Nutzen Sie BlueXP Ransomware-Schutz

BlueXP ransomware protection

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/de-de/bluexp-ransomware-protection/rp-use-overview.html on March 22, 2024. Always check docs.netapp.com for the latest.

Inhalt

Nutzen Sie BlueXP Ransomware-Schutz . . . 1
Nutzen Sie BlueXP Ransomware-Schutz . . . 1
Über das Dashboard können Sie den Workload-Zustand auf einen Blick anzeigen . . . 1
Schutz von Workloads vor Ransomware-Angriffen . . . 4
Reagieren Sie auf einen erkannten Ransomware-Alarm . . . 11
Wiederherstellung nach einem Ransomware-Angriff (nach dem Neutralisieren von Vorfällen) . . . 13

Nutzen Sie BlueXP Ransomware-Schutz

Nutzen Sie BlueXP Ransomware-Schutz

Durch den Ransomware-Schutz von BlueXP können Sie den Workload-Zustand anzeigen und Workloads schützen.

- "Workloads in BlueXP Ransomware-Schutz entdecken".
- "Zeigen Sie Schutz und Workload-Zustand über das Dashboard an".
  - Prüfen Sie Empfehlungen zum Schutz vor Ransomware und handeln Sie entsprechend.
- "Schutz von Workloads":
  - Weisen Sie Workloads eine Ransomware-Schutzrichtlinie zu.
  - Verbessern Sie den Applikationsschutz, um künftige Ransomware-Angriffe zu verhindern.
  - Erstellen, ändern oder löschen Sie eine Schutzrichtlinie.
- "Reagieren Sie auf die Erkennung potenzieller Ransomware-Angriffe".
- "Wiederherstellung nach einem Angriff" (Nach der Neutralisierung von Vorfällen).
- "Konfigurieren Sie die Schutzeinstellungen".

Über das Dashboard können Sie den Workload-Zustand auf einen Blick anzeigen

Das BlueXP Dashboard zum Schutz vor Ransomware bietet auf einen Blick Informationen zum Schutz der Integrität Ihrer Workloads. Sie können schnell ermitteln, welche Workloads gefährdet oder geschützt sind, Workloads identifizieren, die von einem Vorfall oder einer Recovery betroffen sind, und den Umfang der Sicherung abschätzen, indem Sie die Menge des geschützten oder gefährdeten Storage ermitteln.

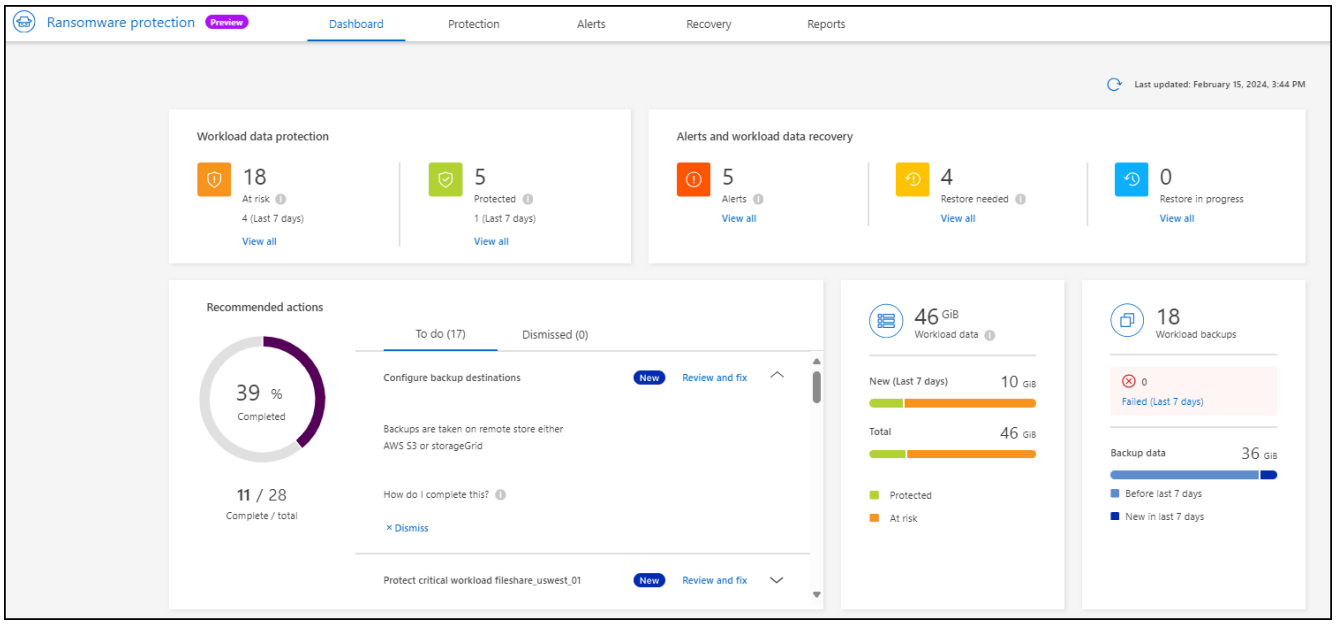
Darüber hinaus können Sie mithilfe des Dashboards Schutzempfehlungen prüfen und umsetzen.

Überprüfen Sie mithilfe des Dashboards den Workload-Systemzustand

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Schutz** > **Ransomware-Schutz**.

   Nach der Erkennung wird über das Dashboard der Systemzustand der Workload-Datensicherung angezeigt.



2. Im Dashboard können Sie in jedem der Teilfenster eine der folgenden Aktionen anzeigen und ausführen:

   - **Workload Data Protection**: Klicken Sie auf **View all**, um alle Workloads anzuzeigen, die gefährdet oder geschützt sind. Workloads sind gefährdet, wenn Sicherungsstufen mit einer Sicherungsrichtlinie nicht übereinstimmen. Siehe "Schutz von Workloads".
   - **Warnungen und Workload-Daten-Recovery**: Klicken Sie auf **Alle anzeigen**, um aktive Vorfälle zu sehen, die sich auf Ihre Arbeitslast ausgewirkt haben, nach Neutralisierung der Vorfälle zur Wiederherstellung bereit sind oder sich in der Wiederherstellung befinden. Siehe "Reagieren Sie auf eine erkannte Warnung".

     Ein Vorfall wird in einen der folgenden Status kategorisiert:

     - Betroffen (wird auf der Seite „Warnungen“ angezeigt)
     - Bereit für die Wiederherstellung (wird auf der Wiederherstellungsseite angezeigt)
     - Wiederherstellen (wird auf der Wiederherstellungsseite angezeigt)
     - Wiederherstellung fehlgeschlagen (wird auf der Wiederherstellungsseite angezeigt)
     - Wiederhergestellt (wird auf der Wiederherstellungsseite angezeigt)
   - **Empfohlene Maßnahmen**: Um den Schutz zu erhöhen, überprüfen Sie jede Empfehlung und klicken Sie auf **Überprüfen und beheben**.

     Siehe "Prüfen Sie die Schutzempfehlungen auf dem Dashboard" Oder "Schutz von Workloads".

     Alle Empfehlungen, die seit dem letzten Besuch des Dashboards hinzugefügt wurden, werden mindestens 24 Stunden lang mit „Neu“ gekennzeichnet. Die Aktionen werden in der Reihenfolge der Priorität aufgelistet, wobei die wichtigsten oben stehen. Sie können jede einzelne Person überprüfen und bearbeiten oder sie ablehnen.

Die Gesamtzahl der Aktionen umfasst keine abgewiesen Aktionen.

   - **Workload-Daten**: Überwachen Sie Änderungen der Schutzabdeckung in den letzten 7 Tagen.
   - **Workload Backups**: Überwachen Sie Änderungen in Workload Backups, die vom Service erstellt wurden und die in den letzten 7 Tagen erfolgreich abgeschlossen wurden.

Prüfen Sie die Schutzempfehlungen auf dem Dashboard

Der Ransomware-Schutz von BlueXP bewertet den Schutz Ihrer Workloads und empfiehlt Maßnahmen, um diesen Schutz zu verbessern.

Sie können eine Empfehlung prüfen und darauf reagieren, wodurch der Empfehlungsstatus auf „Abschließen“ geändert wird. Oder, wenn Sie darauf später reagieren wollen, können Sie es abtun. Wenn Sie eine Aktion abwählen, wird die Empfehlung in eine Liste abgewiesen, die Sie später noch einmal überprüfen können.

Hier eine Auswahl der Empfehlungen, die der Service anbietet.

Empfehlung	Beschreibung	Wie wird das Problem behoben
Fügen Sie eine Schutzrichtlinie für Ransomware hinzu	Der Workload ist derzeit nicht geschützt.	Weisen Sie dem Workload eine Richtlinie zu. Siehe "Schutz von Workloads vor Ransomware-Angriffen".
Konfigurieren Sie Sicherungsziele	Der Workload verfügt derzeit über keine Sicherungsziele.	Fügen Sie diesem Workload Sicherungsziele hinzu, um ihn zu schützen. Siehe "Konfigurieren Sie die Schutzeinstellungen".
Machen Sie eine Politik stärker.	Einige Workloads verfügen möglicherweise nicht über ausreichend Sicherung. Höherer Schutz von Workloads mit einer Richtlinie	Erhöhen Sie die Aufbewahrung, fügen Sie Backups hinzu, erzwingen Sie unveränderliche Backups, blockieren Sie verdächtige Dateierweiterungen, ermöglichen Sie die Erkennung auf sekundärem Storage und vieles mehr. Siehe "Schutz von Workloads vor Ransomware-Angriffen".
Schützen Sie kritische oder wichtige Applikations-Workloads vor Ransomware.	Auf der Seite Schutz werden kritische oder wichtige (auf der Grundlage der Prioritätsstufe zugewiesene) Anwendungs-Workloads angezeigt, die nicht geschützt sind.	Weisen Sie diesen Workloads eine Richtlinie zu. Siehe "Schutz von Workloads vor Ransomware-Angriffen".
Schützen Sie kritische oder wichtige File-Share-Workloads vor Ransomware.	Auf der Seite Schutz werden kritische oder wichtige Workloads des Typs Dateifreigabe oder Datenspeicher angezeigt, die nicht geschützt sind.	Weisen Sie jedem Workload eine Richtlinie zu. Siehe "Schutz von Workloads vor Ransomware-Angriffen".
Überprüfen Sie neue Warnmeldungen	Es sind neue Warnmeldungen vorhanden.	Überprüfen Sie die neuen Warnmeldungen. Siehe "Reagieren Sie auf einen erkannten Ransomware-Alarm".

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Schutz** > **Ransomware-Schutz**.
2. Wählen Sie im Bereich Empfohlene Maßnahmen eine Empfehlung aus und wählen Sie **Überprüfen und**

beheben.

3. Um die Aktion bis zu einem späteren Zeitpunkt zu beenden, wählen Sie **Verwerfen**.

   Die Empfehlung wird aus der To-Do-Liste gelöscht und in der Ablehnte-Liste angezeigt.

   > Sie können ein verworfener Artikel später in ein To-Do-Element ändern. Wenn Sie ein Element als abgeschlossen markieren oder ein verlassener Eintrag in eine Aktion zum Erledigten ändern, erhöht sich die Gesamtzahl der Aktionen um 1.

4. Um Informationen zur Vorgehensweise bei den Empfehlungen zu lesen, wählen Sie das Symbol **information**.

Schutz von Workloads vor Ransomware-Angriffen

Sie können Ihre Workloads gegen Ransomware-Angriffe schützen, indem Sie die folgenden Aktionen durchführen, die BlueXP Ransomware-Schutz nutzen.

- Zeigen Sie den Schutz vorhandener Workloads an.
- Zuweisung einer Richtlinie zu einem Workload
  - Erhöhen Sie den Anwendungsschutz, um zukünftige RW-Angriffe zu verhindern.
  - Ändern Sie den Schutz für eine Arbeitslast, die zuvor im RW-Dienst geschützt war.
- Verwalten von Richtlinien (nur die von Ihnen erstellten).

BlueXP vor Ransomware-Schutz weist jedem Workload während der Erkennung eine Priorität zu. Die Workload-Priorität wird durch die folgenden Snapshot-Häufigkeit festgelegt:

- **Kritisch**: Snapshot Kopien wurden weniger als 1 pro Stunde erstellt (äußerst ambitionierter Schutzplan)
- **Wichtig**: Snapshot-Kopien wurden weniger als 1 pro Tag, aber mehr als 1 pro Stunde erstellt
- **Standard**: Snapshot Kopien wurden pro Tag erstellt

Schutzstatus: Ein Workload kann einen der folgenden Schutzstatus anzeigen, um anzugeben, ob eine Richtlinie angewendet wird oder nicht:

- **Geschützt**: Es wird eine Richtlinie angewendet.
- **In Gefahr**: Es werden keine Richtlinien angewendet.
- **In Bearbeitung**: Eine Richtlinie wird angewendet, aber noch nicht abgeschlossen.
- **Failed**: Eine Richtlinie wird angewendet, funktioniert aber nicht.

Schutzgesundheit: Ein Arbeitsvolumen kann einen der folgenden Schutzgesundheitsstatus haben:

- **Funktionstüchtiger**: Der Workload hat Schutz aktiviert und Backups und Snapshot Kopien wurden abgeschlossen.
- **In Bearbeitung**: Backups oder Snapshot Kopien werden ausgeführt.
- **Failed**: Backups oder Snapshot Kopien wurden nicht erfolgreich abgeschlossen.
- **N/A**: Der Schutz ist für den Workload nicht aktiviert oder ausreichend.

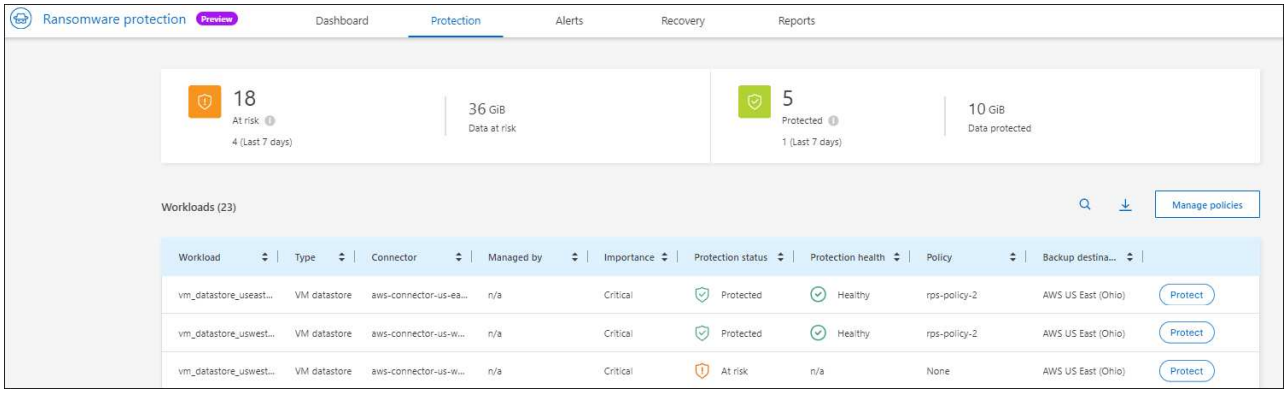
Schutz vor Workload-Ransomware ansehen

Einer der ersten Schritte zum Schutz von Workloads besteht darin, dass Sie Ihre aktuellen Workloads und ihren Sicherungsstatus anzeigen. Es werden die folgenden Workload-Typen angezeigt:

- VM-Workloads
- Workloads für Dateifreigabe

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Schutz** > **Ransomware-Schutz**.
2. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie im Dashboard Data Protection die Option **Alle anzeigen** aus.
    - Wählen Sie im Menü **Schutz**.



3. Auf dieser Seite können Sie einem Workload eine Richtlinie zuweisen.

Weisen Sie Workloads eine vordefinierte Schutzrichtlinie zu

Zum Schutz Ihrer Daten können Sie einer oder mehreren Workloads eine bestehende Richtlinie zum Schutz vor Ransomware zuweisen. Sie können auch einem Workload, der bereits über eine Richtlinie verfügt, eine andere Richtlinie zuweisen.

Der Ransomware-Schutz von BlueXP umfasst die folgenden vordefinierten Richtlinien, die auf die Workload-Priorität ausgerichtet sind:

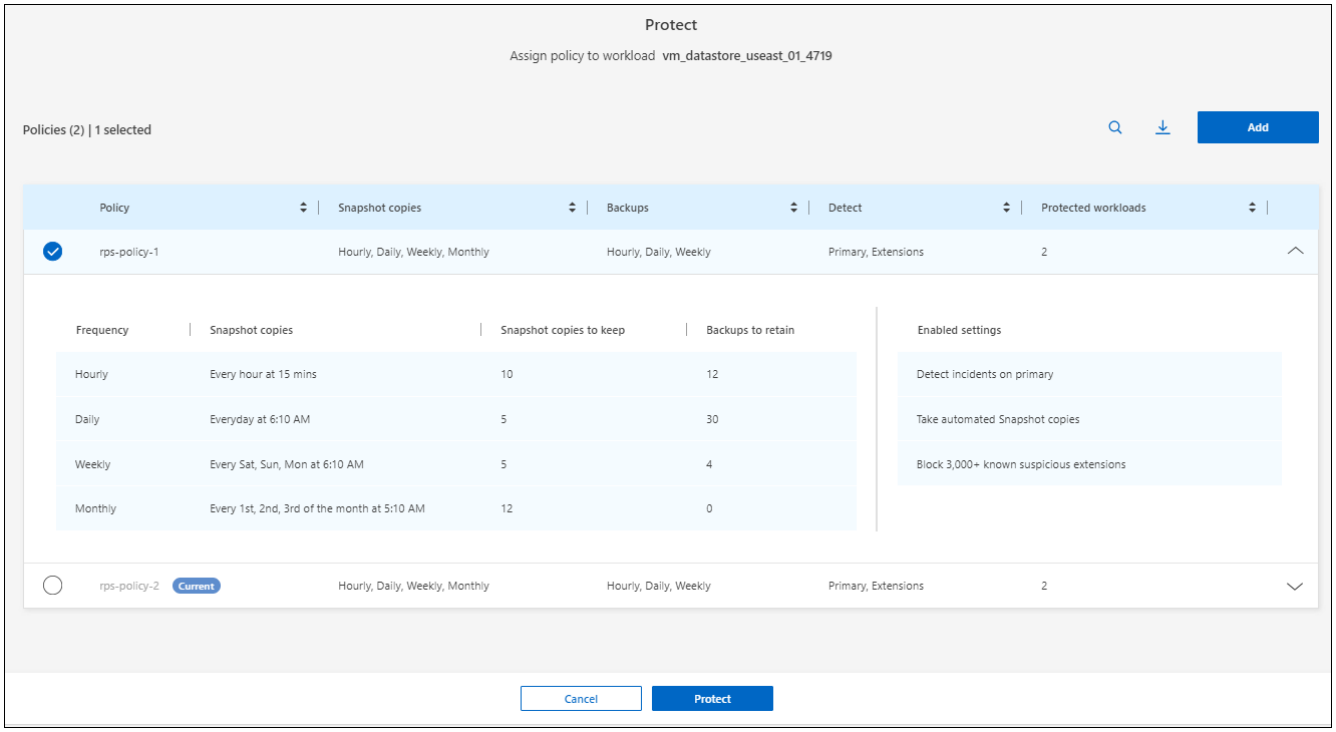
Richtlinienebene	Snapshot	Frequenz	Aufbewahrung (Tage)	# An Snapshot Kopien	Max. # Snapshot Kopien insgesamt
Richtlinie für kritische Workloads	Quartal stündlich	Alle 15 Min	3	288	309
	Täglich	Alle 1 Tag	14	14	309
	Wöchentlich	Alle 1 Woche	35	5	309
	Monatlich	Alle 30 Tage	60	2	309

Richtlinienebene	Snapshot	Frequenz	Aufbewahrung (Tage)	# An Snapshot Kopien	Max. # Snapshot Kopien insgesamt
Wichtige Workload Policy	Quartal stündlich	Alle 30 Minuten	3	144	165
	Täglich	Alle 1 Tag	14	14	165
	Wöchentlich	Alle 1 Woche	35	5	165
	Monatlich	Alle 30 Tage	60	2	165
Richtlinie für Standard-Workloads	Quartal stündlich	Alle 60 Min	3	72	93
	Täglich	Alle 1 Tag	14	14	93
	Wöchentlich	Alle 1 Woche	35	5	93
	Monatlich	Alle 30 Tage	60	2	93

Schritte

1. Von BlueXP vor dem Ransomware-Schutz haben Sie einen der folgenden Möglichkeiten:
   - Wählen Sie im Dashboard Data Protection die Option **Alle anzeigen** aus.
   - Wählen Sie im Dashboard-Empfehlungsfenster eine Empfehlung zum Zuweisen einer Richtlinie aus und wählen Sie **Überprüfen und beheben** aus.
   - Wählen Sie im Menü **Schutz**.
2. Überprüfen Sie auf der Seite Schutz die Workloads, und wählen Sie neben dem Workload **protect** aus.

   Eine Liste der Richtlinien wird angezeigt.



3. Um Details anzuzeigen, klicken Sie auf den Abwärtspfeil einer Richtlinie.
4. Wählen Sie eine Richtlinie aus, die dem Workload zugewiesen werden soll.
5. Wählen Sie **Schutz**.
6. Überprüfen Sie den Fensterbereich Empfohlene Maßnahmen im Dashboard, in dem die Aktion als abgeschlossen angezeigt wird.

Erstellen Sie eine Schutzrichtlinie

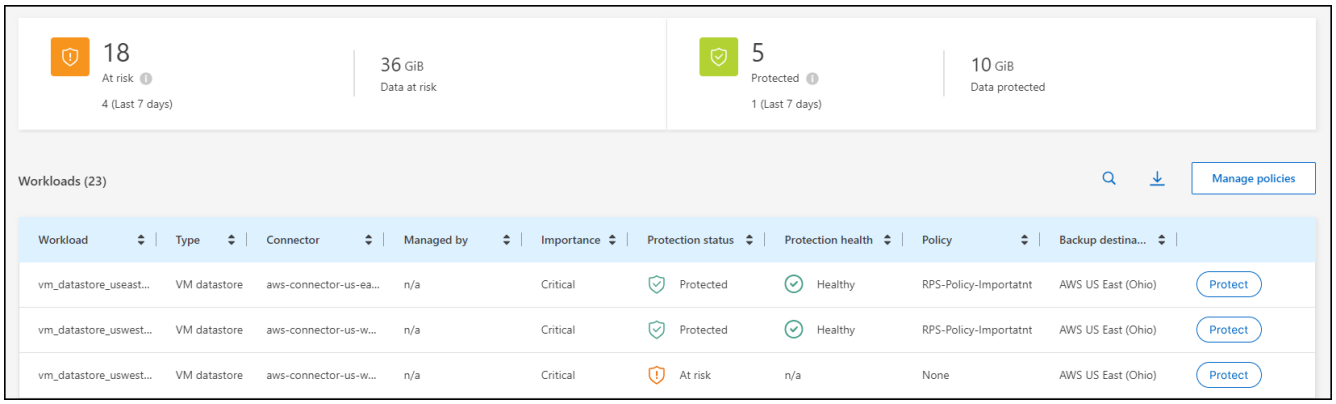
Wenn die vorhandenen Richtlinien Ihren geschäftlichen Anforderungen nicht entsprechen, können Sie eine neue Sicherungsrichtlinie erstellen. Sie können Ihre eigene Richtlinie von Grund auf neu erstellen oder eine vorhandene Richtlinie verwenden und deren Einstellungen ändern.

Sie können Richtlinien erstellen, die für primären und sekundären Storage gelten und primären und sekundären Storage auf dieselbe oder unterschiedliche Weise behandeln.

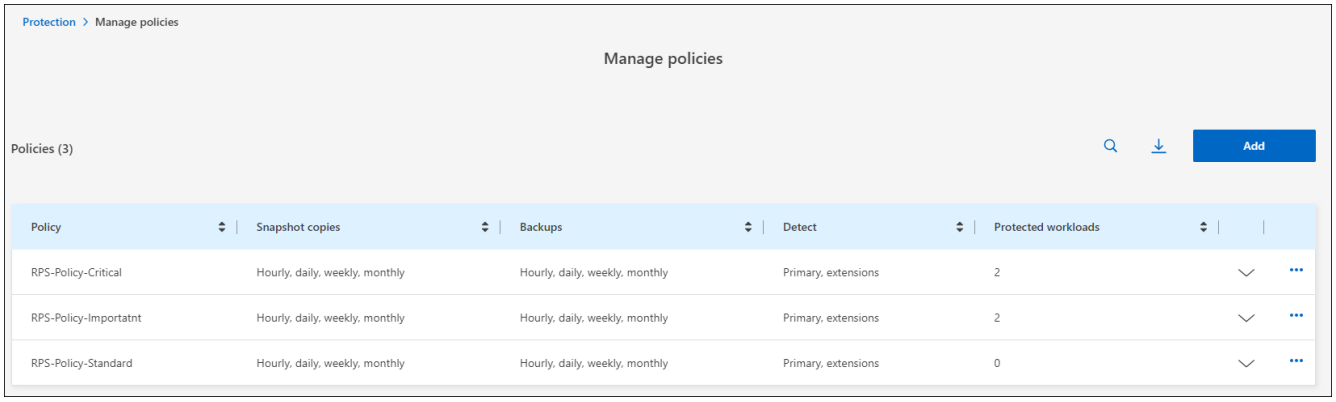
Sie können eine Richtlinie sowohl beim Management als auch beim Zuweisen einer Richtlinie zu einem Workload erstellen.

Schritte zum Erstellen einer Richtlinie während der Richtlinienverwaltung

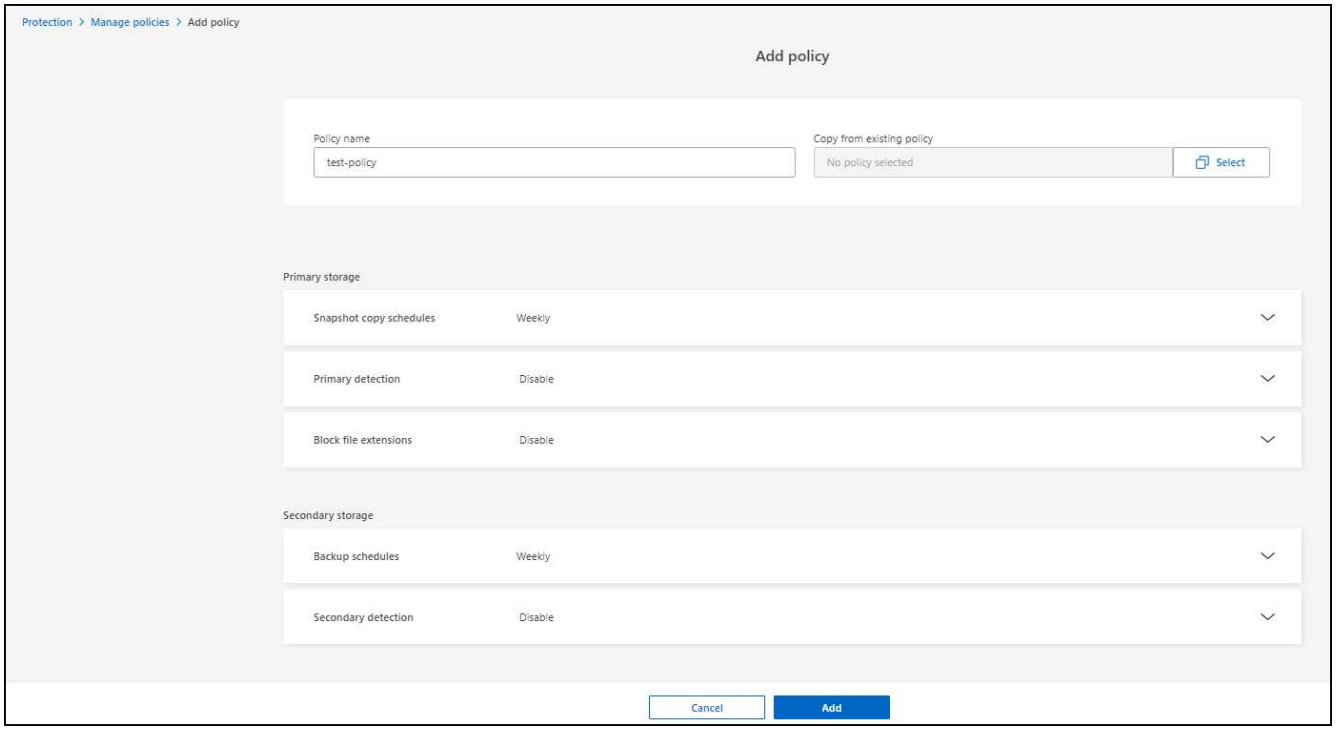
1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Protection** aus.



2. Wählen Sie auf der Seite Schutz die Option **Richtlinien verwalten** aus.



3. Wählen Sie auf der Seite Manage Policies die Option **Add** aus.



4. Geben Sie einen neuen Richtliniennamen ein, oder geben Sie einen vorhandenen Richtliniennamen ein, um ihn zu kopieren. Wenn Sie einen vorhandenen Richtliniennamen eingeben, wählen Sie die zu kopierende Richtlinie aus.

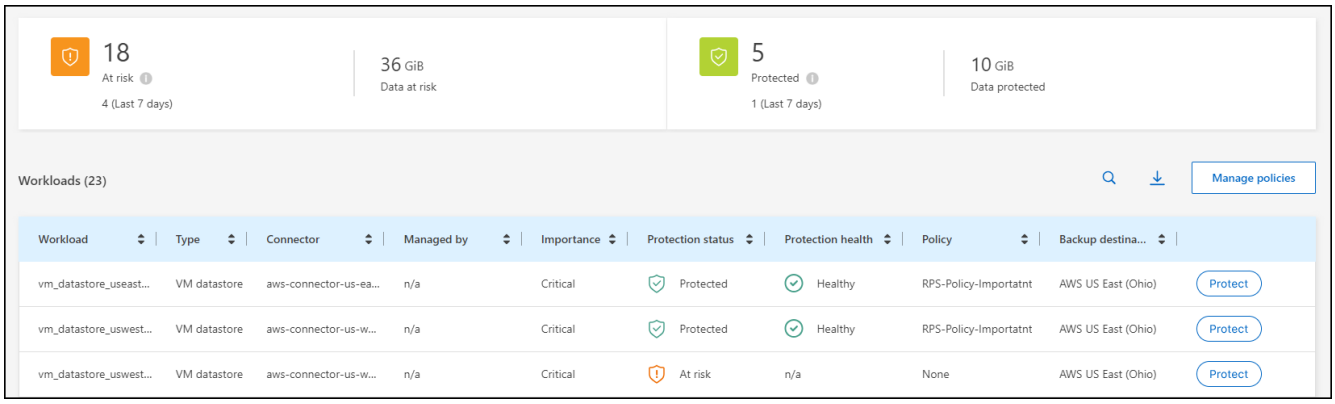
> Wenn Sie eine vorhandene Richtlinie kopieren und ändern möchten, müssen Sie mindestens eine Einstellung ändern, um sie eindeutig zu machen.

5. Wählen Sie für jedes Element den Abwärtspfeil aus.
   - **Primärspeichersysteme**:
     - **Zeitpläne für Snapshot Kopien**: Wählen Sie Zeitplanoptionen, die Anzahl der zu bewahrenden Snapshot Kopien und wählen Sie aus, um den Zeitplan zu aktivieren.
     - **Primärerkennung**: Aktivieren Sie den Service, um Ransomware-Vorfälle auf dem primären Speicher zu erkennen.
     - **Dateierweiterungen blockieren**: Aktivieren Sie diese, damit der Service-Block verdächtige Dateierweiterungen kennt. Der Service erstellt automatisierte Snapshot-Kopien, wenn die primäre Erkennung aktiviert ist.
   - **Sekundärer Speicher**:
     - **Backup-Zeitpläne**: Wählen Sie Zeitplanoptionen für sekundären Speicher und aktivieren Sie den Zeitplan.
     - **Secondary Detection**: Aktivieren Sie den Service, um Ransomware-Vorfälle auf sekundärem Speicher zu erkennen.
     - **Backups sperren**: Wählen Sie diese Option, um zu verhindern, dass Backups auf dem sekundären Speicher für einen bestimmten Zeitraum geändert oder gelöscht werden. Dies wird auch *unveränderlicher Storage* genannt.

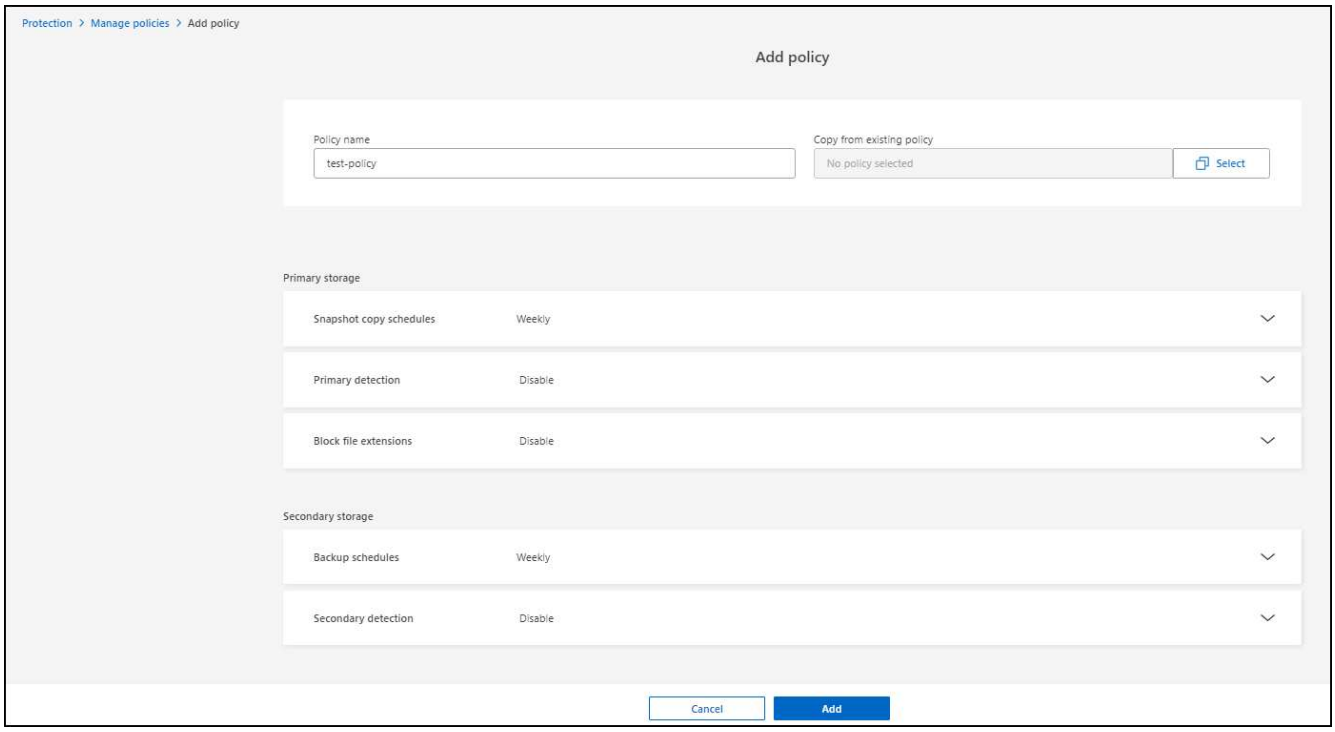
       Diese Option verwendet die NetApp DataLock-Technologie, mit der Backups auf sekundärem Speicher gesperrt werden. Der Zeitraum, in dem die Sicherungsdatei gesperrt (und aufbewahrt) ist, wird als Aufbewahrungszeitraum für DataLock bezeichnet. Er basiert auf dem von Ihnen definierten Zeitplan für die Backup-Richtlinie und der Aufbewahrungseinstellung sowie auf einem Puffer von 14 Tagen. Jede DataLock-Aufbewahrungsrichtlinie, die weniger als 30 Tage beträgt, wird auf mindestens 30 Tage aufgerundet.
6. Wählen Sie **Hinzufügen**.

Schritte zum Erstellen einer Richtlinie während der Zuweisung von Schutzrichtlinien

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Protection** aus.



2. Wählen Sie auf der Seite Schutz die Option **Schutz** aus.
3. Wählen Sie auf der Seite Schutz die Option **Hinzufügen**.



4. Schließen Sie den Prozess ab. Dies entspricht dem Erstellen einer Richtlinie auf der Seite „Richtlinien managen“.

Weisen Sie eine andere Schutzrichtlinie zu

Sie können eine andere Sicherungsrichtlinie für einen Workload auswählen.
Vielleicht möchten Sie den Schutz erhöhen, um zukünftige Ransomware-Angriffe durch eine Änderung der Sicherungsrichtlinie zu verhindern.

Schritte

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Protection** aus.
2. Wählen Sie auf der Seite Schutz einen Workload aus, und wählen Sie **Schutz** aus.
3. Wählen Sie auf der Seite Schutz eine andere Richtlinie für den Workload aus.
4. Um Details für die Richtlinie zu ändern, wählen Sie den Abwärtspfeil auf der rechten Seite aus, und ändern Sie die Details.
5. Wählen Sie **Speichern**, um die Änderung abzuschließen.

Bearbeiten Sie eine vorhandene Richtlinie

Sie können die Details einer Richtlinie nur dann ändern, wenn die Richtlinie nicht mit einem Workload verknüpft ist.

Schritte

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Protection** aus.
2. Wählen Sie auf der Seite Schutz die Option **Richtlinien verwalten** aus.
3. Wählen Sie auf der Seite Manage Policies die Option **actions** für die Richtlinie aus, die Sie ändern möchten.
4. Wählen Sie im Menü Aktionen die Option **Richtlinie bearbeiten**.

5. Ändern Sie die Details.
6. Wählen Sie **Speichern**, um die Änderung abzuschließen.

Löschen Sie eine Richtlinie

Sie können eine Sicherungsrichtlinie löschen, die derzeit keiner Workload zugeordnet ist.

Schritte

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Protection** aus.
2. Wählen Sie auf der Seite Schutz die Option **Richtlinien verwalten** aus.
3. Wählen Sie auf der Seite Manage Policies die Option **actions** für die Richtlinie aus, die Sie löschen möchten.
4. Wählen Sie im Menü Aktionen die Option **Richtlinie löschen**.

Reagieren Sie auf einen erkannten Ransomware-Alarm

Wenn der Ransomware-Schutz von BlueXP einen möglichen Angriff erkennt, wird im BlueXP Ransomware Protection Dashboard und in den BlueXP Benachrichtigungen oben rechts eine Warnmeldung angezeigt, die auf einen potenziellen Ransomware-Angriff hinweist. Der Service initiiert zudem unverzüglich die Erstellung einer Snapshot-Kopie. An dieser Stelle sollten Sie sich das potenzielle Risiko im BlueXP Ransomware-Schutz anschauen **Alerts** Tab.

Um Ihre Daten wiederherzustellen, markieren Sie die Warnmeldung als bereit für die Recovery, damit Ihr Storage-Administrator mit dem Recovery-Prozess beginnen kann.

Jede Warnung kann mehrere Vorfälle auf verschiedenen Volumes mit unterschiedlichen Status haben, achten Sie also darauf, alle Vorfälle zu betrachten.

Der Dienst bietet Informationen, die als *Evidence* bezeichnet werden, über den Grund, aus dem die Warnung ausgegeben wurde, wie z. B.:

- Dateierweiterungen wurden erstellt oder geändert
- Die Dateierstellung ist erfolgt und wird um einen aufgelisteten Prozentsatz erhöht
- Die Dateilöschung ist aufgetreten und wird um einen aufgelisteten Prozentsatz erhöht

Eine Warnung basiert auf den folgenden Verhaltensarten:

- **Potenzieller Angriff**: Ein Alarm tritt auf, wenn Autonomous Ransomware Protection eine neue Erweiterung erkennt und das Auftreten in den letzten 24 Stunden mehr als 20 Mal wiederholt wird (Standardverhalten).
- **Warnung**: Eine Warnung erfolgt auf der Grundlage der folgenden Verhaltensweisen:
  - Die Erkennung einer neuen Erweiterung wurde zuvor nicht identifiziert und dasselbe Verhalten wiederholt nicht genug Male, um sie als Angriff zu deklarieren.
  - Es wird eine hohe Entropie beobachtet.
  - Bei Lese-/Schreib-/Umbenennungs-/Löschvorgängen in Dateien wurde eine Aktivität von 100 % über die Baseline hinaus angestiegt.

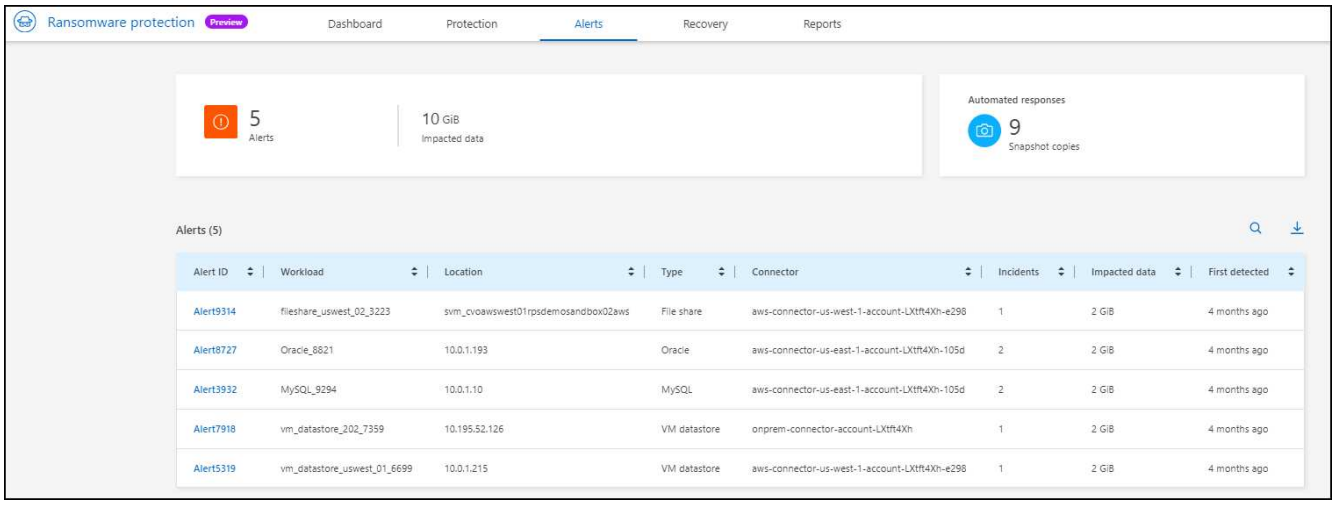
Der Nachweis basiert auf Informationen aus dem Autonomen Ransomware-Schutz in ONTAP. Weitere Informationen finden Sie unter "Autonome Ransomware-Schutz – Übersicht".

Anzeigen von Meldungen

Sie können über das BlueXP Ransomware Protection Dashboard oder über die Registerkarte **Alerts** auf Benachrichtigungen zugreifen.

Schritte

1. Sehen Sie sich im BlueXP Dashboard für Ransomware-Schutz den Bereich „Alerts“ an.
2. Wählen Sie unter einer der Statuen **Alle anzeigen**.
3. Klicken Sie auf eine Warnmeldung, um alle Vorfälle auf jedem Volume für jede Warnmeldung zu überprüfen.
4. Um weitere Warnmeldungen anzuzeigen, klicken Sie in den Paniermehl oben links auf **Alert**.
5. Überprüfen Sie die Warnmeldungen auf der Seite Warnungen.



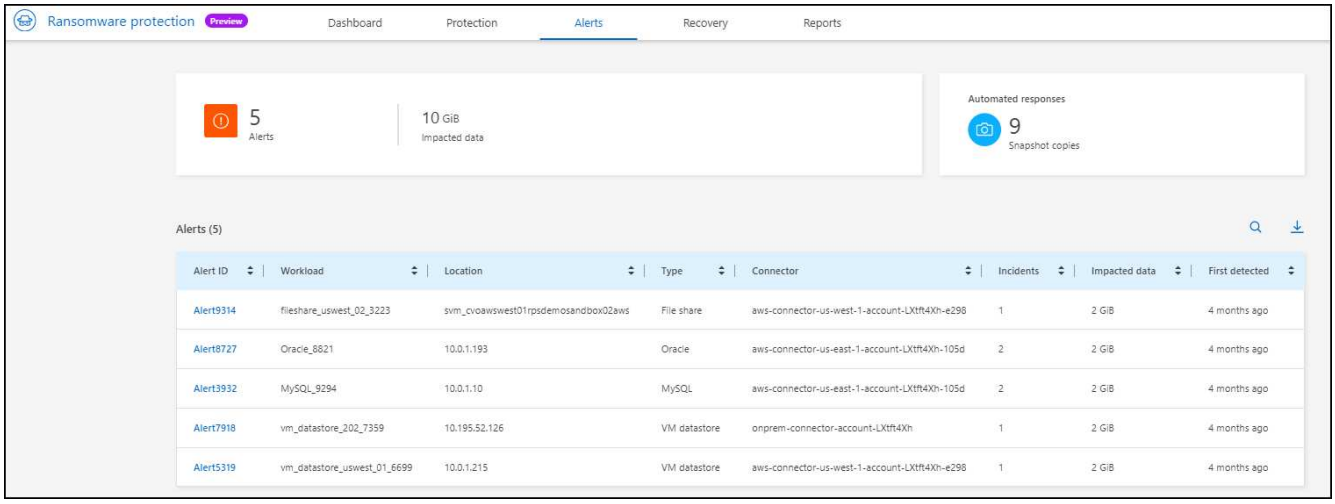
6. Weiter mit Markieren Sie Ransomware-Vorfälle als bereit für die Wiederherstellung (nach der Neutralisierung von Vorfällen)..

Markieren Sie Ransomware-Vorfälle als bereit für die Wiederherstellung (nach der Neutralisierung von Vorfällen).

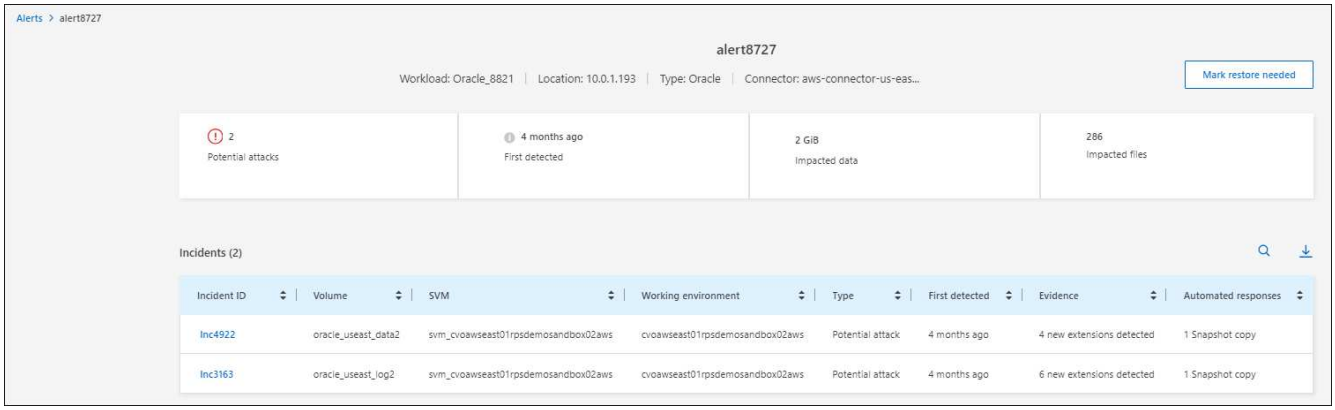
Nachdem der Angriff gemildert und Workloads wiederhergestellt werden können, sollten Sie mit dem Storage-Admin-Team kommunizieren, dass die Daten bereit sind für die Recovery, damit der Recovery-Prozess gestartet werden kann.

Schritte

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Alerts** aus.



2. Wählen Sie auf der Seite Warnungen die Warnmeldung aus.
3. Überprüfen Sie die Vorfälle in der Meldung.



4. Wenn Sie feststellen, dass die Vorfälle für die Wiederherstellung bereit sind, wählen Sie **Wiederherstellung erforderlich markieren**.
5. Bestätigen Sie die Aktion und wählen Sie **Wiederherstellung erforderlich markieren**.
6. Um die Workload-Wiederherstellung zu starten, wählen Sie * Recover * Workload in der Meldung aus oder wählen Sie die Registerkarte * Recovery* aus.

Ergebnis

Nachdem die Warnmeldung für die Wiederherstellung markiert wurde, wechselt die Warnmeldung von der Registerkarte Warnungen zur Registerkarte Wiederherstellung.

Wiederherstellung nach einem Ransomware-Angriff (nach dem Neutralisieren von Vorfällen)

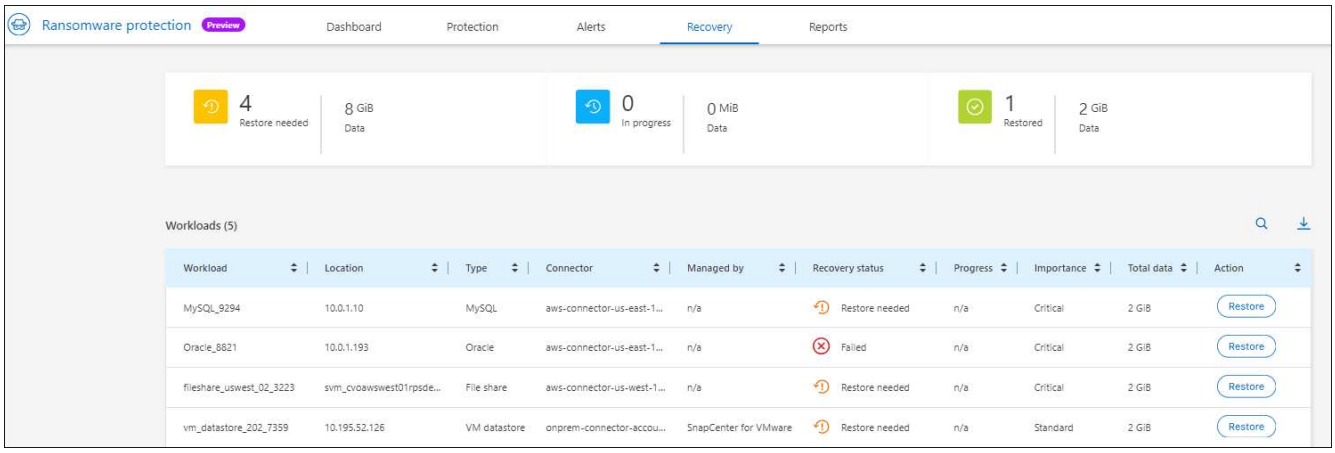
Nachdem die Workloads als „bereit für die Recovery“ markiert wurden, empfiehlt der BlueXP Ransomware-Schutz einen tatsächlichen Recovery-Zeitpunkt (Recovery Point Actual, RPA) und orchestriert den Workflow für eine ausfallsichere Recovery.

Zeigen Sie Workloads an, die wiederhergestellt werden können

Überprüfen Sie die Workloads im Recovery-Status „Restore needed“.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Überprüfen Sie im Dashboard die Gesamtwerte für „benötigte Wiederherstellung“ im Bereich „Warnungen“, und wählen Sie **Alle anzeigen**.
   - Wählen Sie im Menü **Recovery**.
2. Überprüfen Sie die Workload-Informationen auf der Seite **Recovery**.



Wiederherstellung eines Workloads

Durch den Ransomware-Schutz von BlueXP kann der Storage-Administrator bestimmen, wie sich Workloads am besten entweder am empfohlenen Restore-Punkt oder am bevorzugten Restore-Punkt wiederherstellen lassen.

Der Sicherheits-Storage-Administrator kann Daten auf verschiedenen Ebenen wiederherstellen:

- Alle Volumes werden wiederhergestellt
- Stellen Sie eine Anwendung auf Volume- oder Datei- und Ordnerebene wieder her.
- Stellen Sie eine Dateifreigabe auf Volume-, Verzeichnis- oder Datei-/Ordnerebene wieder her.
- Wiederherstellung von einem Datenspeicher auf VM-Ebene

Der Prozess unterscheidet sich je nach Workload-Typ geringfügig.

Schritte

1. Wählen Sie im Menü BlueXP Ransomware Protection die Option **Recovery** aus.
2. Überprüfen Sie die Workload-Informationen auf der Seite **Recovery**.
3. Wählen Sie einen Workload im Status „Restore needed“ aus.
4. Wählen Sie zum Wiederherstellen **Wiederherstellen**.
5. **Umfang wiederherstellen**: Wählen Sie die Art der Wiederherstellung, die Sie abschließen möchten:
   - Alle Volumes
   - Nach Volumen

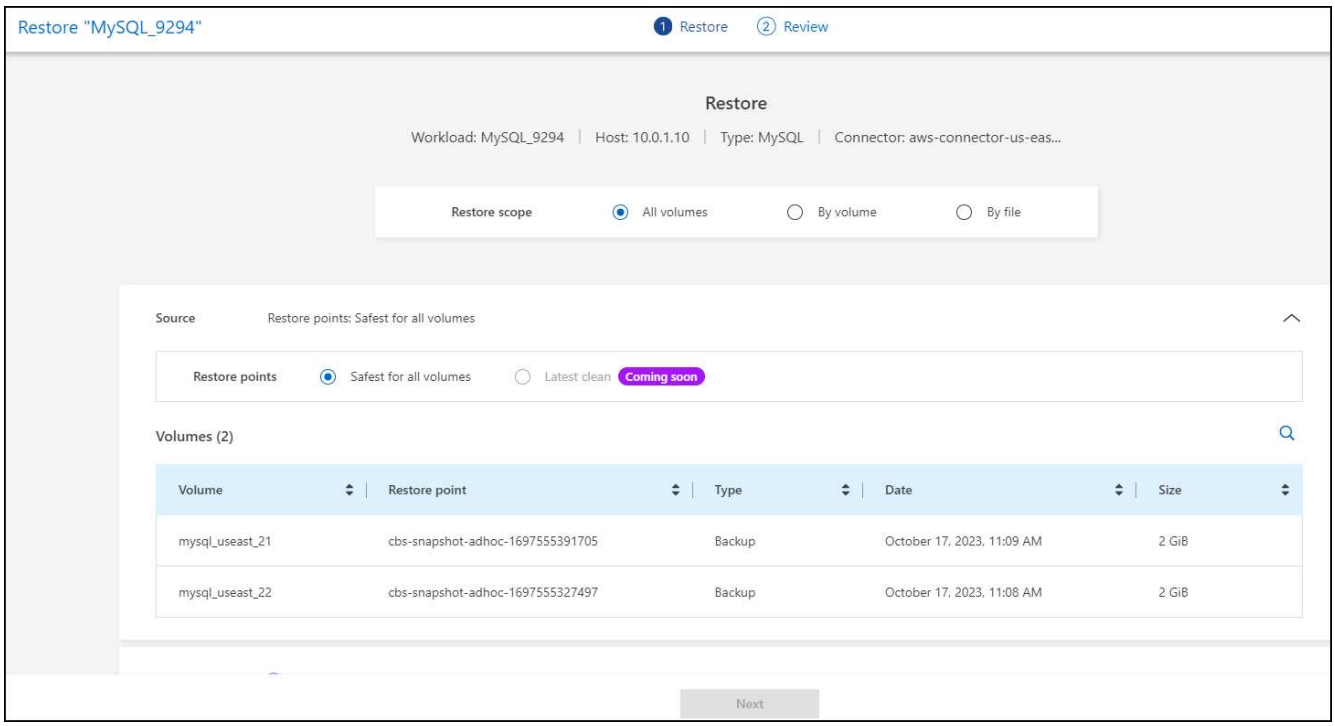
- Nach Datei: Sie können einen Ordner oder einzelne Dateien zur Wiederherstellung angeben.

> Sie können bis zu 100 Dateien oder einen einzelnen Ordner auswählen.

6. Fahren Sie mit einem der folgenden Verfahren fort, je nachdem, ob Sie die Anwendung, das Volume oder die Datei ausgewählt haben.

Alle Volumes wiederherstellen

1. Wählen Sie auf der Seite Wiederherstellen im Bereich Wiederherstellen die Option **Alle Volumes** aus.



2. **Quelle**: Wählen Sie den Pfeil nach unten neben Quelle, um Details zu sehen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

> Der Ransomware-Schutz von BlueXP identifiziert den besten Restore-Punkt als das neueste Backup direkt vor dem Vorfall und zeigt eine „sicherste für alle Volumes“-Anzeige. Dies bedeutet, dass alle Volumes vor dem ersten Angriff auf das erste erkannte Volume auf eine Kopie wiederhergestellt werden.

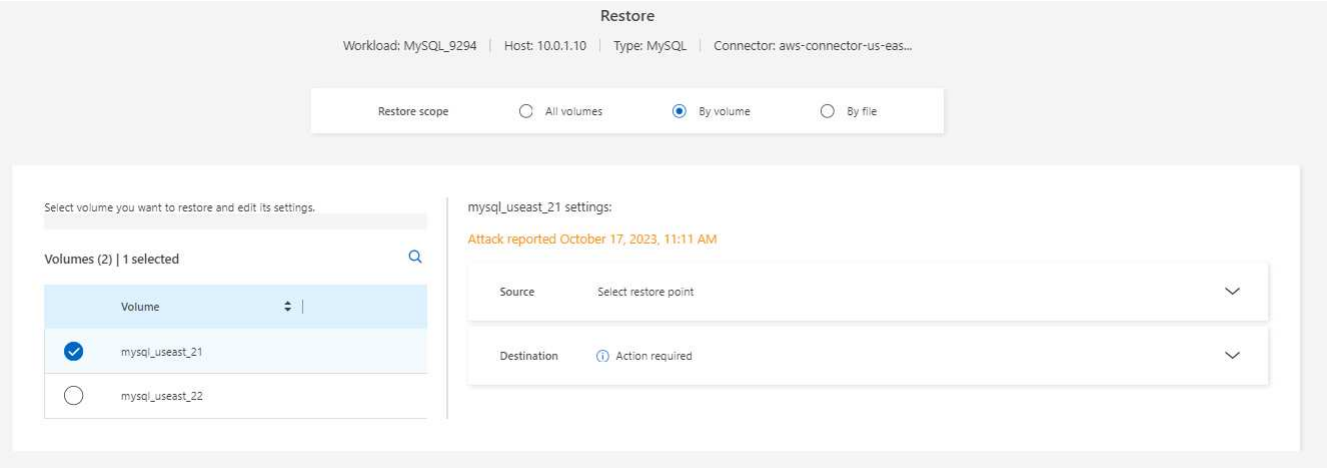
3. **Ziel**: Wählen Sie den Abwärtspfeil neben Ziel, um Details anzuzeigen.
   a. Wählen Sie die Arbeitsumgebung aus.
   b. Wählen Sie Storage VM aus.
   c. Wählen Sie das Aggregat aus.
   d. Ändern Sie das Volume-Präfix, das allen neuen Volumes vorangestellt wird.

> Der neue Volume-Name wird als Präfix + ursprünglicher Volume-Name + Backup-Name + Backup-Datum angezeigt.

4. Wählen Sie **Speichern**.
5. Wählen Sie **Weiter**.
6. Überprüfen Sie Ihre Auswahl.
7. Wählen Sie **Wiederherstellen**.
8. Wählen Sie im oberen Menü **Recovery** aus, um den Workload auf der Seite Recovery zu überprüfen, auf der sich der Status des Vorgangs durch die Zustände bewegt.

Stellen Sie einen Applikations-Workload auf Volume-Ebene wieder her

1. Wählen Sie auf der Seite Wiederherstellen im Bereich Wiederherstellen die Option **nach Volume** aus.



2. Wählen Sie in der Liste der Volumes das Volume aus, das Sie wiederherstellen möchten.
3. **Quelle**: Wählen Sie den Pfeil nach unten neben Quelle, um Details zu sehen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

   Durch den Ransomware-Schutz von BlueXP wird der beste Restore-Punkt als das neueste Backup direkt vor dem Vorfall identifiziert und eine „empfohlene“ Angabe angezeigt.

4. **Ziel**: Wählen Sie den Abwärtspfeil neben Ziel, um Details anzuzeigen.
   a. Wählen Sie die Arbeitsumgebung aus.
   b. Wählen Sie Storage VM aus.
   c. Wählen Sie das Aggregat aus.
   d. Überprüfen Sie den neuen Volume-Namen.

   Der neue Volume-Name wird als ursprünglicher Volume-Name + Backup-Name + Backup-Datum angezeigt.

5. Wählen Sie **Speichern**.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie Ihre Auswahl.

8. Wählen Sie **Wiederherstellen**.
9. Wählen Sie im oberen Menü **Recovery** aus, um den Workload auf der Seite Recovery zu überprüfen, auf der sich der Status des Vorgangs durch die Zustände bewegt.

Stellen Sie einen Applikations-Workload auf Dateiebene wieder her

1. Wählen Sie auf der Seite Wiederherstellen im Bereich Wiederherstellen die Option **nach Datei** aus.
2. Wählen Sie in der Liste der Volumes das Volume aus, das Sie wiederherstellen möchten.
3. **Quelle**: Wählen Sie den Pfeil nach unten neben Quelle, um Details zu sehen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

   > Durch den Ransomware-Schutz von BlueXP wird der beste Restore-Punkt als das neueste Backup direkt vor dem Vorfall identifiziert und eine „empfohlene“ Angabe angezeigt.

   b. Wählen Sie bis zu 100 Dateien oder einen einzelnen Ordner für die Wiederherstellung aus.
4. **Ziel**: Wählen Sie den Abwärtspfeil neben Ziel, um Details anzuzeigen.
   a. Legen Sie fest, wo die Daten wiederhergestellt werden sollen: Ursprünglicher Quellspeicherort oder alternativer Speicherort, den Sie angeben können.

   > Während die ursprünglichen Dateien oder das ursprüngliche Verzeichnis durch die wiederhergestellten Daten überschrieben werden, bleiben die ursprünglichen Datei- und Ordnernamen unverändert, es sei denn, Sie geben neue Namen an.

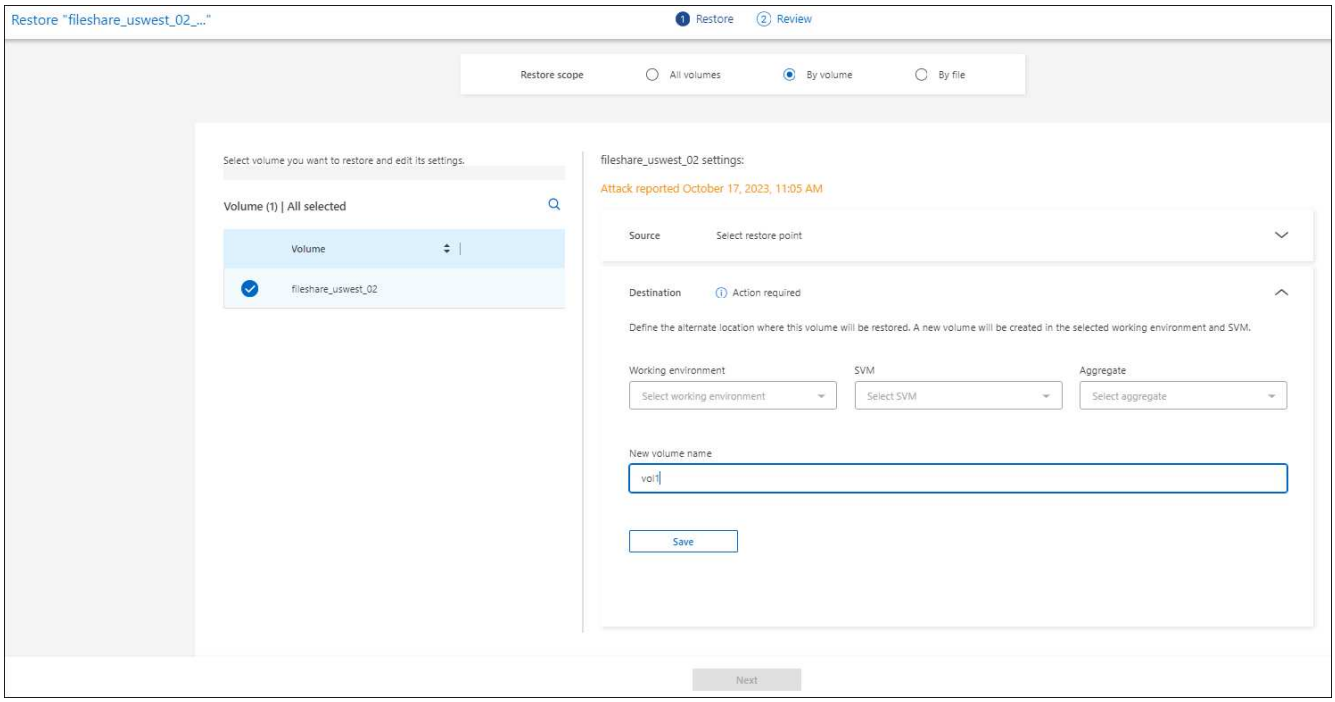
   b. Wählen Sie die Arbeitsumgebung aus.
   c. Wählen Sie Storage VM aus.
   d. Geben Sie optional den Pfad ein.

   > Wenn Sie keinen Pfad für die Wiederherstellung angeben, werden die Dateien auf einem neuen Volume im Verzeichnis der obersten Ebene wiederhergestellt.

   e. Wählen Sie aus, ob die Namen der wiederhergestellten Dateien oder des Verzeichnisses den Namen des aktuellen Speicherorts oder anderer Namen haben sollen.
5. Wählen Sie **Speichern**.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie Ihre Auswahl.
8. Wählen Sie **Wiederherstellen**.
9. Wählen Sie im oberen Menü **Recovery** aus, um den Workload auf der Seite Recovery zu überprüfen, auf der sich der Status des Vorgangs durch die Zustände bewegt.

Stellen Sie eine Dateifreigabe oder einen Datastore auf Volume- oder Dateiebene wieder her

1. Wählen Sie auf der Seite Wiederherstellen im Bereich Wiederherstellen die Option **nach Volume** oder **nach Datei** aus, nachdem Sie eine Dateifreigabe oder einen Datastore ausgewählt haben, die wiederhergestellt werden sollen.



2. Wählen Sie in der Liste der Volumes das Volume aus, das Sie wiederherstellen möchten.
3. **Quelle**: Wählen Sie den Pfeil nach unten neben Quelle, um Details zu sehen.
   a. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.

   Durch den Ransomware-Schutz von BlueXP wird der beste Restore-Punkt als das neueste Backup direkt vor dem Vorfall identifiziert und eine „empfohlene“ Angabe angezeigt.

4. **Ziel**: Wählen Sie den Abwärtspfeil neben Ziel, um Details anzuzeigen.
   a. Legen Sie fest, wo die Daten wiederhergestellt werden sollen: Ursprünglicher Quellspeicherort oder alternativer Speicherort, den Sie angeben können.

   Während die ursprünglichen Dateien oder das ursprüngliche Verzeichnis durch die wiederhergestellten Daten überschrieben werden, bleiben die ursprünglichen Datei- und Ordnernamen unverändert, es sei denn, Sie geben neue Namen an.

   b. Wählen Sie die Arbeitsumgebung aus.
   c. Wählen Sie Storage VM aus.
   d. Geben Sie optional den Pfad ein.

   Wenn Sie keinen Pfad für die Wiederherstellung angeben, werden die Dateien auf einem neuen Volume im Verzeichnis der obersten Ebene wiederhergestellt.

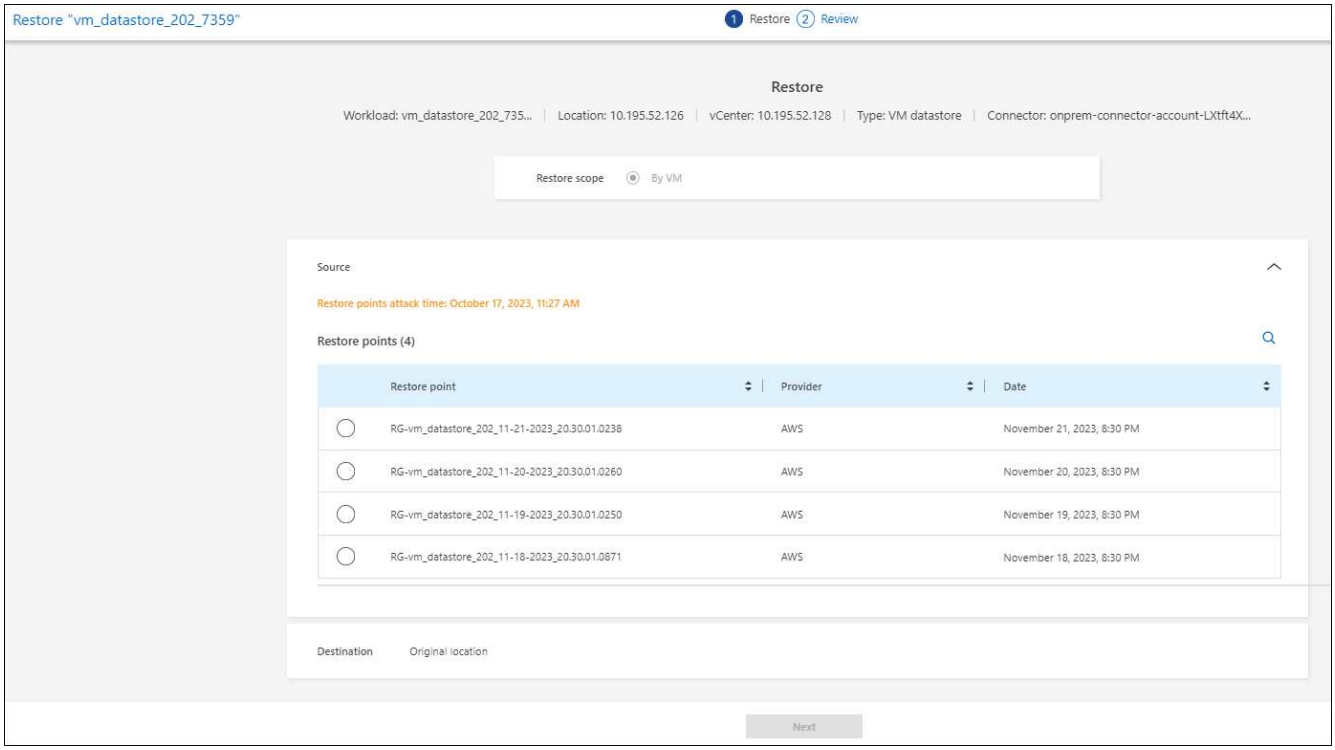
5. Wählen Sie **Speichern**.
6. Überprüfen Sie Ihre Auswahl.
7. Wählen Sie **Wiederherstellen**.
8. Wählen Sie im Menü * Recovery* aus, um die Arbeitslast auf der Seite Recovery zu überprüfen, auf der

sich der Status des Vorgangs durch die Zustände bewegt.

Stellen Sie eine VM-Dateifreigabe auf VM-Ebene wieder her

Fahren Sie auf der Seite Wiederherstellung mit den folgenden Schritten fort, nachdem Sie eine wiederherzustellende VM ausgewählt haben.

1. **Quelle**: Wählen Sie den Pfeil nach unten neben Quelle, um Details zu sehen.



2. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen der Daten verwenden möchten.
3. **Ziel**: Zum ursprünglichen Standort.
4. Wählen Sie **Weiter**.
5. Überprüfen Sie Ihre Auswahl.
6. Wählen Sie **Wiederherstellen**.
7. Wählen Sie im Menü * Recovery* aus, um die Arbeitslast auf der Seite Recovery zu überprüfen, auf der sich der Status des Vorgangs durch die Zustände bewegt.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.