Utilisez la protection BlueXP contre les ransomwares

BlueXP ransomware protection

NetApp
March 22, 2024

Sommaire

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.

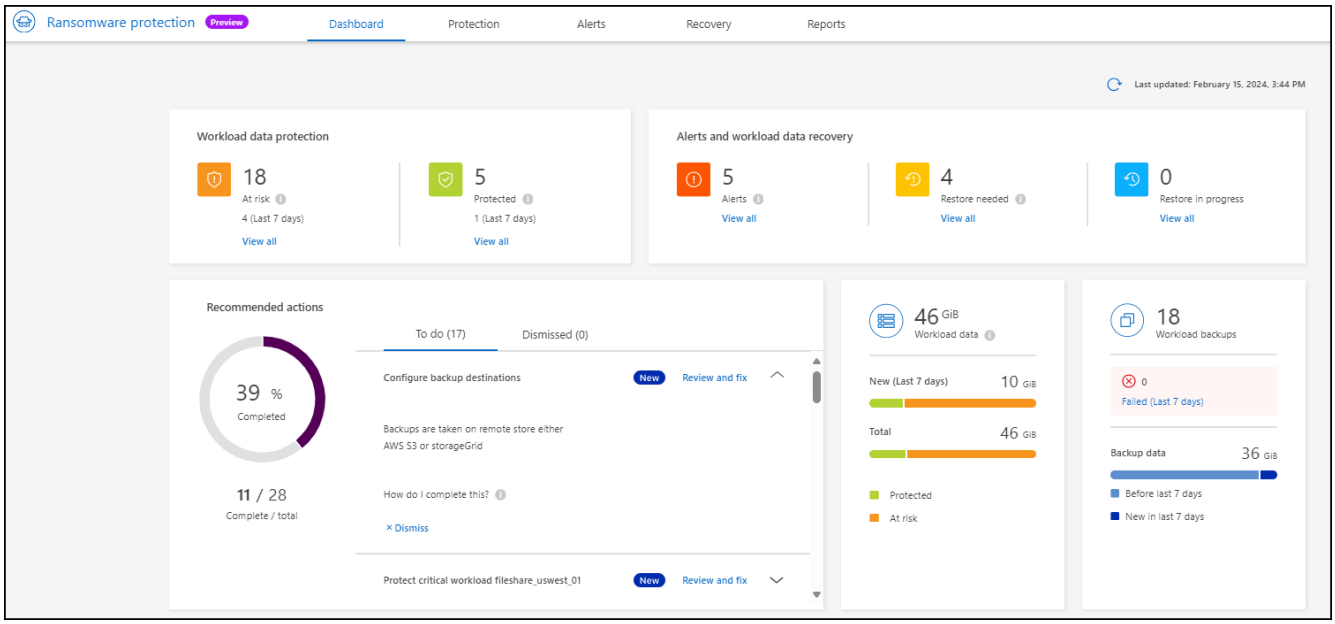
Vous pouvez également utiliser le tableau de bord pour examiner les recommandations de protection et agir en conséquence.

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.

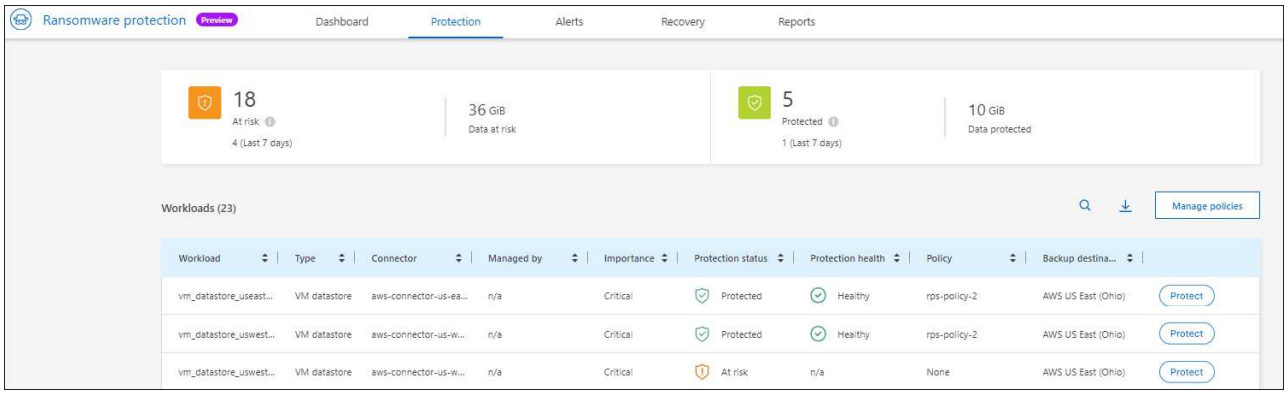
Découvrir la protection des workloads contre les ransomwares

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.

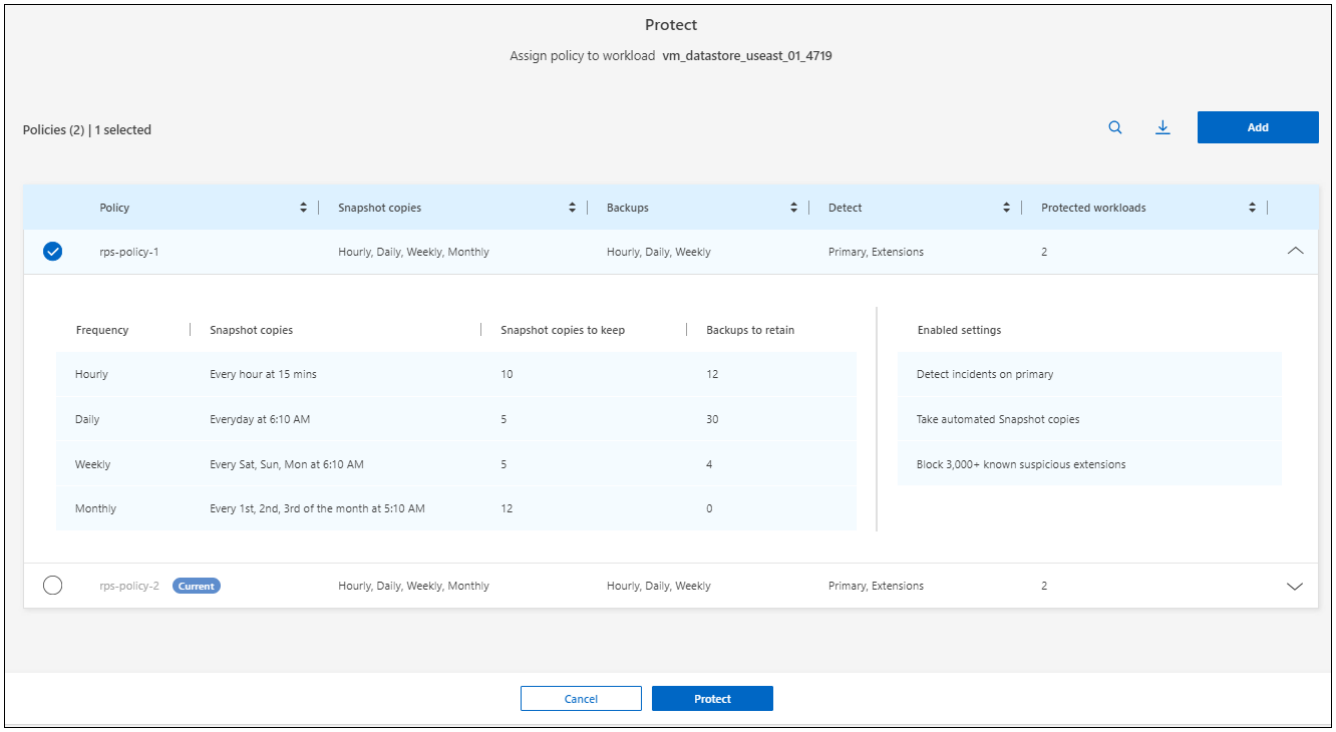
La protection contre les ransomwares BlueXP inclut les règles prédéfinies suivantes qui correspondent à la priorité des workloads :

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

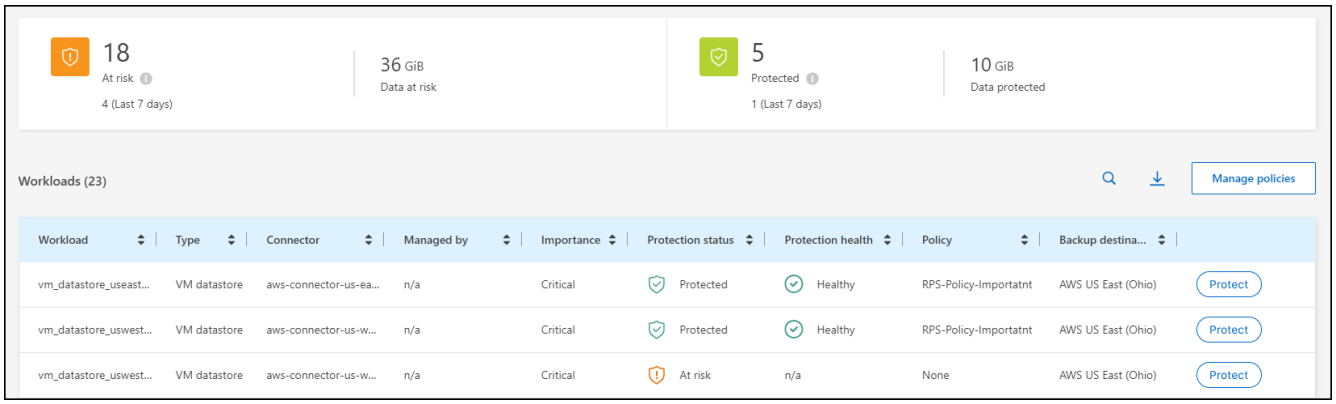
Si les règles existantes ne répondent pas aux besoins de votre entreprise, vous pouvez créer une nouvelle règle de protection. Vous pouvez créer votre propre stratégie à partir de zéro ou utiliser une stratégie existante et modifier ses paramètres.

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.

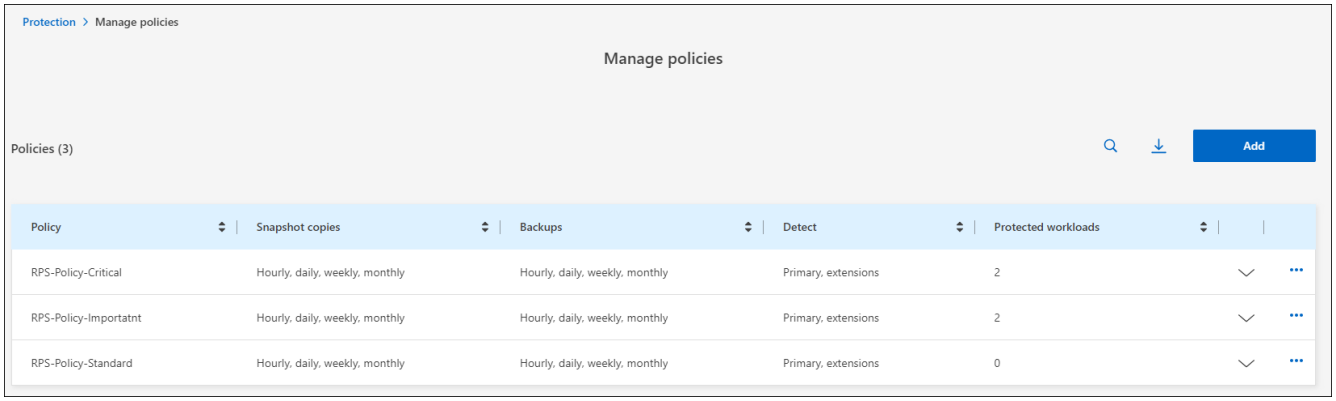
Vous pouvez créer une règle lorsque vous les gérez ou lors du processus d'attribution d'une règle à une charge de travail.

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

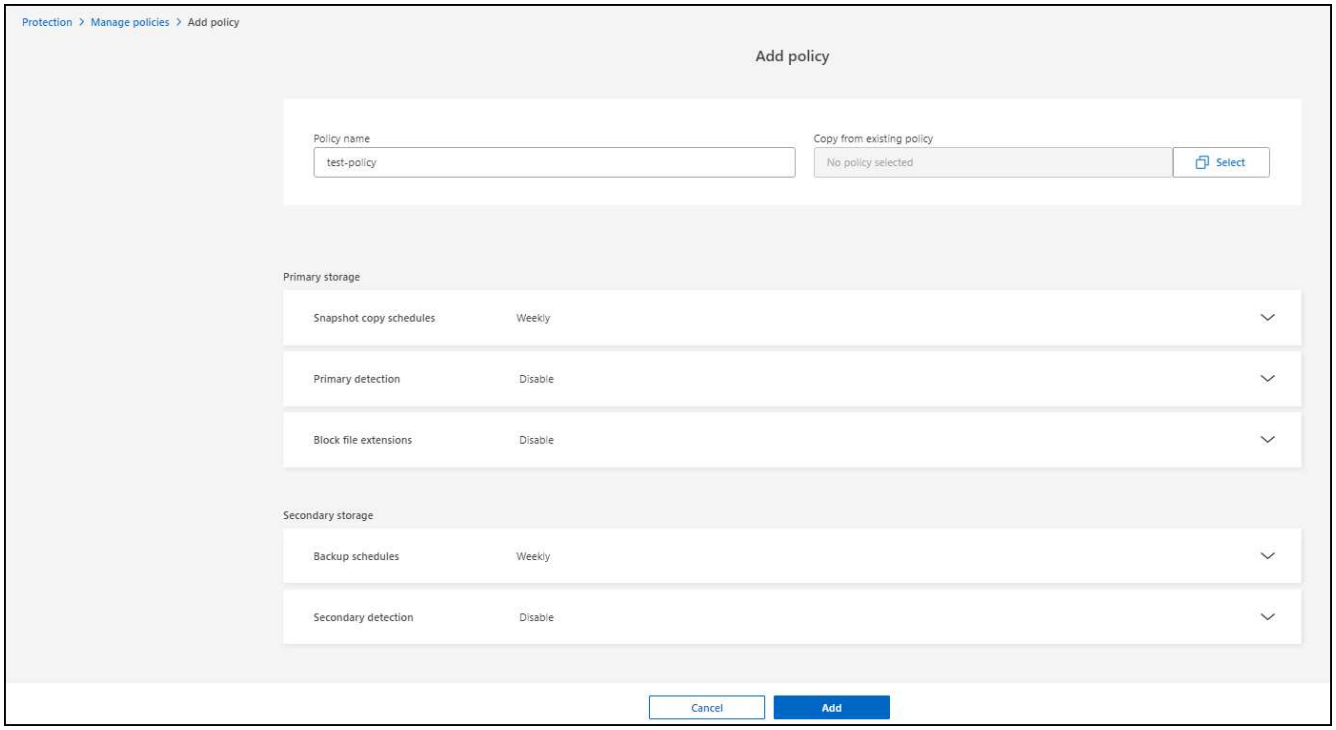
1. Dans le menu BlueXP ransomware protection, sélectionnez **protection**.



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.

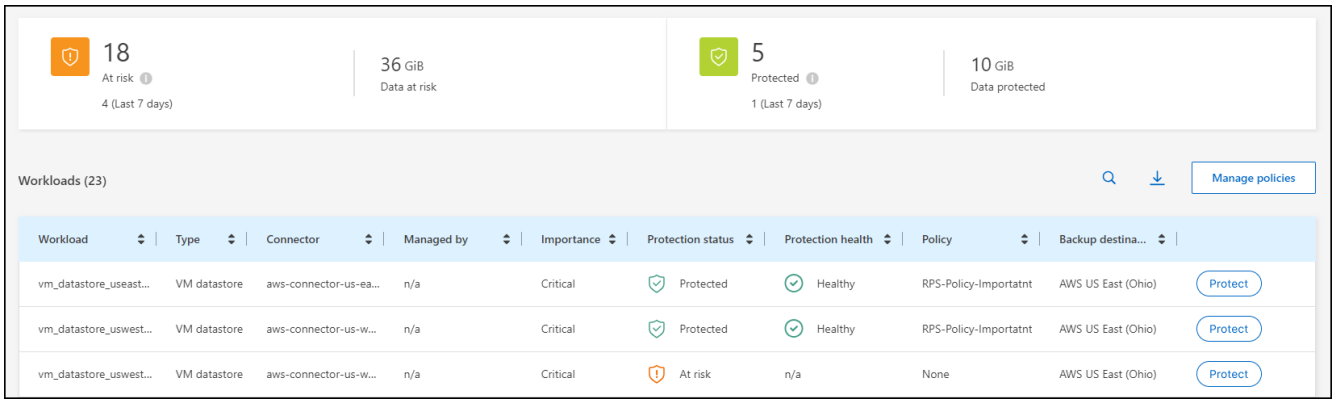
Si vous choisissez de copier et de modifier une stratégie existante, vous devez modifier au moins un paramètre pour la rendre unique.

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*.

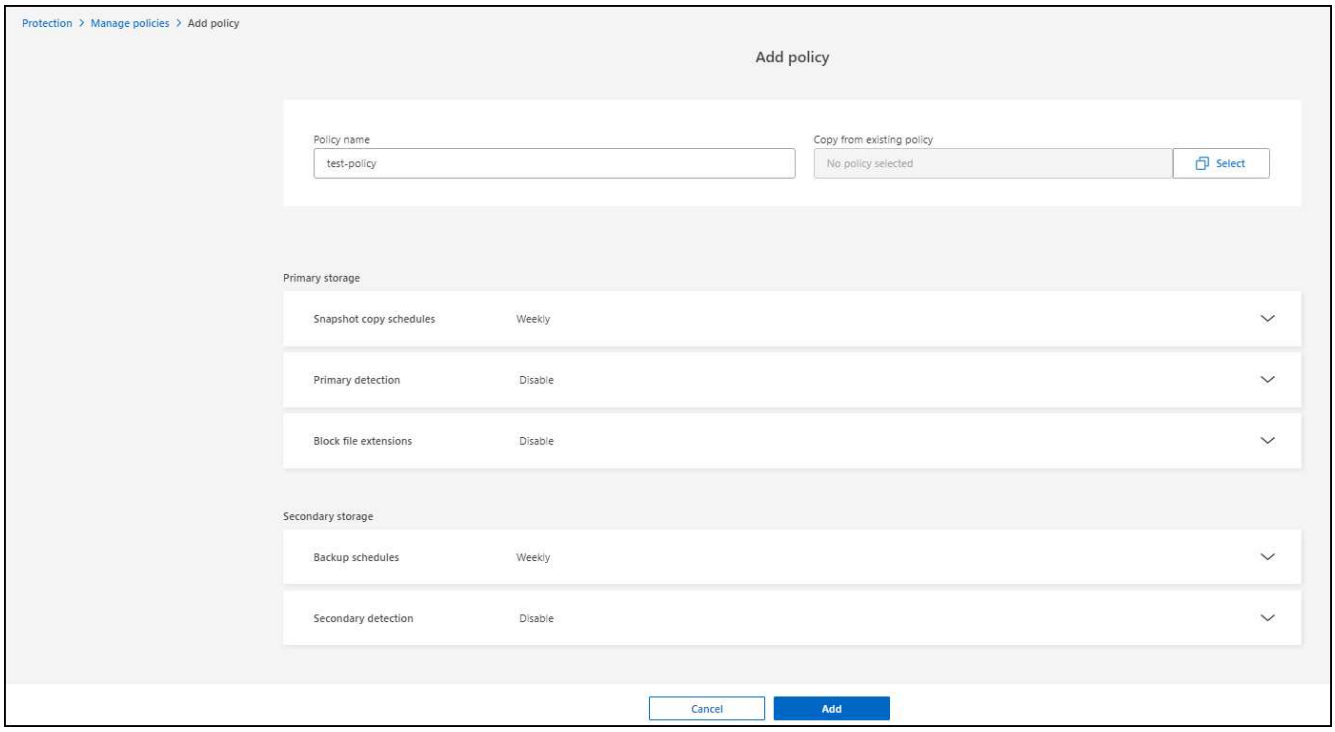
       Cette option utilise la technologie NetApp DataLock, qui verrouille les sauvegardes sur le stockage secondaire. La période pendant laquelle le fichier de sauvegarde est verrouillé (et conservé) est appelée période de rétention de DataLock. Elle est basée sur la planification de la stratégie de sauvegarde 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.

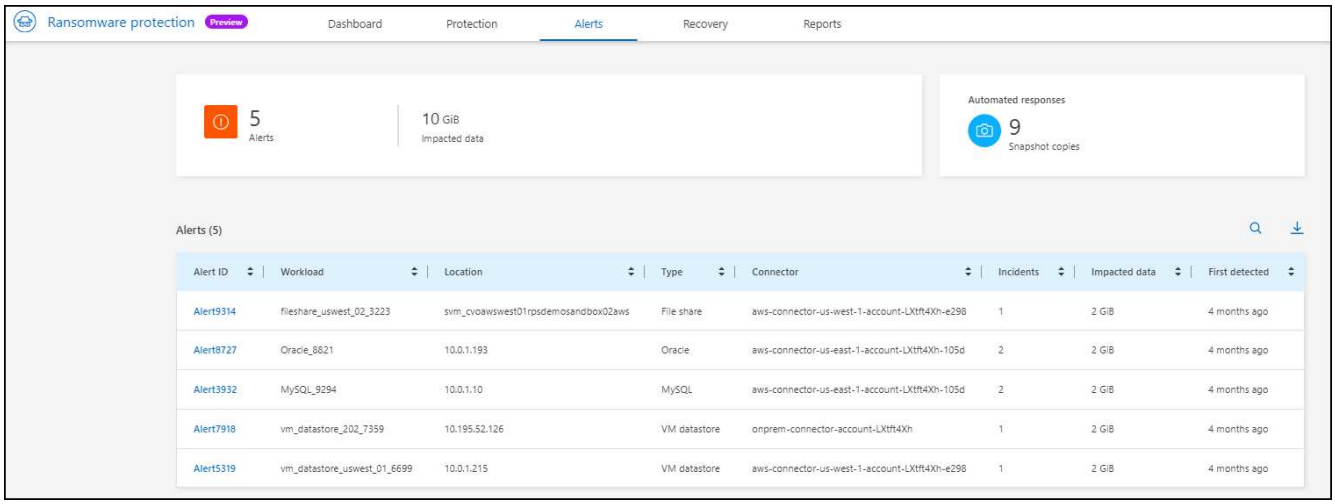
La preuve est basée sur des informations issues de la protection anti-ransomware autonome en ONTAP. Pour plus de détails, reportez-vous à "Présentation de la protection autonome contre les ransomwares".

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.



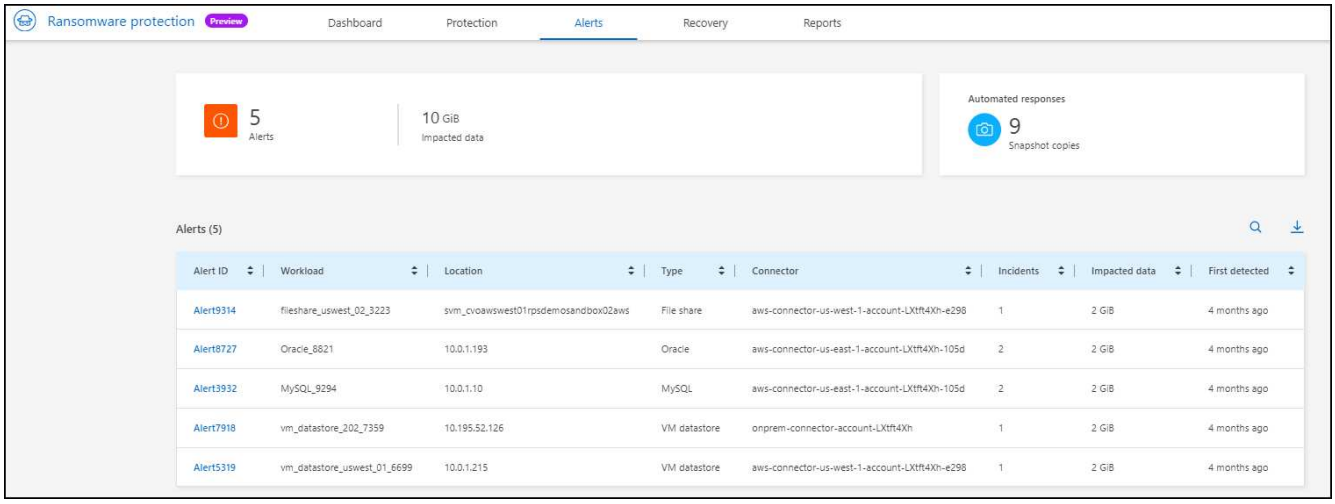
6. Passez à Marquer les incidents de ransomware comme prêts pour la restauration (après neutralisation des incidents).

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

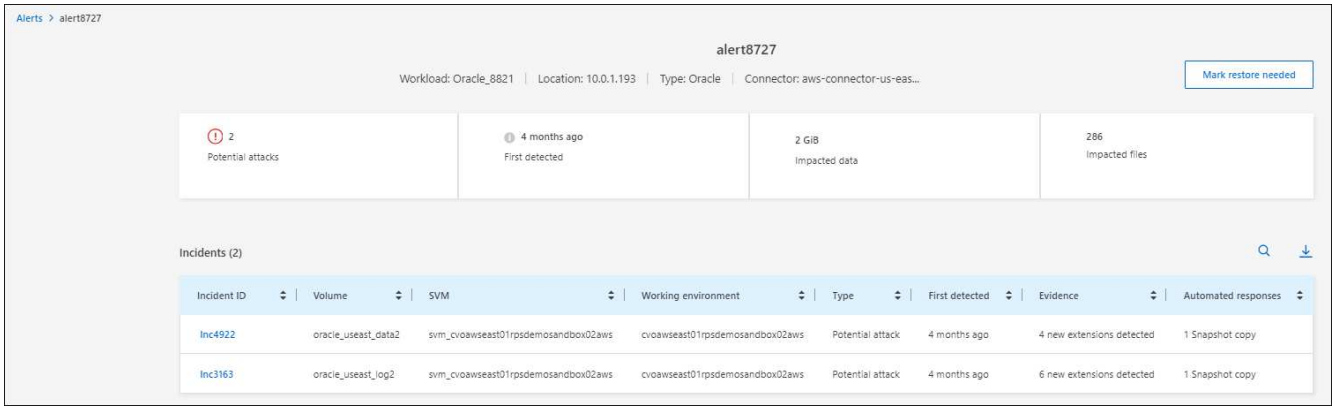
Une fois que vous avez atténué l'attaque et que vous êtes prêt à restaurer des charges de travail, vous devez communiquer avec l'équipe d'administration du stockage que les données sont prêtes pour la restauration afin qu'elles puissent démarrer le processus de restauration.

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)

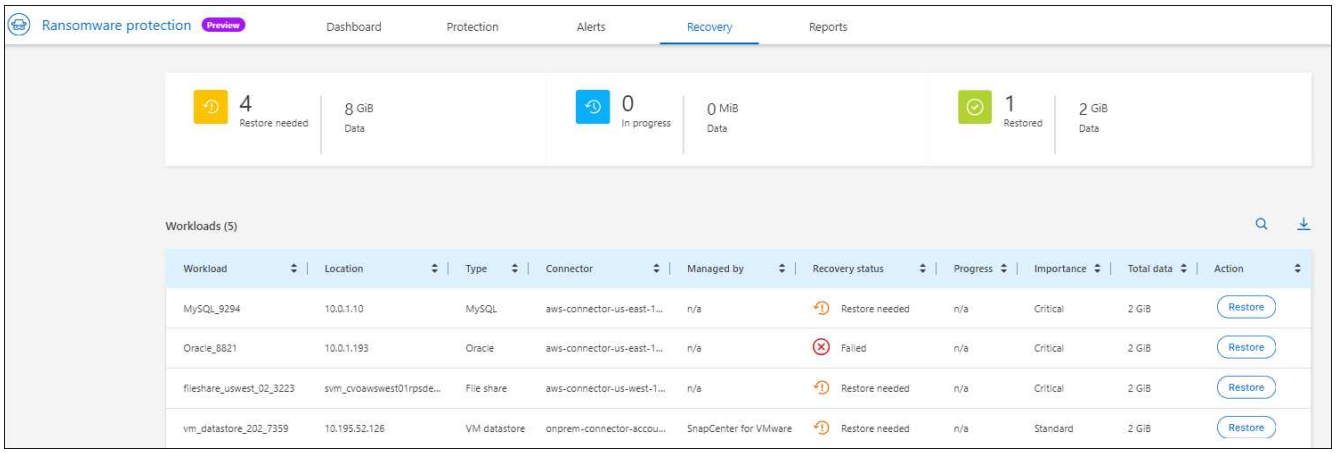
Une fois que les workloads ont été marqués comme « prêts pour la restauration », la protection contre les ransomwares BlueXP recommande une RPA (point de restauration réel) et orchestre le workflow pour une restauration résistante aux pannes.

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

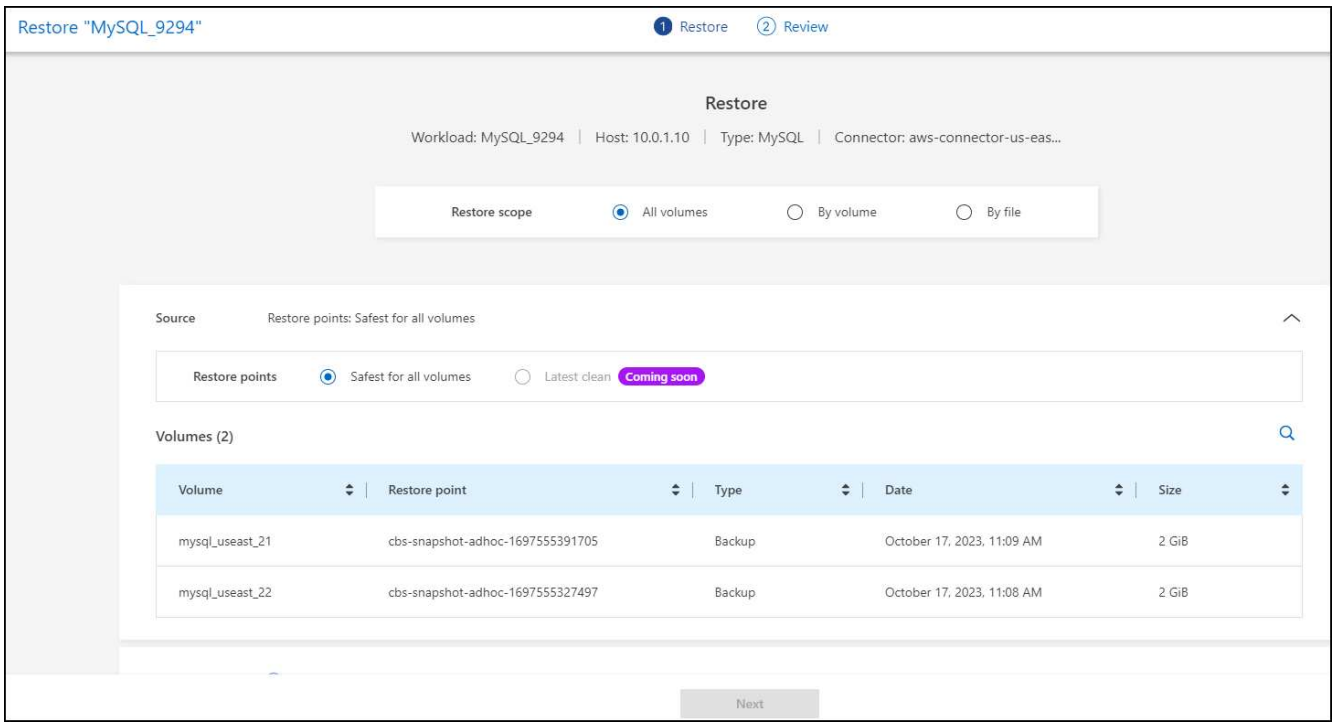
1. Dans le menu BlueXP ransomware protection, sélectionnez **Recovery**.
2. Consultez les informations sur la charge de travail à la page **récupération**.
3. Sélectionnez une charge de travail dont l'état est « Restauration requise ».
4. Pour restaurer, sélectionnez **Restaurer**.
5. **Domaine de restauration** : 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.

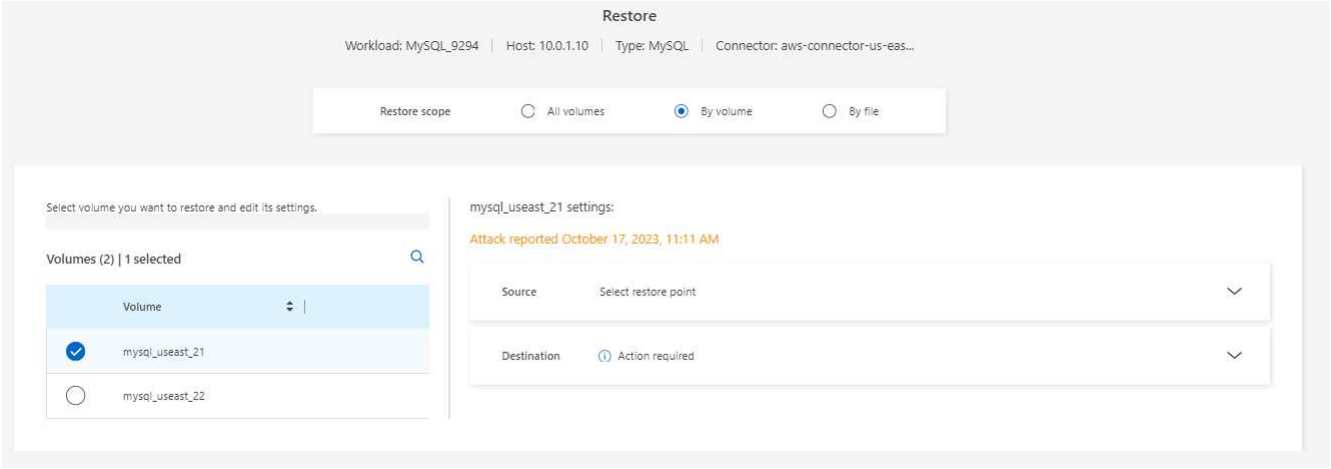
> Le nouveau nom de volume apparaît sous la forme préfixe + nom du volume d'origine + nom de la sauvegarde + date de la sauvegarde.

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.

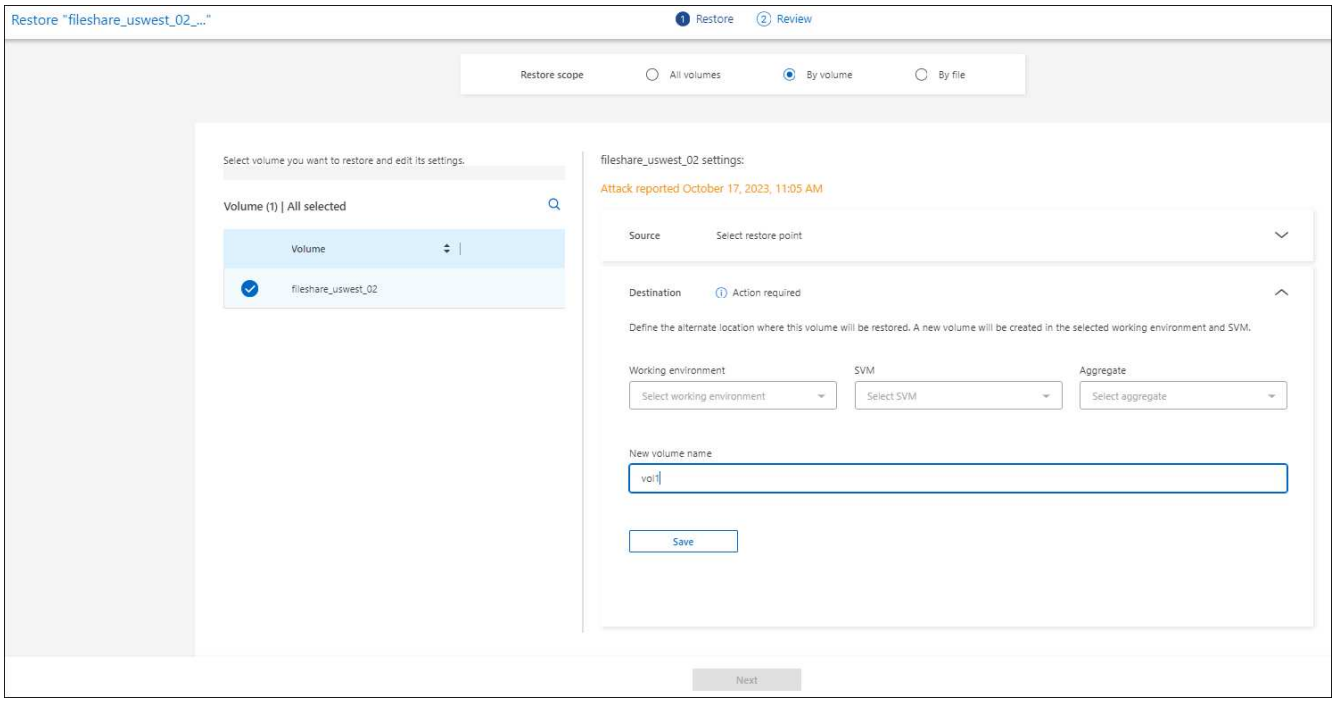
   b. Sélectionnez l'environnement de travail.
   c. Sélectionnez la VM de stockage.
   d. Si vous le souhaitez, saisissez le chemin d'accès.

      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.

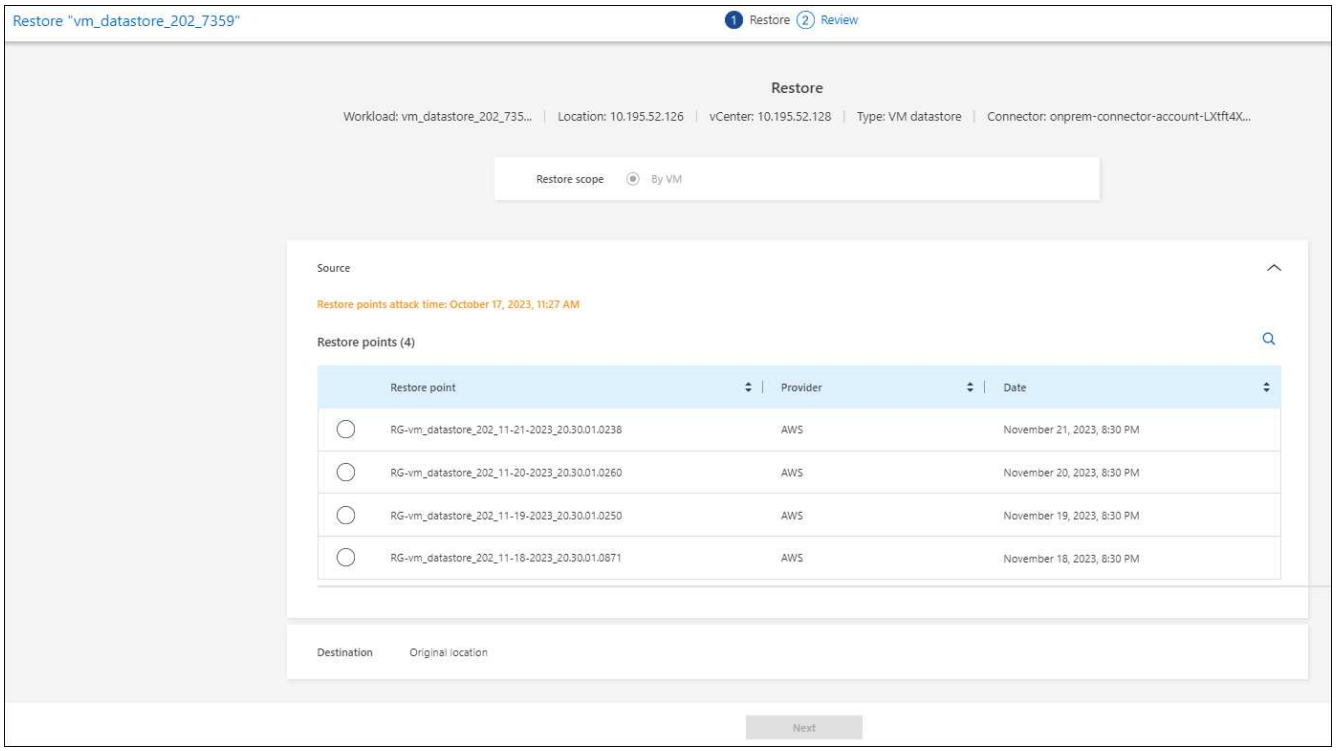
> Si vous ne spécifiez pas de chemin pour la restauration, les fichiers seront restaurés sur un nouveau volume dans le répertoire de niveau supérieur.

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.