Reagieren und wiederherstellen

NetApp Ransomware Resilience

NetApp
April 14, 2026

Inhalt

Reagieren und wiederherstellen

Warnmeldungen in NetApp Ransomware Resilience verwalten

Wenn NetApp Ransomware Resilience einen möglichen Angriff erkennt, wird eine Warnung im Dashboard und im Benachrichtigungsmenü angezeigt. Ransomware Resilience erstellt sofort eine Snapshot. Wenn Sie eine Warnung erhalten, überprüfen Sie das potenzielle Risiko im **Alerts**-Tab von Ransomware Resilience, um die Auswirkungen auf Ihre Daten einzuschätzen und einen möglichen Ransomware-Angriff zu verhindern.

Wenn Ransomware Resilience einen möglichen Angriff erkennt, erscheint eine Benachrichtigung in den Console Notification-Einstellungen und eine E-Mail wird an die konfigurierten Adressen gesendet. Die E-Mail enthält Informationen über den Schweregrad, die betroffene Workload und einen Link zur Warnung im Tab **Alerts** von Ransomware Resilience.

Sie können Fehlalarme ignorieren oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden.

Wenn Sie die Warnung verwerfen, lernt Ransomware Resilience dieses Verhalten, verknüpft es mit normalen Vorgängen und löst keine weitere Warnung aus.

Um mit der Wiederherstellung Ihrer Daten zu beginnen, markieren Sie die Warnung als „bereit zur Wiederherstellung“, damit Ihr Speicheradministrator mit dem Wiederherstellungsprozess beginnen kann.

Jede Warnung kann mehrere Vorfälle mit unterschiedlichem Umfang und Status umfassen. Überprüfen Sie alle Vorfälle.

Wie Warnmeldungen generiert werden

Ransomware Resilience nutzt Erkenntnisse über Datenentropiemuster, Dateierweiterungstypen und Verschlüsselung, um Warnmeldungen zu generieren. Warnmeldungen basieren auf den folgenden Ereignissen:

- Datenpanne
- Datenvernichtung
- Dateierweiterungen wurden erstellt oder geändert
- Dateierstellung mit einem Vergleich der erkannten und erwarteten Raten
- Dateilöschung mit einem Vergleich der erkannten und erwarteten Raten
- Verdächtiges Nutzerverhalten
- Bei hoher Verschlüsselung ohne Änderungen der Dateierweiterung

Für Benachrichtigungen über Datenschutzverletzungen, Datenzerstörung und verdächtiges Benutzerverhalten müssen Sie "Benutzeraktivitätserkennung" konfigurieren.

Alarmtypen und -status

Benachrichtigungen haben einen von zwei Status: **New** oder **Inactive**.

Eine Warnung wird als einer der folgenden Typen klassifiziert:

- **Potenzieller Angriff**: Eine Warnung wird als potenzieller Angriff eingestuft, wenn:
  - Autonomous Ransomware Protection erkennt eine neue Erweiterung, und das Auftreten wiederholt sich in den letzten 24 Stunden mehr als 20 Mal (Standardverhalten).
  - Datenpannen werden erkannt.
  - Datenzerstörung wurde erkannt.
- **Warnung**: Eine Warnung erfolgt aufgrund der folgenden Verhaltensweisen:
  - Die Erkennung einer neuen Erweiterung wurde bisher nicht festgestellt und dasselbe Verhalten wiederholt sich nicht oft genug, um es als Angriff zu deklarieren.
  - Es wird eine hohe Entropie beobachtet.
  - Die Aktivität beim Lesen, Schreiben, Umbenennen oder Löschen von Dateien hat sich im Vergleich zum Normalwert verdoppelt.

Für SAN-Umgebungen basieren Warnungen ausschließlich auf hoher Entropie.

Die Beweise basieren auf Informationen von Autonomous Ransomware Protection in ONTAP. Weitere Einzelheiten finden Sie unter "Übersicht über den autonomen Ransomware-Schutz" .

Alarmzustände

Ein Alarmereignis kann folgende Zustände aufweisen:

Status	Beschreibung
Neu	Alle Vorfälle werden als „neu“ gekennzeichnet, wenn sie erstmals identifiziert werden.
In Überprüfung	Sie können einen Alarmvorfall manuell als „in Bearbeitung“ markieren, während Sie ihn auswerten.
Abgewiesen	Wenn Sie vermuten, dass die Aktivität kein Ransomware-Angriff ist, können Sie den Status auf „abgelehnt“ ändern. + ACHTUNG: Nachdem Sie einen Angriff abgelehnt haben, können Sie seinen Status nicht mehr zurücksetzen. Wenn Sie eine Arbeitslast ablehnen, werden alle automatisch als Reaktion auf den potenziellen Ransomware-Angriff erstellten Snapshot-Kopien dauerhaft gelöscht.
Gelöst	Der Vorfall wurde behoben.
Automatisch aufgelöst	Bei Warnmeldungen mit niedriger Priorität wird der Vorfall automatisch behoben, wenn innerhalb von fünf Tagen keine Maßnahmen ergriffen wurden.

Warnungen anzeigen

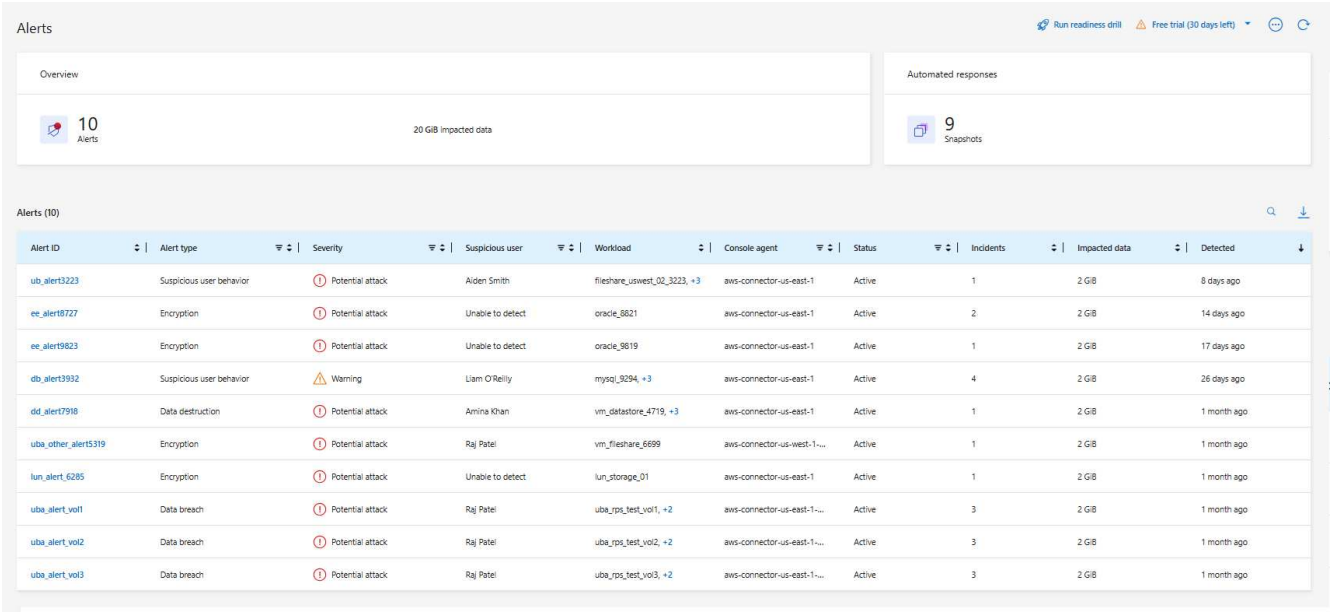
Sie können auf Warnmeldungen über das Ransomware Resilience-Dashboard oder über die Registerkarte **Alerts** zugreifen.

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“, „Ransomware Resilience-Administrator“

oder „Ransomware Resilience-Viewer“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Überprüfen Sie im Dashboard „Ransomware Resilience“ den Bereich „Warnungen“.
2. Wählen Sie unter einem der Status **Alle anzeigen** aus.
3. Wählen Sie eine Warnung aus, um alle Vorfälle auf jedem Datenträger für jede Warnung zu überprüfen.
4. Um weitere Warnungen anzuzeigen, wählen Sie in der Brotkrümelnavigation oben links **Warnung** aus.
5. Überprüfen Sie die Warnungen auf der Seite „Warnungen“.



6. Fahren Sie mit einem der folgenden Schritte fort:
   - Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten .
   - Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden). .
   - bei denen es sich nicht um potenzielle Angriffe handelt .

Auf eine Warn-E-Mail antworten

Wenn Ransomware Resilience einen potenziellen Angriff erkennt, sendet es eine E-Mail-Benachrichtigung an die abonnierten Benutzer basierend auf deren Benachrichtigungseinstellungen, die in den NetApp Console-Einstellungen konfiguriert sind. Die E-Mail enthält Informationen zur Warnung, einschließlich des Schweregrads und der betroffenen Ressourcen.

Informationen zum Einrichten von E-Mail-Benachrichtigungen in der NetApp Console finden Sie unter "E-Mail-Benachrichtigungseinstellungen festlegen".

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“, „Ransomware Resilience-Administrator“ oder „Ransomware Resilience-Viewer“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Sehen Sie sich die E-Mail an.
2. Wählen Sie in der E-Mail **View alert** und melden Sie sich bei Ransomware Resilience an.

   Die Seite „Warnungen“ wird angezeigt.

3. Überprüfen Sie für jede Warnung alle Vorfälle auf jedem Datenträger.
4. Um weitere Warnungen anzuzeigen, wählen Sie in der Brotkrümelnavigation oben links **Warnung** aus.
5. Fahren Sie mit einem der folgenden Schritte fort:
   - Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten .
   - Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden). .
   - bei denen es sich nicht um potenzielle Angriffe handelt .

Erkennen Sie böswillige Aktivitäten und anomales Benutzerverhalten

Auf der Registerkarte „Warnungen“ können Sie erkennen, ob böswillige Aktivitäten oder anomales Benutzerverhalten vorliegen.

Sie müssen einen Benutzeraktivitätsagenten konfiguriert und eine Datensicherungsstrategie mit Benutzerverhaltenserkennung aktiviert haben, um Warnungen auf Benutzerebene anzuzeigen. Die Spalte **Verdächtiger Benutzer** wird im Warnungs-Dashboard nur angezeigt, wenn die Benutzerverhaltenserkennung aktiviert ist. Um die Erkennung verdächtiger Benutzer zu aktivieren, siehe "Verdächtige Benutzeraktivität".

Anzeigen böswilliger Aktivitäten

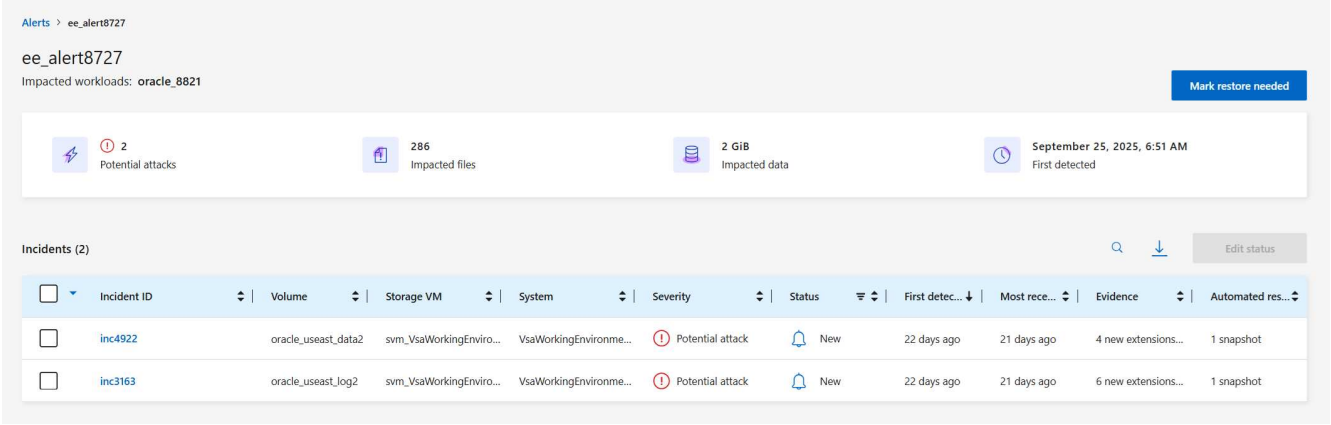
Wenn Autonomous Ransomware Protection in NetApp Ransomware Resilience eine Warnung auslöst, können Sie die folgenden Details einsehen:

- Als die Warnung ausgelöst wurde
- Wenn der Zugriff geändert oder verweigert wurde
- Entropie eingehender Daten
- Erwartete Erstellungsrate neuer Dateien im Vergleich zur erkannten Rate
- Erwartete Löschrate von Dateien im Vergleich zur erkannten Rate
- Erwartete Umbenennungsrate von Dateien im Vergleich zur erkannten Rate
- Betroffene Workloads, Volumes, Dateien und Verzeichnisse

Diese Details sind für NAS-Workloads sichtbar. Für SAN-Umgebungen sind nur die Entropiedaten verfügbar.

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Wählen Sie eine Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.



4. Wählen Sie einen Vorfall aus, um die Details des Vorfalls zu überprüfen.

Anzeigen von anomalem Benutzerverhalten

Wenn Sie die Erkennung verdächtiger Benutzer so konfiguriert haben, dass anomales Benutzerverhalten angezeigt wird, können Sie Benutzerdaten einsehen und bestimmte Benutzer blockieren. Um die Einstellungen für verdächtige Benutzer zu aktivieren, siehe "Agenten und Collector für die Erkennung von Benutzeraktivitäten konfigurieren".

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Wählen Sie eine Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.
   a. Um einen verdächtigen Benutzer in Ihrer Umgebung zu blockieren, wählen Sie **Block** neben dem Namen des Benutzers aus.
   b. Um Benachrichtigungen für einen Benutzer zu deaktivieren, der Gegenstand einer nachweislich falschen Benachrichtigung ist, wählen Sie die drei Punkte (… und anschließend **Diesen Benutzer von der Überwachung ausschließen**. Überprüfen Sie den Dialog und wählen Sie dann **Ausschließen** zur Bestätigung.

Um Benachrichtigungen für einen Benutzer wieder zu aktivieren, rufen Sie die Benachrichtigung auf. Wählen Sie die drei Punkte und dann **Diesen Benutzer in die Überwachung einbeziehen**. Sie können auch "Benutzer ausschließen" aus der Überwachung entfernen.

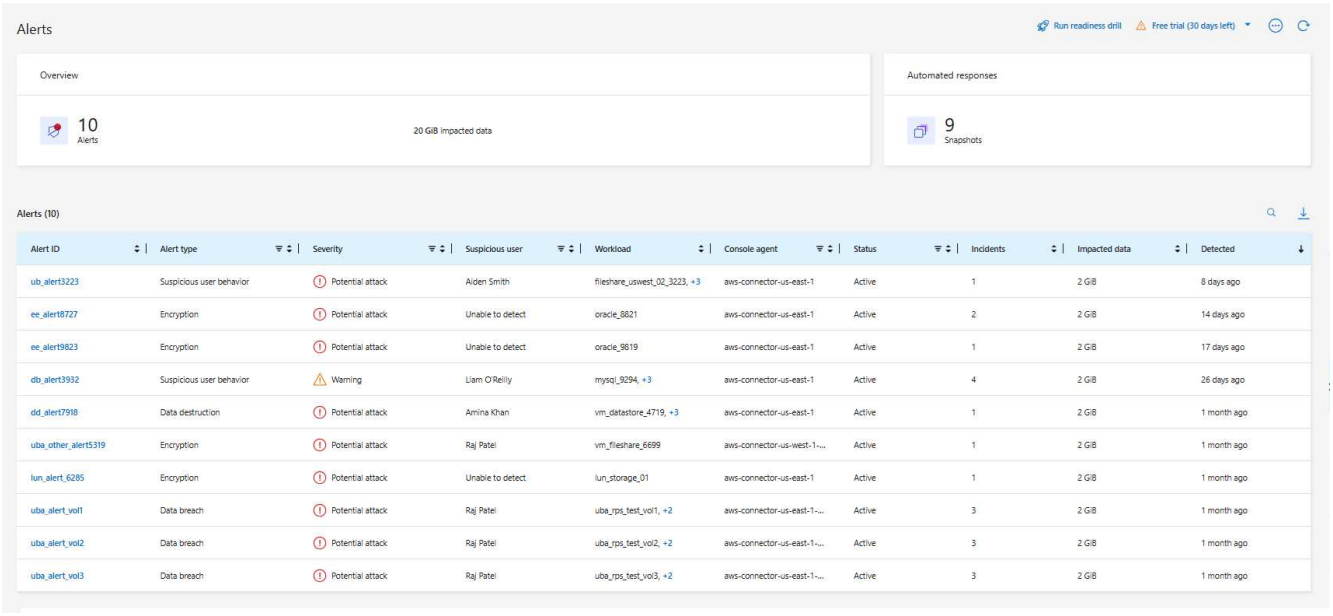
Markieren Sie Ransomware-Vorfälle als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden).

Nachdem der Angriff gestoppt wurde, benachrichtigen Sie Ihren Storage-Administrator, dass die Daten bereit sind, damit dieser den Wiederherstellungsprozess einleiten kann.

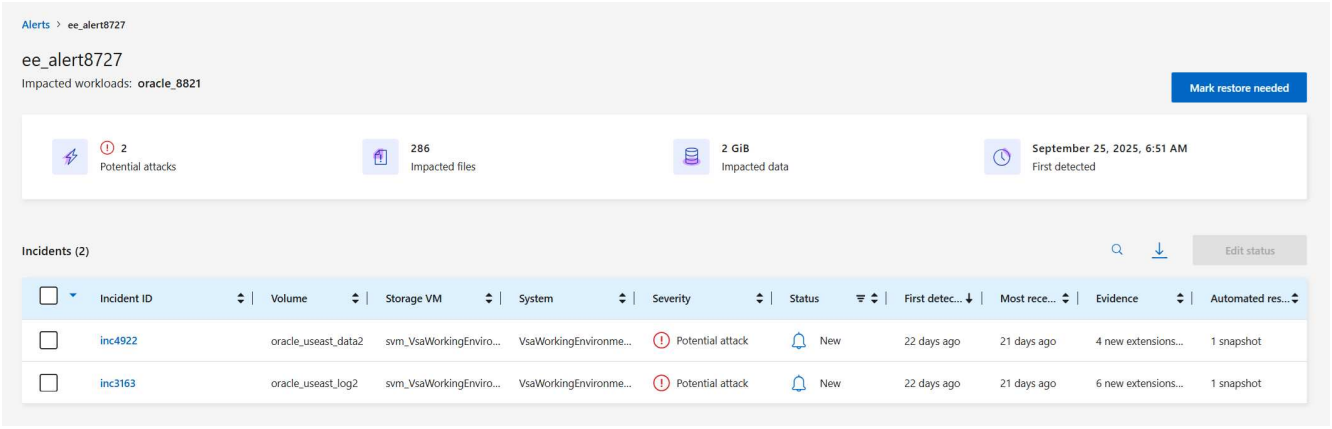
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.



2. Wählen Sie auf der Seite „Warnungen“ die Warnung aus.
3. Überprüfen Sie die Vorfälle in der Warnung.



4. Wenn Sie feststellen, dass die Vorfälle zur Wiederherstellung bereit sind, wählen Sie **Als Wiederherstellung erforderlich markieren**.
5. Bestätigen Sie die Aktion und wählen Sie **Als Wiederherstellung erforderlich markieren**.
6. Um die Workload-Wiederherstellung zu starten, wählen Sie in der Nachricht „Workload wiederherstellen“ oder wählen Sie die Registerkarte „Wiederherstellung“ aus.

Ergebnis

Nachdem die Warnung zur Wiederherstellung markiert wurde, wird sie von der Registerkarte „Warnungen“ zur Registerkarte „Wiederherstellung“ verschoben.

Vorfälle abweisen, bei denen es sich nicht um potenzielle Angriffe handelt

Nachdem Sie die Vorfälle überprüft haben, müssen Sie feststellen, ob es sich bei den Vorfällen um potenzielle Angriffe handelt. Wenn es sich nicht um tatsächliche Bedrohungen handelt, können sie als unbegründet abgetan werden.

Sie können Fehlalarme ignorieren oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden. Wenn Sie die Warnung ignorieren, lernt Ransomware Resilience dieses Verhalten und ordnet es dem

normalen Betrieb zu, sodass bei einem solchen Verhalten keine Warnung mehr ausgelöst wird.

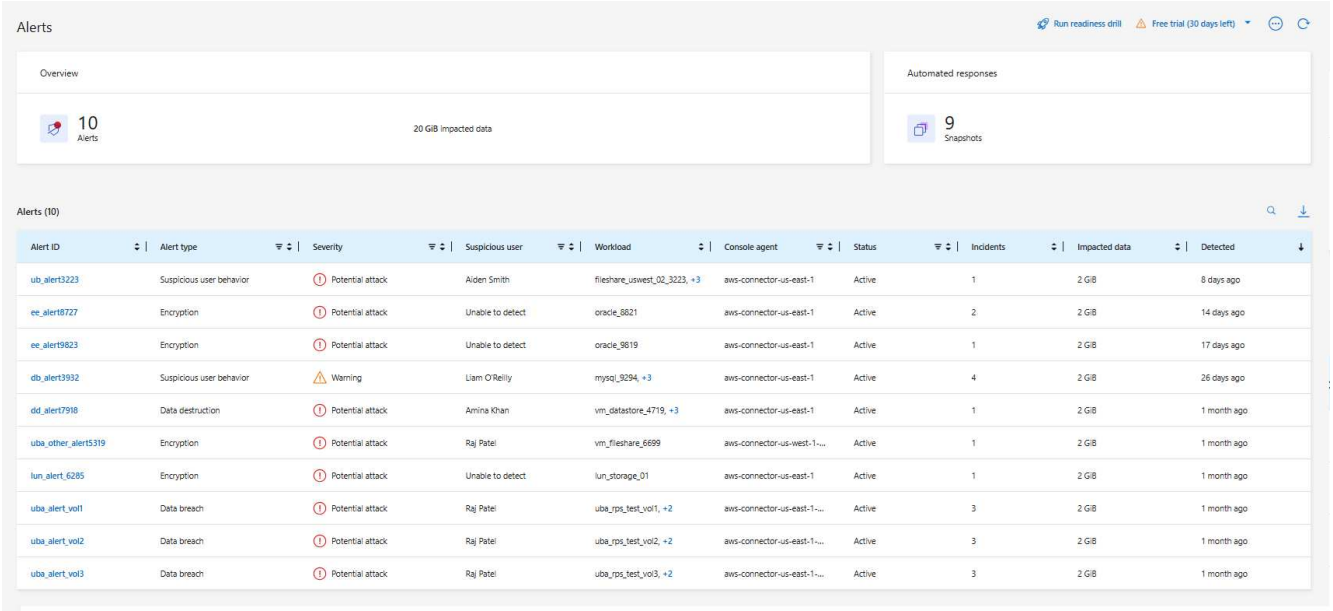
Wenn Sie eine Arbeitslast verwerfen, werden alle Snapshot-Kopien, die automatisch als Reaktion auf einen potenziellen Ransomware-Angriff erstellt wurden, dauerhaft gelöscht.

Wenn Sie eine Warnung verwerfen, können Sie ihren Status nicht ändern oder diese Änderung rückgängig machen.

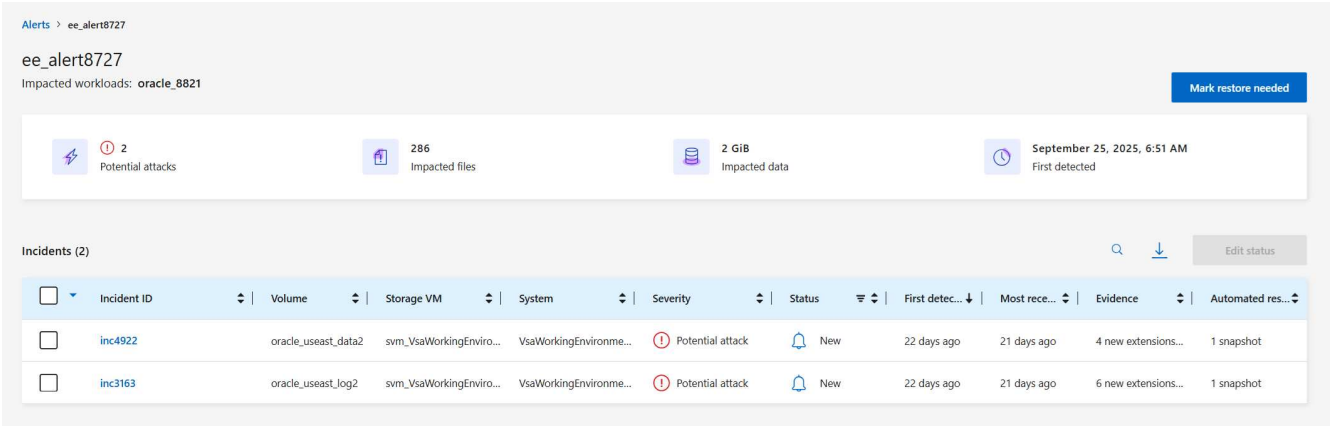
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.

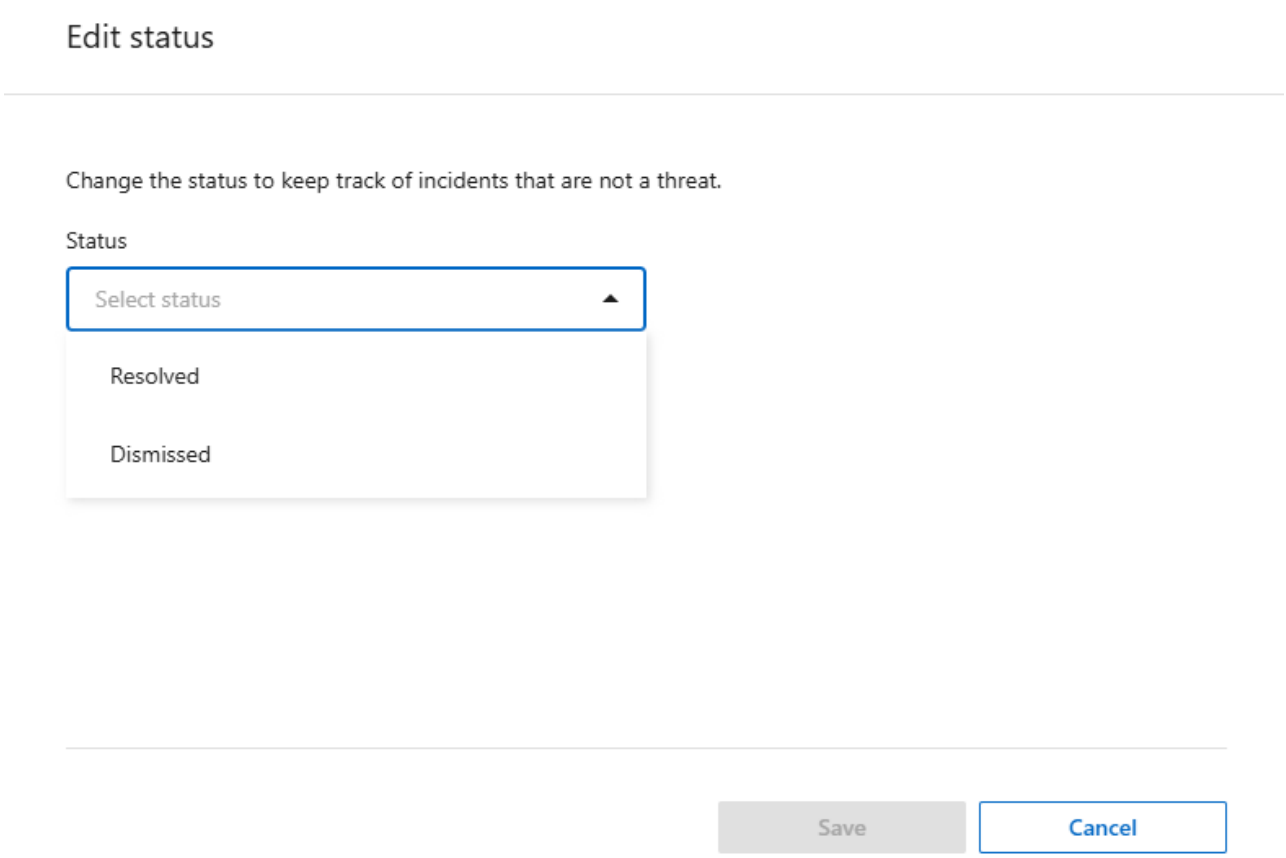


2. Wählen Sie auf der Seite „Warnungen“ die Warnung aus.



3. Wählen Sie einen oder mehrere Vorfälle aus. Alternativ können Sie alle Vorfälle auswählen, indem Sie das Feld „Vorfalls-ID“ oben links in der Tabelle anklicken.
4. Wenn Sie feststellen, dass der Vorfall keine Bedrohung darstellt, verwerfen Sie ihn als falsch-positives Ergebnis:

- Wählen Sie den Vorfall aus.
- Wählen Sie die Schaltfläche **Status bearbeiten** über der Tabelle.



5. Wählen Sie im Dialogfeld „Status bearbeiten“ den Status **Abgelehnt** aus.

   Es werden zusätzliche Informationen über die Arbeitslast und das Löschen der Snapshot-Kopien angezeigt.

6. Wählen Sie **Speichern**.

   Der Status des Vorfalls bzw. der Vorfälle ändert sich zu „Abgewiesen“.

Liste der betroffenen Dateien anzeigen

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie eine Liste der betroffenen Dateien anzeigen. Sie können auf die Seite „Warnungen“ zugreifen, um eine Liste der betroffenen Dateien herunterzuladen. Verwenden Sie dann die Wiederherstellungsseite, um die Liste hochzuladen und auszuwählen, welche Dateien wiederhergestellt werden sollen.

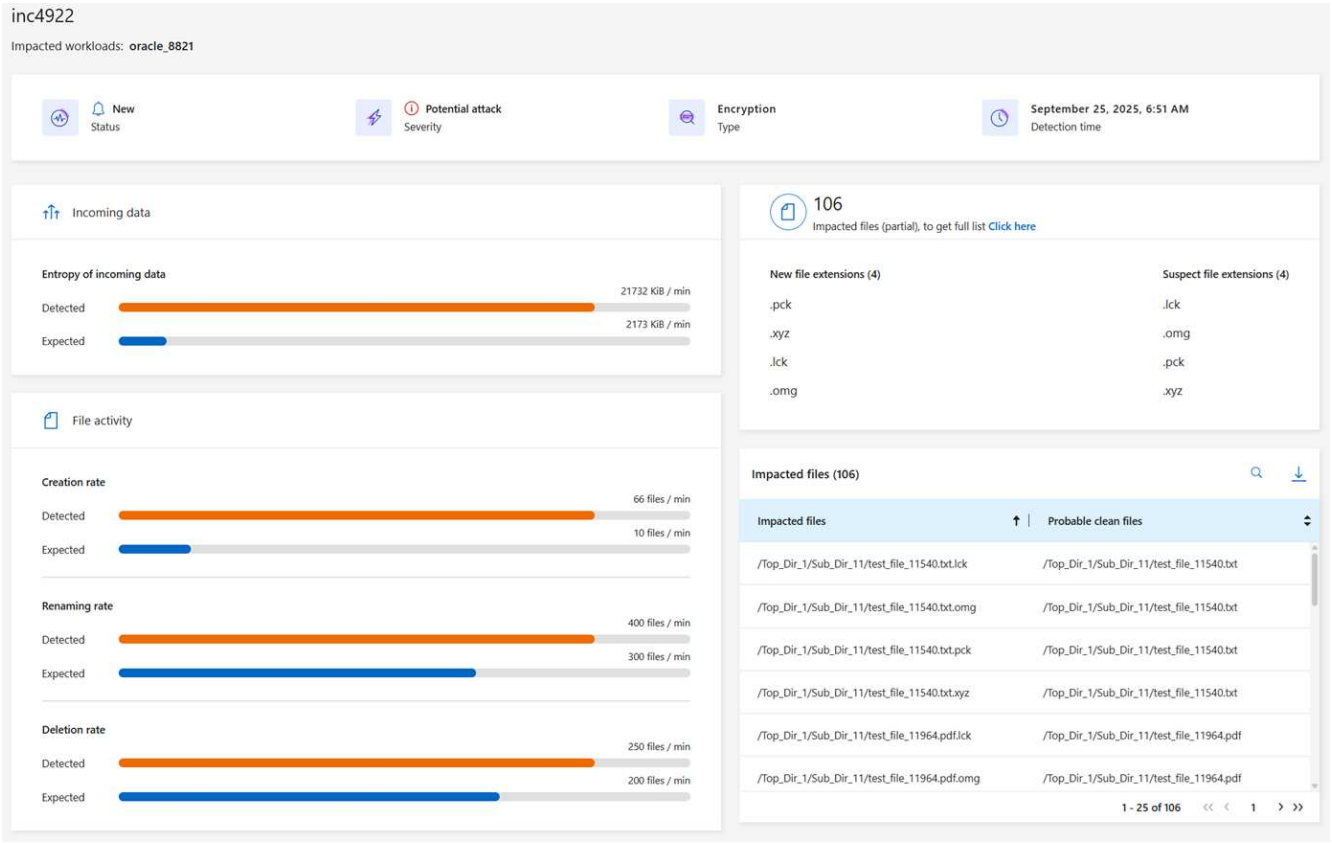
Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Schritte

Verwenden Sie die Seite „Warnungen“, um die Liste der betroffenen Dateien abzurufen.

Wenn ein Volume mehrere Warnungen aufweist, müssen Sie möglicherweise für jede Warnung die CSV-Liste der betroffenen Dateien herunterladen.

1. Wählen Sie im Menü „Ransomware Resilience“ die Option „Warnungen“ aus.
2. Sortieren Sie auf der Seite „Warnungen“ die Ergebnisse nach Arbeitslast, um die Warnungen für die Anwendungsarbeitslast anzuzeigen, die Sie wiederherstellen möchten.
3. Wählen Sie aus der Liste der Warnungen für diese Arbeitslast eine Warnung aus.
4. Wählen Sie für diese Warnung einen einzelnen Vorfall aus.



5. Wählen Sie für diesen Vorfall das Download-Symbol aus, um die Liste der betroffenen Dateien im CSV-Format herunterzuladen.

Überprüfen Sie den Wiederherstellungsstatus in NetApp Ransomware Resilience

Nachdem Workloads als „Wiederherstellung erforderlich“ markiert wurden, empfiehlt NetApp Ransomware Resilience einen tatsächlichen Wiederherstellungspunkt (RPA) und orchestriert den Workflow für eine absturzsichere Wiederherstellung.

- Wenn die Anwendung oder VM von NetApp Backup and Recovery oder Ransomware Resilience verwaltet wird, führt Ransomware Resilience eine absturzkonsistente Wiederherstellung durch, bei der alle Daten, die sich zum gleichen Zeitpunkt auf dem Volume befanden, wiederhergestellt werden, zum Beispiel wenn das System abgestürzt ist.

  Sie können die Arbeitslast wiederherstellen, indem Sie alle Volumes, bestimmte Volumes oder bestimmte

Dateien auswählen.

Die Wiederherstellung der Arbeitslast kann sich auf laufende Arbeitslasten auswirken. Sie sollten die Wiederherstellungsprozesse mit den entsprechenden Beteiligten koordinieren.

Ein Workload kann einen der folgenden Wiederherstellungsstatus haben:

- **Wiederherstellung erforderlich**: Die Arbeitslast muss wiederhergestellt werden.
- **In Bearbeitung**: Der Wiederherstellungsvorgang ist derzeit im Gange.
- **Wiederhergestellt**: Die Arbeitslast wurde wiederhergestellt.
- **Fehlgeschlagen**: Der Workload-Wiederherstellungsprozess konnte nicht abgeschlossen werden.

Anzeigen von Workloads, die zur Wiederherstellung bereit sind

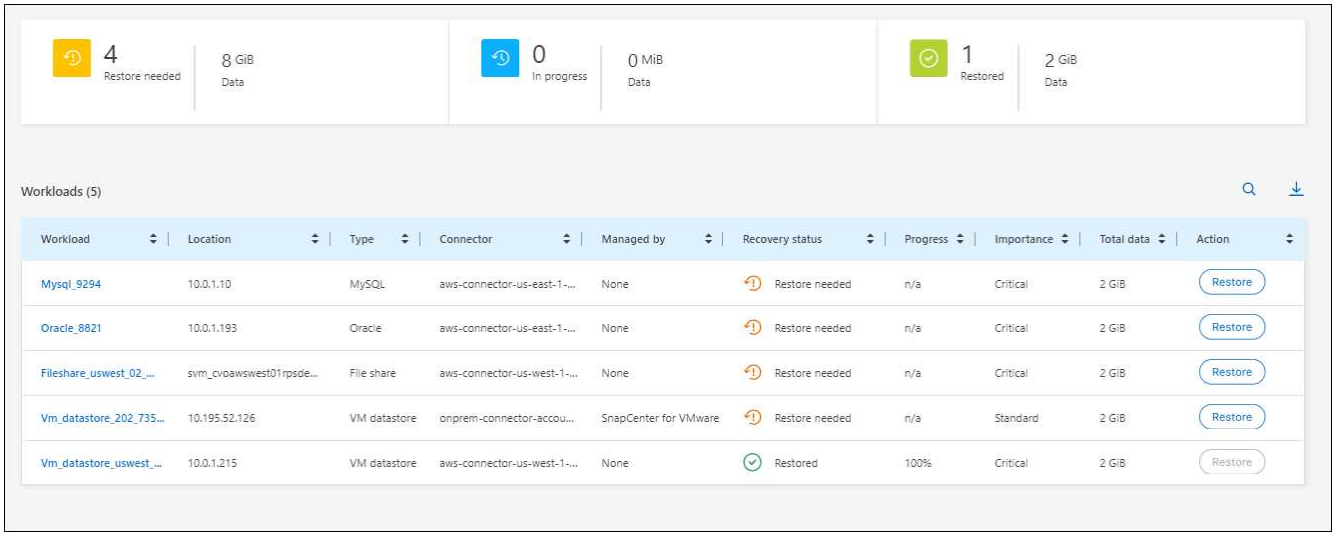
Überprüfen Sie die Workloads, die sich im Wiederherstellungsstatus „Wiederherstellung erforderlich“ befinden.

Schritte

1. Überprüfen Sie im Haupt-Dashboard für Ransomware Resilience die Gesamtzahlen unter „Restore needed“ im Warnbereich und wählen Sie **View all**.

   Alternativ können Sie in der Seitenleiste **Recovery** auswählen.

2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.



Eine Arbeitslast wiederherstellen

Nachdem Sie die Arbeitslasten bewertet haben, haben Sie zwei Möglichkeiten, Ihre Arbeitslast wiederherzustellen:

- Wiederherstellung mit einer benutzerdefinierten Wiederherstellung
- Mit einer sauberen Wiederherstellung wiederherstellen

Überprüfen Sie den Wiederherstellungsstatus in NetApp Ransomware Resilience

Nachdem Workloads als „Wiederherstellung erforderlich“ markiert wurden, empfiehlt NetApp Ransomware Resilience einen tatsächlichen Wiederherstellungspunkt (RPA) und orchestriert den Workflow für eine absturzsichere Wiederherstellung.

- Wenn die Anwendung oder VM von NetApp Backup and Recovery oder Ransomware Resilience verwaltet wird, führt Ransomware Resilience eine absturzkonsistente Wiederherstellung durch, bei der alle Daten, die sich zum gleichen Zeitpunkt auf dem Volume befanden, wiederhergestellt werden, zum Beispiel wenn das System abgestürzt ist.

  Sie können die Arbeitslast wiederherstellen, indem Sie alle Volumes, bestimmte Volumes oder bestimmte Dateien auswählen.

Die Wiederherstellung der Arbeitslast kann sich auf laufende Arbeitslasten auswirken. Sie sollten die Wiederherstellungsprozesse mit den entsprechenden Beteiligten koordinieren.

Ein Workload kann einen der folgenden Wiederherstellungsstatus haben:

- **Wiederherstellung erforderlich**: Die Arbeitslast muss wiederhergestellt werden.
- **In Bearbeitung**: Der Wiederherstellungsvorgang ist derzeit im Gange.
- **Wiederhergestellt**: Die Arbeitslast wurde wiederhergestellt.
- **Fehlgeschlagen**: Der Workload-Wiederherstellungsprozess konnte nicht abgeschlossen werden.

Anzeigen von Workloads, die zur Wiederherstellung bereit sind

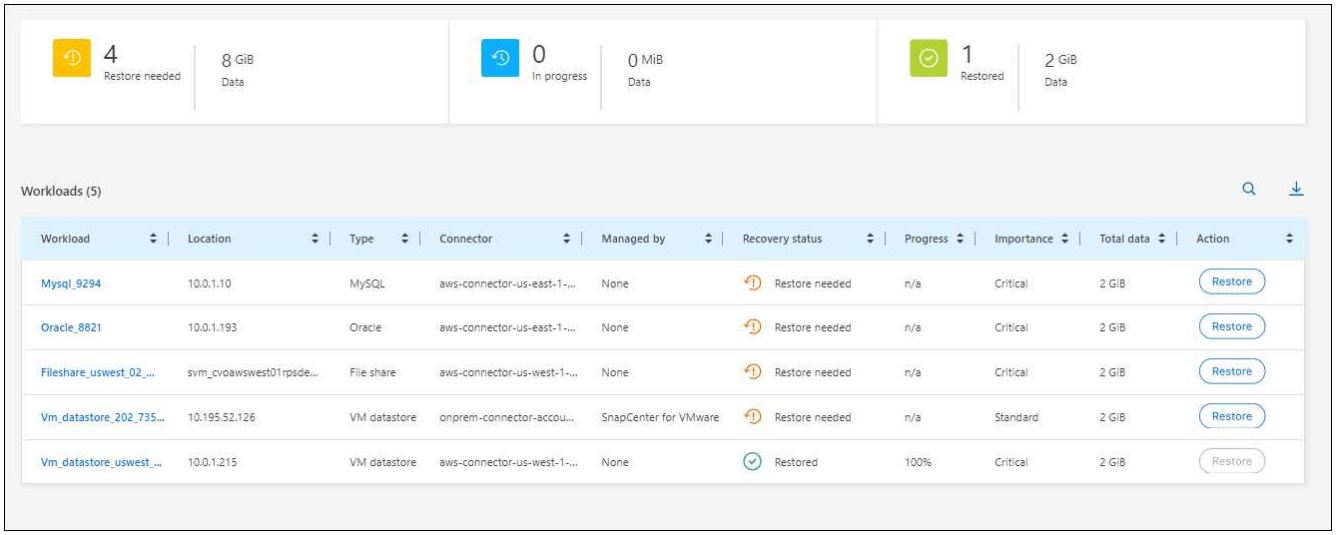
Überprüfen Sie die Workloads, die sich im Wiederherstellungsstatus „Wiederherstellung erforderlich“ befinden.

Schritte

1. Überprüfen Sie im Haupt-Dashboard für Ransomware Resilience die Gesamtzahlen unter „Restore needed“ im Warnbereich und wählen Sie **View all**.

   Alternativ können Sie in der Seitenleiste **Recovery** auswählen.

2. Überprüfen Sie die Arbeitslastinformationen auf der Seite **Wiederherstellung**.



Eine Arbeitslast wiederherstellen

Nachdem Sie die Arbeitslasten bewertet haben, haben Sie zwei Möglichkeiten, Ihre Arbeitslast wiederherzustellen:

- Wiederherstellung mit einer benutzerdefinierten Wiederherstellung
- Mit einer sauberen Wiederherstellung wiederherstellen

Führen Sie eine saubere Wiederherstellung durch

Konfigurieren Sie die Umgebung für eine saubere Wiederherstellung in NetApp Ransomware Resilience

NetApp Ransomware Resilience bietet saubere Wiederherstellungen, die eine geführte Wiederherstellung nach Ransomware-Angriffen ermöglichen. Um eine saubere Wiederherstellung durchzuführen, müssen Sie zunächst eine isolierte Wiederherstellungsumgebung (IRE) erstellen, entweder lokal oder in einer unterstützten Cloud-Umgebung. In der IRE erstellen Sie einen Clean Room, in dem Ransomware Resilience die Arbeitslast isoliert, um zu ermitteln, welche Dateien sauber und welche von Ransomware betroffen sind.

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

Erfahren Sie mehr über Clean Restores

Wenn Sie eine vollständige Wiederherstellung durchführen, führt Sie Ransomware Resilience durch einen mehrstufigen Prozess, der die Wiederherstellung optimiert.

- **EINRICHTUNG**: Für eine vollständige Wiederherstellung müssen Sie zunächst eine IRE erstellen und anschließend die wiederherzustellende Workload auswählen. Ransomware Resilience erstellt einen sauberen Raum, in dem alle Aktionen für die Workload ausgeführt werden.
- **ANALYSE**: Im Clean Room analysiert Ransomware Resilience alle Snapshots, um festzustellen, ob eine

Verschlüsselung vorhanden ist. Clean restore bestimmt eine Wiederherstellungskarte, um den optimalen Wiederherstellungsplan zu bestimmen.

Sobald ein Wiederherstellungspunkt ohne betroffene Dateien gefunden wurde, werden alle vorherigen Wiederherstellungspunkte übersprungen. Wenn der Ransomware-Angriff am 10. Oktober stattfand und am 7. Oktober um 10:21 Uhr ein Wiederherstellungspunkt ohne betroffene Dateien gefunden wurde, werden alle Wiederherstellungspunkte vor dem 7. Oktober um 10:21 Uhr übersprungen.

Im Analyseschritt wird auch die Anzahl der überprüften Dateien angezeigt, wobei angegeben wird, welche betroffen sind und welche nicht.

- **PLAN**: Wählen Sie die bereitgestellten Optionen für die Wiederherstellung:
  - *Letzter unbeeinträchtigter Wiederherstellungspunkt*: der schnellste Wiederherstellungspunkt aus dem aktuellsten unverschlüsselten Snapshot vor dem Angriff
  - *Minimaler Datenverlust*: die aktuellste Version jeder unverschlüsselten Datei aus verschiedenen Snapshots

    Sie können auch im Planungsschritt die Dateihistorien einsehen, um zu sehen, wann Ransomware-Ereignisse die Dateien beeinträchtigt haben und wie der Wiederherstellungspunkt zeitlich zu diesem Ereignis steht.
- **BEREINIGUNG**: Ransomware Resilience entfernt Schadsoftware vom Wiederherstellungspunkt. Wenn Dateien nicht bereinigt werden können, werden sie von der Wiederherstellung ausgeschlossen und in einem separaten Speicherort unter Quarantäne gestellt.
- **WIEDERHERSTELLEN**: Ransomware Resilience stellt die sauberen Daten in der Quellumgebung wieder her.
- **ENDE**: Ransomware Resilience bietet eine detaillierte Zusammenfassung des Prozesses und schließt den Clean Room, wodurch die während der Einrichtung bereitgestellten Ressourcen freigegeben werden, um zukünftige nutzungsabhängige Kosten zu eliminieren.

Unterstützte Konfigurationen

- Pro Ransomware Resilience-Konto kann nur ein IRE erstellt werden. Jedes IRE kann drei Clean Rooms enthalten.
- Eine vollständige Wiederherstellung wird derzeit nur für NAS-Dateifreigaben (NFS/CIFS) unterstützt.
- Sie müssen eine saubere Wiederherstellung der Quellumgebung durchführen.
- Sie können eine IRE in der Cloud oder lokal erstellen. Aktuell werden folgende Konfigurationen unterstützt:

Quelle	Ziel (IRE)	Unterstützte Zielregionen
Vor Ort (nur AFF- oder FAS-Systeme)*	Lokal (VMware vCenter)	k. A.
Vor Ort (nur AFF- oder FAS-Systeme)*	Cloud: AWS	• US East 1 • EU Central 1
Cloud: Cloud Volumes ONTAP mit AWS*	Cloud: AWS	• US East 1 • EU Central 1

Quelle	Ziel (IRE)	Unterstützte Zielregionen
Cloud: Amazon FSxN für ONTAP	Cloud: AWS	• US East 1 • EU Central 1

*Sie müssen ONTAP 9.11.1 oder höher ausführen.

Eine vollständige Wiederherstellung in einer Cloud-basierten Umgebung kann zusätzliche Rechenkosten des Cloud-Anbieters verursachen. Weitere Informationen finden Sie unter "Kosten und Lizenzierung".

Überlegungen

- Sie können nur eine vollständige Wiederherstellung bei einem auf Verschlüsselung basierenden Ransomware-Angriff durchführen.
- Wenn die isolierte Wiederherstellungsumgebung keine Kapazität für einen neuen Vorgang hat, wird dieser in die Warteschlange gestellt, bis Kapazität verfügbar ist.
  - Im Dashboard „Ransomware Resilience Recovery“ können Sie jederzeit den Status aktiver und in der Warteschlange befindlicher Wiederherstellungsvorgänge überwachen.
- Wenn Sie eine vollständige Wiederherstellung durchführen, wird das ursprüngliche Volume ausgehängt, was den E/A-Zugriff beeinträchtigen kann.

Zusätzliche Überlegungen für On-Premises-Umgebungen

Wenn Sie eine lokale IRE bereitstellen und eine Windows-VM für die Wiederherstellungsanalyse im Rahmen einer sauberen Wiederherstellung geklont wird, behält die geklonte VM dieselbe Konfiguration wie die Quelle. Dies kann zu Konflikten führen:

- Die Verwendung desselben Sicherheitsidentifikators (SID) führt zu Authentifizierungs- und Sicherheitskonflikten.
- Die Verwendung desselben Computernamens (CN) führt zu Netzwerkkonflikten.
- Die Verwendung derselben Maschinenidentität führt zu Lizenzierungs- und Aktivierungsproblemen.

Um diese Konflikte zu vermeiden, führt Ransomware Resilience auf der geklonten VM eine Systemvorbereitung (sysprep) durch, wodurch SID, CN und Maschinenidentität zurückgesetzt werden. Durch das Zurücksetzen dieser Werte wird sichergestellt, dass die geklonte VM als eindeutige und unabhängige Instanz funktioniert, ohne die Quell-VM zu beeinträchtigen.

Sekundärquellen

Beim Erstellen des IRE für lokale Quellen haben Sie die Möglichkeit, eine sekundäre Quelle hinzuzufügen.

Wenn die primäre Quelle verfügbar ist, muss die Clean Restore auf der primären Quelle durchgeführt werden. Wenn die primäre Quelle nicht verfügbar ist und Sie eine sekundäre Quelle konfiguriert haben, wird die Clean Restore auf der sekundären Quelle durchgeführt.

Der Clean Restore-Prozess analysiert standardmäßig Snapshots aus der Quellumgebung. Ist entweder die Quellumgebung nicht verfügbar oder kein unverschlüsselter Snapshot auf der Quelle vorhanden, analysiert Clean Restore Snapshots auf einem Sekundärsystem, sofern Sie eines konfiguriert haben.

Kosten und Lizenzierung

Die vollständige Wiederherstellung ist Bestandteil der Ransomware-Resilienz. Für die Durchführung einer vollständigen Wiederherstellung oder die Erstellung einer IRE ist keine zusätzliche Lizenz erforderlich.

Die Aktivierung der sauberen Wiederherstellung kann Gebühren von Drittanbietern für Cloud-Dienste verursachen. Je nach Nutzung des Dienstes können diese Gebühren während der gesamten Laufzeit der sauberen Wiederherstellungsumgebungen wiederholt anfallen.

Gebühren von Drittanbietern können die Erstellung und Bereitstellung von Recheninstanzen sowie zusätzliche Speicherkapazität für die Produktion zur Bereinigung und Wiederherstellung umfassen. Betrachten Sie die folgenden Beispiele:

- Wenn ein IRE in AWS bereitgestellt wird und Sie die saubere Wiederherstellung initiieren, werden zwei t3.medium AWS EC2-Instanzen im Clean Room innerhalb des IRE bereitgestellt, um Verschlüsselung und Malware zu bereinigen.
- In Cloud Volumes ONTAP erstellt clean restore eine Clean Room Storage VM für Metadaten-Volumes und Snapshot-Klone zur Analyse.

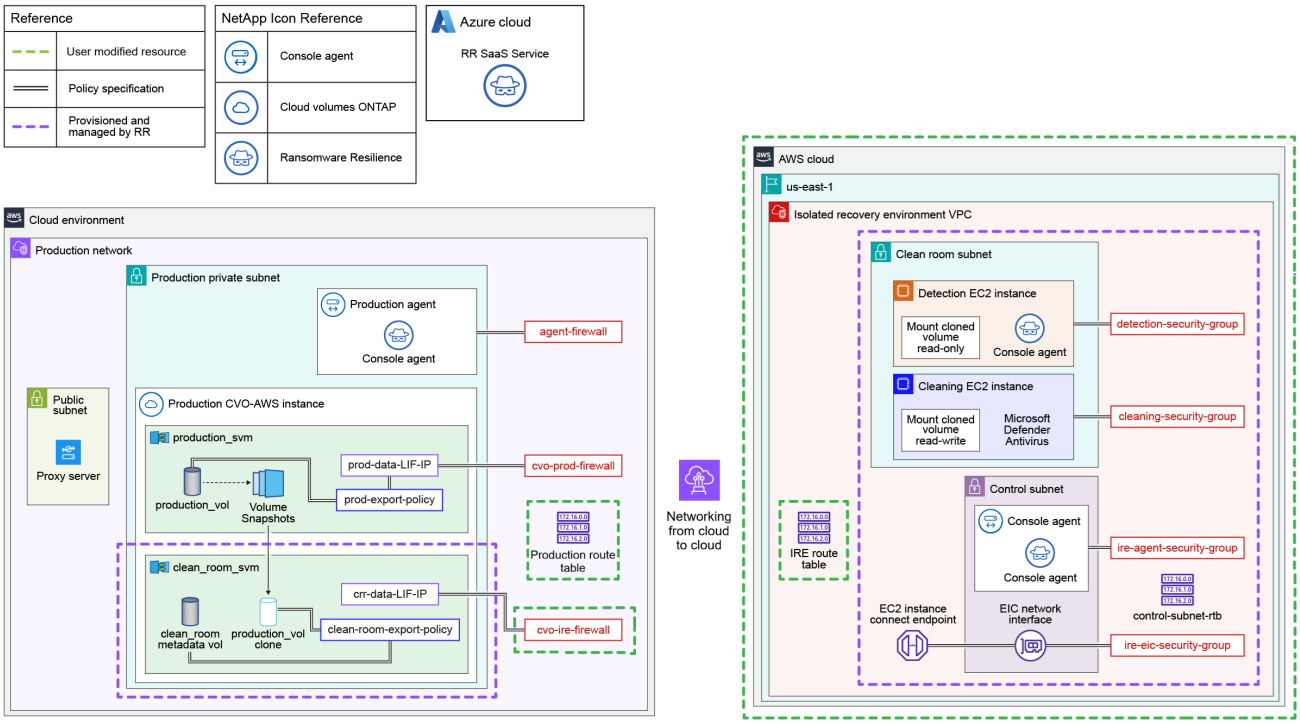
Voraussetzungen

Stellen Sie sicher, dass Sie die Voraussetzungen für den von Ihnen gewählten Bereitstellungstyp „Saubere Wiederherstellung“ erfüllt haben. Wählen Sie die Registerkarte für Ihre gewählte IRE-Konfiguration aus.

Wenn Sie das IRE erstellen, müssen Sie während des Systemauswahlschritts beim Erstellen des IRE jedes System (primär oder sekundär) hinzufügen, das Sie für die Analyse verwenden möchten.

Cloud zu Cloud

Dieses Diagramm veranschaulicht ein Beispiel für die Cloud-zu-Cloud-Clean-Restore-Konfiguration. Sehen Sie sich das Diagramm und die Ressourcen an, die Sie konfigurieren müssen, bevor Sie die IRE erstellen können.



Reinraum-SVM-Daten LIF IP (crr-data-LIF-IP)

- Weisen Sie dem Reinraum-SVM-Daten-LIF eine IP-Adresse zu. Notieren Sie sich die IP-Adresse: Sie benötigen diese IP-Adresse während des IRE-Konfigurationsprozesses.
  - Für Cloud Volumes ONTAP mit AWS unter Verwendung einer Cloud-zu-Cloud-Clean-Restore muss sichergestellt werden, dass die IP-Adresse der Elastic Network Interface zugewiesen ist.
- Routing von der SVM-Daten-LIF-IP zur IRE zulassen.

Wenn Sie ein IRE mit der Quelle in Amazon FSxN für ONTAP konfigurieren, können Sie diese Anforderung an die Clean Room SVM-Daten-LIF-IP überspringen.

Produktionsumgebungs-Routingtabelle

- Die Produktionsroutentabelle muss den Datenverkehr vom IRE-Subnetz zur Clean Restore Data LIF-IP zulassen. Sie müssen diese Route zur Produktionsroutentabelle hinzufügen.
- Sicherheitsgruppen und Firewalls im Produktions-ONTAP-Cluster sollten eingehenden NFSv4- und NFSv3-Datenverkehr zur LIF-IP für saubere Wiederherstellungsdaten zulassen. Die Firewall sollte für eingehenden Datenverkehr aus dem IRE-CIDR-Bereich geöffnet sein.

Protokoll	Zielport	Quelle	Zweck
TCP & UDP	2049	IRE VPC CIDR-Bereich	NFSv4-Zugriff von IRE
TCP & UDP	111	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	635	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE

Protokoll	Zielport	Quelle	Zweck
TCP & UDP	4045	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	4046	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	4049	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE

IRE-Routingtabelle

- Die IRE-Routingtabelle sollte die Hauptroutingtabelle in der IRE VPC sein.
- Die IRE-Routingtabelle sollte das Routing zur sauberen Wiederherstellungsdaten-LIF-IP-Adresse ermöglichen.
- Die IRE-Routingtabelle sollte auch eine Route zum öffentlichen Internet ermöglichen, damit der IRE-Agent funktionieren kann.

Virtual Private Cloud (VPC)

- Für das IRE stellen Sie eine VPC innerhalb des IP-Adressbereichs Ihrer Produktionsumgebung bereit. Die IP-Adresse darf nicht mit bestehenden IP-Adressen in Konflikt stehen.
  - Die VPC sollte eine Mindestkapazität von 64 IP-Adressen (eine /26-Netzmaske) haben.
  - Die VPC muss den öffentlichen Internetzugang zulassen. Andernfalls funktioniert der Konsolenagent nicht.

Cloud-Berechtigungen

- Ransomware Resilience benötigt den AWS Access Key und das Secret mit den korrekten IAM-Berechtigungen, um die Clean Restore in einer AWS-Umgebung durchzuführen. "Erstellen einer IAM-Richtlinie in AWS" mit den folgenden Berechtigungen, und hängen Sie dann die Richtlinie an einen neu erstellten Benutzer an. Nachdem Sie den Benutzer erstellt haben, generieren Sie die IAM-Anmeldeinformationen und stellen Sie sie für die Clean Restore bereit.

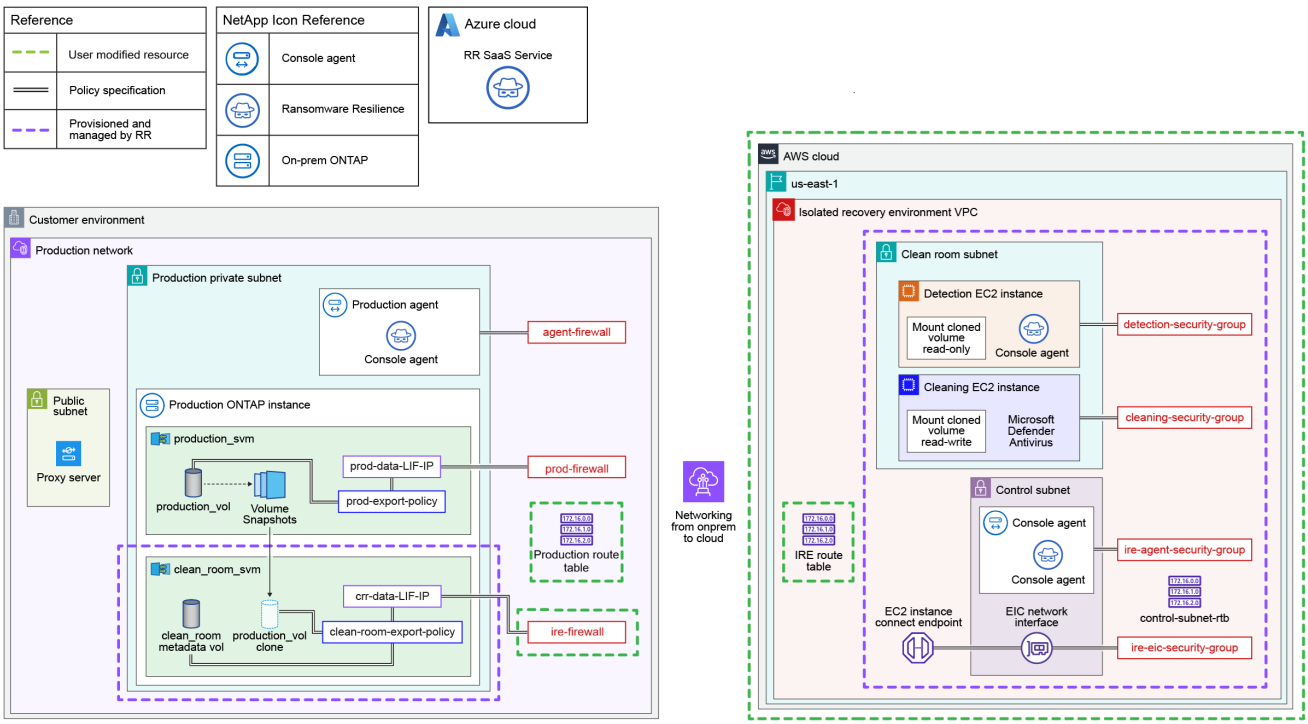
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Isolated recovery environmentFullAccess",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "EC2CreateAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2ReadPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMFullAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketCreation",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketObjects",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket/*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucket",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket"
        }
    ]
}
```

On-Premises zu Cloud

Dieses Diagramm veranschaulicht ein Beispiel für die On-Premises-zu-Cloud-Clean-Restore-Konfiguration. Überprüfen Sie das Diagramm und die Ressourcen, die Sie konfigurieren müssen, bevor Sie die IRE erstellen können.



Reinraum-SVM-Daten LIF IP (crr-data-LIF-IP)

- Weisen Sie dem Reinraum-SVM-Daten-LIF eine IP-Adresse zu. Notieren Sie sich die IP-Adresse: Sie benötigen diese IP-Adresse während des IRE-Konfigurationsprozesses.
  - Für Cloud Volumes ONTAP mit AWS unter Verwendung einer Cloud-zu-Cloud-Clean-Restore muss sichergestellt werden, dass die IP-Adresse der Elastic Network Interface zugewiesen ist.
- Routing von der SVM-Daten-LIF-IP zur IRE zulassen.

Wenn Sie ein IRE mit der Quelle in Amazon FSxN für ONTAP konfigurieren, können Sie diese Anforderung an die Clean Room SVM-Daten-LIF-IP überspringen.

Produktionsumgebungs-Routingtabelle

- Die Produktionsroutentabelle muss den Datenverkehr vom IRE-Subnetz zur Clean Restore Data LIF-

IP zulassen. Sie müssen diese Route zur Produktionsroutentabelle hinzufügen.

- Sicherheitsgruppen und Firewalls im Produktions-ONTAP-Cluster sollten eingehenden NFSv4- und NFSv3-Datenverkehr zur LIF-IP für saubere Wiederherstellungsdaten zulassen. Die Firewall sollte für eingehenden Datenverkehr aus dem IRE-CIDR-Bereich geöffnet sein.

Protokoll	Zielport	Quelle	Zweck
TCP & UDP	2049	IRE VPC CIDR-Bereich	NFSv4-Zugriff von IRE
TCP & UDP	111	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	635	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	4045	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	4046	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE
TCP & UDP	4049	IRE VPC CIDR-Bereich	NFSv3-Zugriff von IRE

IRE-Routingtabelle

- Die IRE-Routingtabelle sollte die Hauptroutingtabelle in der IRE VPC sein.
- Die IRE-Routingtabelle sollte das Routing zur sauberen Wiederherstellungsdaten-LIF-IP-Adresse ermöglichen.
- Die IRE-Routingtabelle sollte auch eine Route zum öffentlichen Internet ermöglichen, damit der IRE-Agent funktionieren kann.

Virtual Private Cloud (VPC)

- Für das IRE stellen Sie eine VPC innerhalb des IP-Adressbereichs Ihrer Produktionsumgebung bereit. Die IP-Adresse darf nicht mit bestehenden IP-Adressen in Konflikt stehen.
  - Die VPC sollte eine Mindestkapazität von 64 IP-Adressen (eine /26-Netzmaske) haben.
  - Die VPC muss den öffentlichen Internetzugang zulassen. Andernfalls funktioniert der Konsolenagent nicht.

Cloud-Berechtigungen

- Ransomware Resilience benötigt den AWS Access Key und das Secret mit den korrekten IAM-Berechtigungen, um die Clean Restore in einer AWS-Umgebung durchzuführen. "Erstellen einer IAM-Richtlinie in AWS" mit den folgenden Berechtigungen, und hängen Sie dann die Richtlinie an einen neu erstellten Benutzer an. Nachdem Sie den Benutzer erstellt haben, generieren Sie die IAM-Anmeldeinformationen und stellen Sie sie für die Clean Restore bereit.

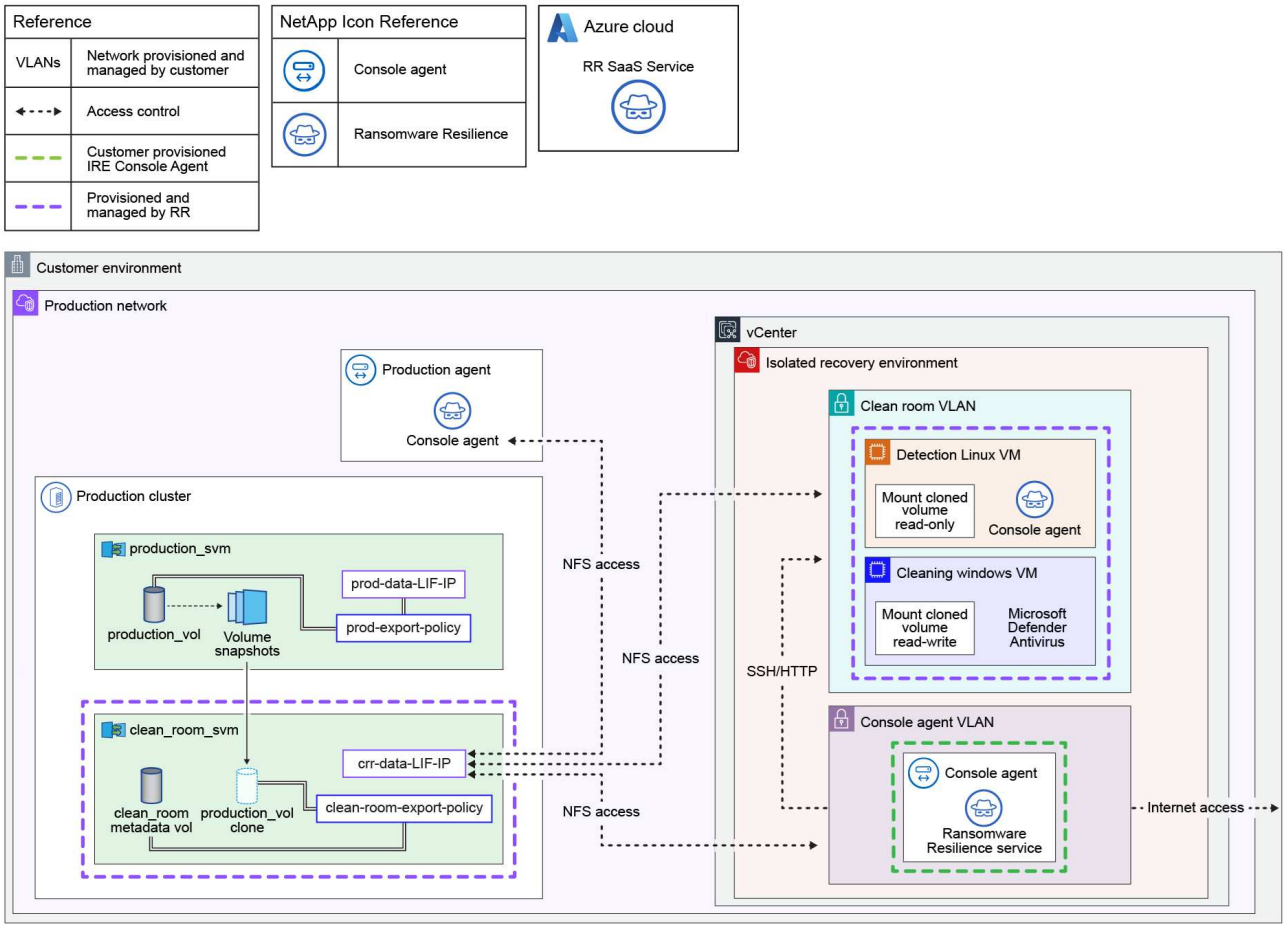
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Isolated recovery environmentFullAccess",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
```

```
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "EC2CreateAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2ReadPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMFullAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/rps::Isolated recovery
environment-name": "*"
                }
            }
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketCreation",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucketObjects",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket/*"
        },
        {
            "Sid": "S3FullAccessToIsolated recovery
environmentStateBucket",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::*-netapp-Isolated recovery
environment-state-bucket"
        }
    ]
}
```

Vor Ort zu Vor Ort

Dieses Diagramm veranschaulicht ein Beispiel für die Konfiguration einer sauberen Wiederherstellung von On-Premises zu On-Premises. Überprüfen Sie das Diagramm und die Ressourcen, die Sie konfigurieren müssen, bevor Sie die IRE erstellen können.



Reinraum-SVM-Daten LIF IP (crr-data-LIF-IP)

- Auf jedem System, das Sie für die Verbindung mit dem IRE zur Wiederherstellung von Workloads auswählen, wird eine Storage Virtual Machine (SVM) erstellt. Sie müssen jedem System, das als Daten-LIF der Clean-Room-SVM verwendet wird, eine dedizierte IP-Adresse zuweisen.

Hosts & vCenter

- Das vCenter muss Version 7.0 oder höher mit mindestens einem Rechenzentrum sein.
- Der ESXi-Host muss ESXi Version 7.0 oder höher sein und mindestens einen Host mit ausreichend CPU- und Arbeitsspeicherressourcen zum Klonen der VMs aufweisen.
- Die angegebenen vCenter Anmeldeinformationen müssen über Berechtigungen zum Auffinden von Ressourcen und zum Klonen von VMs verfügen.

Basis-VMs (Windows oder Linux)

- Bei der Wiederherstellung im Rahmen einer sauberen Wiederherstellung werden die Basis-VMs in ein ausgewähltes Rechenzentrum geklont, auf dem gewählten ESXi-Rechenknoten platziert, dem angegebenen Datenspeicher zugeordnet und mit dem festgelegten Netzwerk verbunden. Beim Klonen werden die VMs mit 2 vCPUs und 4 GB RAM (für Linux- oder Windows-VM) sowie demselben Speicherplatz wie die Basis-VMs konfiguriert. Jede Sitzung zur sauberen Wiederherstellung verwendet zwei IP-Adressen aus dem angegebenen CIDR-Bereich.
- Sie müssen einen ausreichend großen IP-Adressbereich bereitstellen, um mehrere parallele Reinraumsitzungen zu ermöglichen. Die IP-Adressen werden nach Abschluss der Wiederherstellung freigegeben.
- Der Datenspeicher sollte über ausreichend freie Kapazität verfügen, um das Klonen von VMs zu

ermöglichen.

- Der IP-Adressbereich muss im CIDR-Format angegeben werden (z. B. 100.100.0.0/24)
- Für Linux-VMs:
  - Als Betriebssystem muss Ubuntu Linux 20.04 oder höher installiert sein.
  - Das lokale System muss eingeschaltet sein.
  - VMware Tools muss installiert sein und ausgeführt werden.
  - SSH muss aktiviert sein.
  - Sie müssen nfs-common installiert haben.
  - Docker muss installiert sein und ausgeführt werden.
  - Sie benötigen mindestens 40 GB freien Speicherplatz.
- Für Windows-VMs:
  - Windows-VMs sollten über 20 GB freien Speicherplatz verfügen.
  - Das Betriebssystem sollte Windows Server 2022 oder 2025 sein.
  - VMware Tools muss installiert sein und ausgeführt werden.
  - WinRM muss aktiviert sein.
  - Die IP-Adresse sollte konfiguriert werden.
  - Stellen Sie sicher, dass Sie über die entsprechende Lizenz verfügen, die das Klonen von Basis-VMs erlaubt.
  - Die VM muss eingeschaltet sein.

Netzwerk

- Konfigurieren Sie die VLAN-Ressourcen mit dem folgenden Zugriff:

Ressource	Zugang
Reinraum SVM VLAN	NFS-Zugriff auf die: * Produktionskonsolenagent * Konsolenagent VLAN * Reinraum VLAN
Konsolenagent VLAN	• NFS-Zugriff auf das Reinraum-SVM-VLAN • HTTP/SSH-Zugriff auf das Reinraum-VLAN
Reinraum-VLAN	NFS-Zugriff auf das Reinraum-SVM-VLAN

Dedizierter Konsolenagent

- Stellen Sie einen dedizierten NetApp Console-Agenten für das IRE bereit. Der Console-Agent muss im Ziel-vCenter mit Zugriff auf das Clean Room-VLAN bereitgestellt werden. Weitere Informationen zum Bereitstellungsprozess finden Sie unter "Einen Konsolenagenten lokal bereitstellen".

Erstellen Sie eine isolierte Wiederherstellungsumgebung

Vor der Durchführung einer vollständigen Wiederherstellung muss ein isolierter Wiederherstellungsraum eingerichtet werden.

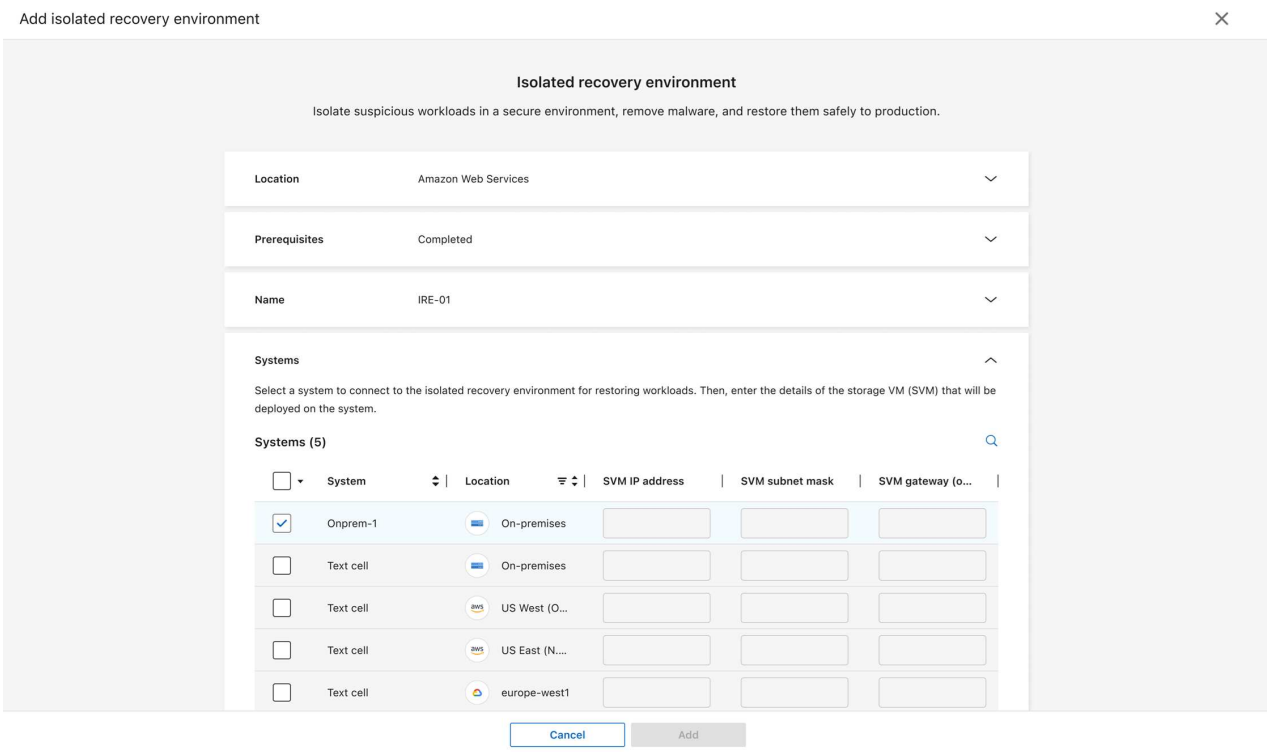
Die Vorgehensweise zum Einrichten eines isolierten Wiederherstellungsraums unterscheidet sich je nachdem,

ob sich die Umgebung in der Cloud oder lokal befindet. Stellen Sie sicher, dass Sie die Anweisungen für den richtigen Standort befolgen.

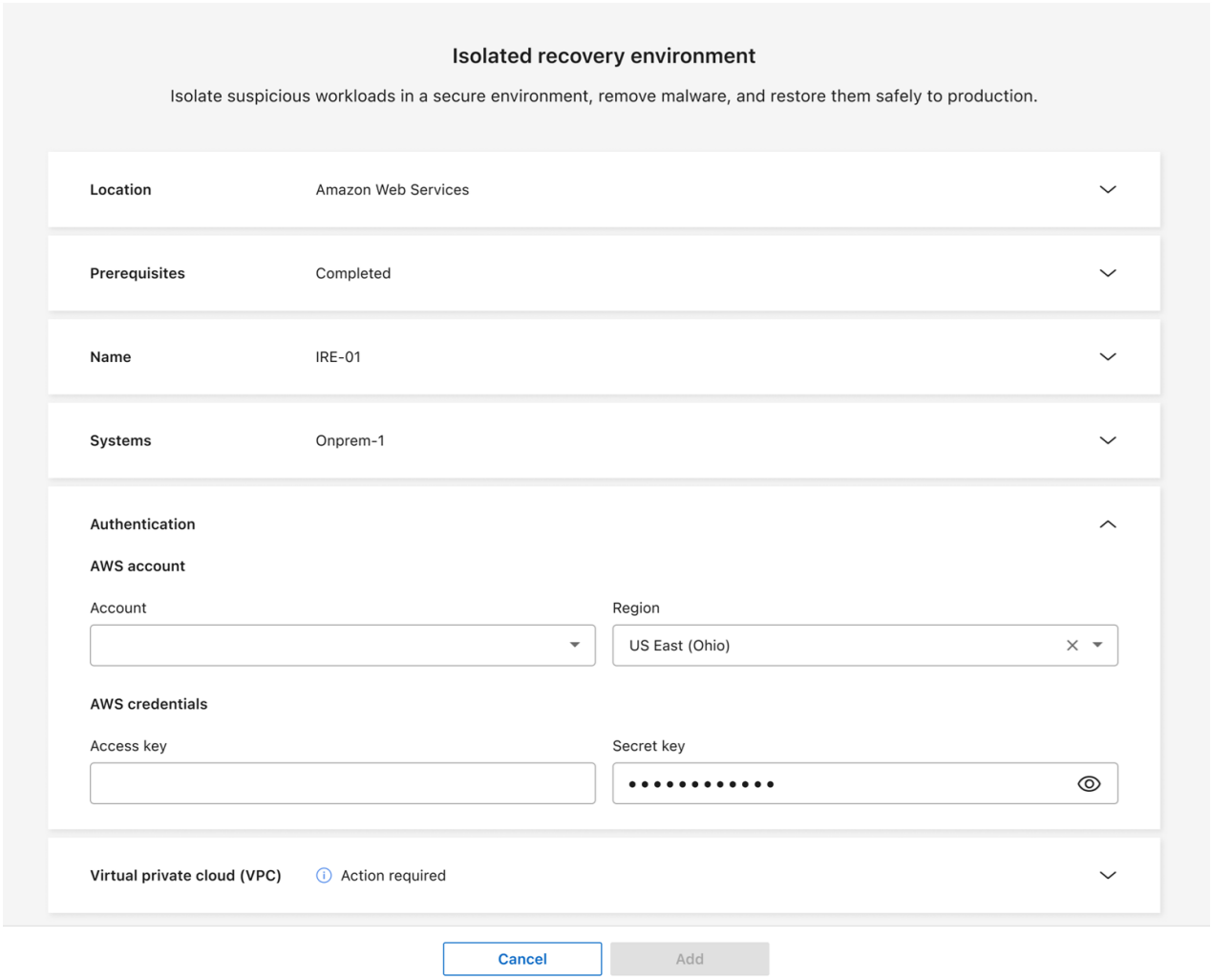
Cloud

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Wählen Sie in der Karte „Saubere Wiederherstellung“ die Option **Hinzufügen**, um die isolierte Wiederherstellungsumgebung zu erstellen.
3. Für ein Cloud-basiertes IRE wählen Sie **Amazon Web Services**.
4. Erweitern Sie den Abschnitt **Name**. Geben Sie einen **Name** für die Umgebung ein.
5. Erweitern Sie den Abschnitt **Systeme**. Wählen Sie die Systeme aus, die Sie mit dem IRE verbinden möchten. Für jedes ausgewählte System müssen Sie die IP-Adresse, die Subnetzmaske und das Gateway der Speicher-VM angeben.

   Für IREs, die auf Amazon FSxN für ONTAP bereitgestellt werden, müssen Sie diese Informationen nicht angeben.



6. Erweitern Sie den Abschnitt **Authentifizierung**.
   - Geben Sie die **Account**-ID in der Cloud ein und wählen Sie im Dropdown-Menü die **Region** für das Konto aus. Sie können eine IRE nur in einer unterstützten Region bereitstellen.
   - Geben Sie den **Zugriffsschlüssel** und den **Geheimschlüssel** für das Konto ein.
7. Erweitern Sie den Abschnitt **Virtuelle private Cloud (VPC)**. Geben Sie die VPC-ID ein, in der die IRE bereitgestellt werden soll.



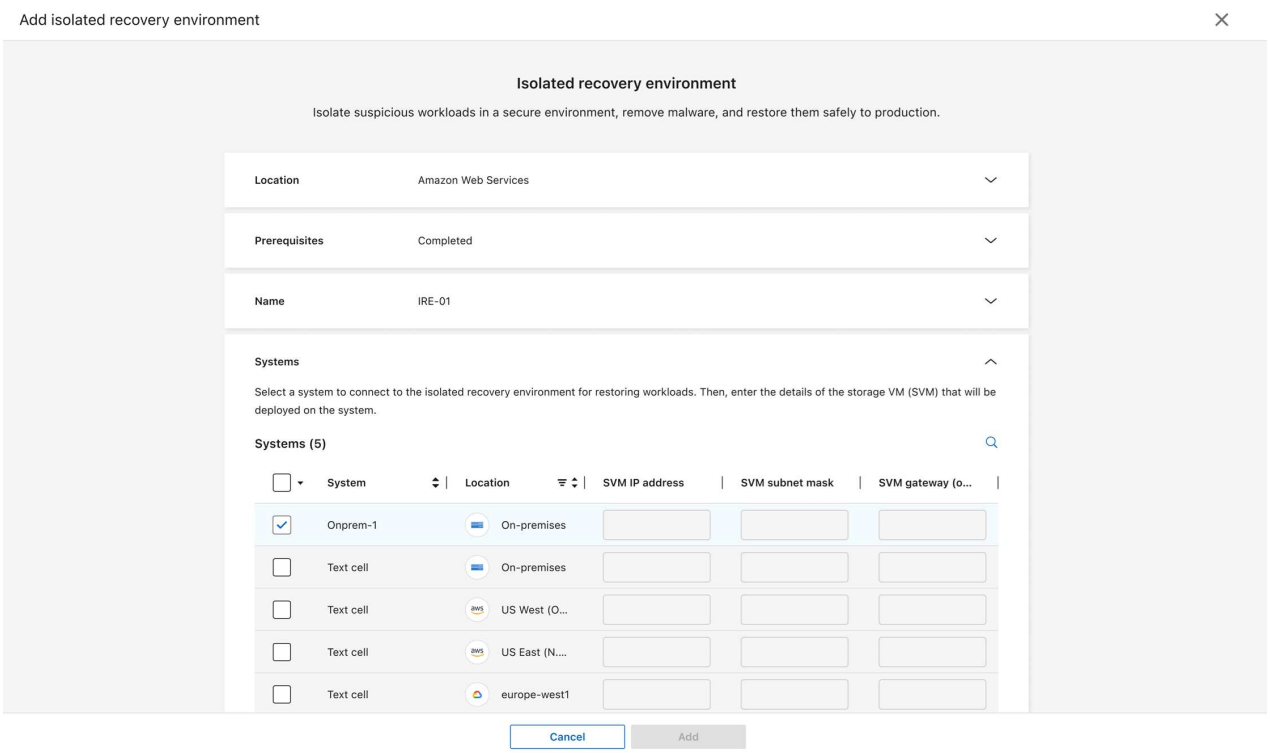
8. Wählen Sie **Hinzufügen**, um den IRE zu erstellen.

   Ransomware Resilience testet die Verbindung, nachdem Sie „Hinzufügen“ ausgewählt haben, was einige Minuten dauern kann. Die IRE wurde erfolgreich bereitgestellt, wenn ihr Status als „deployed“ angezeigt wird.

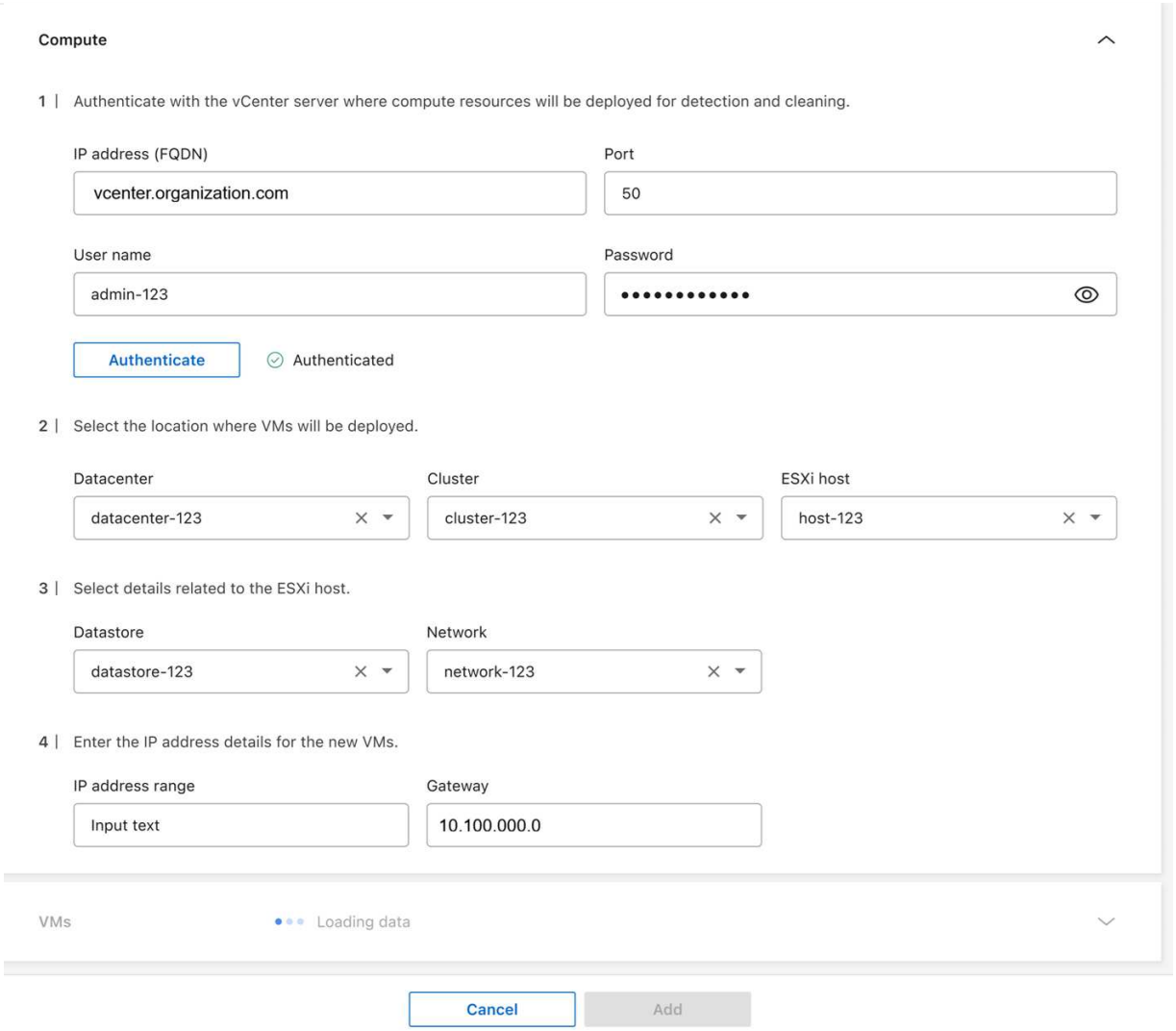
Vor Ort

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Wählen Sie auf der Karte „Clean restores“ die Option **Hinzufügen**, wenn dies Ihre erste Umgebung ist, oder **Verwalten**, wenn Sie bereits eine erstellt haben.
3. Wählen Sie als Standort **On-premises** aus.
4. Erweitern Sie den Abschnitt **Name**. Weisen Sie dem IRE einen **Namen** zu.
5. Erweitern Sie den Abschnitt **Systeme**. Wählen Sie die Systeme aus, die Sie mit dem IRE verbinden möchten. Weisen Sie jedem System, dessen Workloads im IRE wiederhergestellt werden sollen, eine Speicher-VM-IP-Adresse, eine Subnetzmaske und ein Gateway zu.

   Jedem ausgewählten System muss eine IP-Adresse zugewiesen sein. Sie können primäre oder sekundäre Systeme auswählen. Sekundäre Systeme können für Analyse und Wiederherstellung verwendet werden, falls das primäre System keine unverschlüsselten Snapshots enthält oder nicht verfügbar ist.



6. Erweitern Sie den Abschnitt **Konsolenagent**. Wählen Sie den Konsolenagenten aus dem Dropdown-Menü aus, der im IRE bereitgestellt ist.
7. Erweitern Sie den Abschnitt **Compute**.
   a. Geben Sie die Anmeldeinformationen zur Authentifizierung des vCenter Servers an: **IP-Adresse** oder vollqualifizierter Domänenname (FQDN), **Port**, **Benutzername** und **Passwort**.
   b. Wählen Sie **Authentifizieren**, um die Anmeldeinformationen zu bestätigen. Warten Sie, bis die Benutzeroberfläche Ihre Anmeldeinformationen bestätigt hat, bevor Sie fortfahren.
   c. Wählen Sie das **Rechenzentrum** und den **Cluster** aus, in dem die VMs bereitgestellt werden sollen.
   d. Wählen Sie den **Datenspeicher** und das **Netzwerk** für den ESXi-Host aus.
   e. Geben Sie den **IP-Adressbereich** im CIDR-Format (z. B. 10.0.0.1/24), die **Subnetzmaske** und das **Gateway** für die VMs ein.



8. Erweitern Sie den Abschnitt **VMs**, der anhand Ihrer Eingaben im Abschnitt **Compute** befüllt wird.
   a. Wählen Sie für die Linux-VM, die Ransomware Resilience zum Scannen nach Ransomware verwendet, die VM aus dem Dropdown-Menü und geben Sie dann den **Benutzernamen** und das **Passwort** für die VM ein.
   b. Wählen Sie für die zum Scannen verwendete Windows-VM die VM aus dem Dropdown-Menü aus und geben Sie anschließend den **Benutzernamen** und das **Passwort** für die VM ein.
9. Wählen Sie **Hinzufügen**, um die IRE zu erstellen. Ransomware Resilience testet die Verbindung, nachdem Sie Hinzufügen ausgewählt haben; dieser Vorgang kann einige Minuten dauern. Die IRE wurde erfolgreich bereitgestellt, wenn ihr Status als „bereitgestellt“ angezeigt wird.

Sie können den Fortschritt verfolgen. Wählen Sie im Tab „Einstellungen“ **Isolierte Wiederherstellungsumgebungen** aus. Die Seite „Isolierte Wiederherstellungsumgebungen“ zeigt die IRE und deren Status an. Wählen Sie **Aufträge anzeigen** für eine Aufschlüsselung aller Aufträge, die zu dieser Umgebung gehören.

Sie können die Systeme in einer IRE nach deren Erstellung bearbeiten. Wählen Sie im Tab „Einstellungen“ **Isolierte Wiederherstellungsumgebungen** aus. Suchen Sie die gewünschte IRE, wählen Sie das Aktionsmenü … und dann **Bearbeiten**. Fahren Sie fort, um die Systeme zu bearbeiten. Wählen Sie **Speichern**, wenn Sie fertig sind.

Um Details der IRE zu ändern, wählen Sie **Einstellungen** in der Ransomware Resilience-Seitenleiste und dann in der Clean restore-Karte **Verwalten**. Wählen Sie das Aktionsmenü für die IRE und dann **Bearbeiten**, um die Konfiguration zu ändern.

Löschen einer isolierten Wiederherstellungsumgebung

Eine IRE kann nicht gelöscht werden, während ein Wiederherstellungsvorgang aktiv ist; Sie können den Wiederherstellungsvorgang abbrechen oder warten, bis die Wiederherstellung abgeschlossen ist, dann die IRE löschen.

Wenn Sie die IRE löschen, werden auch die Clean-Room-SVM und das Metadaten-Volume gelöscht. Sobald diese Assets gelöscht wurden, können Sie keine Berichte mehr für die Clean Restore generieren.

1. Gehen Sie zu **Einstellungen**.
2. Wählen Sie in der Karte „Clean restore“ die Option **Verwalten**.
3. Identifizieren Sie den Reinraum, den Sie löschen möchten. Wählen Sie das Aktionsmenü (...) für den IRE und dann **Löschen**.
4. Wählen Sie im Dialogfeld **Löschen**, um den Vorgang zu bestätigen.

Workloads mit sauberer Wiederherstellung in NetApp Ransomware Resilience wiederherstellen

Mit NetApp Ransomware Resilience können Sie nach einem Ransomware-Angriff mit Verschlüsselung eine geführte Wiederherstellung mittels einer sauberen Wiederherstellung durchführen. Die saubere Wiederherstellung identifiziert optimierte Wiederherstellungspfade, um Datenverlust zu minimieren und Ihre Workloads in kürzester Zeit wieder online zu bringen.

Bevor Sie beginnen

Erforderliche Konsolenrolle Um diese Aufgabe auszuführen, benötigen Sie die Rolle „Organisationsadministrator“, „Ordner- oder Projektadministrator“ oder „Ransomware Resilience-Administrator“. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console" .

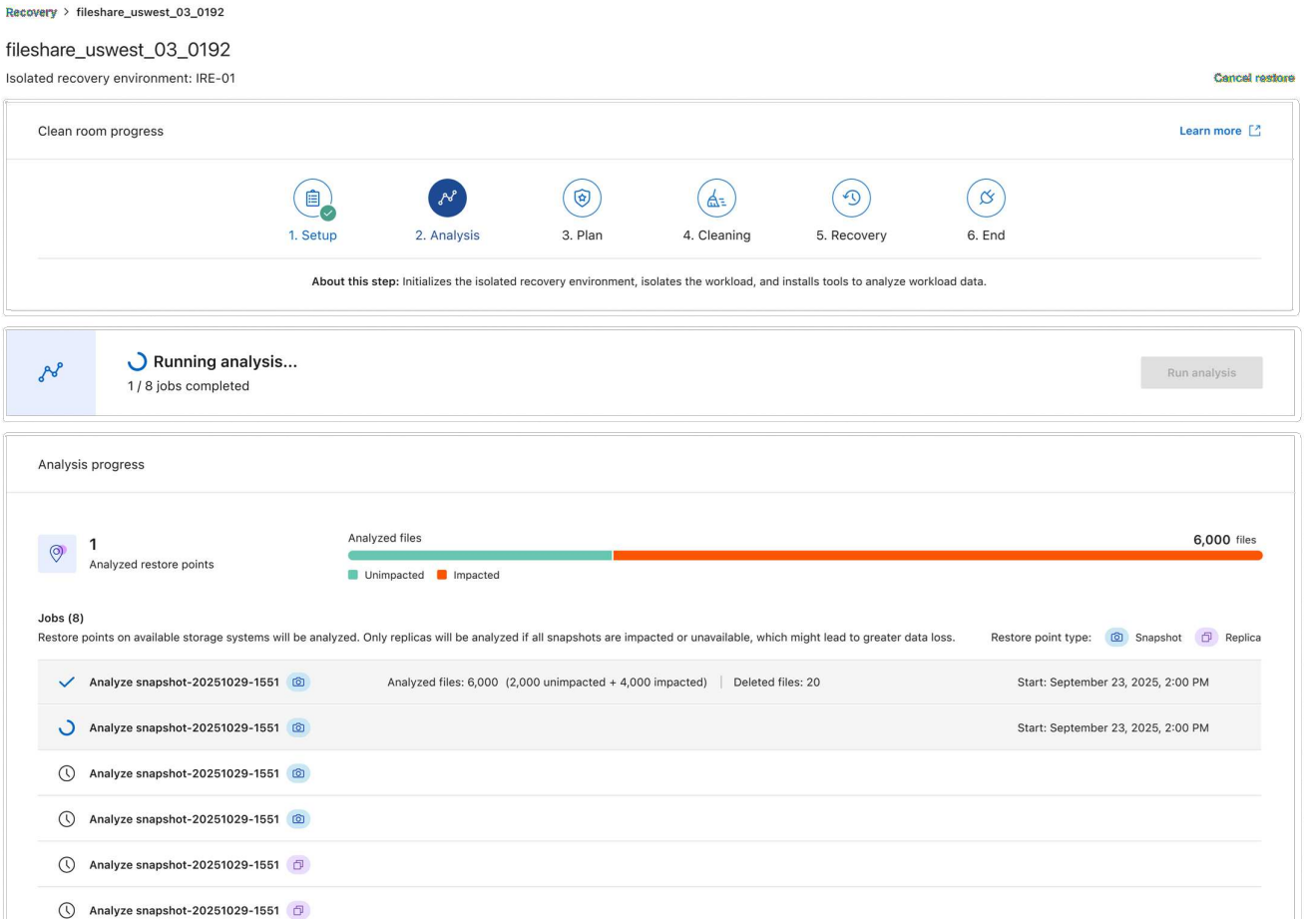
Sie müssen eine "isolierte Wiederherstellungsumgebung" konfiguriert haben, bevor Sie eine vollständige Wiederherstellung durchführen können.

Überlegungen

- Sie können nur eine vollständige Wiederherstellung bei einem auf Verschlüsselung basierenden Ransomware-Angriff durchführen.
- Wenn die isolierte Wiederherstellungsumgebung keine Kapazität für einen neuen Vorgang hat, wird dieser in die Warteschlange gestellt, bis Kapazität verfügbar ist.
  - Im Dashboard „Ransomware Resilience Recovery“ können Sie jederzeit den Status aktiver und in der Warteschlange befindlicher Wiederherstellungsvorgänge überwachen.
- Wenn Sie eine vollständige Wiederherstellung durchführen, wird das ursprüngliche Volume ausgehängt, was den E/A-Zugriff beeinträchtigen kann.

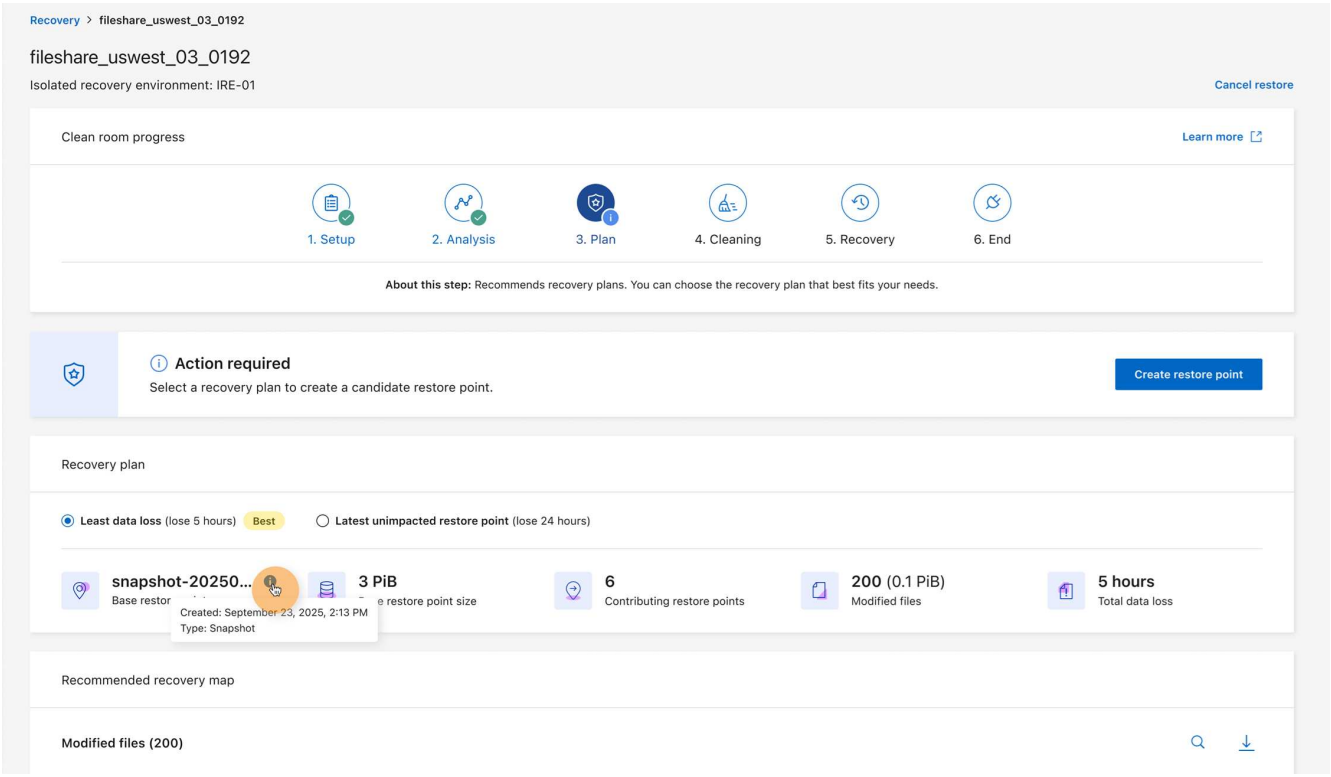
Führen Sie eine saubere Wiederherstellung durch

1. Wählen Sie im Abschnitt **Wiederherstellung** die Workload aus, die Sie wiederherstellen möchten. Wählen Sie **Wiederherstellen**.
2. Wählen Sie unter den Optionen für den Wiederherstellungstyp **Saubere Wiederherstellung** und dann **Weiter** aus.
3. Wählen Sie die gewünschte isolierte Wiederherstellungsumgebung aus und klicken Sie dann auf **Weiter**.
4. Überprüfen Sie die isolierte Wiederherstellungsumgebung und vergewissern Sie sich, dass es sich um den richtigen Speicherort handelt. Wählen Sie **Wiederherstellen**.
5. Ransomware Resilience führt die erforderlichen Einstellungen durch. Nach erfolgreichem Abschluss der Einrichtung zeigt Ransomware Resilience **Setup complete** an. Um mit der Analyse fortzufahren, wählen Sie **Next**.
6. Nach Abschluss der Einrichtung wählen Sie **Analyse ausführen**. Ransomware Resilience analysiert alle verfügbaren Wiederherstellungspunkte in den sieben Tagen vor dem Ransomware-Ereignis und zeigt das Datum und den Typ des Wiederherstellungspunkts an.



7. Nach Abschluss der Analyse wählen Sie **Weiter**, um Ihre Wiederherstellung zu planen. Ransomware Resilience präsentiert zwei Optionen: **Least data loss** und **Latest unimpacted restore point**. Wählen Sie eine der beiden Optionen und sehen Sie sich optional die einzelnen Dateidaten für den jeweiligen Wiederherstellungspunkt an.

   Um detaillierte Dateiereignisdaten anzuzeigen, wählen Sie eine Datei aus, um ihren Verschlüsselungsstatus zu analysieren; wann sie erstellt, geändert oder gelöscht wurde und welcher Wiederherstellungspunkt welcher Aktion entspricht.



8. Nachdem Sie Ihren Wiederherstellungspunkt ausgewählt haben, klicken Sie auf **Weiter**, um mit der Bereinigung Ihrer Dateien zu beginnen.
9. Ransomware Resilience beginnt mit der Bereinigung der Arbeitslast.

   Wenn die Reinigung abgeschlossen ist, wählen Sie **Wiederherstellung starten**, um die Wiederherstellung einzuleiten.

10. Wählen Sie, ob Sie die ursprüngliche Arbeitslast speichern möchten. Um die ursprüngliche Arbeitslast nicht zu speichern, wählen Sie **Nein, ursprüngliche Arbeitslast ersetzen**. Um sie zu speichern, wählen Sie **Ja, ursprüngliche Arbeitslast speichern** und geben Sie anschließend einen neuen Namen für die Arbeitslast ein.
11. Wählen Sie **Wiederherstellung starten**, um die Wiederherstellung einzuleiten.
12. Wenn die Wiederherstellung abgeschlossen ist, wählen Sie **Weiter**, um zur letzten Phase zu gelangen.
13. Wählen Sie **Ressourcen freigeben und beenden**, um die Ressourcen freizugeben und den Reinraum zu schließen. Um zu bestätigen, dass Sie die Ressource freigeben möchten, wählen Sie **Beenden**.