Utilizzare la protezione ransomware BlueXP

BlueXP ransomware protection

NetApp
March 22, 2024

Sommario

Utilizzare la protezione ransomware BlueXP

Utilizzare la protezione ransomware BlueXP

Utilizzando la protezione dal ransomware di BlueXP, puoi visualizzare la salute dei carichi di lavoro e proteggere i carichi di lavoro.

- "Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP".
- "Visualizza protezione e salute del workload dalla Dashboard".
  - Esaminare e agire in base ai consigli sulla protezione dal ransomware.
- "Proteggere i carichi di lavoro":
  - Assegna una policy di protezione dal ransomware ai carichi di lavoro.
  - Aumentare la protezione delle applicazioni per prevenire futuri attacchi ransomware.
  - Creare, modificare o eliminare un criterio di protezione.
- "Rispondi al rilevamento di potenziali attacchi ransomware".
- "Ripristino in seguito a un attacco" (dopo che gli incidenti sono neutralizzati).
- "Configurare le impostazioni di protezione".

Visualizza lo stato dei carichi di lavoro con un'occhiata utilizzando la dashboard

La dashboard per la protezione dal ransomware di BlueXP fornisce informazioni immediate sulla salute della protezione dei workload. Puoi determinare rapidamente i workload a rischio o protetti, identificare i workload che ne sono influenzati da un incidente o nel recovery e misurare il grado di protezione tenendo conto della quantità di storage protetto o a rischio.

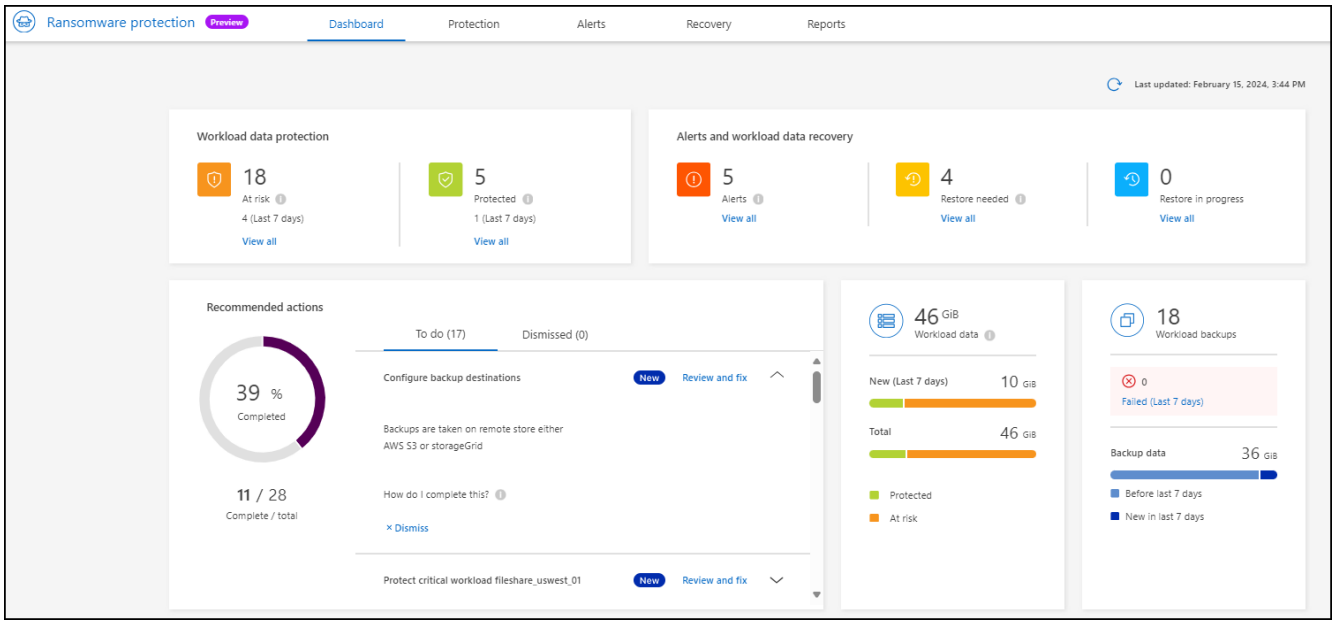
È inoltre possibile utilizzare la dashboard per esaminare e agire in base ai consigli sulla protezione.

Esaminare lo stato dei carichi di lavoro utilizzando la dashboard

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

   Dopo il rilevamento, la Dashboard mostra la salute della data Protection dei carichi di lavoro.



2. Dal dashboard, è possibile visualizzare ed eseguire una delle seguenti operazioni in ciascuno dei riquadri:

   - **Protezione dei dati del carico di lavoro**: Fare clic su **Visualizza tutto** per visualizzare tutti i carichi di lavoro a rischio o protetti nella pagina protezione. I carichi di lavoro sono a rischio quando i livelli di protezione non corrispondono a una policy di protezione. Fare riferimento a. "Proteggere i carichi di lavoro".
   - **Avvisi e recupero dati del carico di lavoro**: Fare clic su **Visualizza tutto** per visualizzare gli incidenti attivi che hanno influito sul carico di lavoro, sono pronti per il ripristino dopo che gli incidenti sono stati neutralizzati o sono in fase di recupero. Fare riferimento a. "Rispondere a un avviso rilevato".

     Un incidente è classificato in uno dei seguenti stati:

     - Interessato (visualizzato nella pagina Avvisi)
     - Pronto per il ripristino (visualizzato nella pagina di ripristino)
     - Ripristino (viene visualizzato nella pagina di ripristino)
     - Ripristino non riuscito (visualizzato nella pagina di ripristino)
     - Recuperato (visualizzato nella pagina di ripristino)
   - **Azioni consigliate**: Per aumentare la protezione, rivedere ogni raccomandazione e fare clic su **Rivedi e correggi**.

     Fare riferimento a. "Rivedere i consigli sulla protezione sulla dashboard" oppure "Proteggere i carichi di lavoro".

     Tutti i suggerimenti aggiunti dall'ultima volta che si è visitato il Dashboard sono indicati con "nuovo" per almeno 24 ore. Le azioni sono elencate in ordine di priorità, con le più importanti in alto. È possibile rivedere e agire su ciascuno di essi o eliminarlo.

   Il numero totale di azioni non include le azioni respinte.

   - **Dati del carico di lavoro**: Monitoraggio delle modifiche apportate alla copertura di protezione negli ultimi 7 giorni.
   - **Backup del carico di lavoro**: Monitoraggio delle modifiche apportate ai backup dei carichi di lavoro creati dal servizio che non sono riusciti o sono stati completati correttamente negli ultimi 7 giorni.

Rivedere i consigli sulla protezione sulla dashboard

La protezione dal ransomware di BlueXP valuta la protezione sui carichi di lavoro e raccomanda azioni per migliorare tale protezione.

È possibile rivedere un suggerimento e agire su di esso, che cambia lo stato del suggerimento in completo. Oppure, se si desidera agire in seguito, è possibile eliminarlo. L'annullamento di un'azione sposta il suggerimento in un elenco di azioni respinte, che è possibile rivedere in un secondo momento.

Ecco un esempio delle raccomandazioni che il servizio offre.

Consiglio	Descrizione	Come risolvere il problema
Aggiungi una policy di protezione dal ransomware	Il carico di lavoro non è attualmente protetto.	Assegnare una policy al carico di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Configurare le destinazioni di backup	Il workload non dispone al momento di destinazioni di backup.	Aggiungete destinazioni di backup a questo workload per proteggerlo. Fare riferimento a. "Configurare le impostazioni di protezione".
Rafforzare una politica.	Alcuni carichi di lavoro potrebbero non disporre di una protezione sufficiente. Rafforza la protezione sui carichi di lavoro con una policy.	Aumenta la conservazione, Aggiungi i backup, applica i backup immutabili, blocca le estensioni di file sospette, abilita il rilevamento sullo storage secondario e molto altro ancora. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Proteggi i workload dell'applicazione critici o importanti da ransomware.	La pagina protezione visualizza i carichi di lavoro dell'applicazione critici o importanti (in base al livello di priorità assegnato) che non sono protetti.	Assegnare una policy a questi carichi di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Proteggi i carichi di lavoro critici o importanti di condivisione file dal ransomware.	La pagina protezione visualizza i carichi di lavoro critici o importanti del tipo file Share o Datastore non protetti.	Assegnazione di una policy a ciascun carico di lavoro. Fare riferimento a. "Proteggi i carichi di lavoro dagli attacchi ransomware".
Rivedere i nuovi avvisi	Esistono nuovi avvisi.	Rivedere i nuovi avvisi. Fare riferimento a. "Rispondi a un avviso ransomware rilevato".

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Dal riquadro azioni consigliate, selezionare un suggerimento e selezionare **Rivedi e correggi**.
3. Per chiudere l'azione in un secondo momento, selezionare **Chiudi**.

Il suggerimento scompare dall'elenco delle attività e viene visualizzato nell'elenco delle attività respinte.

È possibile modificare in un secondo momento un elemento da liquidare in un elemento da fare. Quando si contrassegna un elemento completato o si modifica un elemento respinto in un'azione attività, le azioni totale aumentano di 1.

4. Per rivedere le informazioni su come agire in base alle raccomandazioni, selezionare l'icona **informazioni**.

Proteggi i carichi di lavoro dagli attacchi ransomware

Puoi proteggere i workload dagli attacchi ransomware eseguendo le seguenti azioni utilizzando la protezione dal ransomware di BlueXP.

- Visualizza la protezione dei carichi di lavoro esistenti.
- Assegnazione di una policy a un carico di lavoro.
  - Aumentare la protezione delle applicazioni per evitare futuri attacchi RW.
  - Modificare la protezione per un carico di lavoro precedentemente protetto nel servizio RW.
- Gestire i criteri (solo quelli creati).

La protezione dal ransomware di BlueXP assegna una priorità a ogni workload durante il rilevamento. La priorità del carico di lavoro è determinata dalle seguenti frequenze di istantanea:

- **Critico**: Copie snapshot acquisite meno di 1 TB all'ora (pianificazione di protezione altamente aggressiva)
- **Importante**: Le copie snapshot sono state acquisite meno di 1 al giorno e più di 1 all'ora
- **Standard**: Le copie snapshot sono state acquisite più di 1 copie al giorno

Stato di protezione: Un carico di lavoro può mostrare uno dei seguenti stati di protezione per indicare se un criterio è applicato o meno:

- **Protetto**: Viene applicato un criterio.
- **A rischio**: Non viene applicata alcuna politica.
- **In corso**: È in corso l'applicazione di un criterio, ma non è ancora stato completato.
- **Non riuscito**: Un criterio è applicato ma non funziona.

Stato di protezione: Un carico di lavoro può avere uno dei seguenti stati di integrità di protezione:

- **Integro**: La protezione del carico di lavoro è abilitata e i backup e le copie Snapshot sono stati completati.
- **In corso**: Sono in corso backup o copie Snapshot.
- **Non riuscito**: I backup o le copie Snapshot non sono stati completati correttamente.
- **N/A**: La protezione non è abilitata o sufficiente sul carico di lavoro.

Visualizza la protezione ransomware del carico di lavoro

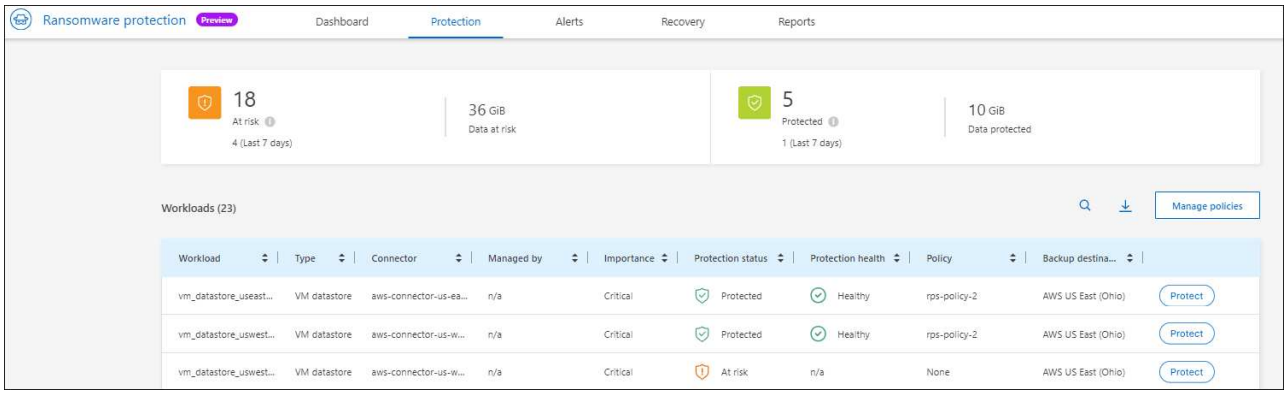
Uno dei primi passi nella protezione dei carichi di lavoro è la visualizzazione dei carichi di lavoro attuali e del loro stato di protezione. Sono visualizzabili i seguenti tipi di carichi di lavoro:

- Workload VM

- Workload di condivisione di file

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Effettuare una delle seguenti operazioni:
   - Nel riquadro protezione dati dashboard, selezionare **Visualizza tutto**.
   - Dal menu, selezionare **protezione**.



3. Da questa pagina è possibile assegnare un criterio a un carico di lavoro.

Assegnazione di una policy di protezione predefinita ai carichi di lavoro

Per proteggere i tuoi dati, puoi assegnare una policy di protezione dal ransomware esistente a uno o più carichi di lavoro. È inoltre possibile assegnare un criterio diverso a un carico di lavoro che dispone già di un criterio.

La protezione dal ransomware di BlueXP include le seguenti policy predefinite allineate con la priorità dei workload:

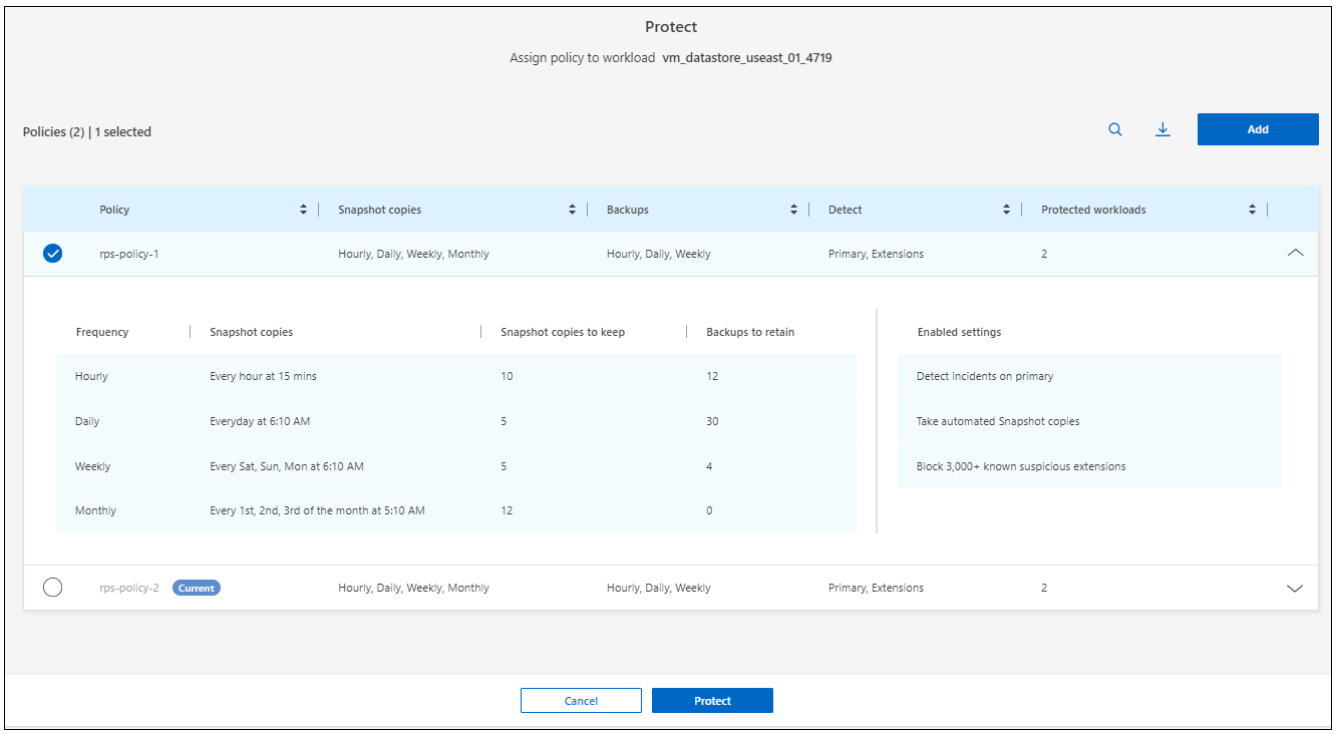
Livello dei criteri	Snapshot	Frequenza	Conservazione (giorni)	N. di copie Snapshot	Numero massimo totale di copie Snapshot
Politica critica dei carichi di lavoro	Quarto ogni ora	Ogni 15 minuti	3	288	309
	Ogni giorno	Ogni 1 giorni	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni	60	2	309

Livello dei criteri	Snapshot	Frequenza	Conservazione (giorni)	N. di copie Snapshot	Numero massimo totale di copie Snapshot
Policy importante sui carichi di lavoro	Quarto ogni ora	Ogni 30 minuti	3	144	165
	Ogni giorno	Ogni 1 giorni	14	14	165
	Settimanale	Ogni 1 settimana	35	5	165
	Mensile	Ogni 30 giorni	60	2	165
Norma sui carichi di lavoro standard	Quarto ogni ora	Ogni 60 minuti	3	72	93
	Ogni giorno	Ogni 1 giorni	14	14	93
	Settimanale	Ogni 1 settimana	35	5	93
	Mensile	Ogni 30 giorni	60	2	93

Fasi

1. Dalla protezione dal ransomware di BlueXP, esegui una delle seguenti operazioni:
   - Nel riquadro protezione dati dashboard, selezionare **Visualizza tutto**.
   - Nel riquadro Dashboard Recommendation (Consiglio dashboard), selezionare un suggerimento sull'assegnazione di un criterio e selezionare **Review and fix** (Rivedi e correggi*).
   - Dal menu, selezionare **protezione**.
2. Nella pagina protezione, esaminare i carichi di lavoro e selezionare **Proteggi** accanto al carico di lavoro.

   Viene visualizzato un elenco di criteri.



3. Per visualizzare i dettagli, fare clic sulla freccia rivolta verso il basso di un criterio.
4. Selezionare un criterio da assegnare al carico di lavoro.
5. Selezionare **Proteggi**.
6. Esaminare il riquadro azioni consigliate del dashboard, che mostra l'azione come "completata".

Creare un criterio di protezione

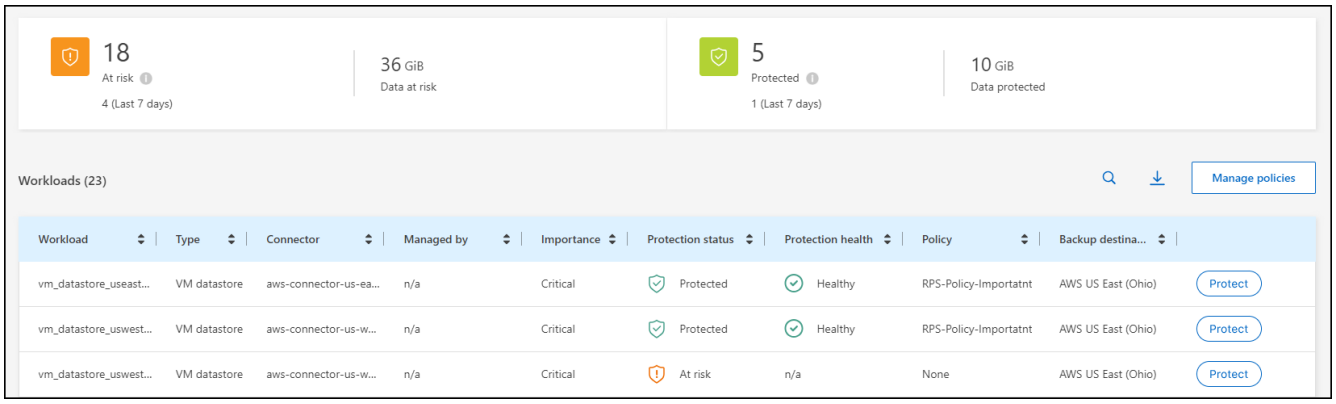
Se i criteri esistenti non soddisfano le esigenze aziendali, è possibile creare un nuovo criterio di protezione. È possibile creare da zero i propri criteri oppure utilizzarne uno esistente e modificarne le impostazioni.

È possibile creare policy che governano lo storage primario e secondario e trattano allo stesso tempo lo storage primario e secondario o in modo diverso.

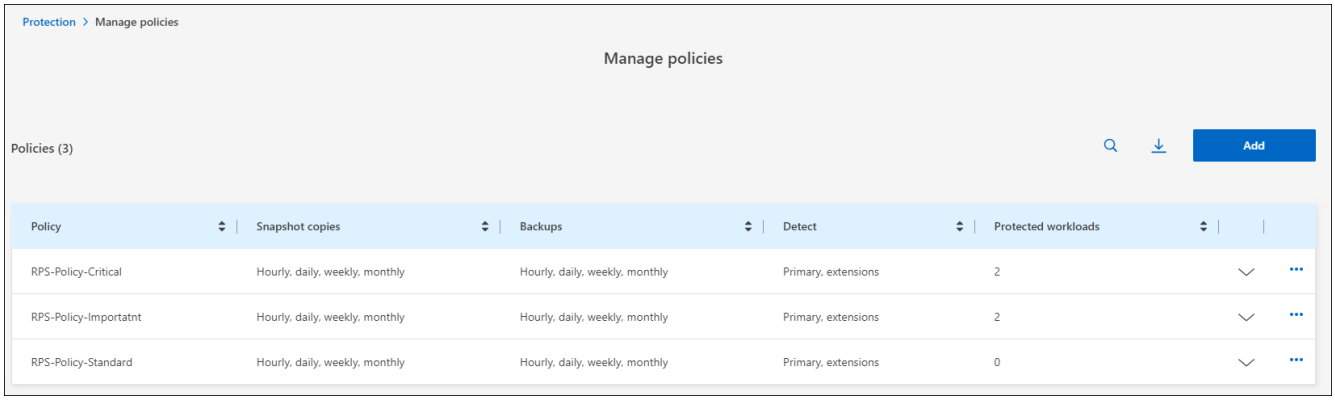
È possibile creare un criterio durante la loro gestione o durante il processo di assegnazione di un criterio a un carico di lavoro.

Procedura per la creazione di un criterio durante la gestione dei criteri

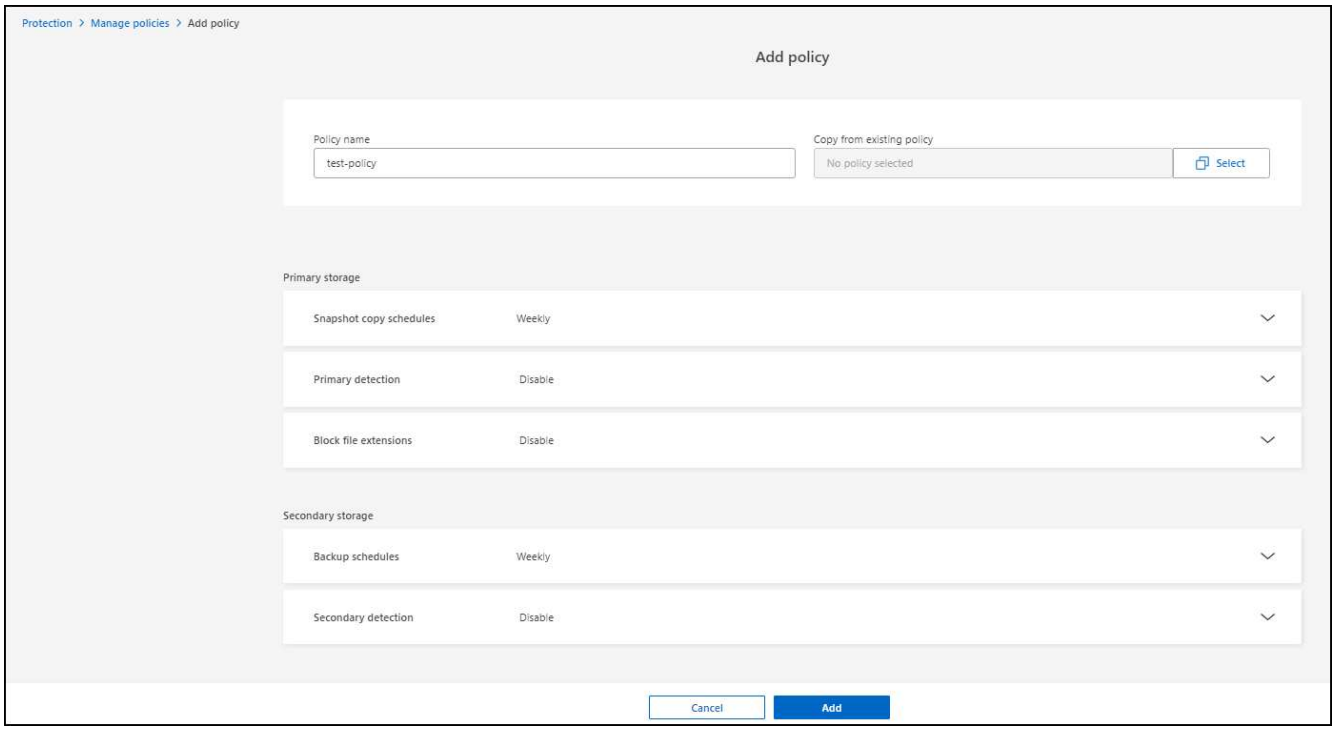
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



2. Nella pagina protezione, selezionare **Gestisci criteri**.



3. Nella pagina Gestisci criteri, selezionare **Aggiungi**.



4. Immettere il nome di un nuovo criterio o un nome di criterio esistente per copiarlo. Se si immette un nome di criterio esistente, scegliere il criterio da copiare.

> Se si sceglie di copiare e modificare un criterio esistente, è necessario modificare almeno un'impostazione per renderla univoca.

5. Per ciascun elemento, selezionare la freccia verso il basso.
   - **Archiviazione primaria**:
     - **Pianificazioni copie snapshot**: Scegliere le opzioni di pianificazione, il numero di copie snapshot da conservare e selezionare per attivare la pianificazione.
     - **Rilevamento primario**: Abilita il servizio per rilevare gli incidenti ransomware sullo storage primario.
     - **Blocca estensioni file**: Abilitare questa opzione affinché il blocco di servizio conosca le estensioni file sospette. Il servizio esegue copie Snapshot automatizzate quando è abilitato il rilevamento

primario.

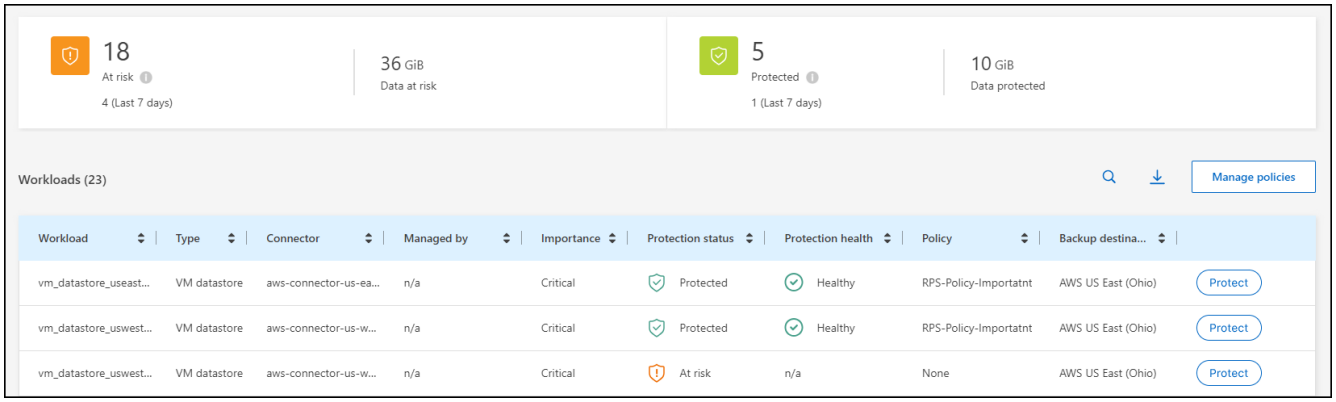
- **Archiviazione secondaria**:
  - **Pianificazioni di backup**: Scegliere le opzioni di pianificazione per l'archiviazione secondaria e attivare la pianificazione.
  - **Rilevamento secondario**: Abilita il servizio per rilevare gli incidenti ransomware sullo storage secondario.
  - **Blocca backup**: Scegliere questa opzione per evitare che i backup sullo storage secondario vengano modificati o eliminati per un determinato periodo di tempo. Questo viene anche chiamato *storage immutabile*.

    Questa opzione utilizza la tecnologia DataLock di NetApp, che blocca i backup sullo storage secondario. Il periodo di tempo in cui il file di backup viene bloccato (e conservato) viene definito periodo di conservazione DataLock. E si basa sulla pianificazione dei criteri di backup e sull'impostazione di conservazione definita, oltre a un buffer di 14 giorni. Qualsiasi policy di conservazione DataLock inferiore a 30 giorni viene arrotondata al minimo di 30 giorni.

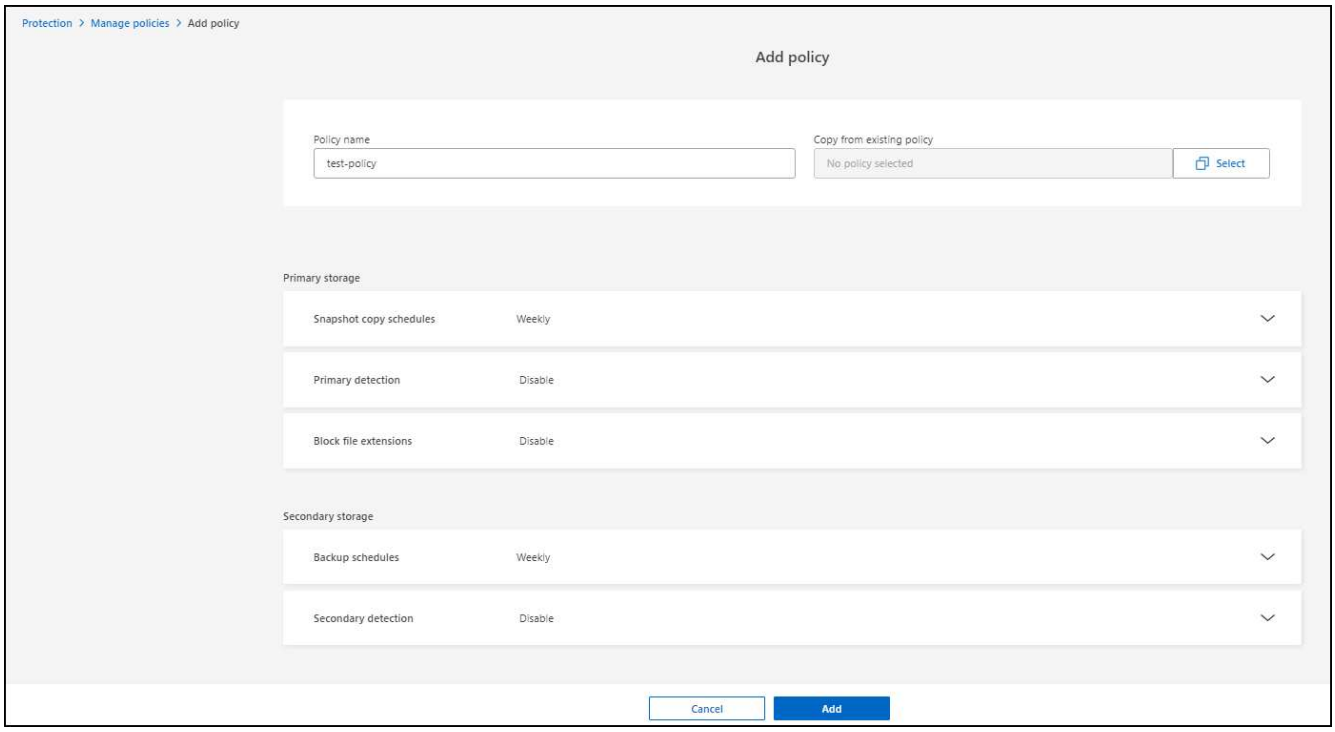
6. Selezionare **Aggiungi**.

Procedura per creare un criterio durante l'assegnazione dei criteri di protezione

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



2. Nella pagina protezione, selezionare **protezione**.
3. Dalla pagina di protezione, selezionare **Aggiungi**.



4. Completare il processo, che equivale alla creazione di un criterio dalla pagina Gestisci criteri.

Assegnare un criterio di protezione diverso

È possibile scegliere una policy di protezione diversa per un carico di lavoro.
Potresti voler aumentare la protezione per prevenire futuri attacchi ransomware modificando la policy di protezione.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Dalla pagina di protezione, selezionare un carico di lavoro e selezionare **Proteggi**.
3. Nella pagina protezione, selezionare un criterio diverso per il carico di lavoro.
4. Per modificare i dettagli del criterio, selezionare la freccia verso il basso a destra e modificare i dettagli.
5. Selezionare **Salva** per terminare la modifica.

Modificare un criterio esistente

È possibile modificare i dettagli di un criterio solo quando il criterio non è associato a un carico di lavoro.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare **Gestisci criteri**.
3. Nella pagina Gestisci criteri, selezionare l'opzione **azioni** per il criterio che si desidera modificare.
4. Dal menu azioni, selezionare **Modifica criterio**.
5. Modificare i dettagli.
6. Selezionare **Salva** per terminare la modifica.

Eliminazione di un criterio

È possibile eliminare una policy di protezione non attualmente associata a alcun carico di lavoro.

Fasi

1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.
2. Nella pagina protezione, selezionare **Gestisci criteri**.
3. Nella pagina Gestisci criteri, selezionare l'opzione **azioni** per il criterio che si desidera eliminare.
4. Dal menu azioni, selezionare **Elimina criterio**.

Rispondi a un avviso ransomware rilevato

Se la protezione ransomware di BlueXP rileva un possibile attacco, viene visualizzato un avviso nella dashboard di protezione dal ransomware di BlueXP e nelle notifiche di BlueXP, in alto a destra, che indica un potenziale attacco ransomware. Inoltre, il servizio avvia immediatamente l'acquisizione di una copia Snapshot. A questo punto, dovresti valutare il rischio potenziale nella scheda **Avvisi** della protezione dal ransomware di BlueXP.

Per iniziare il ripristino dei dati, contrassegnare l'avviso come pronto per il ripristino in modo che l'amministratore dello storage possa avviare il processo di ripristino.

Ogni avviso potrebbe avere più incidenti su volumi diversi con stati diversi, quindi assicurati di esaminare tutti gli incidenti.

Il servizio fornisce informazioni denominate *prove* su ciò che ha causato l'emissione dell'avviso, come le seguenti:

- Le estensioni dei file sono state create o modificate
- Si è verificata la creazione del file ed è stato aumentato di una percentuale elencata
- Si è verificata l'eliminazione dei file e l'aumento è stato calcolato in percentuale

Un avviso si basa sui seguenti tipi di comportamento:

- **Potenziale attacco**: Si verifica un avviso quando la protezione autonoma dal ransomware rileva una nuova estensione e l'evento viene ripetuto più di 20 volte nelle ultime 24 ore (comportamento predefinito).
- **Avvertenza**: Si verifica un avviso basato sui seguenti comportamenti:
  - Il rilevamento di una nuova estensione non è stato identificato in precedenza e lo stesso comportamento non si ripete abbastanza volte per dichiararla come attacco.
  - Si osserva un'elevata entropia.
  - Le operazioni di lettura/scrittura/ridenominazione/eliminazione dei file hanno subito un aumento dell'attività del 100% oltre la baseline.

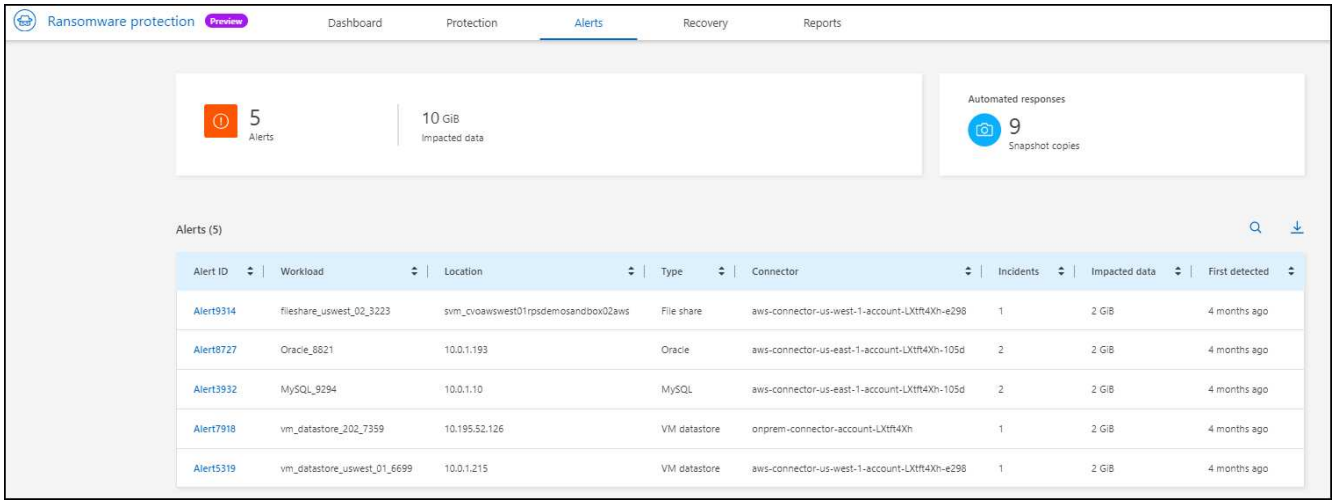
Le prove si basano sulle informazioni fornite dalla protezione autonoma dal ransomware in ONTAP. Per ulteriori informazioni, fare riferimento a. "Panoramica della protezione ransomware autonoma".

Visualizza avvisi

Puoi accedere agli avvisi dalla dashboard della protezione dal ransomware di BlueXP o dalla scheda **Alerts**.

Fasi

1. Nella dashboard di protezione dal ransomware di BlueXP, consulta il pannello Alerts.
2. Selezionare **Visualizza tutto** sotto una delle statue.
3. Fare clic su un avviso per esaminare tutti gli incidenti su ciascun volume per ciascun avviso.
4. Per rivedere gli avvisi aggiuntivi, fare clic su **Alert** nella barra di navigazione in alto a sinistra.
5. Esaminare gli avvisi nella pagina Avvisi.



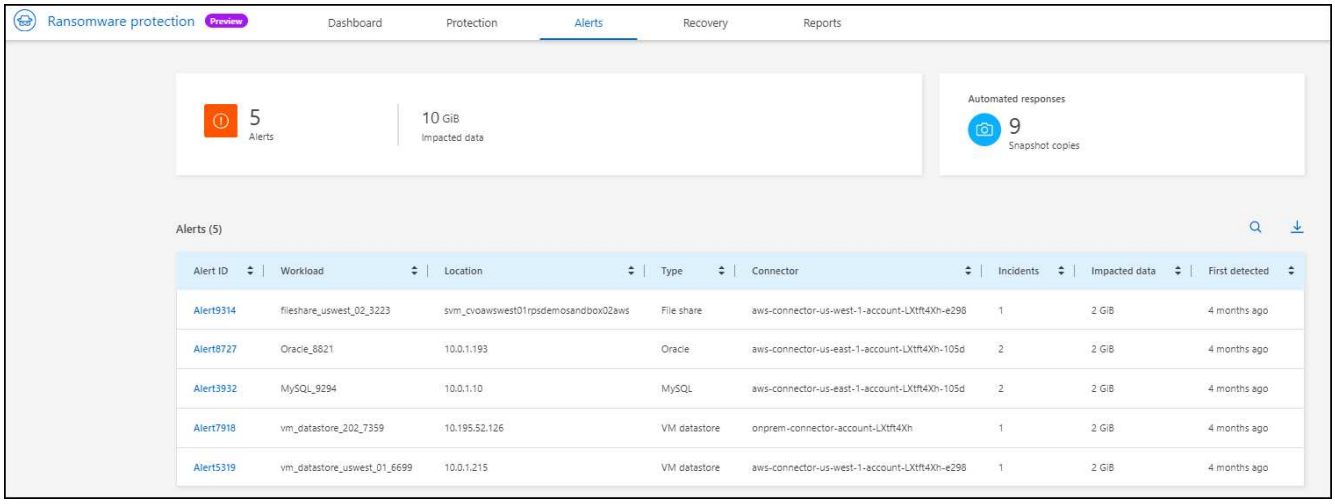
6. Continuare con Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti).

Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti)

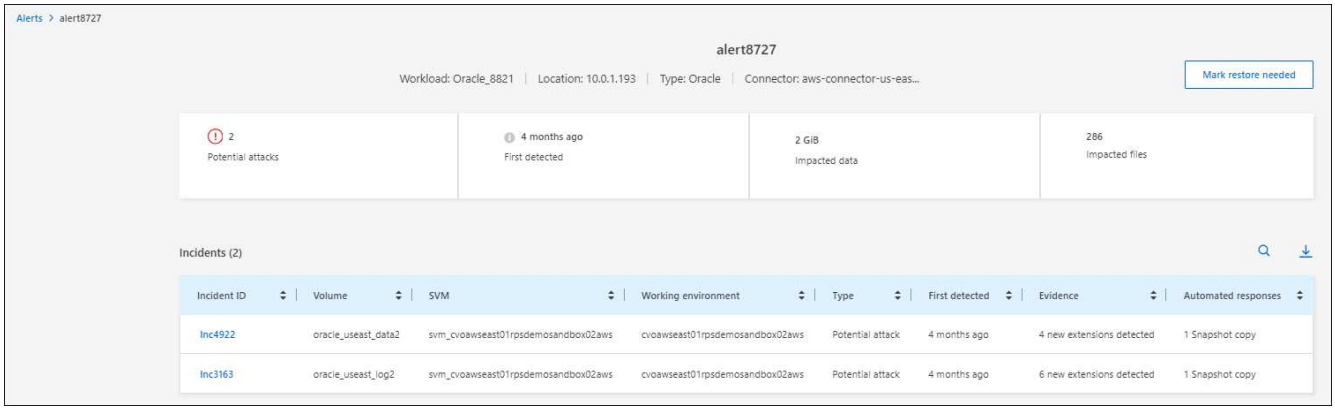
Una volta mitigato l'attacco e sei pronto a ripristinare i carichi di lavoro, dovresti comunicare con il tuo team di amministrazione dello storage che i dati sono pronti per il recovery, in modo che possano avviare il processo di recovery.

Fasi

1. Dal menu di protezione dal ransomware BlueXP, seleziona **Avvisi**.



2. Nella pagina Avvisi, selezionare l'avviso.
3. Esaminare gli incidenti nell'avviso.



4. Se si stabilisce che gli incidenti sono pronti per il ripristino, selezionare **Segna ripristino necessario**.
5. Confermare l'azione e selezionare **Segna ripristino necessario**.
6. Per avviare il ripristino del carico di lavoro, selezionare **Recupera** carico di lavoro nel messaggio o selezionare la scheda **Recovery**.

Risultato

Dopo aver contrassegnato l'avviso per il ripristino, l'avviso passa dalla scheda Avvisi alla scheda Ripristino.

Ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti)

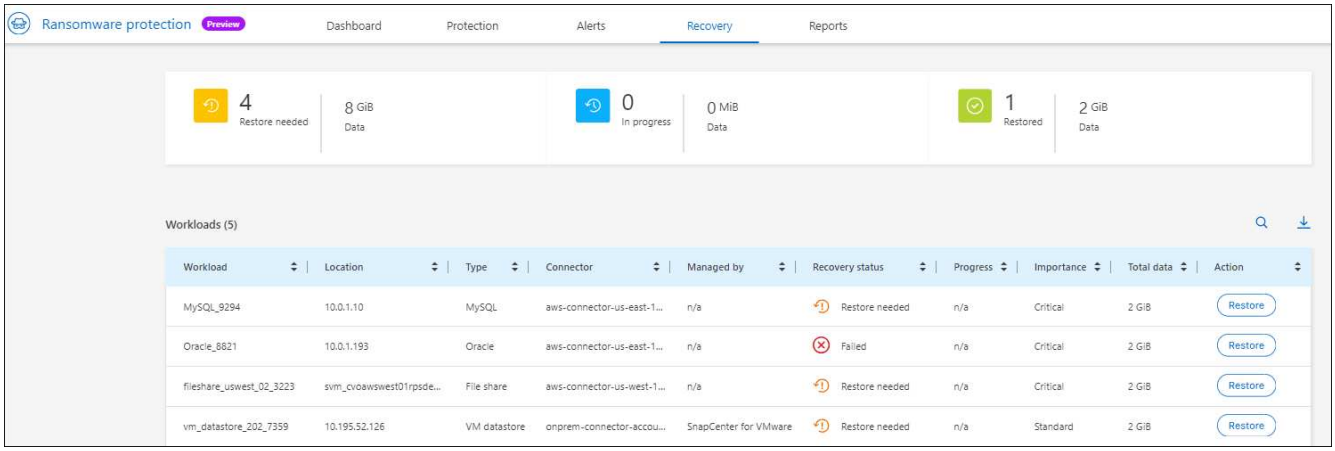
Dopo che i carichi di lavoro sono stati contrassegnati come "pronti per il recovery", la protezione dal ransomware di BlueXP consiglia un recovery point effettivo (RPA) e orchestra il workflow per un recovery resistente ai crash.

Visualizza i carichi di lavoro pronti per il ripristino

Esaminare i carichi di lavoro che si trovano nello stato di ripristino "necessario ripristino".

Fasi

1. Effettuare una delle seguenti operazioni:
   - Dal dashboard, esaminare i totali "Ripristina necessario" nel riquadro Avvisi e selezionare **Visualizza tutto**.
   - Dal menu, selezionare **Ripristino**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.



Ripristinare un carico di lavoro

Utilizzando la protezione dal ransomware di BlueXP, l'amministratore dello storage può determinare il modo migliore per ripristinare i workload dal punto di ripristino consigliato o dal punto di ripristino preferito.

L'amministratore dello storage di sicurezza può ripristinare i dati a diversi livelli:

- Recovery di tutti i volumi
- Ripristinare un'applicazione a livello di volume o di file e cartella.
- Ripristinare una condivisione file a livello di volume, directory o file/cartella.
- Eseguire il ripristino da un datastore a livello di macchina virtuale.

Il processo varia leggermente a seconda del tipo di carico di lavoro.

Fasi

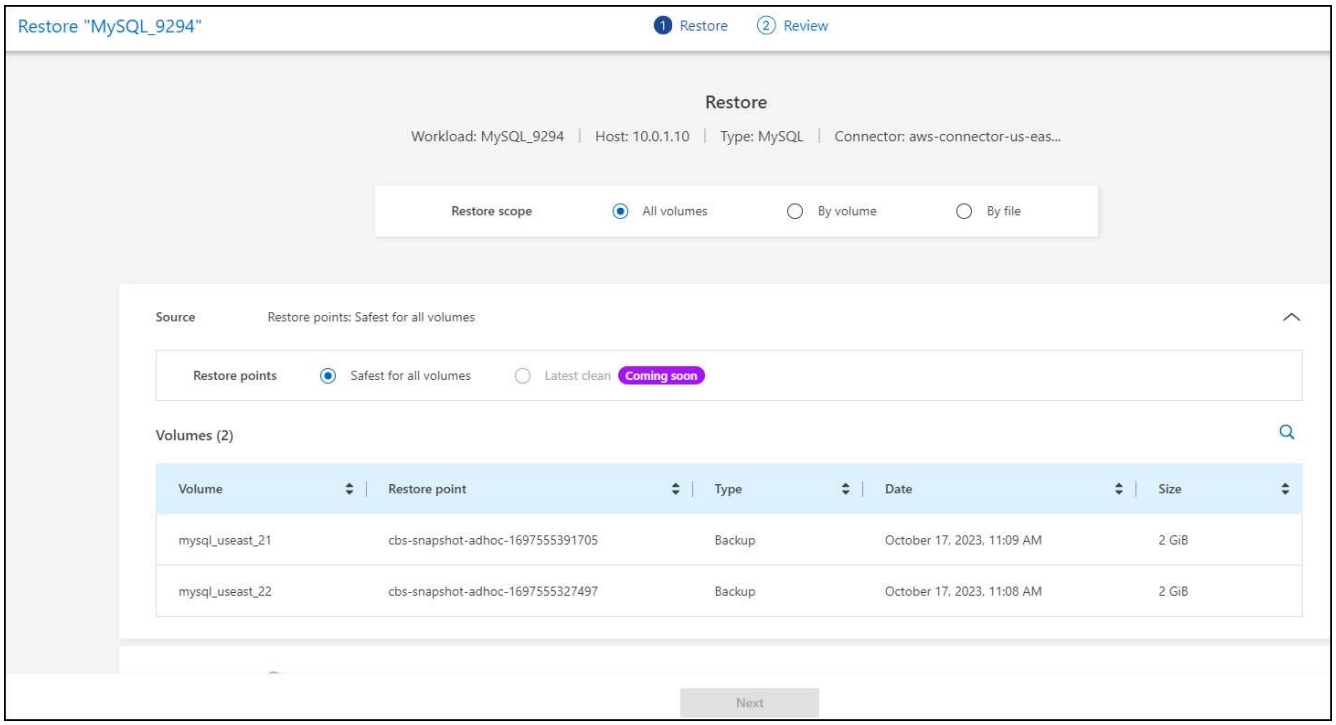
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.
3. Seleziona un carico di lavoro in stato "Ripristino necessario".
4. Per ripristinare, selezionare **Ripristina**.
5. **Ripristina ambito**: Selezionare il tipo di ripristino che si desidera completare:
   - Tutti i volumi
   - Per volume
   - Per file: È possibile specificare una cartella o singoli file da ripristinare.

     È possibile selezionare fino a 100 file o una singola cartella.
6. Continuare con una delle seguenti procedure a seconda che sia stata scelta l'applicazione, il volume o il

file.

Ripristinare tutti i volumi

1. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **tutti i volumi**.



2. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione di "più sicuro per tutti i volumi". Ciò significa che tutti i volumi verranno ripristinati in una copia prima del primo attacco sul primo volume rilevato.

3. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Selezionare l'ambiente di lavoro.
   b. Selezionare la VM di storage.
   c. Selezionare l'aggregato.
   d. Modificare il prefisso del volume che verrà anteposto a tutti i nuovi volumi.

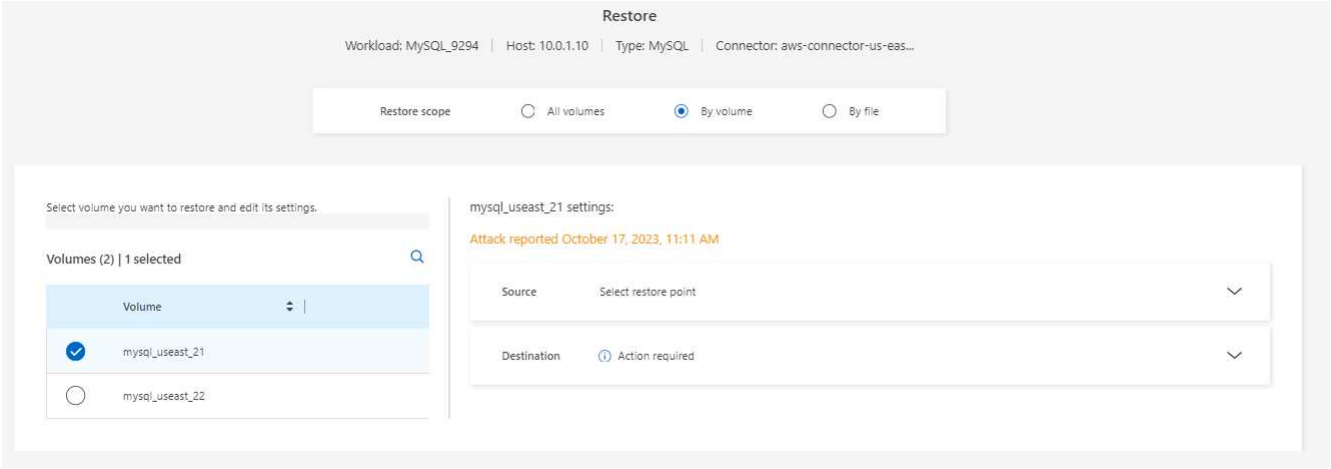
> Il nome del nuovo volume viene visualizzato come prefisso + nome del volume originale + nome del backup + data di backup.

4. Selezionare **Salva**.
5. Selezionare **Avanti**.
6. Rivedere le selezioni.
7. Selezionare **Restore** (Ripristina).

8. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristinare un workload dell'applicazione a livello di volume

1. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **per volume**.



2. Nell'elenco dei volumi, selezionare il volume che si desidera ripristinare.
3. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione "consigliata".

4. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Selezionare l'ambiente di lavoro.
   b. Selezionare la VM di storage.
   c. Selezionare l'aggregato.
   d. Rivedere il nuovo nome del volume.

> Il nome del nuovo volume viene visualizzato come nome originale del volume + nome del backup + data di backup.

5. Selezionare **Salva**.
6. Selezionare **Avanti**.
7. Rivedere le selezioni.
8. Selezionare **Restore** (Ripristina).
9. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristinare un workload dell'applicazione a livello di file

1. Nella pagina Ripristina, nell'ambito Ripristina, selezionare **per file**.

2. Nell'elenco dei volumi, selezionare il volume che si desidera ripristinare.
3. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

      La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione "consigliata".

   b. Selezionare fino a 100 file o una singola cartella da ripristinare.
4. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Scegliere dove ripristinare i dati: Percorso di origine originale o percorso alternativo che è possibile specificare.

      Mentre i file o la directory originali verranno sovrascritti dai dati ripristinati, i nomi dei file e delle cartelle originali rimarranno gli stessi a meno che non si specifichino nuovi nomi.

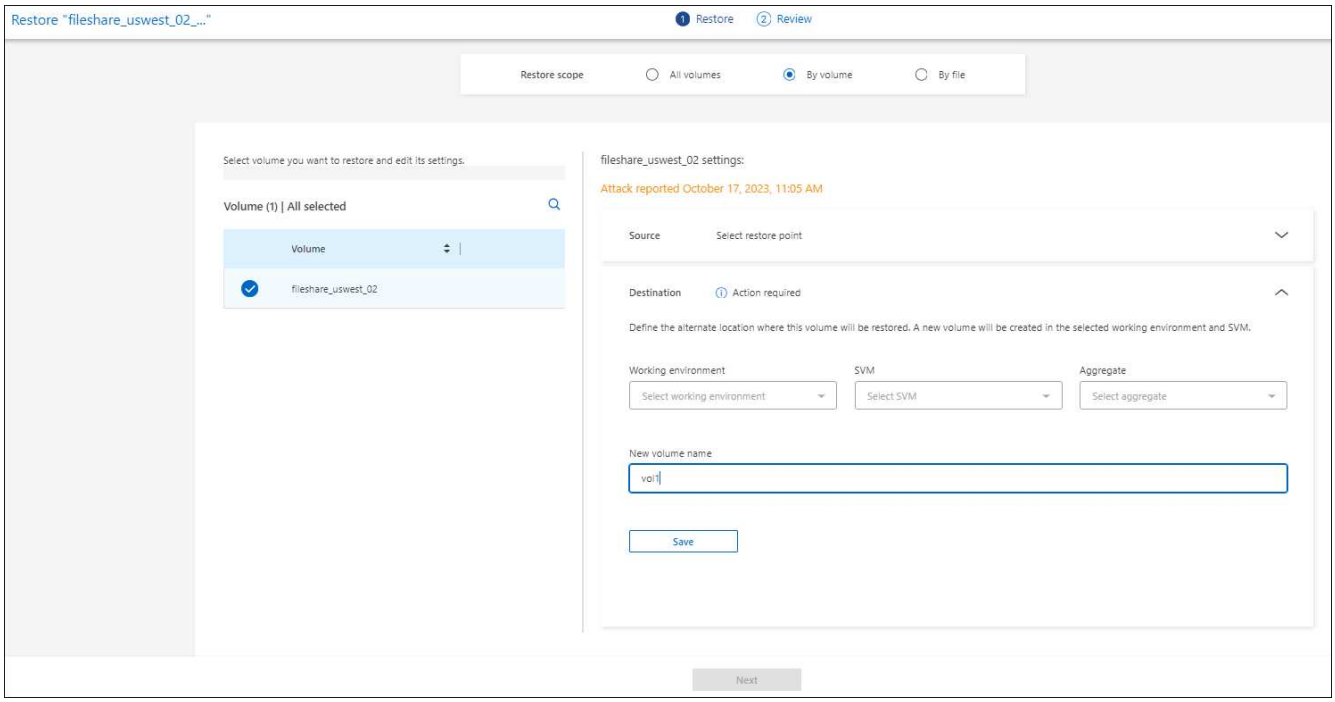
   b. Selezionare l'ambiente di lavoro.
   c. Selezionare la VM di storage.
   d. Facoltativamente, immettere il percorso.

      Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

   e. Selezionare se si desidera che i nomi dei file o della directory ripristinati siano gli stessi nomi della posizione corrente o nomi diversi.
5. Selezionare **Salva**.
6. Selezionare **Avanti**.
7. Rivedere le selezioni.
8. Selezionare **Restore** (Ripristina).
9. Dal menu superiore, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati.

Ripristino di una condivisione di file o di un datastore a livello di volume o file

1. Dopo aver selezionato una condivisione di file o un archivio dati da ripristinare, nella pagina Ripristina, nell'ambito Ripristina, selezionare **per volume** o **per file**.



2. Nell'elenco dei volumi, selezionare il volume che si desidera ripristinare.
3. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.
   a. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.

> La protezione ransomware di BlueXP identifica il punto di ripristino migliore come l'ultimo backup poco prima dell'incidente e mostra un'indicazione "consigliata".

4. **Destinazione**: Selezionare la freccia verso il basso accanto a destinazione per visualizzare i dettagli.
   a. Scegliere dove ripristinare i dati: Percorso di origine originale o percorso alternativo che è possibile specificare.

> Mentre i file o la directory originali verranno sovrascritti dai dati ripristinati, i nomi dei file e delle cartelle originali rimarranno gli stessi a meno che non si specifichino nuovi nomi.

   b. Selezionare l'ambiente di lavoro.
   c. Selezionare la VM di storage.
   d. Facoltativamente, immettere il percorso.

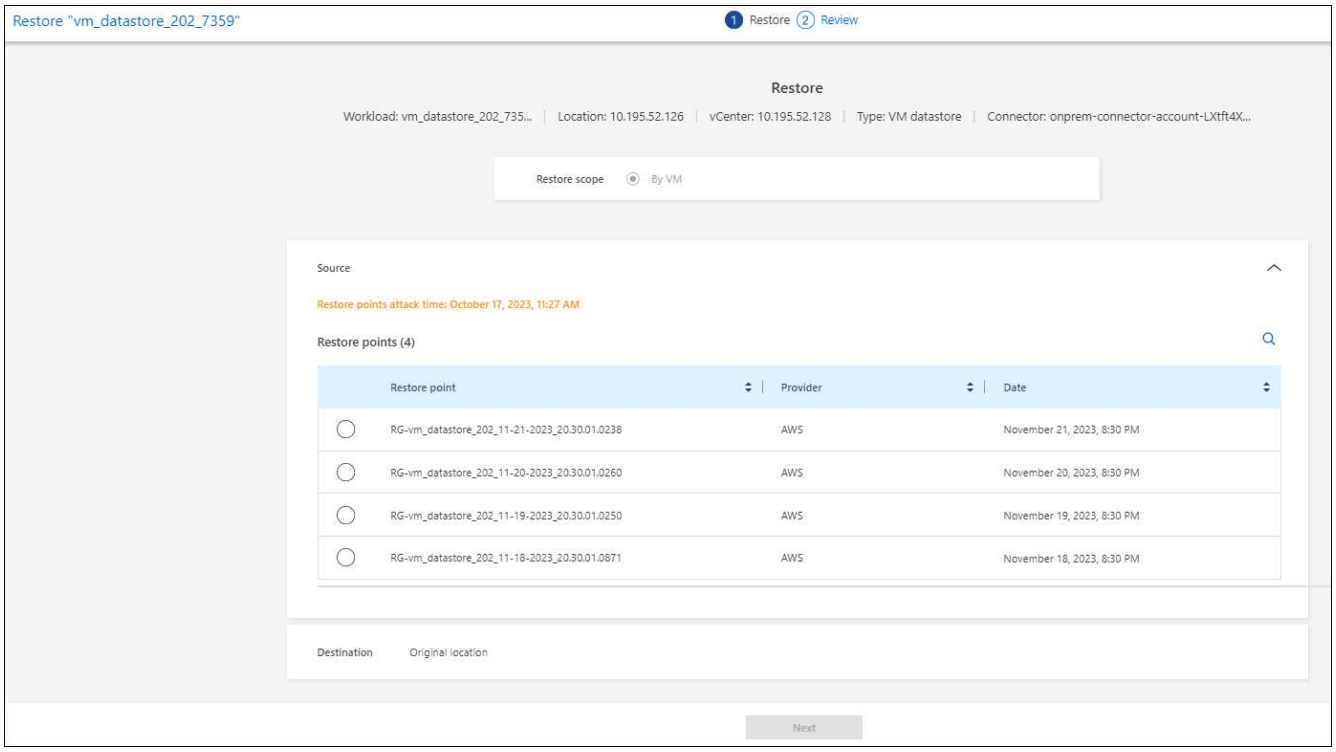
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

5. Selezionare **Salva**.
6. Rivedere le selezioni.
7. Selezionare **Restore** (Ripristina).
8. Dal menu, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione passa attraverso gli stati.

Ripristinare una condivisione di file VM a livello di VM

Nella pagina Recovery (Ripristino), dopo aver selezionato una macchina virtuale da ripristinare, continuare con la procedura descritta di seguito.

1. **Sorgente**: Selezionare la freccia verso il basso accanto a sorgente per visualizzare i dettagli.



2. Selezionare il punto di ripristino che si desidera utilizzare per ripristinare i dati.
3. **Destinazione**: Alla posizione originale.
4. Selezionare **Avanti**.
5. Rivedere le selezioni.
6. Selezionare **Restore** (Ripristina).
7. Dal menu, selezionare **Recovery** (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione passa attraverso gli stati.

Informazioni sul copyright

Informazioni sul marchio commerciale