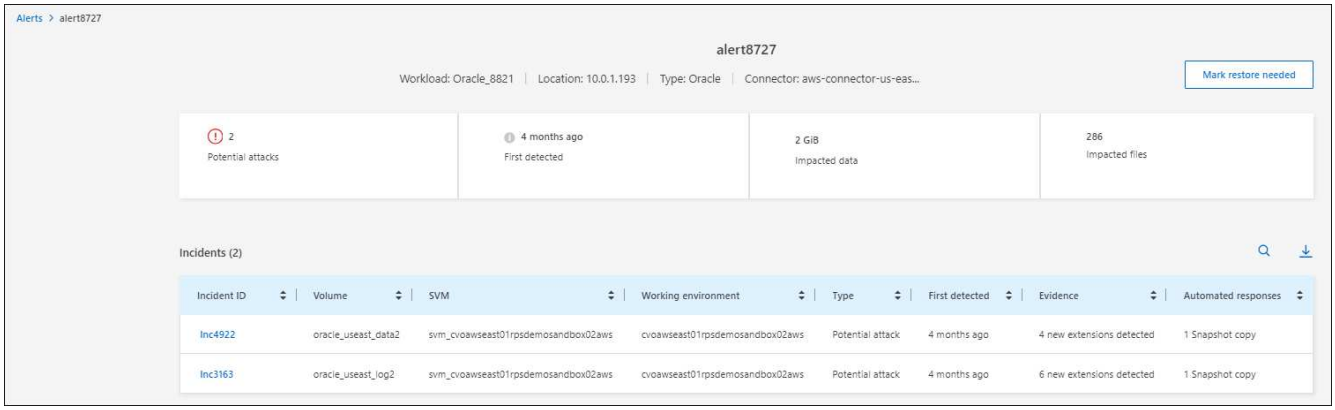
Une fois que vous avez atténué l'attaque et que vous êtes prêt à restaurer des charges de travail, vous devez communiquer avec l'équipe d'administration du stockage que les données sont prêtes pour la restauration afin qu'elles puissent démarrer le processus de restauration.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **Alerts**.



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



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

Résultat

Une fois l'alerte marquée pour la restauration, elle passe de l'onglet alertes à l'onglet récupération.

Récupération après une attaque par ransomware (après neutralisation des incidents)

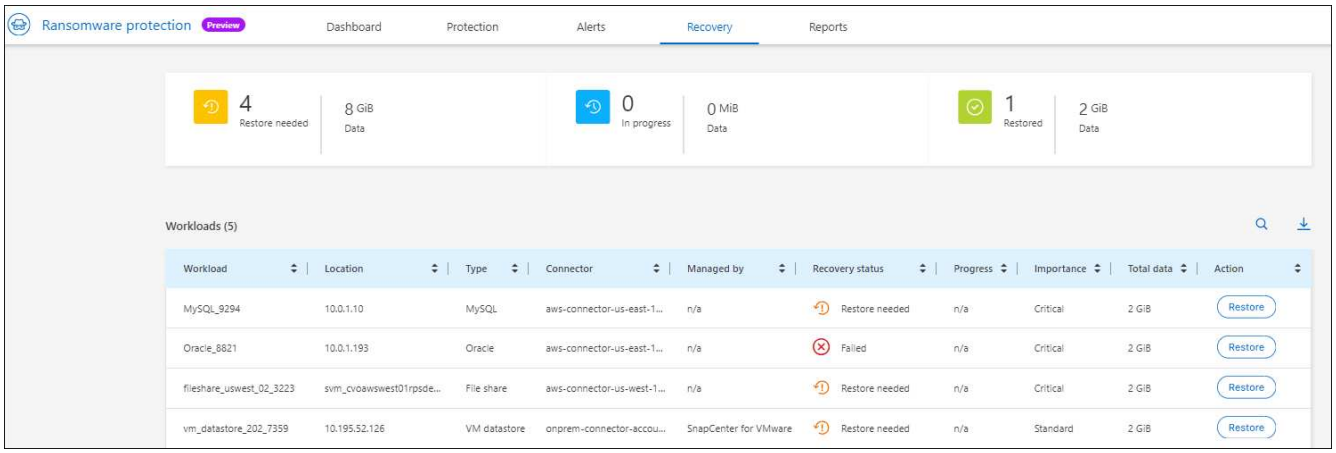
Une fois que les workloads ont été marqués comme « prêts pour la restauration », la protection contre les ransomwares BlueXP recommande une RPA (point de restauration réel) et orchestre le workflow pour une restauration résistante aux pannes.

Consultez les workloads prêts à être restaurés

Passez en revue les charges de travail dont l'état de restauration est « Restauration nécessaire ».

Étapes

1. Effectuez l'une des opérations suivantes :
   - Dans le tableau de bord, vérifiez les totaux « Restaurer les données requises » dans le volet alertes et sélectionnez **Afficher tout**.
   - Dans le menu, sélectionnez **récupération**.
2. Consultez les informations sur la charge de travail à la page **récupération**.



Récupération d'une charge de travail

Avec la protection contre les ransomwares BlueXP, l'administrateur du stockage peut déterminer la meilleure façon de restaurer les workloads à partir du point de restauration recommandé ou de son point de restauration préféré.

L'administrateur du stockage de sécurité peut restaurer les données à différents niveaux :

- Restaurer tous les volumes
- Restaurez une application au niveau du volume ou du fichier et du dossier.
- Restaurez un partage de fichiers au niveau du volume, du répertoire ou du fichier/dossier.
- Restaurez vos données à partir d'un datastore au niveau d'une VM.

Le processus diffère légèrement selon le type de charge de travail.

Étapes

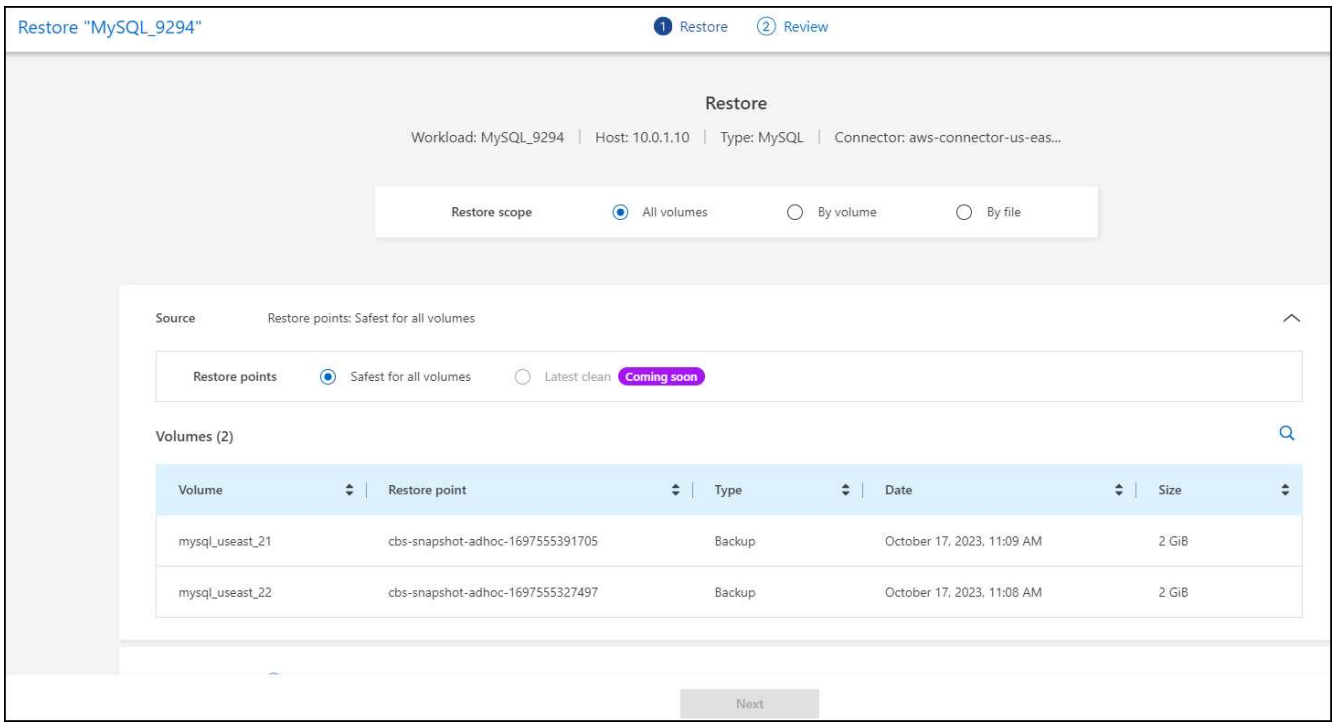
1. Dans le menu BlueXP ransomware protection, sélectionnez **Recovery**.
2. Consultez les informations sur la charge de travail à la page **récupération**.
3. Sélectionnez une charge de travail dont l'état est « Restauration requise ».
4. Pour restaurer, sélectionnez **Restaurer**.
5. **Domaine de restauration** : sélectionnez le type de restauration que vous souhaitez effectuer :
   - Tous volumes
   - Par volume
   - Par fichier : vous pouvez spécifier un dossier ou des fichiers individuels à restaurer.

     Vous pouvez sélectionner jusqu'à 100 fichiers ou un seul dossier.

6. Poursuivez l'une des procédures suivantes selon que vous choisissez une application, un volume ou un fichier.

Restaurer tous les volumes

1. Sur la page Restaurer, dans la portée Restaurer, sélectionnez **tous les volumes**.



2. **Source** : sélectionnez la flèche vers le bas en regard de Source pour afficher les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

> La protection contre les ransomwares BlueXP identifie le meilleur point de restauration comme la sauvegarde la plus récente juste avant l'incident et indique « la plus sûre pour tous les volumes ». Cela signifie que tous les volumes seront restaurés sur une copie avant la première attaque sur le premier volume détecté.

3. **Destination** : sélectionnez la flèche vers le bas en regard de destination pour afficher les détails.
   a. Sélectionnez l'environnement de travail.
   b. Sélectionnez la VM de stockage.
   c. Sélectionner l'agrégat.
   d. Modifiez le préfixe du volume qui sera ajouté à tous les nouveaux volumes.

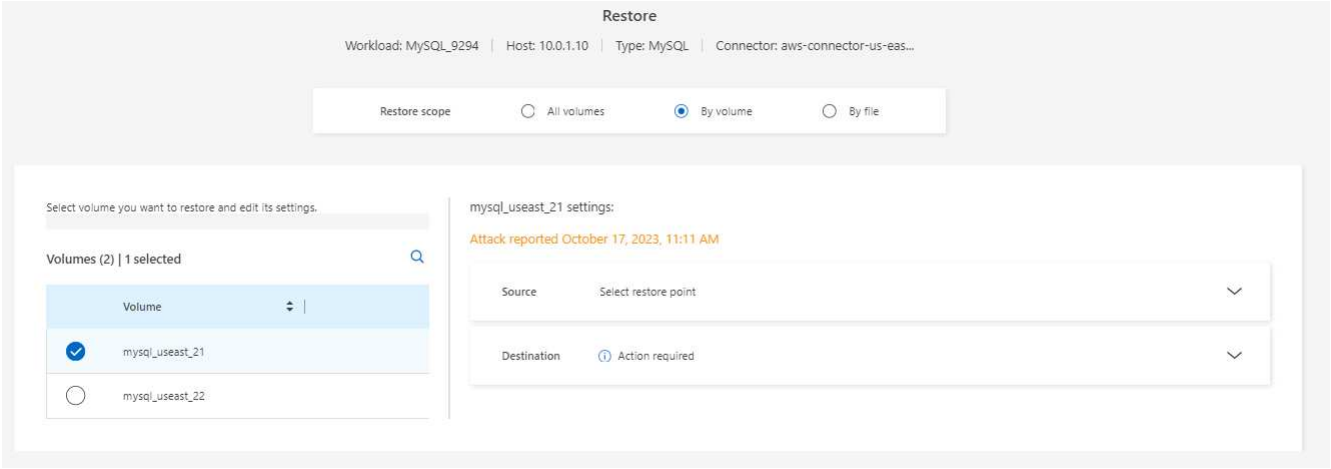
> Le nouveau nom de volume apparaît sous la forme préfixe + nom du volume d'origine + nom de la sauvegarde + date de la sauvegarde.

4. Sélectionnez **Enregistrer**.
5. Sélectionnez **Suivant**.
6. Vérifiez vos sélections.
7. Sélectionnez **Restaurer**.

8. Dans le menu supérieur, sélectionnez **récupération** pour examiner la charge de travail sur la page récupération, où l'état de l'opération se déplace dans les États.

Restaurez une charge de travail applicative au niveau du volume

1. Sur la page Restaurer, dans l'étendue Restaurer, sélectionnez **par volume**.



2. Dans la liste des volumes, sélectionnez le volume à restaurer.
3. **Source** : sélectionnez la flèche vers le bas en regard de Source pour afficher les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

> La protection contre les ransomwares BlueXP identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et une indication « recommandée ».

4. **Destination** : sélectionnez la flèche vers le bas en regard de destination pour afficher les détails.
   a. Sélectionnez l'environnement de travail.
   b. Sélectionnez la VM de stockage.
   c. Sélectionner 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 la sauvegarde.

5. Sélectionnez **Enregistrer**.
6. Sélectionnez **Suivant**.
7. Vérifiez vos sélections.
8. Sélectionnez **Restaurer**.
9. Dans le menu supérieur, sélectionnez **récupération** pour examiner la charge de travail sur la page récupération, où l'état de l'opération se déplace dans les États.

Restaurez une charge de travail applicative au niveau des fichiers

1. Sur la page Restaurer, dans l'étendue Restaurer, sélectionnez **par fichier**.

2. Dans la liste des volumes, sélectionnez le volume à restaurer.
3. **Source** : sélectionnez la flèche vers le bas en regard de Source pour afficher les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

      La protection contre les ransomwares BlueXP identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et une indication « recommandée ».

   b. Sélectionnez jusqu'à 100 fichiers ou un seul dossier à restaurer.
4. **Destination** : sélectionnez la flèche vers le bas en regard de destination pour afficher les détails.
   a. Choisissez l'emplacement de restauration des données : emplacement source d'origine ou autre emplacement que vous pouvez spécifier.

      Alors que les fichiers ou répertoires d'origine seront remplacés par les données restaurées, les noms de fichiers et de dossiers d'origine resteront les mêmes, sauf si vous spécifiez de nouveaux noms.

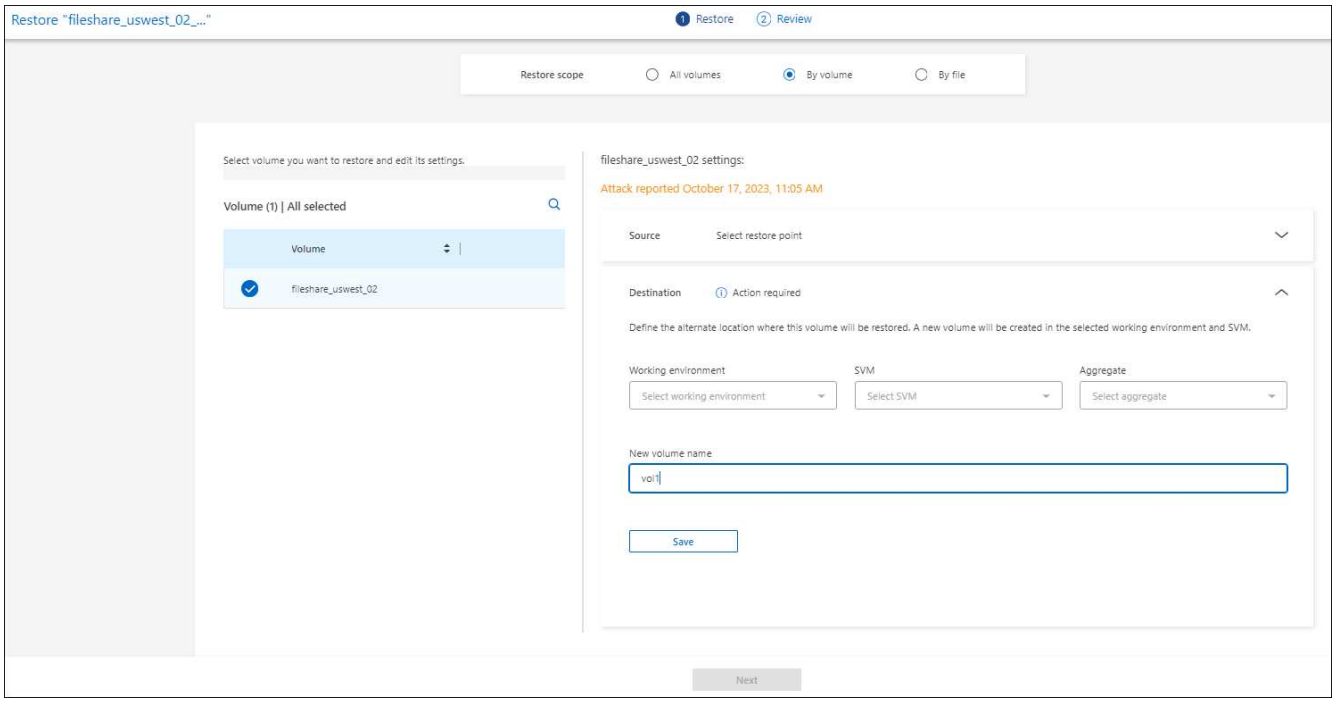
   b. Sélectionnez l'environnement de travail.
   c. Sélectionnez la VM de stockage.
   d. Si vous le souhaitez, saisissez le chemin d'accès.

      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. Indiquez 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.
5. Sélectionnez **Enregistrer**.
6. Sélectionnez **Suivant**.
7. Vérifiez vos sélections.
8. Sélectionnez **Restaurer**.
9. Dans le menu supérieur, sélectionnez **récupération** pour examiner la charge de travail sur la page récupération, où l'état de l'opération se déplace dans les États.

Restaurez un partage de fichiers ou un datastore au niveau du volume ou du fichier

1. Après avoir sélectionné un partage de fichiers ou un datastore à restaurer, sur la page Restaurer, dans la portée Restaurer, sélectionnez **par volume** ou **par fichier**.



2. Dans la liste des volumes, sélectionnez le volume à restaurer.
3. **Source** : sélectionnez la flèche vers le bas en regard de Source pour afficher les détails.
   a. Sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer les données.

> La protection contre les ransomwares BlueXP identifie le meilleur point de restauration comme la dernière sauvegarde juste avant l'incident et une indication « recommandée ».

4. **Destination** : sélectionnez la flèche vers le bas en regard de destination pour afficher les détails.
   a. Choisissez l'emplacement de restauration des données : emplacement source d'origine ou autre emplacement que vous pouvez spécifier.

> Alors que les fichiers ou répertoires d'origine seront remplacés par les données restaurées, les noms de fichiers et de dossiers d'origine resteront les mêmes, sauf si vous spécifiez de nouveaux noms.

   b. Sélectionnez l'environnement de travail.
   c. Sélectionnez la VM de stockage.
   d. Si vous le souhaitez, saisissez le chemin d'accès.

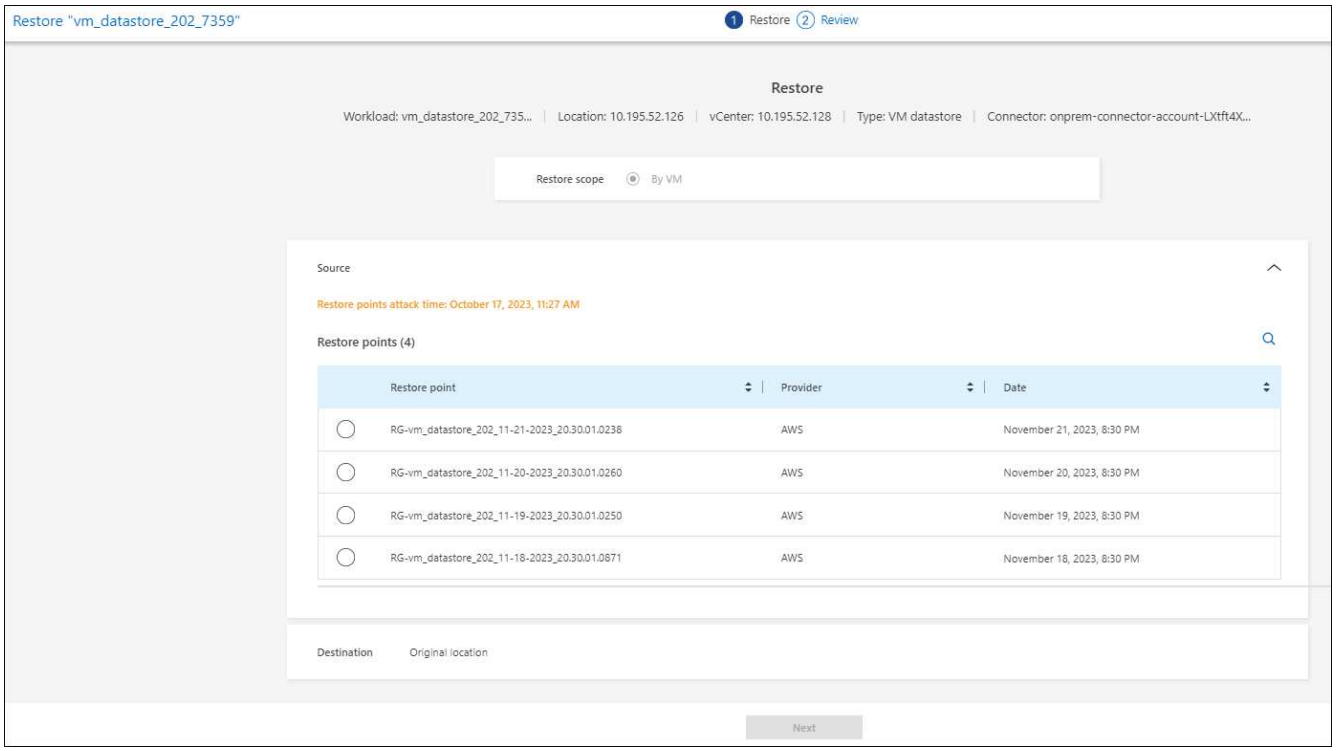
> Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

5. Sélectionnez **Enregistrer**.
6. Vérifiez vos sélections.
7. Sélectionnez **Restaurer**.
8. Dans le menu, sélectionnez **récupération** pour revoir la charge de travail sur la page récupération, où l'état de l'opération se déplace dans les États.

Restaurer un partage de fichiers de machine virtuelle au niveau des machines virtuelles

Sur la page récupération après avoir sélectionné une machine virtuelle à restaurer, procédez comme suit.

1. **Source** : sélectionnez la flèche vers le bas en regard de Source pour afficher les détails.



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

Connaissances et support

S’inscrire pour obtenir de l’aide

L’enregistrement au support est requis pour recevoir le support technique spécifique à BlueXP et à ses solutions et services de stockage. L’enregistrement au support est également requis pour activer les principaux workflows des systèmes Cloud Volumes ONTAP.

L’inscription au support n’active pas le support NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir de l’aide concernant un service de fichiers d’un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d’aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Présentation de l’inscription au support

Il existe deux types d’inscription pour activer les droits d’assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxxx se trouve sur la page des ressources de support de BlueXP).

  Il sert d’ID d’abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

  Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L’enregistrement des deux types de numéros de série offre des fonctionnalités telles que l’ouverture de tickets de support et la génération automatique de tickets. L’inscription est terminée en ajoutant des comptes du site de support NetApp (NSS) à BlueXP, comme décrit ci-dessous.

Enregistrez votre compte BlueXP pour bénéficier de la prise en charge NetApp

Pour vous inscrire au support et activer les droits de support, un utilisateur de votre compte BlueXP doit associer un compte sur le site de support NetApp à sa connexion BlueXP. Le fait de vous inscrire au support NetApp dépend de la présence ou non d’un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

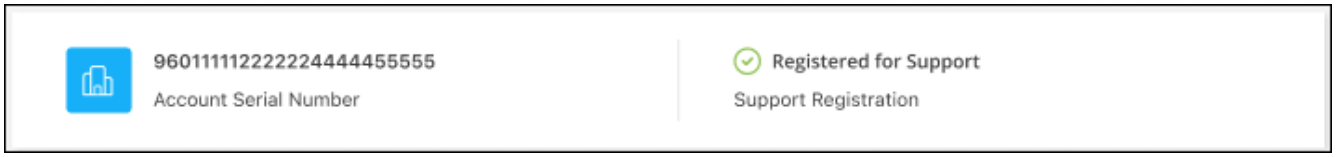
Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l’icône Paramètres, puis sélectionnez

informations d'identification.

2. Sélectionnez **informations d'identification utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'enregistrement a réussi, sélectionnez l'icône aide et sélectionnez **support**.

   La page **Ressources** doit indiquer que votre compte est enregistré pour le support.



   Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé de compte sur le site de support NetApp à leur identifiant BlueXP. Toutefois, cela ne signifie pas que votre compte BlueXP n'est pas enregistré pour le support. Tant qu'un utilisateur du compte a suivi ces étapes, votre compte a été enregistré.

Client existant mais aucun compte NSS

Si vous possédez déjà des licences et des numéros de série NetApp, mais que vous possédez un compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP.

Étapes

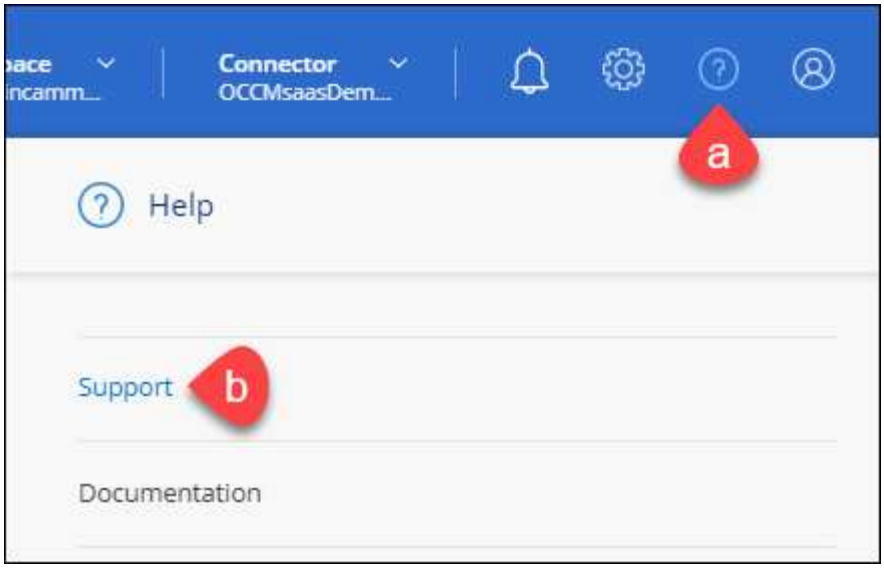
1. Créez un compte sur le site de support NetApp en complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Découvrez la toute nouvelle gamme NetApp

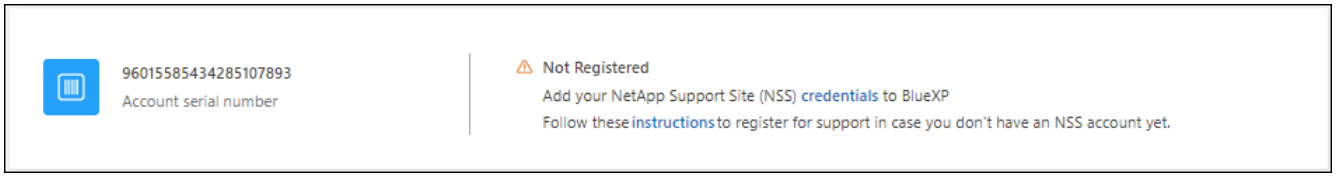
Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

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 l'ID de compte sur la page d'inscription au support.



3. Accédez à "Site d'inscription au support 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 **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

   Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

   La confirmation de la soumission de 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 complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Une fois que vous avez 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 possédez votre compte sur le site de support NetApp, associez-le à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP

Pour activer les workflows clés suivants pour Cloud Volumes ONTAP, vous devez associer les informations d'identification du site de support NetApp à votre compte BlueXP :

- Enregistrement des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation pour bénéficier d'une assistance

  Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Déploiement d'Cloud Volumes ONTAP avec modèle BYOL (Bring Your Own License)

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

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

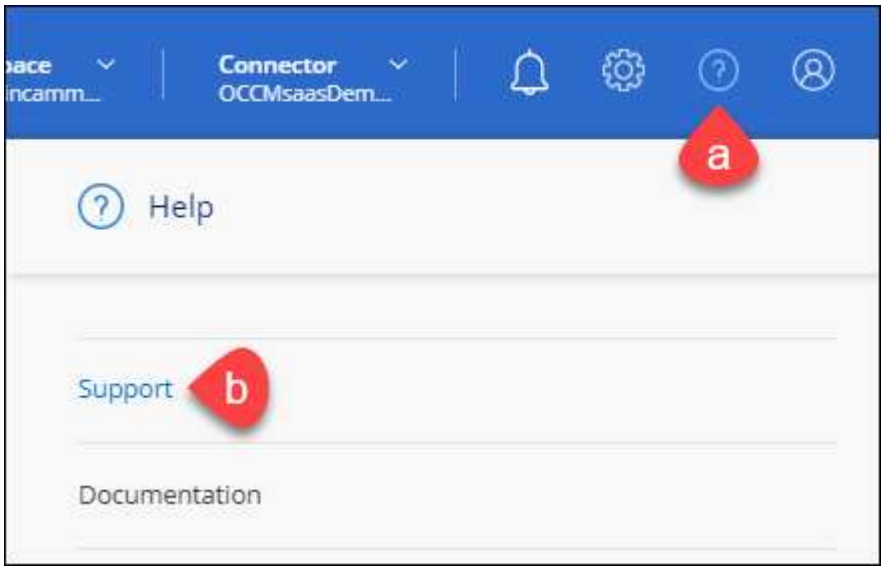
L'association des informations d'identification NSS à votre compte BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP.

Ces informations d'identification NSS sont associées à votre ID de compte BlueXP spécifique. Les utilisateurs qui appartiennent au compte BlueXP peuvent accéder à ces informations d'identification depuis **support > gestion NSS**.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du 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 à la prise en charge et à l'octroi de licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

   Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

   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 de 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 de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

     "Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de type différent."

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

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

     Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel 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.

     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.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Bénéficiez du support pour les services de fichiers d'un fournisseur cloud

Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Pour bénéficier du support technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options de support décrites ci-dessous.

Utilisation d'options de support en libre-service

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 des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

Créez un dossier de demande de support auprès du support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un cas**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP. "Découvrez comment gérer les identifiants associés 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 avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un cas** 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.

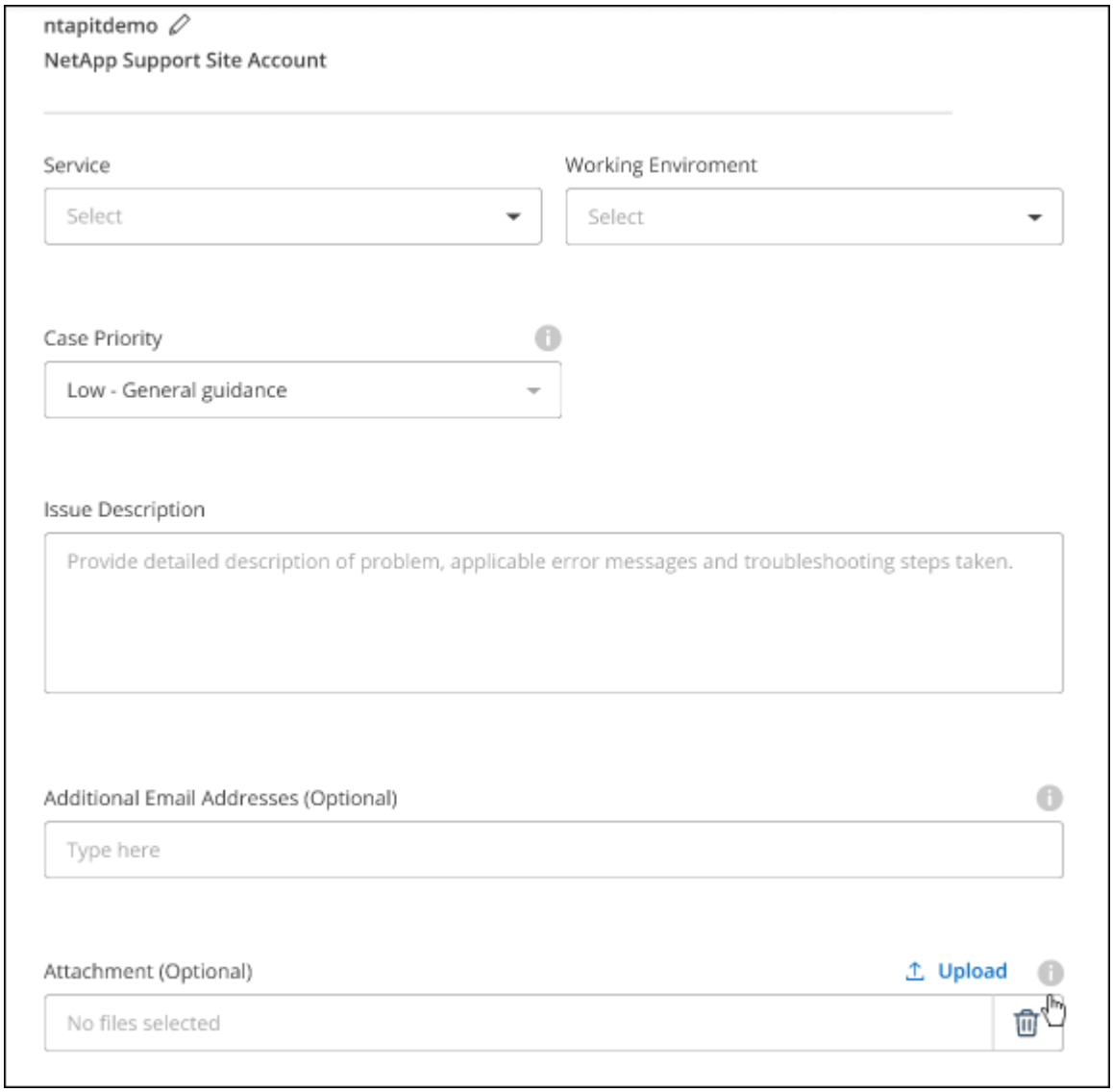
        La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

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

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez 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 fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.



Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour un historique de vos dossiers de support, vous pouvez sélectionner **Paramètres > Chronologie** et

rechercher les actions nommées "Créer un dossier de support". Un bouton situé à l'extrême droite vous permet de développer l'action pour afficher les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

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

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 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 du produit
- Soumettre un dossier non technique à https://mysupport.netapp.com/site/help

Gestion de vos dossiers de demande de support (aperçu)

Vous pouvez afficher et gérer les dossiers de support actifs et résolus directement à partir de BlueXP. Vous pouvez gérer les dossiers associés à votre compte NSS et à votre entreprise.

La gestion des dossiers est disponible en tant qu'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Notez ce qui suit :

- Le tableau de bord de gestion des dossiers en haut de la page propose deux vues :
  - La vue de gauche affiche le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte NSS utilisateur 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 NSS utilisateur.

  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 offrent uniquement des fonctions de tri.

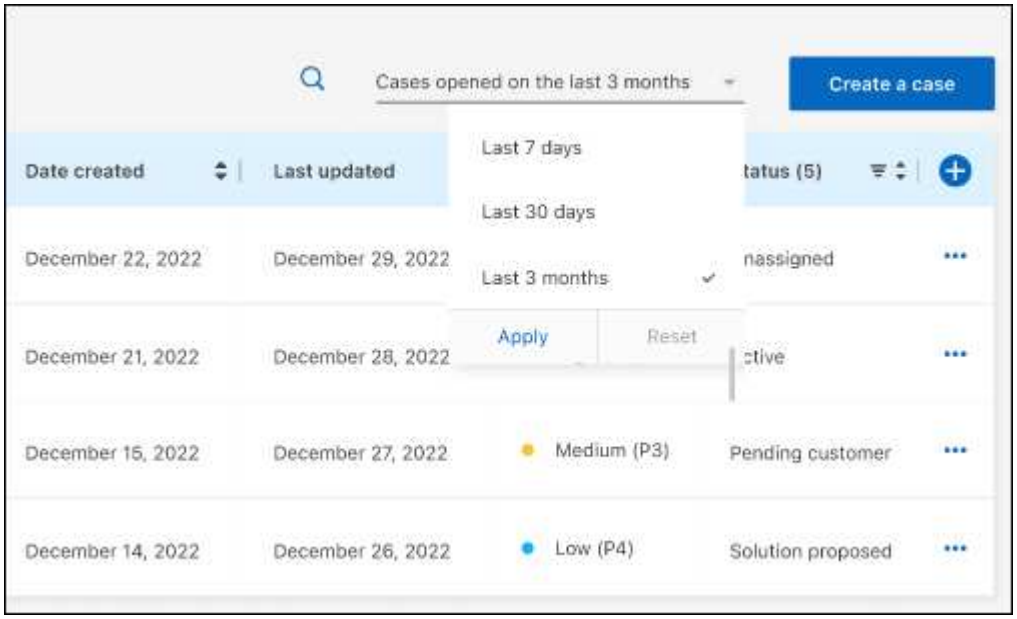
  Pour plus d'informations, consultez les étapes ci-dessous.
- Au niveau de chaque dossier, nous offrons la possibilité de mettre à jour les notes de dossier ou de fermer un dossier qui n'est pas déjà à l'état fermé ou en attente fermée.

Étapes

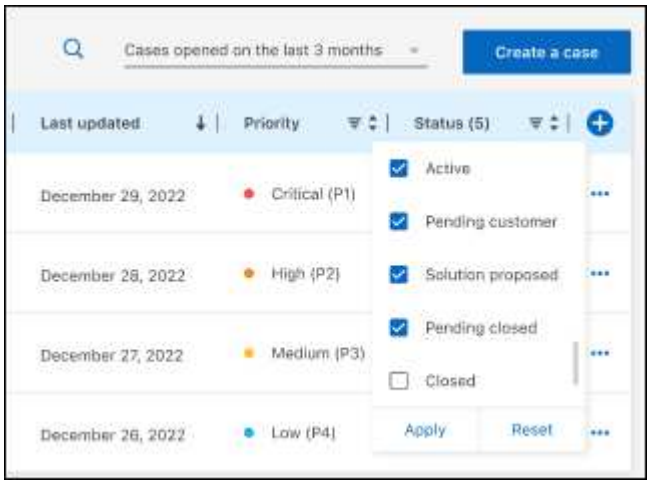
1. Dans BlueXP, sélectionnez **aide > support**.
2. Sélectionnez **case Management** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

   La page **gestion des cas** affiche les cas ouverts associés 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 société.
   - Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une autre

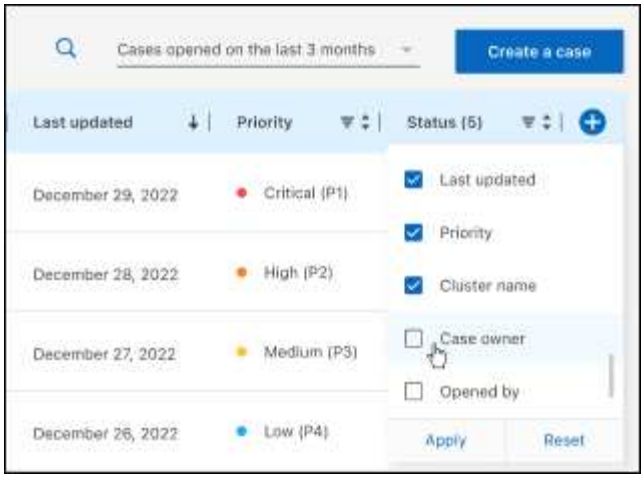
période.



- Filtrez le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant puis choisissez les colonnes que vous souhaitez afficher.

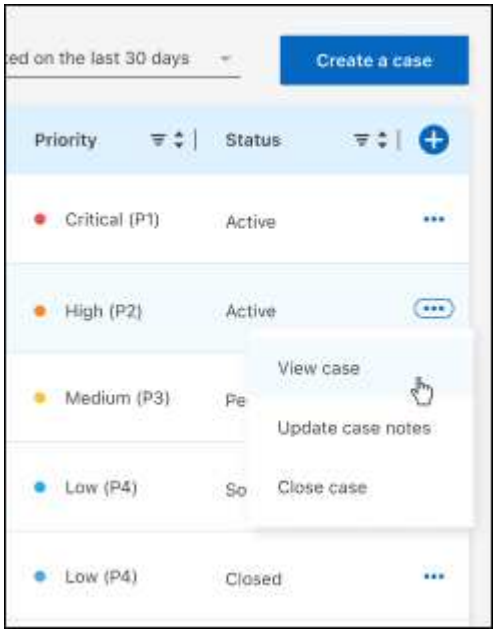


4. Gérer un dossier existant en sélectionnant ••• et en sélectionnant l'une des options disponibles :

   - **Voir cas**: Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes de cas** : fournir des détails supplémentaires sur votre problème ou sélectionner **Télécharger les fichiers** pour joindre jusqu'à cinq fichiers.

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

   - **Fermer le cas** : fournissez des détails sur la raison pour laquelle vous fermez le cas et sélectionnez **Fermer le cas**.



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

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

Marques déposées

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

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

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

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

Politique de confidentialité

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

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Note pour BlueXP"