



Protégez les workloads

BlueXP ransomware protection

NetApp
October 07, 2024

Sommaire

- Protégez les workloads 1
- Protégez vos workloads avec des stratégies de ransomware 1

Protégez les workloads

Protégez vos workloads avec des stratégies de ransomware

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

- Bénéficiez d'une protection cohérente avec les charges de travail, qui fonctionne avec le logiciel SnapCenter ou le plug-in SnapCenter pour VMware vSphere.
- Créez ou gérez des stratégies de protection contre les ransomware, notamment des règles que vous créez pour les copies Snapshot, les sauvegardes et la protection contre les ransomware (connues sous le nom de *règles de détection*).
- Importez une stratégie et ajustez-la.
- Regroupez les partages de fichiers pour simplifier la protection des workloads au lieu de les protéger individuellement.
- Supprimez une stratégie de protection contre les ransomware.

Quels services sont utilisés dans la protection? Les services suivants peuvent être utilisés pour gérer les règles de protection. Les informations de protection de ces services sont disponibles dans BlueXP ransomware protection :

- Sauvegarde et restauration BlueXP pour les partages de fichiers et les partages de fichiers de machines virtuelles
- SnapCenter pour VMware pour les datastores de VM
- SnapCenter pour Oracle et MySQL

Règles de protection

Il peut être utile de consulter des informations sur les stratégies de protection que vous pouvez modifier et sur les types de stratégies qui figurent dans une stratégie de protection.

Quelles politiques de protection pouvez-vous modifier ?

Vous pouvez modifier des règles de protection en fonction de la protection des workloads dont vous disposez :

- **Charges de travail non protégées par les applications NetApp** : ces charges de travail ne sont pas gérées par SnapCenter, le plug-in SnapCenter pour VMware vSphere ou la sauvegarde et restauration BlueXP . Des snapshots peuvent être effectués dans ces workloads avec ONTAP ou d'autres produits. Si la protection ONTAP FPolicy est en place, vous pouvez la modifier à l'aide de ONTAP.
- **Charges de travail avec protection existante par les applications NetApp** : ces charges de travail disposent de stratégies de sauvegarde ou de snapshot gérées par SnapCenter, SnapCenter pour VMware vSphere ou la sauvegarde et la restauration BlueXP .
 - Si les snapshots ou les politiques de sauvegarde sont gérés par SnapCenter, SnapCenter pour VMware ou la sauvegarde et la restauration BlueXP , ils continueront à être gérés par ces applications. Avec la protection contre les ransomware de BlueXP , vous pouvez également appliquer une stratégie de détection des ransomwares à ces workloads.
 - Si une politique de détection des ransomware est gérée par la protection anti-ransomware autonome (ARP) et FPolicy dans ONTAP, ces workloads sont protégés et continueront d'être gérés par ARP et

FPolicy.

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

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

- Politique de détection des ransomwares
- Règle Snapshot

Aucune règle de sauvegarde n'est requise dans la stratégie de protection contre les ransomwares de BlueXP .

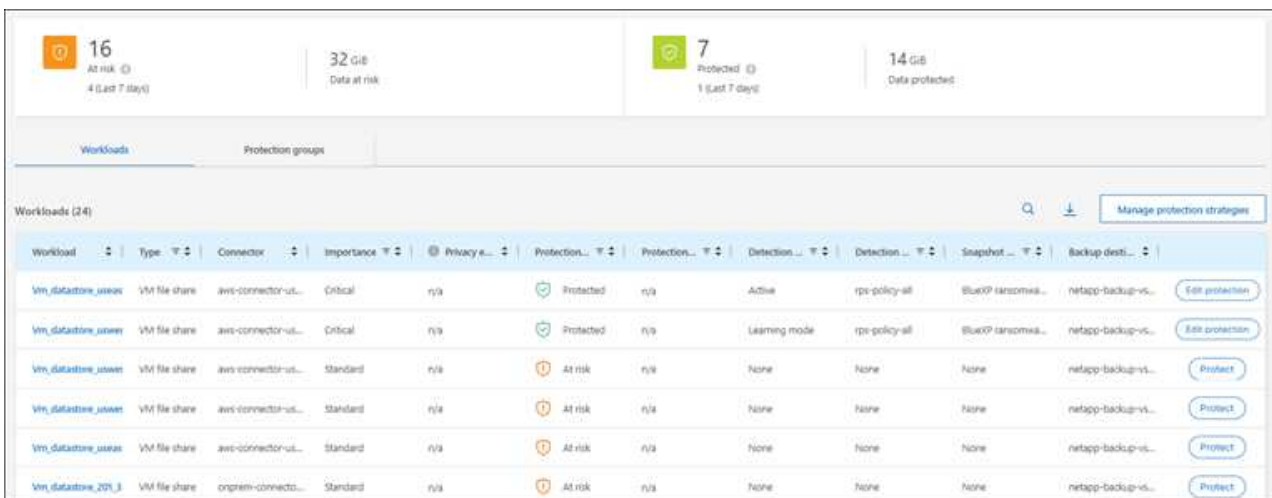
Afficher la protection contre les ransomwares sur un workload

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 applicatifs
- 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**.



| Workload | Type | Connector | Importance | Privacy | Protection | Protection | Detection | Detection | Snapshot | Backup dest. | |
|---------------------|---------------|---------------------|------------|---------|------------|------------|---------------|----------------|-------------------|---------------------|-----------------|
| Win_datastore_usawr | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Active | rpe-policy-all | BlueXP ransomw... | netapp-backup-vs... | Edit protection |
| Win_datastore_usawr | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Learning mode | rpe-policy-all | BlueXP ransomw... | netapp-backup-vs... | Edit protection |
| Win_datastore_usawr | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_usawr | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_usawr | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_209_3 | VM file share | ongram-connecto... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |

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



Pour les charges de travail qui disposent déjà d'une règle de protection avec le service de sauvegarde et de restauration SnapCenter ou BlueXP, vous ne pouvez pas modifier la protection. Pour ces workloads, le ransomware BlueXP active la protection anti-ransomware autonome et/ou la protection FPolicy s'ils sont déjà activés dans d'autres services. En savoir plus sur "[Protection autonome contre les ransomwares](#)", "[Sauvegarde et restauration BlueXP](#)" et "[ONTAP FPolicy](#)".

Détails de la protection sur la page protection

La page protection affiche les informations suivantes sur la protection des charges de travail :

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. ARP est activé sur tous les volumes liés à la charge de travail.
- **À risque**: Aucune politique n'est appliquée. Si aucune règle de détection primaire n'est activée pour une charge de travail, elle est « à risque » même si une règle de snapshot et de sauvegarde est activée.
- **En cours**: Une politique est appliquée mais pas encore terminée.
- **Échec** : une politique est appliquée mais ne fonctionne pas.

Statut de détection : une charge de travail peut avoir l'un des États de détection de ransomware suivants :

- **Learning** : une politique de détection des ransomware a été récemment assignée à la charge de travail et le service analyse les charges de travail.
- **Actif** : une politique de protection contre la détection des ransomware est assignée.
- **Not Set** : aucune politique de protection contre la détection des ransomware n'est attribuée.
- **Erreur** : une stratégie de détection des ransomware a été attribuée, mais le service a rencontré une erreur.



Lorsque la protection est activée dans la protection contre les ransomware BlueXP , la détection des alertes et le reporting commencent après que l'état de la règle de détection des ransomwares passe du mode apprentissage au mode actif.

Politique de détection : le nom de la politique de détection des ransomware apparaît, si elle a été attribuée. Si la stratégie de détection n'a pas été affectée, « N/A » apparaît.

Instantanés et politiques de sauvegarde : cette colonne affiche les règles de snapshot et de sauvegarde appliquées à la charge de travail et au produit ou service qui gère ces stratégies.

- Géré par SnapCenter
- Géré par le plug-in SnapCenter pour VMware vSphere
- Gestion par la sauvegarde et la restauration BlueXP
- Nom de la règle de protection contre les ransomware qui régit les snapshots et les sauvegardes
- Aucune

Importance de la charge de travail

La protection contre les ransomwares BlueXP attribue une importance ou une priorité à chaque workload lors de sa découverte, sur la base d'une analyse de chaque workload. L'importance de la charge de travail est déterminée par les fréquences d'instantanés suivantes :

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

Politiques de détection prédéfinies

Vous pouvez choisir l'une des règles de protection anti-ransomware prédéfinies de BlueXP suivantes, adaptées à l'importance 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 30 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 |

SnapCenter protège de manière cohérente les applications et les machines virtuelles

La protection cohérente au niveau des applications ou des machines virtuelles vous aide à protéger de manière cohérente vos charges de travail applicatives ou de machines virtuelles, en atteignant un état de repos et cohérent pour éviter toute perte potentielle de données par la suite en cas de restauration.

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

Après avoir activé la protection cohérente avec les workloads, vous pouvez gérer les stratégies de protection dans la protection BlueXP contre les ransomware. La stratégie de protection inclut les règles de copie Snapshot et de sauvegarde gérées ailleurs, ainsi qu'une politique de détection des ransomwares gérée dans la solution BlueXP de protection contre les ransomwares.

Pour en savoir plus sur l'enregistrement de SnapCenter ou du plug-in SnapCenter pour VMware vSphere à

l'aide de la sauvegarde et de la restauration BlueXP, consultez les informations suivantes :

- ["Enregistrez le logiciel serveur SnapCenter"](#)
- ["Enregistrez le plug-in SnapCenter pour VMware vSphere"](#)

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **Dashboard**.
2. Dans le volet recommandations, recherchez l'une des recommandations suivantes et sélectionnez **revoir et corriger** :
 - Enregistrez le serveur SnapCenter disponible avec BlueXP
 - Enregistrez le plug-in SnapCenter disponible pour VMware vSphere (SCV) avec BlueXP
3. Suivez les informations pour enregistrer le plug-in SnapCenter ou SnapCenter pour l'hôte VMware vSphere à l'aide de la sauvegarde et de la restauration BlueXP.
4. Revenez à la protection BlueXP contre les ransomware.
5. Depuis la protection BlueXP contre les ransomwares, accédez au tableau de bord et relancez le processus de détection.
6. Depuis la protection BlueXP contre les ransomware, sélectionnez **protection** pour afficher la page protection.
7. Consultez les détails de la colonne snapshot and backup policies de la page protection pour voir si les règles sont gérées ailleurs.

Ajouter une stratégie de protection contre les ransomwares

Vous pouvez ajouter une stratégie de protection contre les ransomwares à vos workloads. La façon dont vous procédez dépend si les règles de snapshot et de sauvegarde existent déjà :

- **Créez une stratégie de protection contre les ransomware si vous n'avez pas de stratégie de snapshot ou de sauvegarde.** Si des snapshots ou des règles de sauvegarde n'existent pas sur le workload, vous pouvez créer une stratégie de protection contre les ransomware, qui peut inclure les règles suivantes que vous créez dans BlueXP de protection contre les ransomware :
 - Règle Snapshot
 - Politique de sauvegarde
 - Politique de détection des ransomwares
- **Créez une stratégie de détection pour les charges de travail qui ont déjà des stratégies de snapshot et de sauvegarde,** qui sont gérées dans d'autres produits ou services NetApp. La politique de détection ne modifie pas les politiques gérées dans d'autres produits.

Créez une stratégie de protection contre les ransomwares (si vous n'avez pas de règles de Snapshot ou de sauvegarde)

Si des snapshots ou des règles de sauvegarde n'existent pas sur le workload, vous pouvez créer une stratégie de protection contre les ransomware, qui peut inclure les règles suivantes que vous créez dans BlueXP de protection contre les ransomware :

- Règle Snapshot
- politique de sauvegarde
- Politique de détection des ransomwares

Étapes de création d'une stratégie de protection contre les ransomwares

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

The screenshot shows the BlueXP ransomware protection dashboard. At the top, there are three summary cards: 'At risk' (16 items, 4 last 7 days), 'Data at risk' (32 GiB), and 'Protected' (7 items, 1 last 7 days, 14 GiB data protected). Below these are tabs for 'Workloads' and 'Protection groups'. The 'Workloads' tab is active, displaying a table of 24 workloads. The table has columns for Workload, Type, Connector, Importance, Privacy, Protection status, Protection policy, Detection policy, Detection mode, Snapshot, Backup destination, and an 'Edit protection' button.

| Workload | Type | Connector | Importance | Privacy | Protection | Protection... | Detection... | Detection... | Snapshot... | Backup desti... | |
|---------------------|---------------|---------------------|------------|---------|------------|---------------|---------------|----------------|--------------------|---------------------|-----------------|
| Win_datastore_juwei | VM file share | aws-connector-ut... | Critical | n/a | Protected | n/a | Active | rps-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwei | VM file share | aws-connector-ut... | Critical | n/a | Protected | n/a | Learning mode | rps-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwei | VM file share | aws-connector-ut... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_juwei | VM file share | aws-connector-ut... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_juwei | VM file share | aws-connector-ut... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_201_3 | VM file share | ongram-connecto... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |

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

The screenshot shows the 'Ransomware protection strategies' page. It features a table with columns for Ransomware protection strategy, Snapshot policy, Backup policy, Detection policy, and Protected workloads. There are three strategies listed: 'rps-strategy-critical', 'rps-strategy-important', and 'rps-strategy-standard'. Each strategy has a dropdown arrow and a plus sign icon.

| Ransomware protection strategy | Snapshot policy | Backup policy | Detection policy | Protected workloads | |
|--------------------------------|---------------------|---------------------|------------------|---------------------|-----|
| rps-strategy-critical | critical-ss-policy | critical-bu-policy | rps-policy-all | 3 | ▼ + |
| rps-strategy-important | important-ss-policy | important-bu-policy | rps-policy-all | 1 | ▼ + |
| rps-strategy-standard | standard-ss-policy | standard-bu-policy | rps-policy-all | 0 | ▼ + |

3. Dans la page stratégies de protection contre les ransomware, sélectionnez **Ajouter**.

The screenshot shows the 'Add ransomware protection strategy' form. It includes a text input for 'Ransomware protection strategy name' with the value 'RPS strategy 1'. There is a 'Copy from existing ransomware protection strategy' section with a 'Select' button and a dropdown menu showing 'No policy selected'. Below this are three dropdown menus for 'Detection policy' (rps-policy-primary), 'Snapshot policy' (important-ss-policy), and 'Backup policy' (None). At the bottom, there are 'Cancel' and 'Add' buttons.

4. Entrez un nouveau nom de stratégie ou un nom existant pour le copier. Si vous entrez un nom existant, choisissez celui à copier et sélectionnez **Copier**.



Si vous choisissez de copier et de modifier une stratégie existante, le service 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 préconçues.
- **Détection primaire :** activez la détection des ransomware pour que le service détecte les attaques potentielles par ransomware.
- **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.

Si vous souhaitez modifier les extensions de fichier bloquées, modifiez-les dans System Manager.

◦ **Politique Snapshot :**

- **Nom de la base de règles de snapshot :** sélectionnez une stratégie ou sélectionnez **Créer** et entrez un nom pour la stratégie de snapshot.
- **Verrouillage Snapshot :** activez cette option pour verrouiller les copies Snapshot sur le stockage primaire afin qu'elles ne puissent pas être modifiées ou supprimées pendant un certain temps, même si une attaque par ransomware parvient à se rendre à la destination du stockage de sauvegarde. On parle également de *stockage immuable*. Cela permet une restauration plus rapide.

Lorsqu'un snapshot est verrouillé, la durée d'expiration du volume est définie sur l'heure d'expiration de la copie Snapshot.

Le verrouillage des copies Snapshot est disponible avec ONTAP 9.12.1 et les versions ultérieures. Pour en savoir plus sur SnapLock, reportez-vous à la section "[SnapLock à ONTAP](#)".

- **Plannings d'instantanés :** choisissez les options de planification, le nombre de copies d'instantanés à conserver et sélectionnez pour activer le planning.

◦ **Politique de sauvegarde :**

- **Nom de base de la règle de sauvegarde :** entrez un nouveau nom ou choisissez un nom existant.
- **Plannings de sauvegarde :** choisissez des options de planification pour le stockage secondaire et activez le planning.



Pour activer le verrouillage des sauvegardes sur le stockage secondaire, configurez vos destinations de sauvegarde à l'aide de l'option **Settings**. Pour plus de détails, voir "[Configurer les paramètres](#)".

6. Sélectionnez **Ajouter**.

Ajoutez une stratégie de détection aux charges de travail qui disposent déjà de règles de snapshots et de sauvegarde

Avec la protection BlueXP contre les ransomware, vous pouvez attribuer une stratégie de détection des

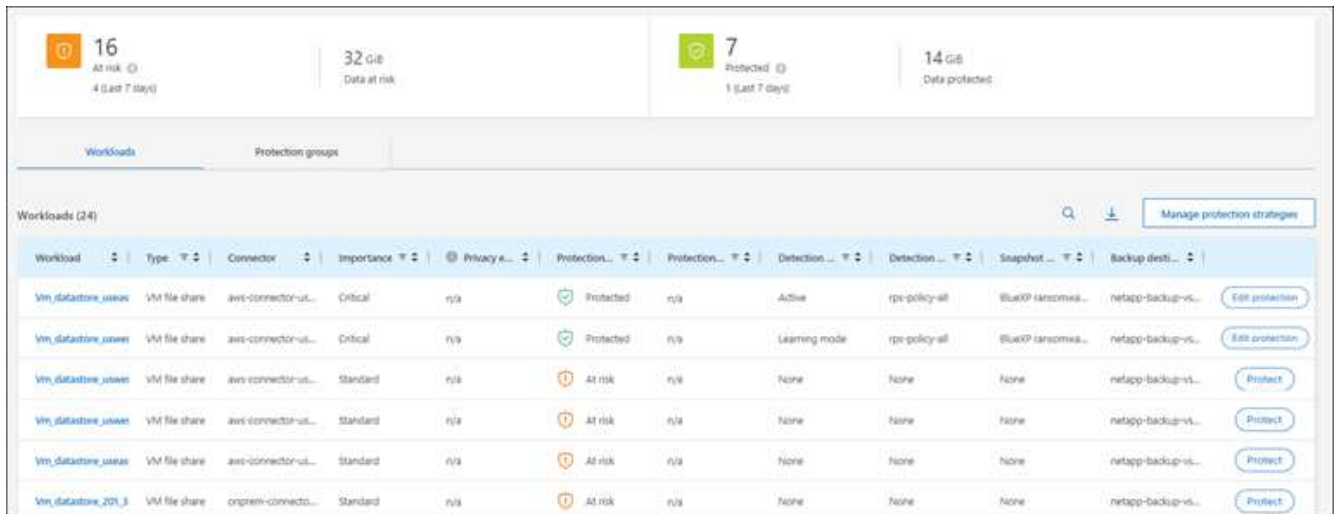
ransomwares à des workloads qui disposent déjà de copies Snapshot et de politiques de sauvegarde, gérées par d'autres produits ou services NetApp. La politique de détection ne modifie pas les politiques gérées dans d'autres produits.

D'autres services, tels que la sauvegarde et la restauration BlueXP et SnapCenter, utilisent les types de règles suivants pour régir les charges de travail :

- Règles régissant les snapshots
- Règles régissant la réplication sur le stockage secondaire
- Règles régissant les sauvegardes vers le stockage objet

Étapes

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



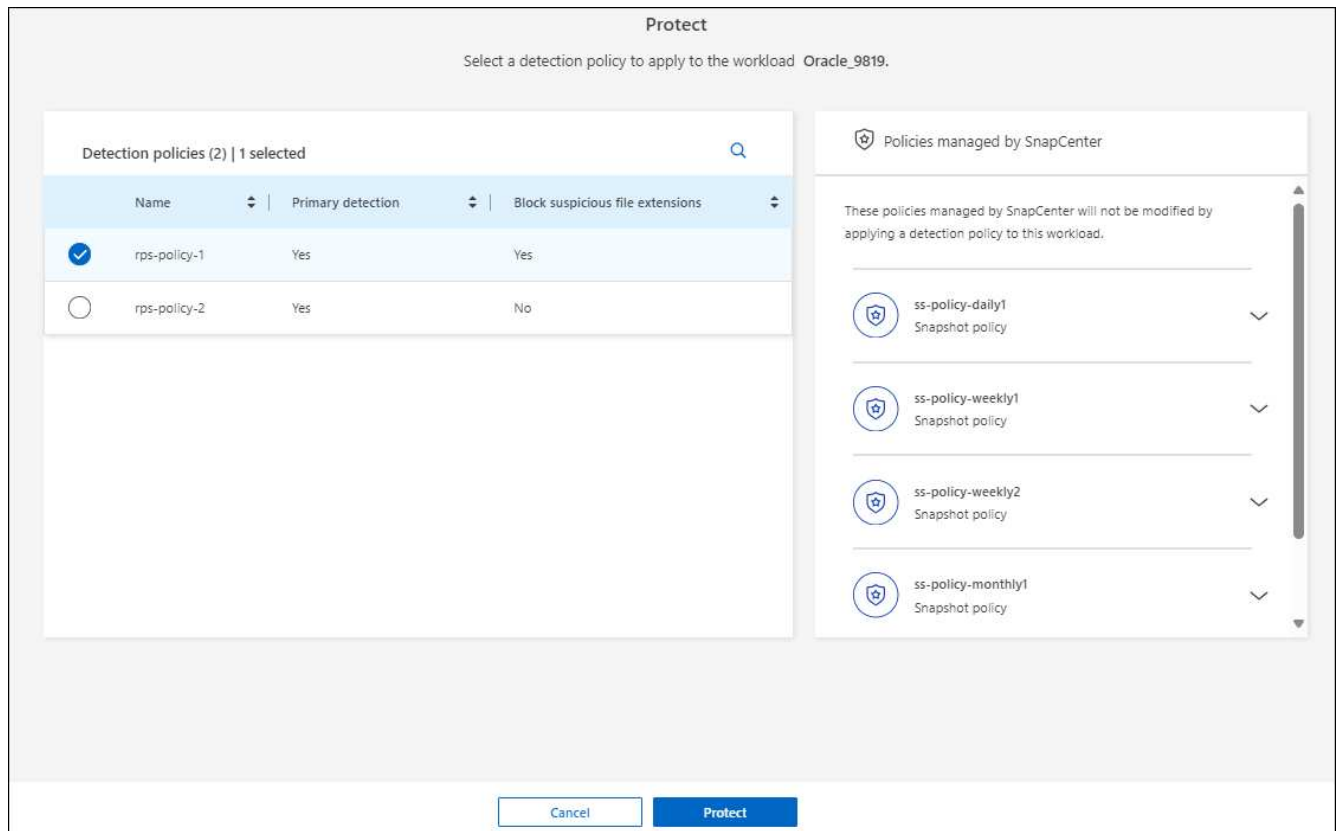
The screenshot shows the BlueXP ransomware protection dashboard. At the top, there are three summary cards: 'At risk' (16 items, 4 last 7 days), 'Data at risk' (32 GiB), and 'Protected' (7 items, 1 last 7 days), 'Data protected' (14 GiB). Below these are tabs for 'Workloads' and 'Protection groups'. The 'Workloads' tab is active, displaying a table with 24 workloads. The table has columns for Workload, Type, Connector, Importance, Privacy, Protection status, Detection status, Detection policy, Snapshot, and Backup destination. Each row includes a 'Protect' button.

| Workload | Type | Connector | Importance | Privacy | Protection | Protection | Detection | Detection | Snapshot | Backup dest. | |
|-----------------------|---------------|---------------------|------------|---------|------------|------------|---------------|----------------|--------------------|---------------------|-----------------|
| Win_datastore_juwa... | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Active | ipe-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwa... | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Learning mode | ipe-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwa... | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_juwa... | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_juwa... | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_201_3 | VM file share | ongrem-connecto... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |

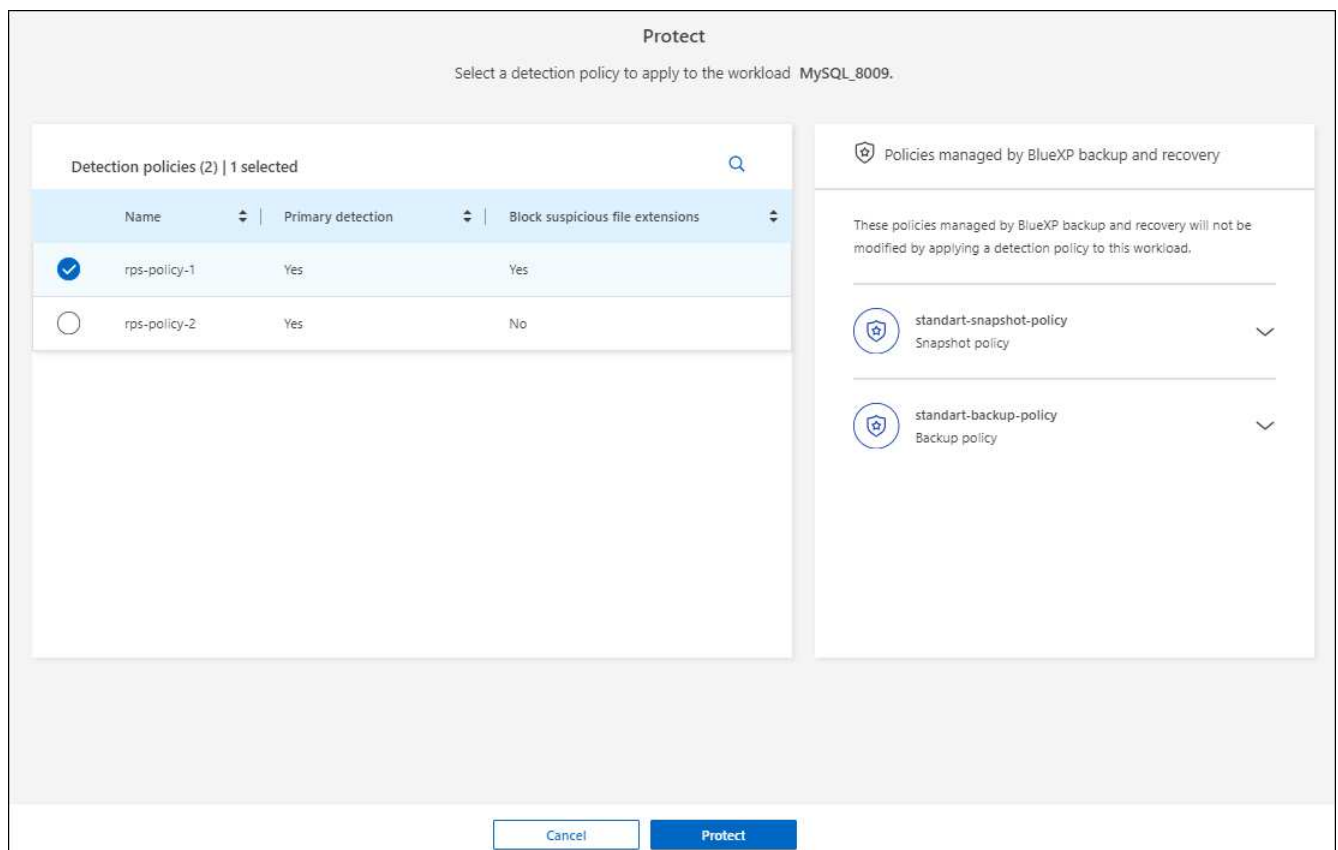
2. Dans la page protection, sélectionnez une charge de travail et sélectionnez **protéger**.

La page protéger affiche les règles gérées par le logiciel SnapCenter, SnapCenter pour VMware vSphere et la sauvegarde et restauration BlueXP.

L'exemple suivant montre les règles gérées par SnapCenter :



L'exemple suivant montre les règles gérées par BlueXP Backup and Recovery :



3. Pour afficher les détails des politiques gérées ailleurs, cliquez sur la flèche **Bas**.

4. Pour appliquer une stratégie de détection en plus des règles de snapshot et de sauvegarde gérées ailleurs, sélectionnez la règle de détection.
5. Sélectionnez **protéger**.
6. Sur la page protection, consultez la colonne politique de détection pour voir la stratégie de détection attribuée. Par ailleurs, la colonne snapshot et backup policies affiche le nom du produit ou service qui gère les règles.

Attribuez une autre stratégie

Vous pouvez attribuer une stratégie de protection différente en remplacement de la stratégie actuelle.

Étapes

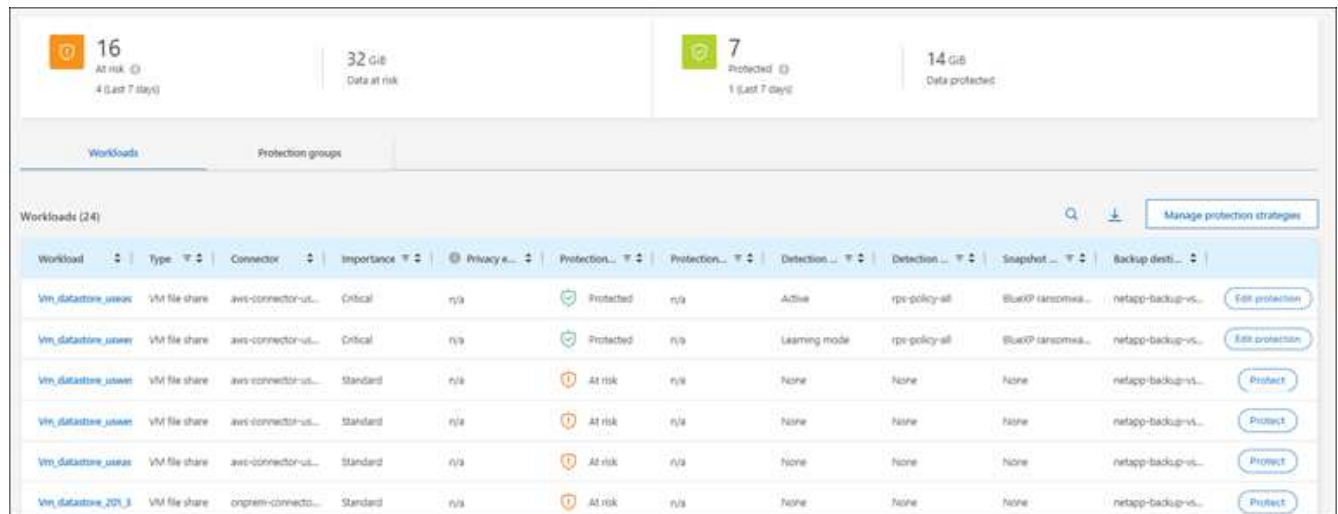
1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sur la ligne charge de travail, sélectionnez **Modifier la protection**.
3. Dans la page stratégies, cliquez sur la flèche vers le bas de la stratégie que vous souhaitez affecter pour examiner les détails.
4. Sélectionnez la stratégie à attribuer.
5. Sélectionnez **Protect** pour terminer la modification.

Regroupez les partages de fichiers pour simplifier la protection

Le regroupement des partages de fichiers simplifie la protection de votre patrimoine de données. Ce service peut protéger simultanément tous les volumes d'un groupe au lieu de protéger chaque volume séparément.

Étapes

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



| Workload | Type | Connector | Importance | Privacy | Protection | Protection | Detection | Detection | Snapshot | Backup desti | |
|---------------------|---------------|---------------------|------------|---------|------------|------------|---------------|----------------|--------------------|---------------------|-----------------|
| Win_datastore_juwei | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Active | rpe-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwei | VM file share | aws-connector-us... | Critical | n/a | Protected | n/a | Learning mode | rpe-policy-all | BlueXP ransomwa... | netapp-backup-vs... | Edit protection |
| Win_datastore_juwei | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_juwei | VM file share | aws-connector-us... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |
| Win_datastore_20v_8 | VM file share | onprem-connecto... | Standard | n/a | At risk | n/a | None | None | None | netapp-backup-vs... | Protect |

2. Dans la page protection, sélectionnez l'onglet **groupes de protection**.

The dashboard displays three summary cards: 'At risk' (16 items, 4 last 7 days), 'Data at risk' (32 GiB), 'Protected' (7 items, 1 last 7 days), and 'Data protected' (14 GiB). Below, the 'Protection groups' section shows a table with columns for Protection group, Detection policy, Snapshot and backup policies, Protection status, Protected count, and Backup destination. One group is visible: 'isp-dev-apps group' with policy 'igs-policy-all', SnapCenter, Protected status, 4/4 protected count, and backup destinations 'aws-s3-dest-1, aws-s3-dest-2'.

3. Sélectionnez **Ajouter**.

The 'Workloads' step of the 'Add protection group' wizard. It includes a 'Protection group name' field with the value 'protect-group-xyz'. A section for 'Workloads with snapshot and backup policies managed by' has 'SnapCenter or Backup and recovery' selected. Below is a table of workloads with 4 items, 2 selected.

| Workload | Type | Connector | Importance | Privacy exposure | Protection status |
|---|--------|-----------------------------|------------|------------------|-------------------|
| <input checked="" type="checkbox"/> Oracle_9819 | Oracle | aws-connector-us-east-1-... | Important | n/a | Protected |
| <input checked="" type="checkbox"/> Oracle_2115 | Oracle | aws-connector-us-east-1-... | Critical | n/a | At risk |
| <input type="checkbox"/> MySQL_3294 | MySQL | aws-connector-us-east-1-... | Critical | n/a | Protected |
| <input type="checkbox"/> MySQL_8009 | MySQL | aws-connector-us-east-1-... | Critical | n/a | At risk |

4. Entrez un nom pour le groupe de protection.

5. Effectuez l'une des opérations suivantes :

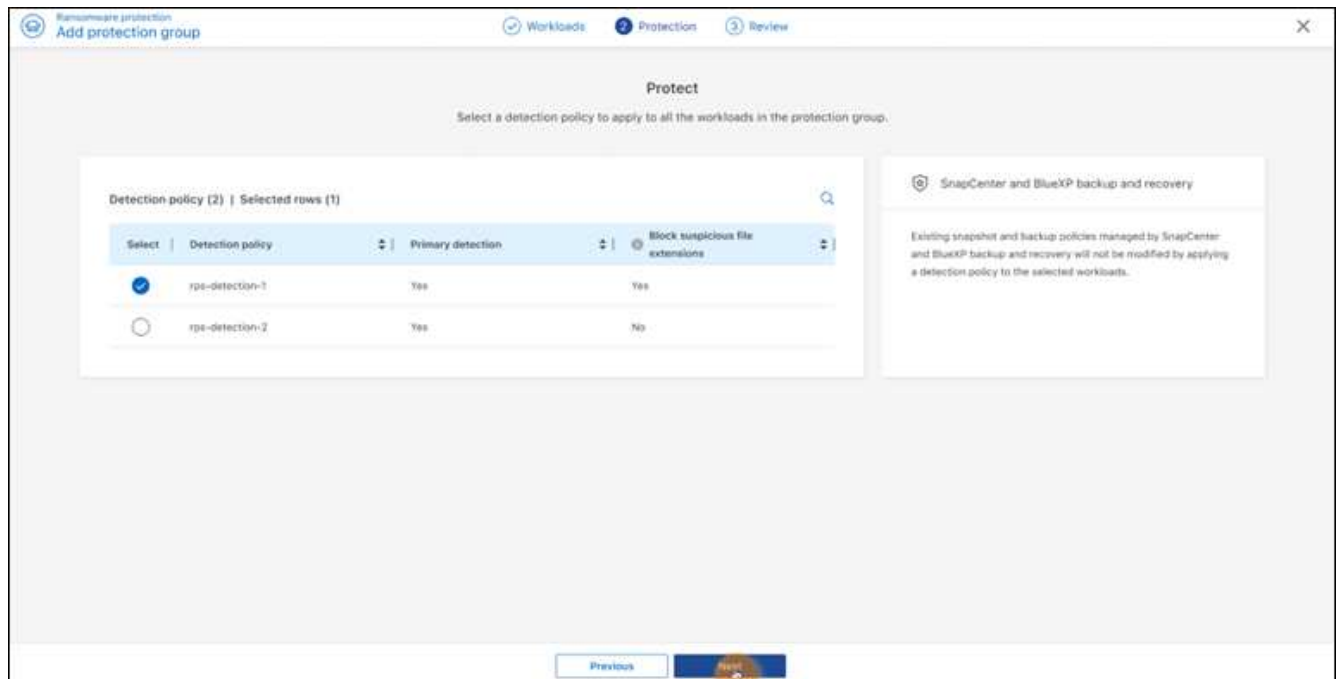
- Si vous avez déjà mis en place des règles de protection, indiquez si vous souhaitez regrouper les charges de travail selon qu'elles sont gérées par l'une des méthodes suivantes :
 - Protection BlueXP contre les ransomware
 - Sauvegarde et restauration SnapCenter ou BlueXP
- Si vous ne disposez pas encore de règles de protection, la page affiche les stratégies préconfigurées de protection contre les ransomware.
 - Choisissez-en un pour protéger votre groupe et sélectionnez **Suivant**.
 - Si la charge de travail que vous avez choisie comporte des volumes dans plusieurs environnements de travail, sélectionnez la destination de sauvegarde pour les différents environnements de travail afin qu'ils puissent être sauvegardés dans le cloud.

6. Sélectionnez les charges de travail à ajouter au groupe.



Pour plus d'informations sur les charges de travail, faites défiler vers la droite.

7. Sélectionnez **Suivant**.



8. Sélectionnez la stratégie qui régira la protection de ce groupe.

9. Sélectionnez **Suivant**.

10. Passez en revue les sélections pour le groupe de protection.

11. Sélectionnez **Ajouter**.

Ajouter d'autres charges de travail à un groupe

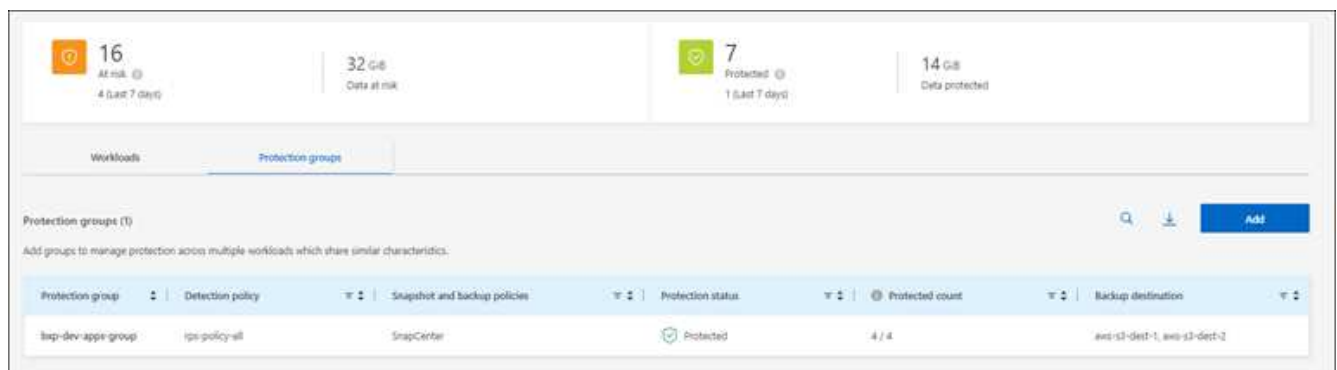
Vous devrez peut-être ajouter d'autres charges de travail à un groupe existant.

Si le groupe comprend des workloads gérés uniquement par la protection contre les ransomware BlueXP (et non par la sauvegarde et la restauration SnapCenter ou BlueXP), vous devez utiliser des groupes distincts pour les workloads gérés par la protection contre les ransomware BlueXP uniquement et par un autre groupe pour les workloads gérés par d'autres services.

Étapes

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

2. Dans la page protection, sélectionnez l'onglet **groupes de protection**.



3. Sélectionnez le groupe auquel vous souhaitez ajouter d'autres charges de travail.

| Workload | Type | Connector | Importance | Privacy exposure | Protection status | Detection status |
|-----------------------|--------------|----------------------------|------------|------------------|-------------------|------------------|
| vm_datastore_202_7359 | VM datastore | onprem-connector-accou... | Standard | n/a | Protected | Active |
| vm_datastore_203_2676 | VM datastore | onprem-connector-accou... | Important | n/a | At risk | None |
| fileshare_useast_01 | File share | aws-connector-us-east-1... | Standard | n/a | At risk | None |

4. Sur la page du groupe de protection sélectionné, sélectionnez **Ajouter**.

La protection contre les ransomwares BlueXP affiche uniquement les workloads qui ne font pas déjà partie du groupe et qui utilisent les mêmes règles de copie Snapshot et de sauvegarde que le groupe.



Le haut de la page indique quel service gère les règles de snapshots, de sauvegarde et de détection.

5. Sélectionnez les charges de travail supplémentaires à ajouter au groupe.

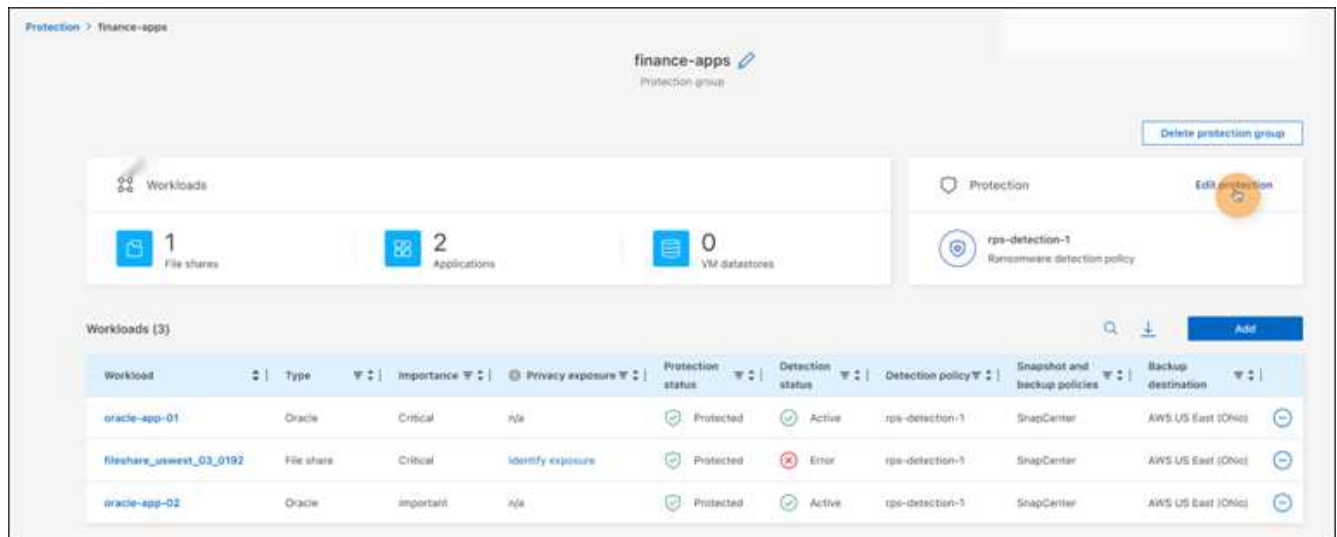
6. Sélectionnez **Enregistrer**.

Modifier la protection de groupe

Vous pouvez modifier la stratégie de détection d'un groupe existant. Si la stratégie de détection n'est pas déjà ajoutée à ce groupe, vous pouvez l'ajouter maintenant.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez l'onglet **groupes de protection**.



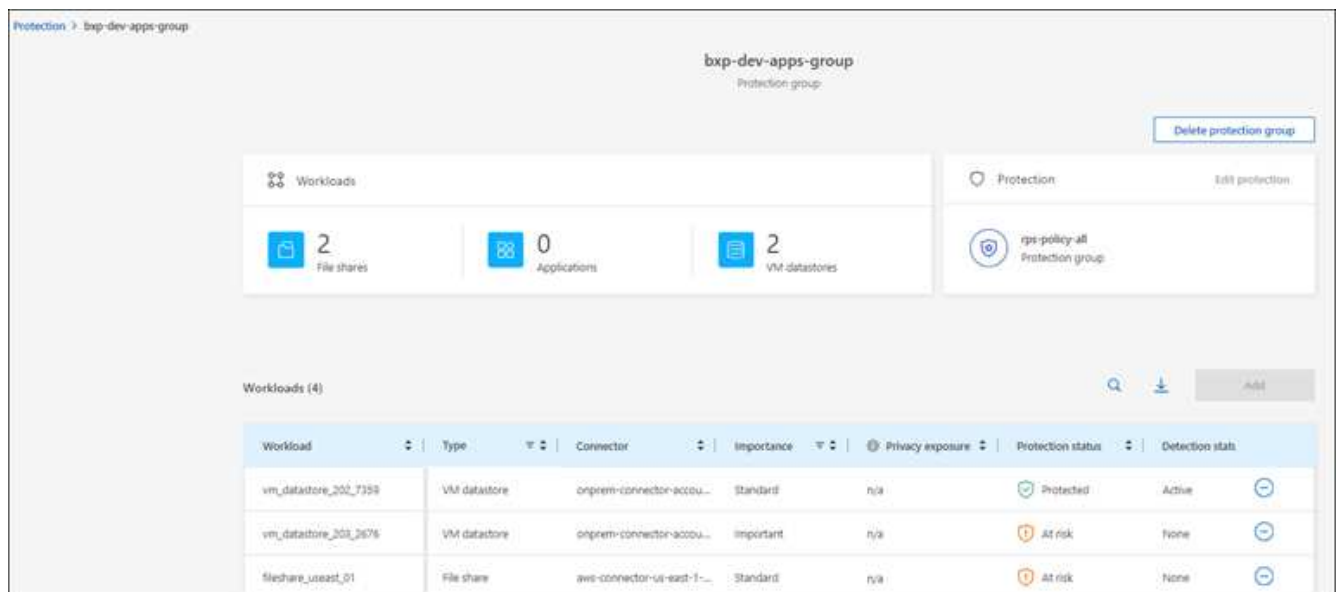
3. Dans le volet protection, sélectionnez **Modifier la protection**.
4. Sélectionnez ou ajoutez une stratégie de détection à ce groupe.

Supprimer des charges de travail d'un groupe

Vous devrez peut-être supprimer les workloads d'un groupe existant.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez l'onglet **groupes de protection**.
3. Sélectionnez le groupe dont vous souhaitez supprimer une ou plusieurs charges de travail.



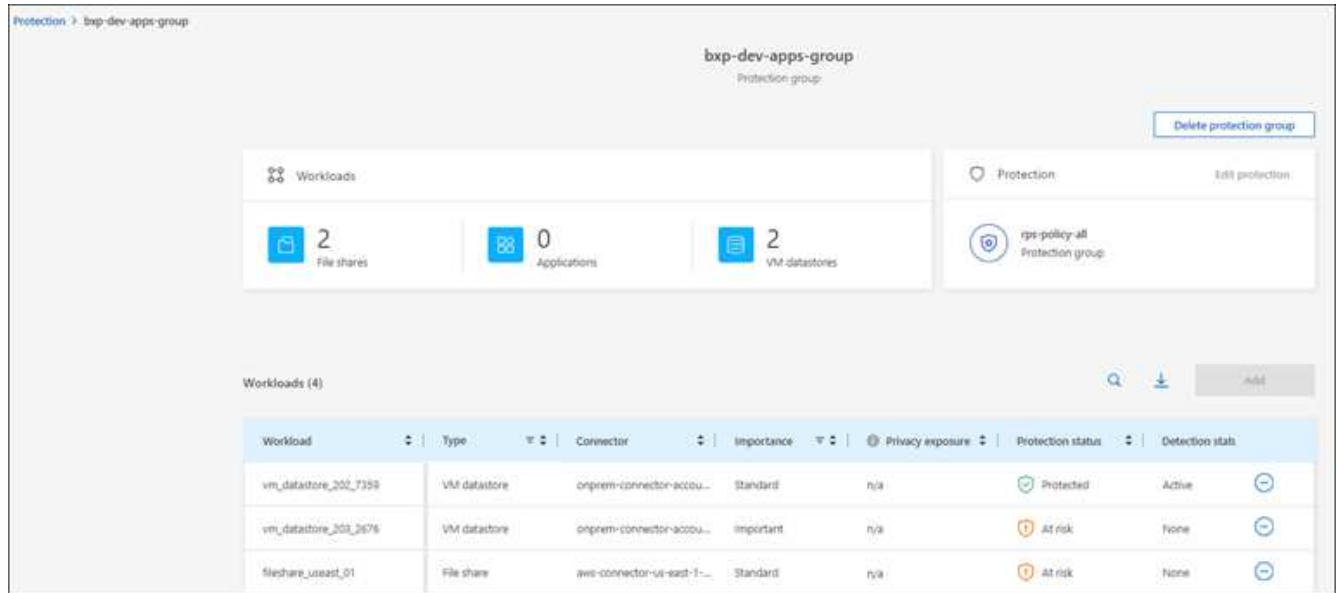
4. Dans la page Groupe de protection sélectionné, sélectionnez la charge de travail à supprimer du groupe et sélectionnez l'option ***actions***...
5. Dans le menu actions, sélectionnez **Supprimer la charge de travail**.
6. Confirmez que vous souhaitez supprimer la charge de travail et sélectionnez **Supprimer**.

Supprimer le groupe de protection

La suppression du groupe de protection supprime le groupe et sa protection, mais ne supprime pas chaque charge de travail.

Étapes

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez l'onglet **groupes de protection**.
3. Sélectionnez le groupe dont vous souhaitez supprimer une ou plusieurs charges de travail.



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

Gérer les stratégies de protection contre les ransomware

Vous pouvez supprimer une stratégie de ransomware.

Affichez les workloads protégés par une stratégie de protection contre les ransomwares

Avant de supprimer une stratégie de protection contre les ransomwares, vous pouvez consulter les workloads qui sont protégés 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 lors de l'affichage de la liste des stratégies

1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.
2. Dans la page protection, sélectionnez **gérer les stratégies de protection**.

La page stratégies de protection contre les ransomware affiche une liste de stratégies.

Protection > Ransomware protection strategies

Ransomware protection strategies

Ransomware protection strategies (4)

| Ransomware protection strategy | Snapshot policy | Backup policy | Detection policy | Protected workloads | | |
|--------------------------------|------------------------|------------------------|------------------|---------------------|---|-----|
| rpi-strategy-critical | critical-si-policy | critical-bu-policy | rpe-policy-all | 3 | ▼ | *** |
| rpi-strategy-important | important-si-policy | important-bu-policy | rpe-policy-all | 1 | ▼ | *** |
| rpi-strategy-standard | standard-si-policy | standard-bu-policy | rpe-policy-all | 0 | ▼ | *** |
| RPS strategy 4 | standard-si-policy-344 | standard-bu-policy-344 | rpe-policy-all | 0 | ▼ | *** |

list policy
Delete policy

3. Sur la page stratégies de protection contre les ransomwares, dans la colonne workloads protégés, cliquez sur la flèche vers le bas à la fin de la ligne.

Supprimez une stratégie de protection contre les ransomware

Vous pouvez supprimer une stratégie 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 de protection**.
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**.

Informations sur le copyright

Copyright © 2024 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.