Documentazione sulla protezione ransomware BlueXP

BlueXP ransomware protection

NetApp
March 22, 2024

Sommario

Documentazione sulla protezione ransomware BlueXP

Note della release: Novità dell'anteprima della protezione dal ransomware BlueXP

Scopri le novità dell'anteprima della protezione dal ransomware BlueXP.

5 marzo 2024

Questa release di anteprima della protezione dal ransomware di BlueXP include i seguenti aggiornamenti:

- **Gestione dei criteri di protezione**: Oltre a utilizzare i criteri predefiniti, è ora possibile creare, modificare ed eliminare i criteri. "Ulteriori informazioni sulla gestione dei criteri".
- **Immutabilità nello storage secondario (DataLock)**: È ora possibile rendere immutabile il backup nello storage secondario utilizzando la tecnologia NetApp DataLock nell'archivio oggetti. "Ulteriori informazioni sulla creazione di criteri di protezione".
- **Backup automatico su NetApp StorageGRID**: Oltre a utilizzare AWS, è ora possibile scegliere StorageGRID come destinazione di backup. "Ulteriori informazioni sulla configurazione delle destinazioni di backup".
- **Caratteristiche aggiuntive per esaminare i potenziali attacchi**: Ora puoi visualizzare ulteriori dettagli forensi per analizzare il potenziale attacco rilevato. "Scopri di più sulla risposta a un avviso ransomware rilevato".
- **Processo di ripristino**. Il processo di ripristino è stato migliorato. Ora è possibile eseguire il ripristino di un volume per volume, di tutti i volumi per un carico di lavoro o anche di alcuni file dal volume, tutto in un singolo flusso di lavoro. "Scopri di più sul ripristino in seguito a un attacco ransomware (dopo la neutralizzazione degli incidenti)".

"Scopri di più sulla protezione ransomware di BlueXP".

6 ottobre 2023

Il servizio di protezione dal ransomware BlueXP è una soluzione SaaS per la protezione dei dati, il rilevamento di potenziali attacchi e il recovery dei dati da un attacco ransomware.

Per la versione in anteprima, il servizio protegge i carichi di lavoro basati sull'applicazione dei datastore Oracle, MySQL, VM e file share nello storage NAS on-premise, oltre che in Cloud Volumes ONTAP su AWS (utilizzando il protocollo NFS) attraverso i singoli account BlueXP ed esegue il backup dei dati nel cloud storage di Amazon Web Services.

Il servizio di protezione dal ransomware di BlueXP offre un utilizzo completo di diverse tecnologie NetApp per permettere all'amministratore della sicurezza dei dati o al Security Operations Engineer di raggiungere i seguenti obiettivi:

- Visualizza rapidamente la protezione dal ransomware su tutti i tuoi workload.
- Ottieni informazioni dettagliate sulle raccomandazioni relative alla protezione dal ransomware
- Migliora il livello di protezione in base alle raccomandazioni di protezione dal ransomware BlueXP.
- Assegna policy di protezione dal ransomware per proteggere i tuoi carichi di lavoro principali e i dati ad alto rischio dagli attacchi ransomware.
- Monitora la salute dei carichi di lavoro contro gli attacchi ransomware che cercano anomalie nei dati.

- Valutare rapidamente l’impatto degli incidenti ransomware sul carico di lavoro.
- Esegui il ripristino in maniera intelligente dai ransomware eseguendo il ripristino dei dati e garantendo che non si verifichi una nuova infezione da tali dati.

"Scopri di più sulla protezione ransomware di BlueXP".

Inizia subito

Scopri l'anteprima della protezione dal ransomware BlueXP

Gli attacchi ransomware possono bloccare l'accesso ai sistemi e i dati, mentre gli autori degli attacchi possono chiedere riscatti in cambio del rilascio o della decrittografia dei dati. Secondo IDC, non è raro che le vittime del ransomware subiscano diversi attacchi ransomware. L'attacco può interrompere l'accesso ai tuoi dati tra un giorno e diverse settimane.

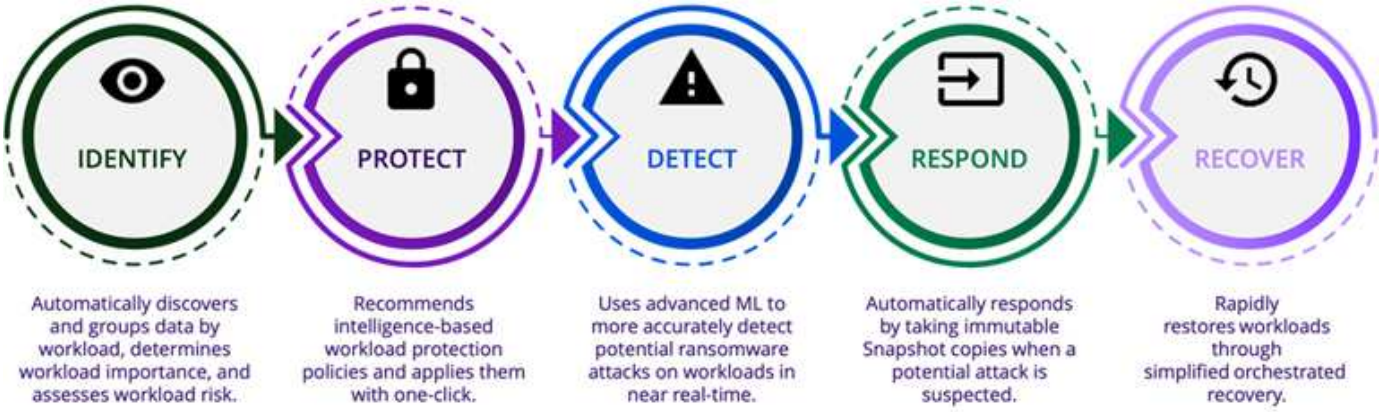
La protezione dal ransomware di BlueXP è un servizio di orchestrazione per protezione, rilevamento e recovery del ransomware. Per la versione in anteprima, il servizio protegge i carichi di lavoro basati su applicazioni dei datastore Oracle, MySQL, VM, e condivisioni di file sullo storage NAS on-premise oltre che su Cloud Volumes ONTAP in Amazon Web Services (utilizzando il protocollo NFS) tra gli account BlueXP ed effettua il backup dei dati su cloud storage Amazon Web Services o NetApp StorageGRID.

QUESTA DOCUMENTAZIONE VIENE FORNITA COME ANTEPRIMA TECNOLOGICA. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli dell'offerta, i contenuti e la tempistica prima della disponibilità generale.

Cosa puoi fare con la protezione dal ransomware di BlueXP

Il servizio di protezione dal ransomware di BlueXP offre un utilizzo completo di diverse tecnologie NetApp così che il tuo amministratore dello storage, amministratore della sicurezza dei dati o ingegnere delle operazioni di sicurezza possano raggiungere i seguenti obiettivi:

- **Identifica** tutti i workload basati su applicazioni, condivisioni di file o gestiti da VMware in NAS NetApp on-premise con ambienti di lavoro NFS in BlueXP, tra account BlueXP, aree di lavoro e connettori BlueXP. Quindi, il servizio categorizza la priorità dei dati e offre consigli per i miglioramenti alla protezione dal ransomware.
- **Proteggi** i tuoi carichi di lavoro abilitando backup e copie Snapshot sui tuoi dati.
- **Detect** anomalie che potrebbero essere attacchi ransomware.
- **Rispondi** ai potenziali attacchi ransomware avviando automaticamente una copia Snapshot NetApp ONTAP.
- **Recupera** i tuoi workload che aiutano ad accelerare l'uptime dei workload orchestrando diverse tecnologie NetApp. È possibile scegliere di ripristinare volumi, cartelle o file specifici. Il servizio fornisce consigli sulle opzioni migliori.



Vantaggi dell'utilizzo della protezione dal ransomware di BlueXP

La protezione dal ransomware BlueXP offre i seguenti benefici:

- Rileva i carichi di lavoro e i set di dati, analizza la priorità in base all'indice di utilizzo e classifica la relativa importanza.
- Valuta il livello di protezione ransomware e lo visualizza in un dashboard di facile comprensione.
- Fornisce consigli sulle fasi successive in base al rilevamento e all'analisi della postura di protezione.
- Applica raccomandazioni di data Protection ai/ML con un solo clic.
- Protegge i dati nei principali carichi di lavoro basati sull'applicazione, come i datastore e le condivisioni di file MySQL, Oracle e VMware.
- Rileva gli attacchi ransomware sui dati in tempo reale sullo storage primario utilizzando la tecnologia ai.
- Avvia azioni automatizzate in risposta ai potenziali attacchi rilevati creando copie Snapshot e avviando avvisi relativi ad attività anomale.
- Applica una recovery ridotta per soddisfare le policy di RPO. La protezione ransomware di BlueXP orchestra il recovery dagli incidenti ransomware utilizzando diversi servizi di recovery di NetApp, tra cui backup e recovery di BlueXP (in precedenza Cloud Backup).

Costo

NetApp non ti addebita i costi per l'utilizzo della versione di anteprima della protezione dal ransomware di BlueXP.

Licensing

L'anteprima della protezione dal ransomware di BlueXP non richiede licenze speciali. Tutte le licenze di anteprima sono licenze di valutazione.

Per la versione di anteprima, NetApp aiuta a configurare la valutazione e le eventuali licenze richieste.

L'anteprima della protezione dal ransomware di BlueXP richiede le seguenti licenze:

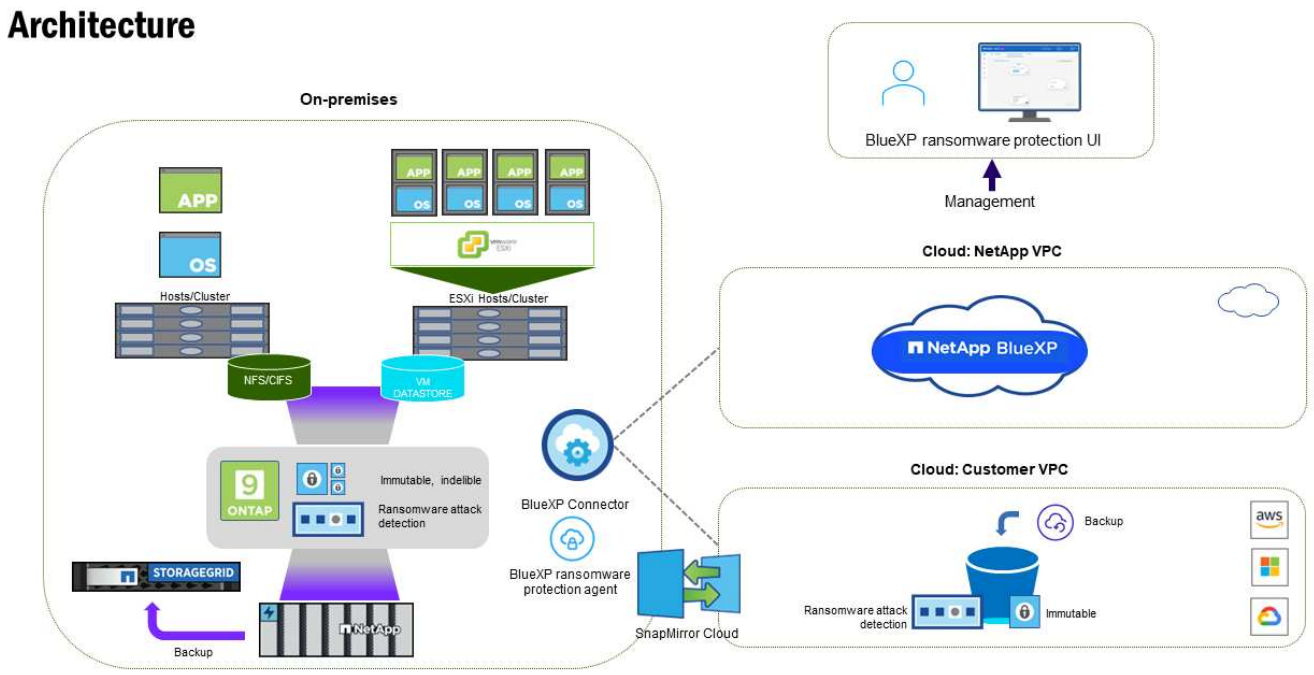
- ONTAP
- Tecnologia per la protezione autonoma dal ransomware NetApp. Fare riferimento a. "Panoramica della

protezione ransomware autonoma" per ulteriori informazioni.

- Servizio di backup e recovery di BlueXP

Come funziona la protezione ransomware di BlueXP

A un livello elevato, la protezione dal ransomware di BlueXP funziona in questo modo.



Funzione	Descrizione
IDENTIFICA	• Trova tutti i dati NAS (NFS mount) on-premise del cliente connessi ad BlueXP. • Identifica i dati dei clienti dalle API di servizio ONTAP e li associa ai workload. Scopri di più "ONTAP" e. "Software SnapCenter". • Rileva il livello di protezione corrente di ogni volume delle copie Snapshot NetApp e delle policy di backup, oltre a qualsiasi funzionalità di rilevamento on-box. Il servizio associa quindi questa postura di protezione ai workload utilizzando backup e recovery di BlueXP, il Digital Advisor di BlueXP, i servizi e le tecnologie NetApp e ONTAP come protezione autonoma da ransomware, FPolicy, policy di backup e policy Snapshot. Scopri di più "Protezione ransomware autonoma" e. "Backup e ripristino BlueXP", "Digital Advisor di BlueXP", e. "FPolicy di ONTAP". • Assegna una priorità aziendale a ogni carico di lavoro in base ai livelli di protezione rilevati automaticamente e consiglia policy di protezione per i carichi di lavoro in base alla priorità aziendale. • La protezione dal ransomware inoltre apprende le associazioni di policy e consiglia policy personalizzate per carichi di lavoro simili.

Funzione	Descrizione
PROTEGGI	• Monitora attivamente i workload e orchestra l'utilizzo di backup e recovery di BlueXP e le API ONTAP applicando policy a ciascuno dei workload identificati.
RILEVA	• Rileva i potenziali attacchi con un modello di machine learning (ML) integrato che rileva crittografia e attività potenzialmente anomale. • Rilevamento a doppio livello che inizia con il rilevamento di potenziali attacchi ransomware nello storage primario e risponde ad attività anomale creando ulteriori copie Snapshot automatizzate per creare i punti di ripristino dei dati più vicini. Il servizio offre la possibilità di approfondire per identificare con maggiore precisione i potenziali attacchi, senza influire sulle performance dei carichi di lavoro primari. • Determina i file sospetti specifici e mappa gli attacchi ai carichi di lavoro associati, utilizzando le tecnologie ONTAP, protezione autonoma dal ransomware e FPolicy.
RISPONDI	• Mostra i dati pertinenti, come l'attività dei file, l'attività dell'utente e l'entropia, per aiutarti a completare revisioni forensi sull'attacco. • Avvia copie Snapshot rapide utilizzando tecnologie e prodotti NetApp come ONTAP, protezione autonoma da ransomware e FPolicy.
RECUPERA	• Determina la snapshot o il backup migliori e consiglia il recovery point effettivo (RPA) utilizzando backup e recovery di BlueXP, ONTAP, protezione autonoma da ransomware e tecnologie e servizi FPolicy. • Orchestra il recovery dei workload, tra cui VM, condivisioni di file e database, con coerenza delle applicazioni.

Destinazioni di backup supportate, ambienti di lavoro e origini dati

Utilizza l'anteprima della protezione ransomware di BlueXP per scoprire quanto siano resilienti i tuoi dati a un attacco informatico sui seguenti tipi di destinazioni di backup, ambienti di lavoro e origini dati:

Target di backup supportati

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Ambienti di lavoro supportati

- NAS ONTAP on-premise (con protocollo NFS)
- ONTAP Select
- Cloud Volumes ONTAP in AWS (utilizzando il protocollo NFS)

Origini dati

Per la versione di anteprima, il servizio protegge i seguenti carichi di lavoro basati su applicazioni:

- Condivisioni di file NetApp
- Datastore VMware

- Database (per la versione di anteprima, Oracle e MySQL)

Termini che potrebbero aiutarti con la protezione dal ransomware

Potresti trarre beneficio dalla comprensione di una certa terminologia relativa alla protezione dal ransomware.

- **Protezione**: La protezione nel ransomware di BlueXP significa garantire che snapshot e backup immutabili vengano eseguiti regolarmente su un dominio di sicurezza diverso utilizzando policy di protezione.
- **Carico di lavoro**: Un carico di lavoro nell'anteprima della protezione dal ransomware di BlueXP può includere database MySQL o Oracle, datastore VMware o condivisioni di file.

Prerequisiti della protezione dal ransomware di BlueXP

Inizia subito con la protezione dal ransomware di BlueXP verificando la preparazione del tuo ambiente operativo, dell'accesso, dell'accesso alla rete e del browser web.

Per utilizzare la versione di anteprima della protezione dal ransomware di BlueXP, sono necessari i seguenti prerequisiti:

- Un account in NetApp StorageGRID o AWS S3 per le destinazioni di backup e il set di autorizzazioni di accesso

  Fare riferimento a. "Elenco delle autorizzazioni AWS" per ulteriori informazioni.

- ONTAP 9.11.1 e versioni successive
  - Autorizzazioni ONTAP di amministrazione cluster
  - Una licenza per la protezione autonoma da ransomware NetApp, utilizzata dalla protezione BlueXP, abilitata sull'istanza ONTAP on-premise, a seconda della versione di ONTAP che stai utilizzando. Fare riferimento a. "Panoramica della protezione ransomware autonoma".

    Per ulteriori informazioni sulle licenze, fare riferimento a. "Scopri di più sulla protezione ransomware di BlueXP".

- In BlueXP:
  - Configurare un connettore BlueXP per ogni cloud privato virtuale (VPC) o in un'area on-premise in BlueXP. Fare riferimento a. "Documentazione di BlueXP per configurare il connettore".

    Se disponi di più connettori BlueXP, il servizio scansionerà i dati su tutti i connettori oltre a quello attualmente visualizzato nell'interfaccia utente di BlueXP.

  - Servizio di backup e recovery di BlueXP con backup abilitato nell'ambiente di lavoro
  - Un ambiente di lavoro BlueXP con storage NAS NetApp on-premise
  - Un account BlueXP con almeno un connettore attivo che si connette ai cluster ONTAP on-premise. Tutti gli ambienti di origine e lavoro devono trovarsi sullo stesso account BlueXP.
  - Un account utente BlueXP con privilegi di account Admin per rilevare le risorse
  - "Requisiti standard di BlueXP"

Avvio rapido per la protezione dal ransomware di BlueXP

Ecco una panoramica dei passaggi necessari per iniziare con la protezione dal ransomware di BlueXP. I collegamenti all'interno di ogni passaggio consentono di accedere a una pagina che fornisce ulteriori dettagli.

1 **Esaminare i prerequisiti**

"Assicurati che il tuo ambiente soddisfi questi requisiti".

2 **Configurare il servizio di protezione dal ransomware**

- "Preparare NetApp StorageGRID o Amazon Web Services come destinazione di backup".
- "Configurare un connettore in BlueXP".
- "Configurare le destinazioni di backup".
- "Scopri i carichi di lavoro in BlueXP".

3 **Quali sono le prossime novità?**

Dopo aver configurato il servizio, ecco cosa fare in seguito.

- "Visualizza la salute della protezione dei carichi di lavoro sulla Dashboard".
- "Proteggere i carichi di lavoro".
- "Rispondi al rilevamento di potenziali attacchi ransomware".
- "Recupero da un attacco (dopo che gli incidenti sono neutralizzati)".

Imposta la protezione dal ransomware BlueXP

Per utilizzare la protezione dal ransomware di BlueXP, esegui alcuni passaggi per configurarla.

Prima di iniziare, rivedere "prerequisiti" per garantire che il tuo ambiente sia pronto.

Preparare la destinazione di backup

Preparare una delle seguenti destinazioni di backup:

- NetApp StorageGRID
- Amazon Web Services

Dopo aver configurato le opzioni nella destinazione di backup stessa, la configurerai in seguito come destinazione di backup nel servizio di protezione dal ransomware di BlueXP.

Preparare StorageGRID a diventare una destinazione di backup

Se si desidera utilizzare StorageGRID come destinazione di backup, fare riferimento alla sezione

"Documentazione StorageGRID" Per ulteriori informazioni su StorageGRID.

Prepara AWS a diventare una destinazione di backup

- Configurare un account in AWS.
- Configurare "Autorizzazioni AWS" In AWS.

Per informazioni sulla gestione dello storage AWS in BlueXP, fare riferimento a. "Gestisci i bucket Amazon S3".

Configurare BlueXP

Il passo successivo è la configurazione di BlueXP e del servizio di protezione dal ransomware di BlueXP.

Revisione "Requisiti standard di BlueXP".

Creare un connettore in BlueXP

Per provare questo servizio, contattare il rappresentante di vendita NetApp. Quindi, quando usi il connettore BlueXP, includerai le funzionalità appropriate per il servizio di protezione dal ransomware.

Per creare un connettore in BlueXP prima di utilizzare il servizio, consultare la documentazione di BlueXP che descrive "Come creare un connettore BlueXP".

> Se disponi di più connettori BlueXP, il servizio scansionerà i dati su tutti i connettori oltre a quello attualmente visualizzato nell'interfaccia utente di BlueXP. Questo servizio rileva tutte le aree di lavoro e tutti i connettori associati a questo account.

Accedi alla protezione dal ransomware di BlueXP

USA NetApp BlueXP per accedere al servizio di protezione dal ransomware di BlueXP. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.

Per ulteriori informazioni, fare riferimento a. "Accedi alla protezione dal ransomware di BlueXP".

Configura destinazioni di backup nella protezione dal ransomware di BlueXP

Utilizza l'opzione delle destinazioni di backup della protezione anti-ransomware di BlueXP per configurare le destinazioni di backup. Per ulteriori informazioni, fare riferimento a. "Configurare le opzioni delle impostazioni".

Accedi alla protezione dal ransomware di BlueXP

USA NetApp BlueXP per accedere al servizio di protezione dal ransomware di BlueXP.

Per accedere a BlueXP, puoi utilizzare le credenziali del sito di supporto NetApp oppure iscriverti per un login cloud NetApp utilizzando la tua email e una password. "Scopri di più sull'accesso".

Fasi

1. Aprire un browser Web e accedere a. "Console BlueXP".

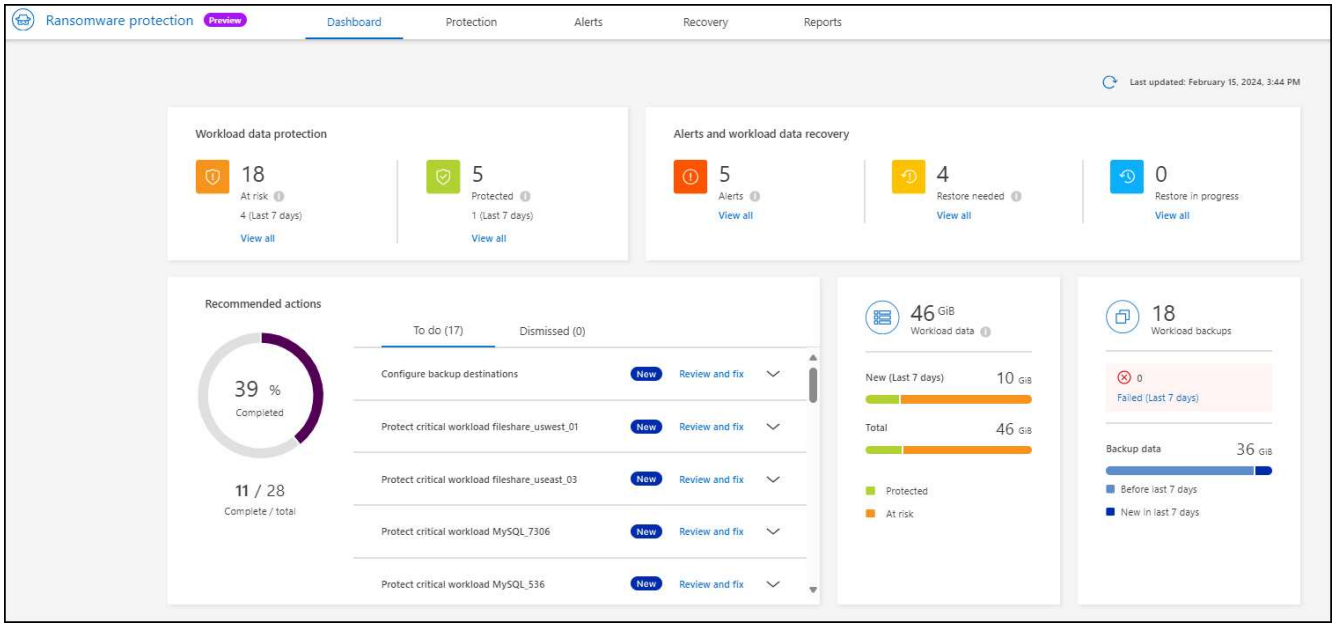
   Viene visualizzata la pagina di accesso a NetApp BlueXP.

2. Accedere a BlueXP.

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

   Se è la prima volta che accedi a questo servizio, viene visualizzata la pagina iniziale.

   In caso contrario, verrà visualizzata la dashboard di protezione dal ransomware BlueXP.



4. Iniziare a utilizzare il servizio.
   - Se non hai un connettore BlueXP o non è quello per questa anteprima, potrebbe essere necessario contattare il supporto NetApp o seguire i messaggi per iscriverti a questa anteprima.
   - Se sei un nuovo utente di BlueXP e non hai utilizzato alcun connettore, quando selezioni "**ransomware Protection**", viene visualizzato un messaggio sulla registrazione. Procedi e invia il modulo. NetApp ti contatterà in merito alla tua richiesta di valutazione.
   - Se sei un utente BlueXP con un connettore esistente, quando selezioni "**ransomware Protection**", viene visualizzato un messaggio sulla registrazione.
   - Se stai già partecipando all'anteprima, quando selezioni "**ransomware Protection**", puoi procedere con il servizio. Se non l'hai già fatto, seleziona l'opzione **rileva carichi di lavoro**.

Rileva i carichi di lavoro nella protezione dal ransomware di BlueXP

Per utilizzare la protezione dal ransomware di BlueXP, il servizio deve prima rilevare i dati. Durante il rilevamento, la protezione dal ransomware BlueXP analizza tutti i volumi e i file degli ambienti di lavoro in tutti i connettori e gli spazi di lavoro BlueXP all'interno di un account.

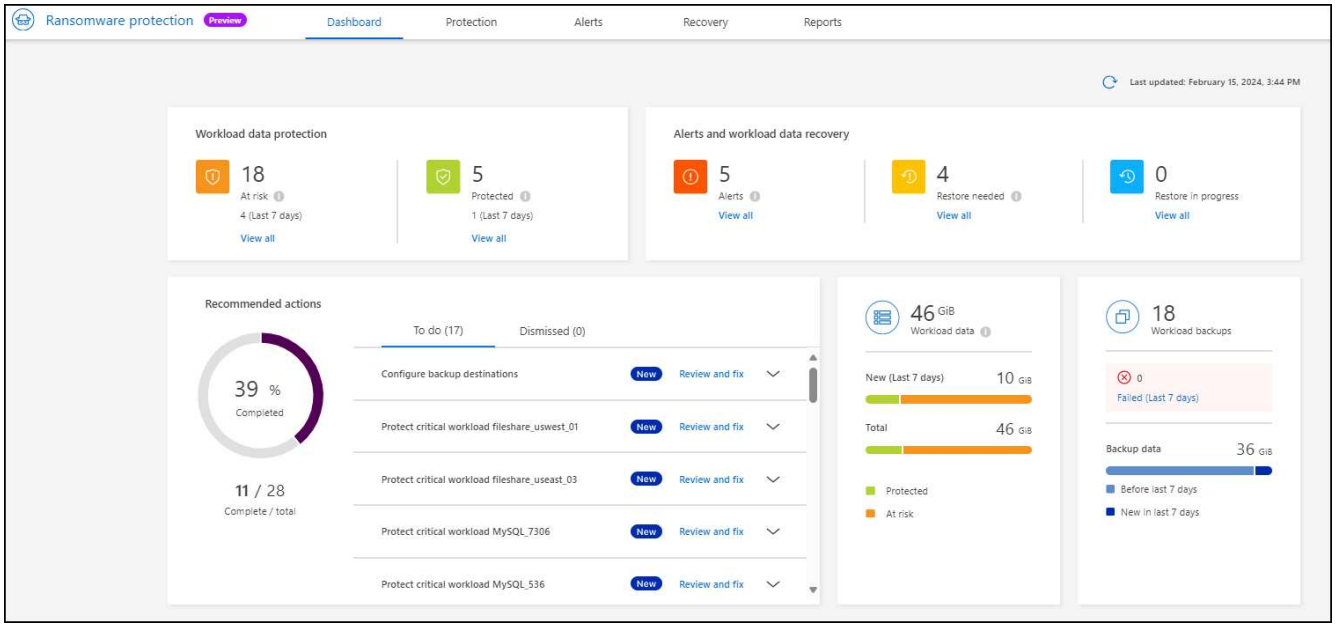
Per la versione di anteprima, la protezione dal ransomware BlueXP valuta applicazioni MySQL, applicazioni Oracle, datastore VMware e file share.

Il servizio valuta il livello di protezione esistente, incluse le opzioni di protezione di backup correnti, le copie Snapshot e le opzioni di protezione autonoma da ransomware NetApp. In base alla valutazione, il servizio consiglia quindi come migliorare la tua protezione dal ransomware.

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, seleziona **protezione** > **protezione dal ransomware**.
2. Selezionare **rileva carichi di lavoro** dalla landing page iniziale.

   Il servizio rileva i dati del carico di lavoro e mostra lo stato di salute della protezione dei dati nella Dashboard.



Configurare le impostazioni di protezione dal ransomware BlueXP

È possibile configurare una destinazione di backup esaminando i suggerimenti sul dashboard.

Aggiungere una destinazione di backup

La protezione dal ransomware di BlueXP identifica i workload che non hanno ancora backup e anche quelli che non hanno ancora destinazioni di backup assegnate.

Per proteggere questi workload, è necessario aggiungere una destinazione di backup. È possibile scegliere una delle seguenti destinazioni di backup:

- NetApp StorageGRID
- Amazon Web Services (AWS)

È possibile aggiungere una destinazione di backup in base all'azione consigliata dal Dashboard.

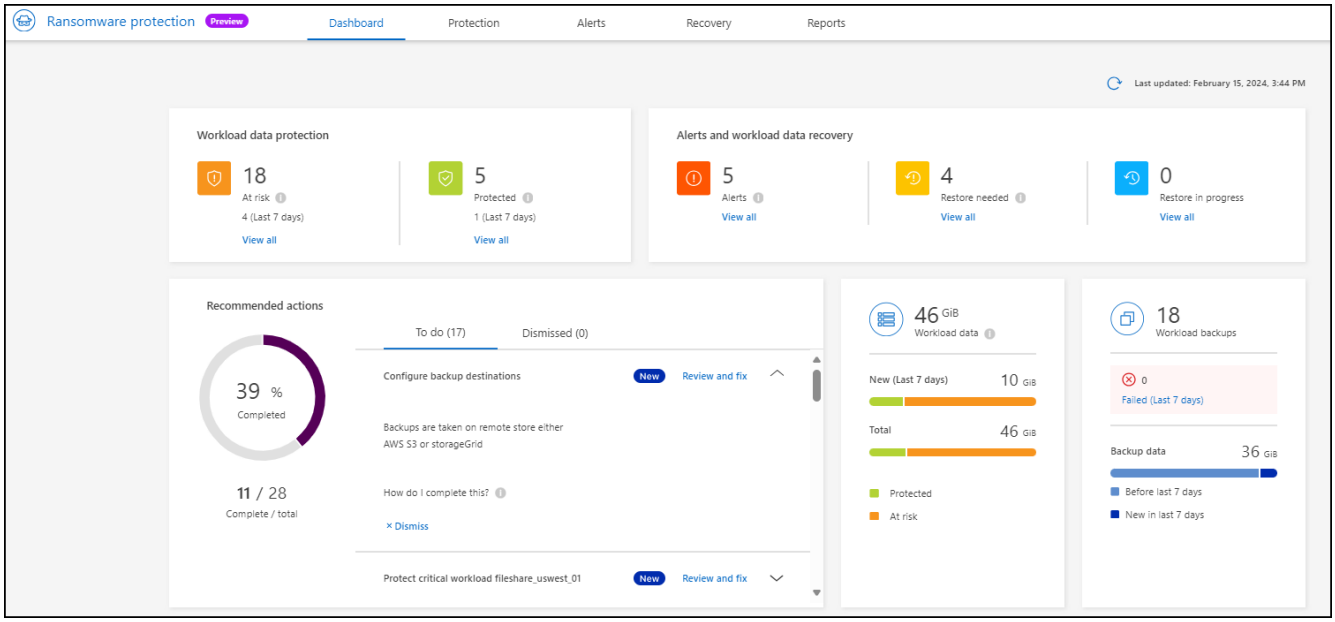
Accedere alle opzioni destinazione backup dalle azioni consigliate del dashboard

Il Dashboard fornisce molti consigli. Si consiglia di configurare una destinazione di backup.

Fasi

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

2. Esaminare il riquadro delle azioni consigliate del dashboard.

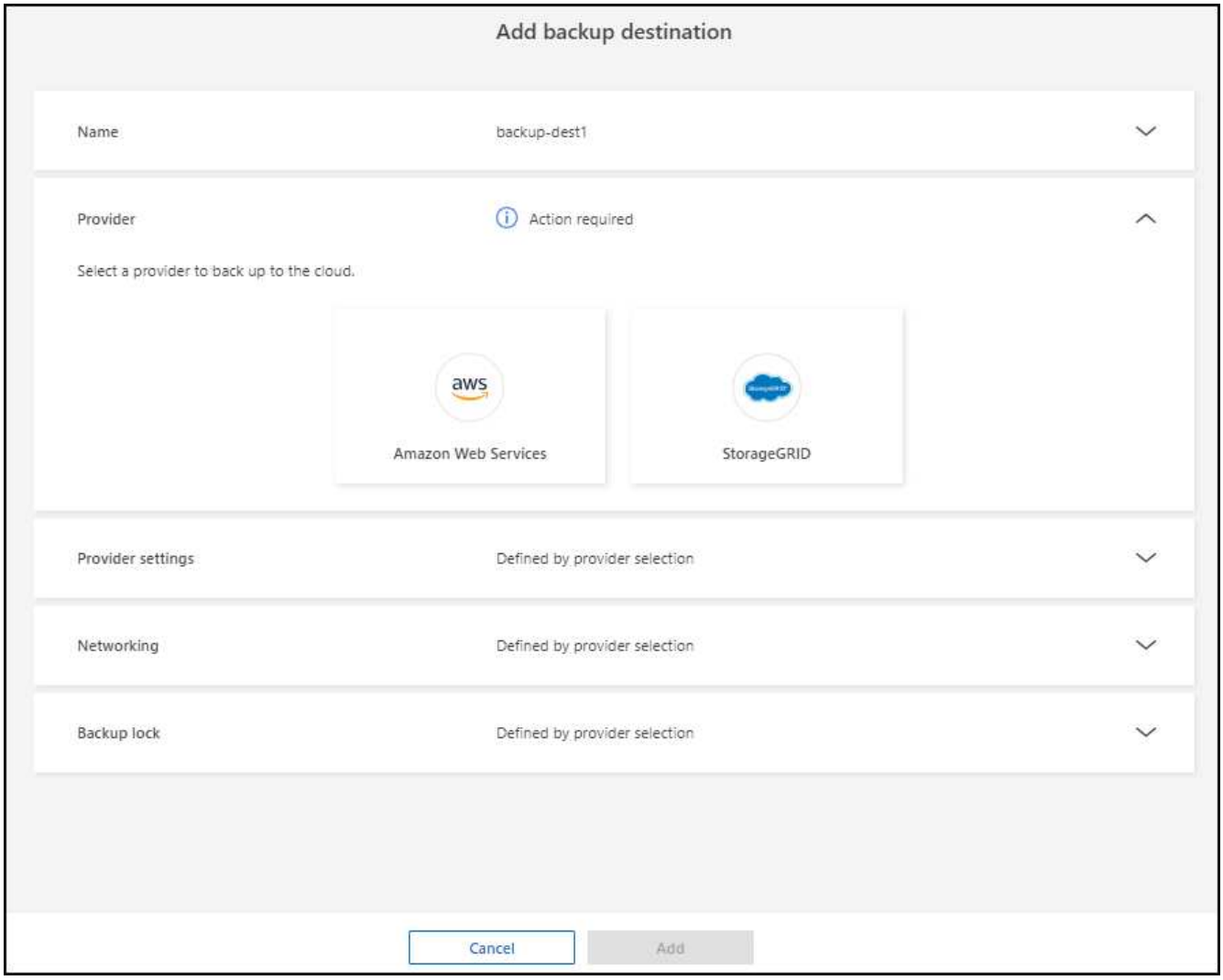


3. Nel dashboard, selezionare **Rivedi e correggi** per la raccomandazione "Configura destinazioni di backup".
4. Continuare con le istruzioni a seconda del provider di backup.

Aggiungere StorageGRID come destinazione di backup

Per impostare NetApp StorageGRID come destinazione di backup, immettere le seguenti informazioni.

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.
2. Immettere un nome per la destinazione di backup.



3. Selezionare **StorageGRID**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni provider**:
     - Creare un nuovo bucket o portare il proprio bucket che memorizzerà i backup.
     - Nodo gateway StorageGRID Nome di dominio, porta, chiave di accesso StorageGRID e credenziali chiave segreta completi.
   - **Networking**: Scegliere IPSpace.
     - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
   - **Blocco di backup**: Scegliere se si desidera che il servizio protegga i backup dalla modifica o dall'eliminazione. Questa opzione utilizza la tecnologia DataLock di NetApp. Ciascun backup verrà bloccato durante il periodo di conservazione o per un minimo di 30 giorni, più un periodo di buffer massimo di 14 giorni.

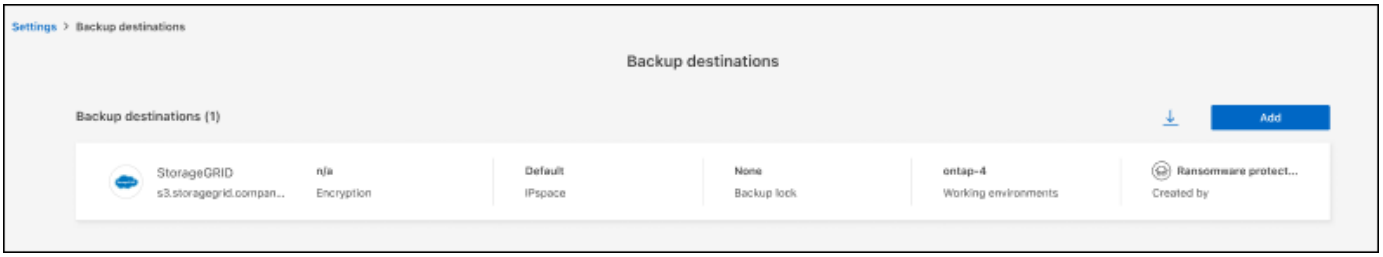
     Se si configura ora l'impostazione del blocco di backup, non sarà possibile modificarla in un secondo momento dopo la configurazione della destinazione di backup.

     - **Modalità conformità**: Gli utenti non possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.

5. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.

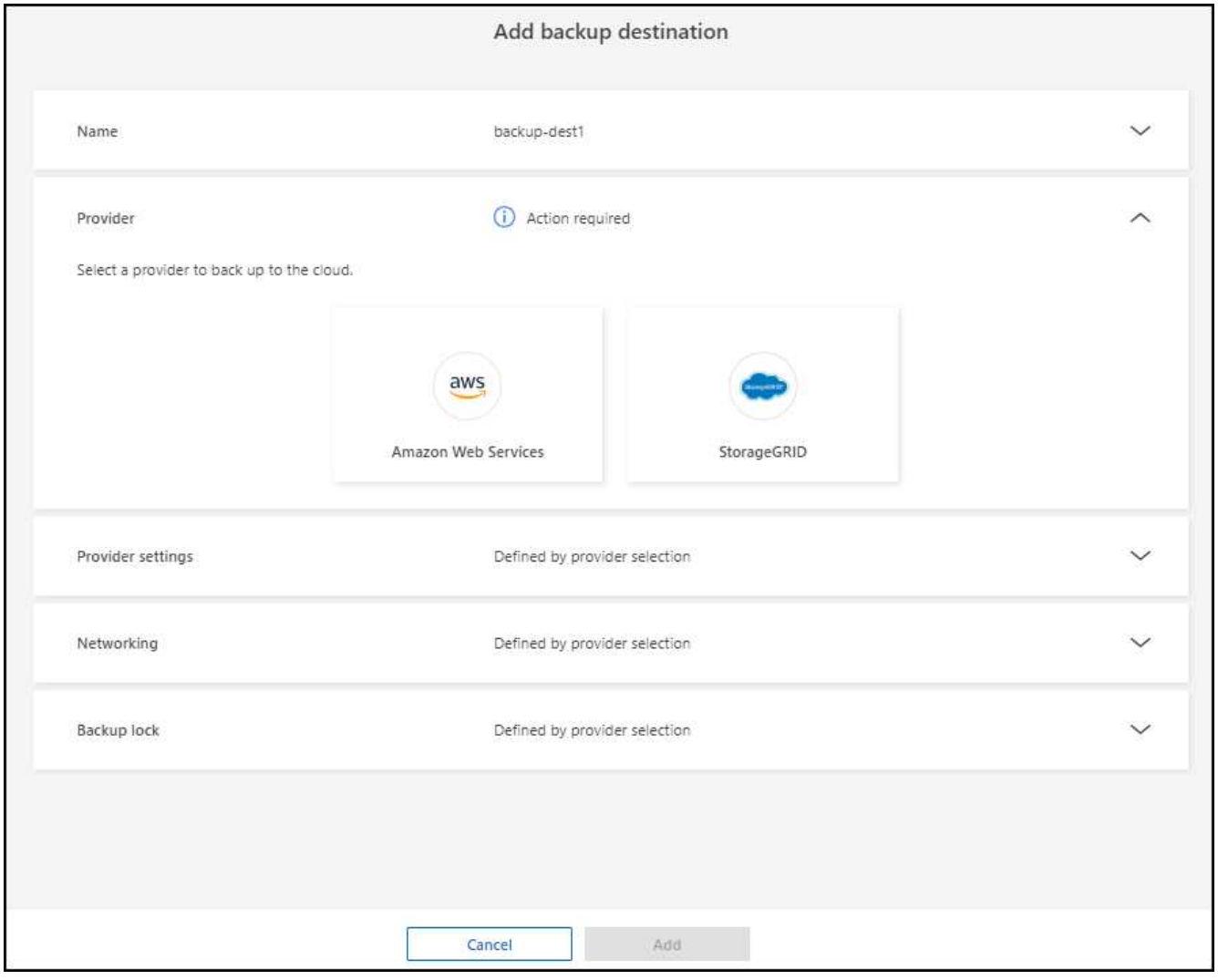


Aggiungere Amazon Web Services come destinazione di backup

Per configurare AWS come destinazione di backup, immettere le seguenti informazioni.

Per informazioni sulla gestione dello storage AWS in BlueXP, fare riferimento a. "Gestisci i bucket Amazon S3".

1. Nella pagina **Impostazioni > Destinazioni di backup**, selezionare **Aggiungi**.
2. Immettere un nome per la destinazione di backup.



3. Selezionare **Amazon Web Services**.
4. Selezionare la freccia verso il basso accanto a ciascuna impostazione e immettere o selezionare i valori:
   - **Impostazioni provider**:
     - Crea un nuovo bucket, seleziona un bucket esistente se già esistente in BlueXP o porta il tuo bucket in cui archiviare i backup.
     - Account AWS, regione, chiave di accesso e chiave segreta per le credenziali AWS

       "Se si desidera portare il proprio secchio, fare riferimento a Aggiungi S3 secchielli".
   - **Crittografia**: Se si sta creando un nuovo bucket S3, immettere le informazioni sulla chiave di crittografia fornite dal provider. Se si sceglie un bucket esistente, le informazioni di crittografia sono già disponibili.

     I dati nel bucket sono criptati con chiavi gestite da AWS per impostazione predefinita. Puoi continuare a utilizzare le chiavi gestite da AWS oppure gestire la crittografia dei tuoi dati con le tue chiavi.
   - **Rete**: Scegliere IPSpace e se si utilizza un endpoint privato.
     - IPSpace è il cluster in cui risiedono i volumi di cui si desidera eseguire il backup. Le LIF intercluster per questo IPSpace devono disporre di accesso a Internet in uscita.
     - In alternativa, è possibile scegliere se utilizzare un endpoint privato AWS (PrivateLink) precedentemente configurato.

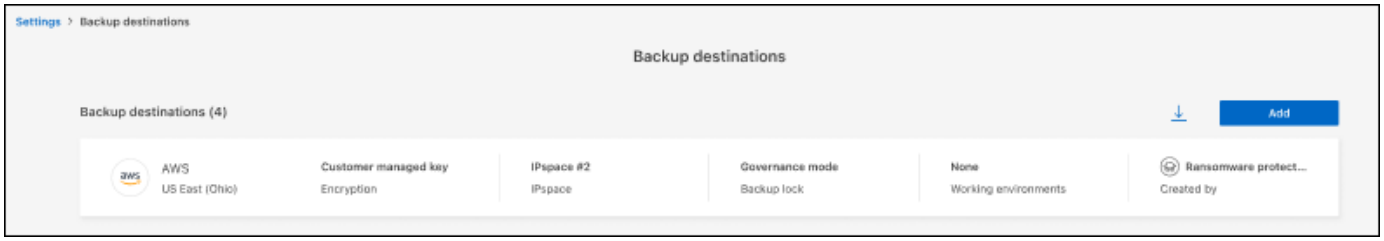
       Per utilizzare AWS PrivateLink, consultare la sezione "AWS PrivateLink per Amazon S3".
   - **Blocco di backup**: Scegliere se si desidera che il servizio protegga i backup dalla modifica o dall'eliminazione. Questa opzione utilizza la tecnologia DataLock di NetApp. Ciascun backup verrà bloccato durante il periodo di conservazione o per un minimo di 30 giorni, più un periodo di buffer massimo di 14 giorni.

     > Se si configura ora l'impostazione del blocco di backup, non sarà possibile modificarla in un secondo momento dopo la configurazione della destinazione di backup.

     - **Governance mode**: Utenti specifici (con autorizzazione S3:BypassGovernanceRetention) possono sovrascrivere o eliminare i file protetti durante il periodo di conservazione.
     - **Modalità conformità**: Gli utenti non possono sovrascrivere o eliminare i file di backup protetti durante il periodo di conservazione.
5. Selezionare **Aggiungi**.

Risultato

La nuova destinazione di backup viene aggiunta all'elenco delle destinazioni di backup.



Domande frequenti sulla protezione dal ransomware BlueXP

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

Accesso

Qual è l'URL di protezione dal ransomware BlueXP?
Per l'URL, in un browser, immettere: "https://console.bluexp.netapp.com/" Per accedere alla console BlueXP.

Ti serve una licenza per usare la protezione da ransomware di BlueXP?
Non è richiesto un file di licenza NetApp (NLF). L'anteprima della protezione dal ransomware di BlueXP non richiede licenze speciali. Tutte le licenze di anteprima sono licenze di valutazione.

La versione in anteprima di questo servizio richiede una licenza del servizio di backup e recovery di BlueXP.

Per la versione di anteprima, NetApp aiuta a configurare la valutazione e le eventuali licenze richieste.

In che modo abiliti la protezione dal ransomware BlueXP?
La protezione dal ransomware di BlueXP non richiede alcuna abilitazione. L'opzione di protezione dal ransomware viene automaticamente abilitata nel sistema di navigazione BlueXP a sinistra.

Per la versione di anteprima, devi iscriverti o contattare il tuo commerciale NetApp per provare questo servizio. Quindi, quando si utilizza il connettore BlueXP, esso includerà le funzionalità appropriate per il servizio.

La protezione anti-ransomware BlueXP è disponibile in modalità standard, limitata e privata?
Al momento, la protezione dal ransomware di BlueXP è disponibile solo in modalità standard. Continua a seguirci per saperne di più.

Per una spiegazione di queste modalità in tutti i servizi BlueXP, fare riferimento a. "Modalità di implementazione di BlueXP".

Come vengono gestite le autorizzazioni di accesso?
Solo gli amministratori degli account possono avviare il servizio e rilevare i carichi di lavoro (perché questo implica impegnarsi all'utilizzo di una risorsa). Le interazioni successive possono essere effettuate da qualsiasi ruolo.

Qual è la migliore risoluzione del dispositivo?
La risoluzione consigliata del dispositivo per la protezione dal ransomware BlueXP è di 1920x1080 o superiore.

Quale browser devo utilizzare?
Qualsiasi browser moderno funzionerà.

Interazione con altri servizi

La protezione dal ransomware di BlueXP è a conoscenza delle impostazioni di protezione di NetApp ONTAP?
Sì, la protezione dal ransomware BlueXP rileva le pianificazioni Snapshot impostate in ONTAP.

Se imposti una policy utilizzando la protezione dal ransomware di BlueXP, devi apportare modifiche

future solo in questo servizio?
Ti consigliamo di apportare modifiche alla policy dal servizio di protezione dal ransomware di BlueXP.

Carichi di lavoro

Che cosa costituisce un carico di lavoro?
Un carico di lavoro include tutti i volumi utilizzati da una singola istanza dell'applicazione. Ad esempio, un'istanza di Oracle DB implementata in ora3.host.com può avere vol1 GB e vol2 GB rispettivamente per dati e registri. Questi volumi costituiscono insieme il carico di lavoro per quella specifica istanza dell'istanza del database Oracle.

In che modo la protezione dal ransomware di BlueXP assegna la priorità ai dati del carico di lavoro?
La priorità dei dati per la versione di anteprima è determinata dalle copie Snapshot effettuate e dai backup pianificati.

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

Aggiunto nuovo volume, ma non appare ancora
Se è stato aggiunto un nuovo volume al proprio ambiente, ripetere il rilevamento e applicare criteri di protezione per proteggere il nuovo volume.

La Dashboard non mostra tutti i miei workload. Che cosa potrebbe essere sbagliato?
Al momento sono supportati solo volumi NFS. I volumi iSCSI, i volumi CIFS e altre configurazioni non supportate vengono filtrati e non vengono visualizzati sulla dashboard.

Policy di protezione

Le policy ransomware di BlueXP coesistono con altri tipi di policy dei workload?
Al momento, il backup e recovery di BlueXP (Cloud Backup) supporta una policy di backup per ogni volume. Pertanto, il backup e recovery di BlueXP e la protezione dal ransomware di BlueXP condividono le policy di backup.

Le copie Snapshot non sono limitate e possono essere aggiunte separatamente da ciascun servizio.

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.

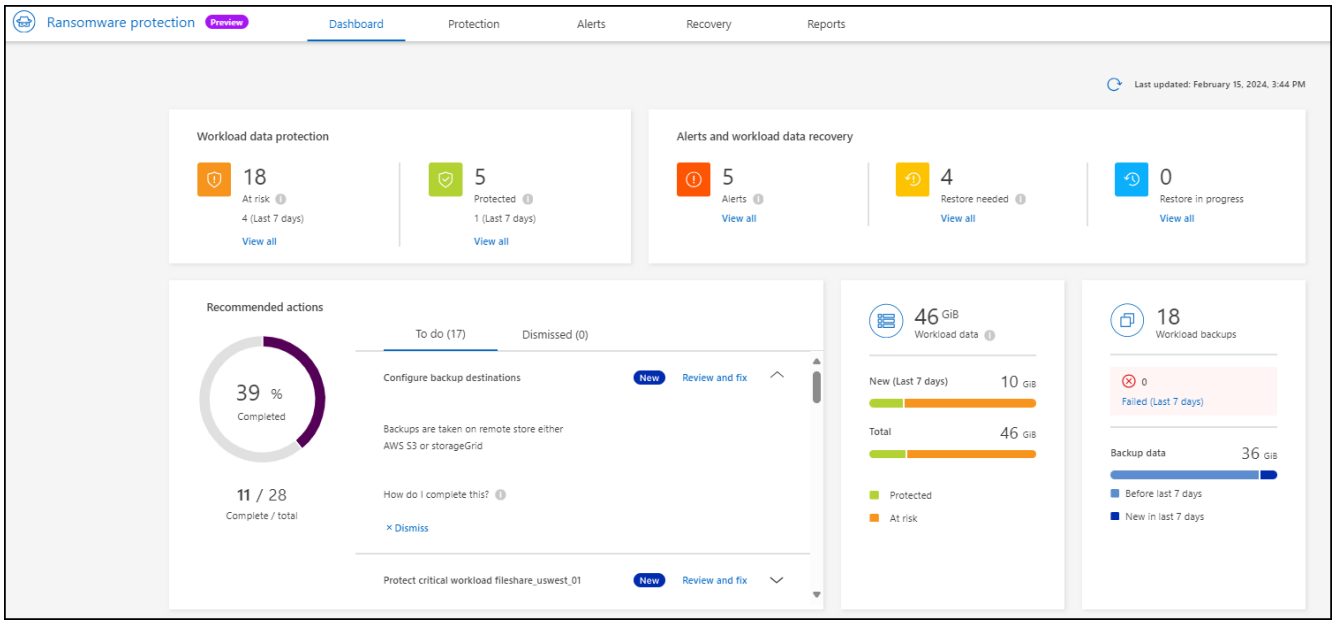
È inoltre possibile utilizzare la dashboard per esaminare e agire in base ai consigli sulla protezione.

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

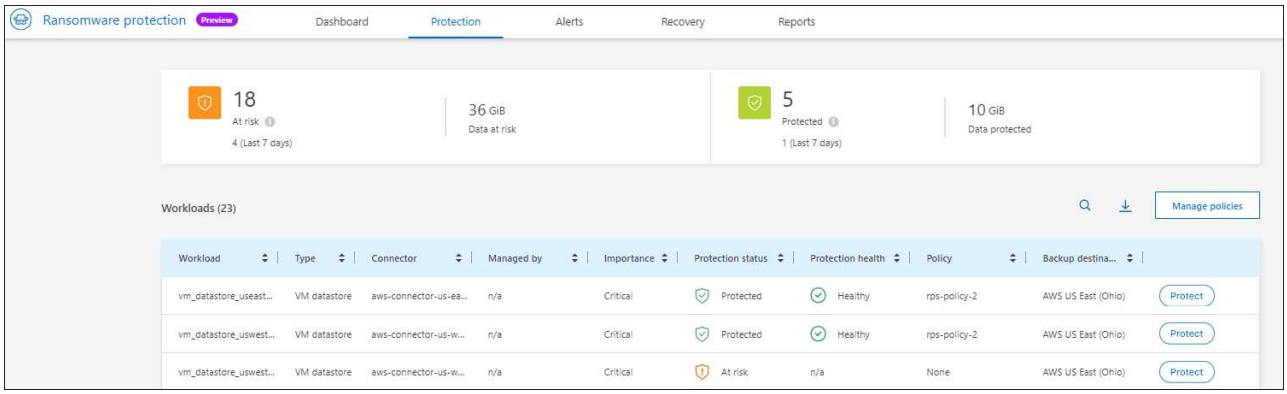
Uno dei primi passi nella protezione dei carichi di lavoro è la visualizzazione dei carichi di lavoro attuali e del loro stato di protezione. Sono visualizzabili i seguenti tipi di carichi di lavoro:

- 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:

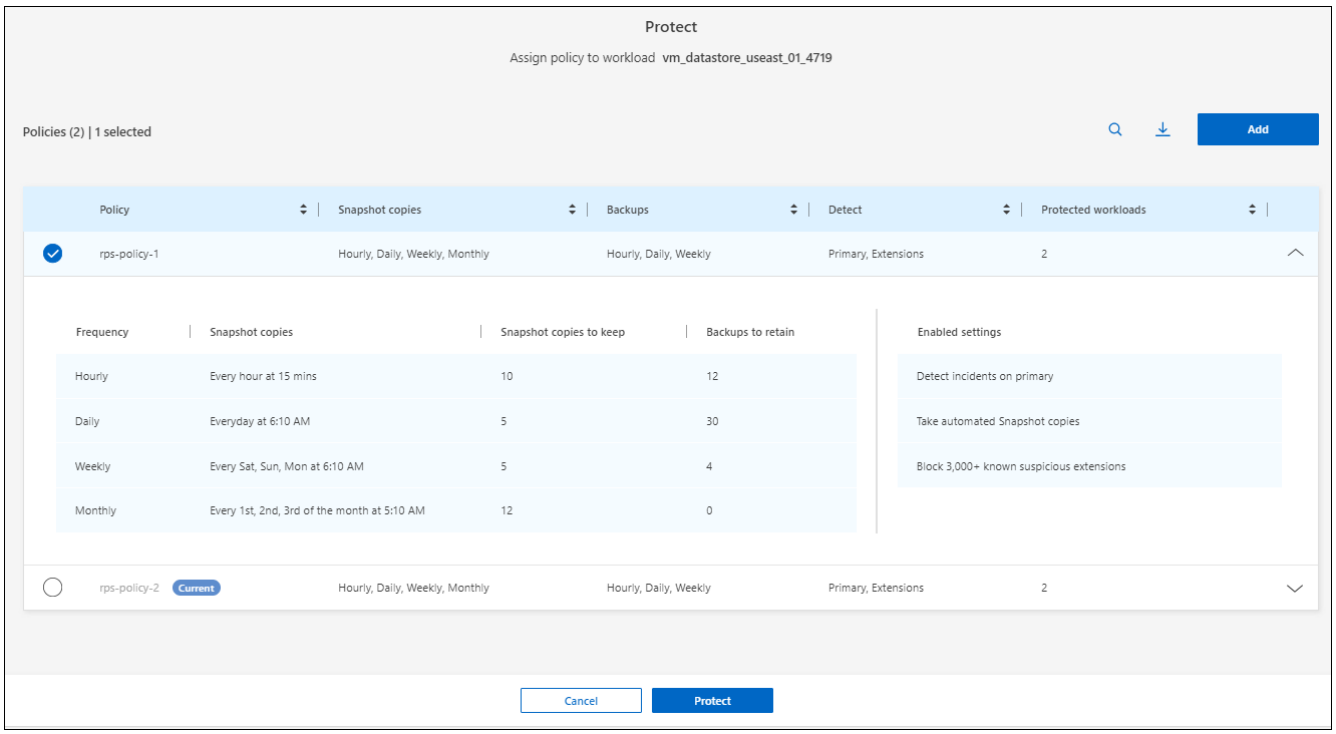
Livello dei criteri	Snapshot	Frequenza	Conservazione (giorni)	N. di copie Snapshot	Numero massimo totale di copie Snapshot
Politica critica dei carichi di lavoro	Quarto ogni ora	Ogni 15 minuti	3	288	309
	Ogni giorno	Ogni 1 giorni	14	14	309
	Settimanale	Ogni 1 settimana	35	5	309
	Mensile	Ogni 30 giorni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

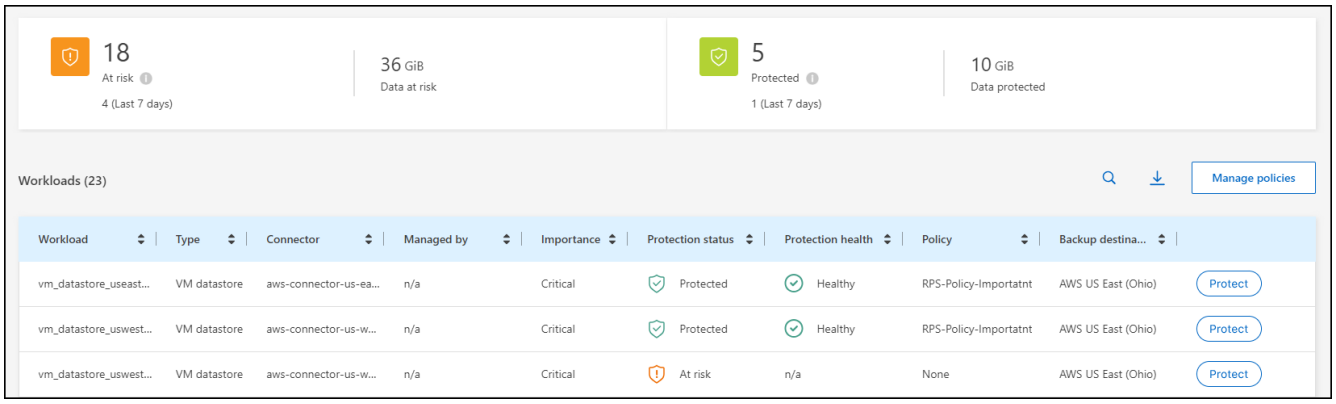
Se i criteri esistenti non soddisfano le esigenze aziendali, è possibile creare un nuovo criterio di protezione. È possibile creare da zero i propri criteri oppure utilizzarne uno esistente e modificarne le impostazioni.

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.

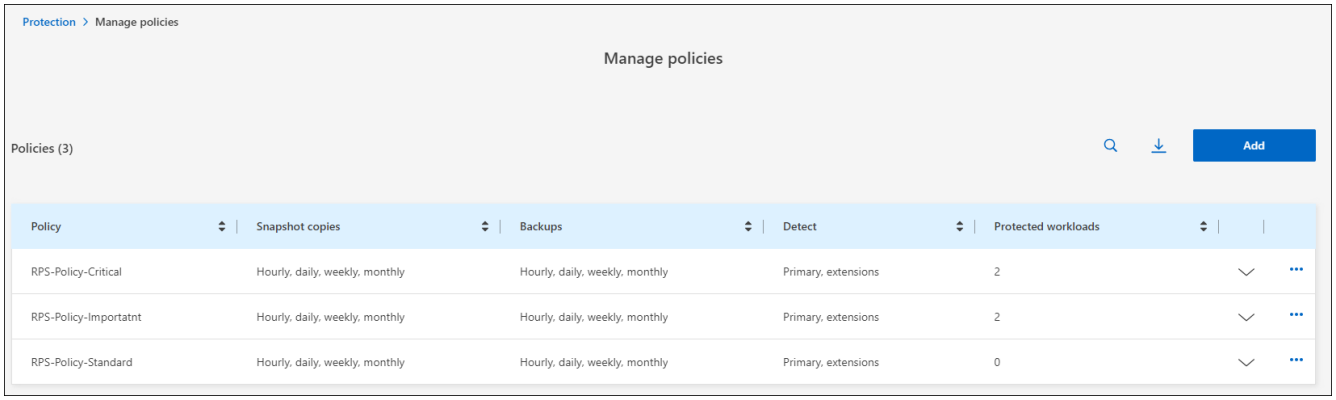
È possibile creare un criterio durante la loro gestione o durante il processo di assegnazione di un criterio a un carico di lavoro.

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

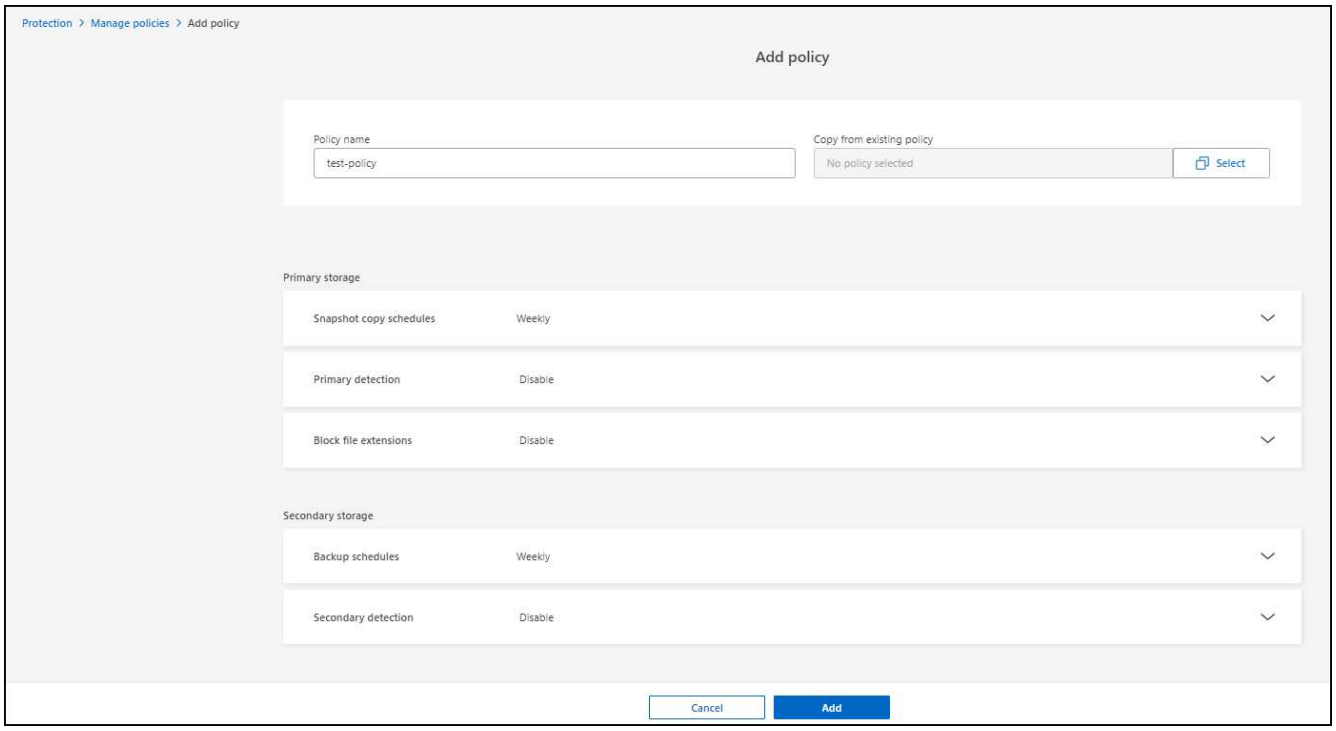
1. Dal menu protezione dal ransomware di BlueXP, seleziona **protezione**.



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.

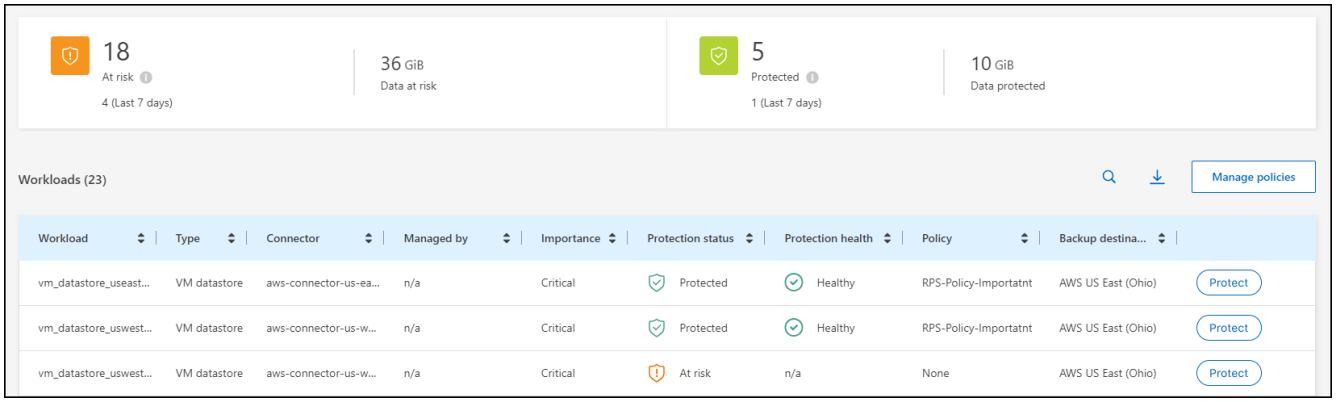
- **Archiviazione secondaria**:
  - **Pianificazioni di backup**: Scegliere le opzioni di pianificazione per l'archiviazione secondaria e attivare la pianificazione.
  - **Rilevamento secondario**: Abilita il servizio per rilevare gli incidenti ransomware sullo storage secondario.
  - **Blocca backup**: 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.

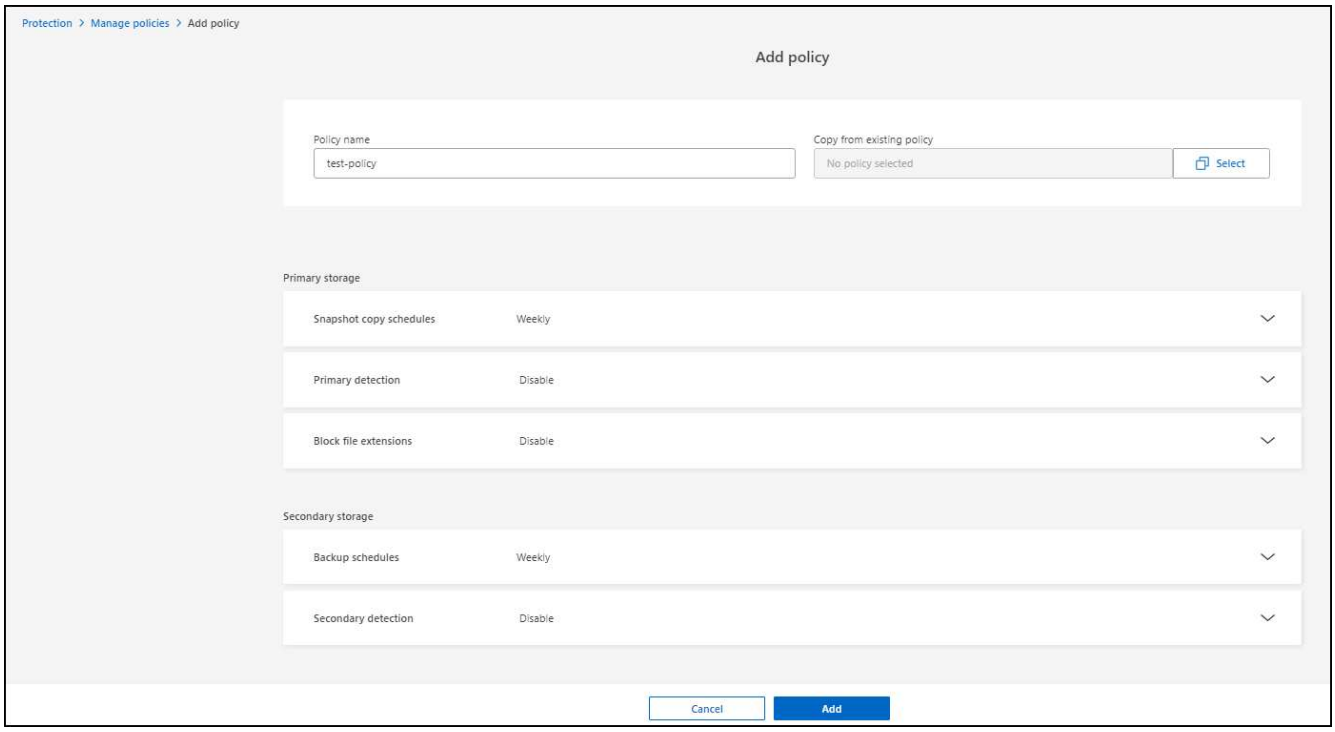
6. Selezionare **Aggiungi**.

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.

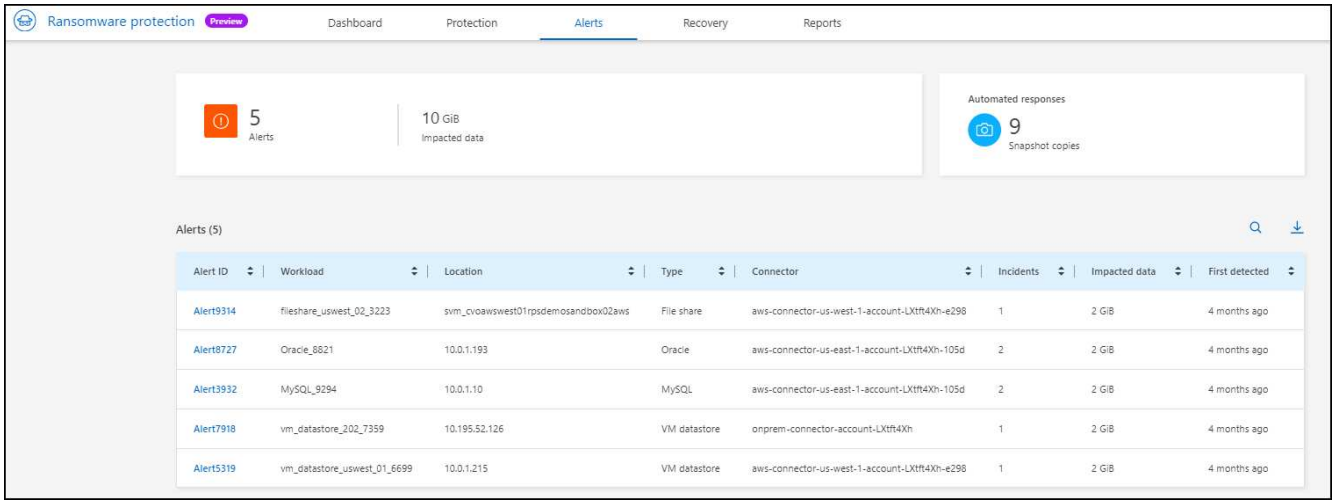
Le prove si basano sulle informazioni fornite dalla protezione autonoma dal ransomware in ONTAP. Per ulteriori informazioni, fare riferimento a. "Panoramica della protezione ransomware autonoma".

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.



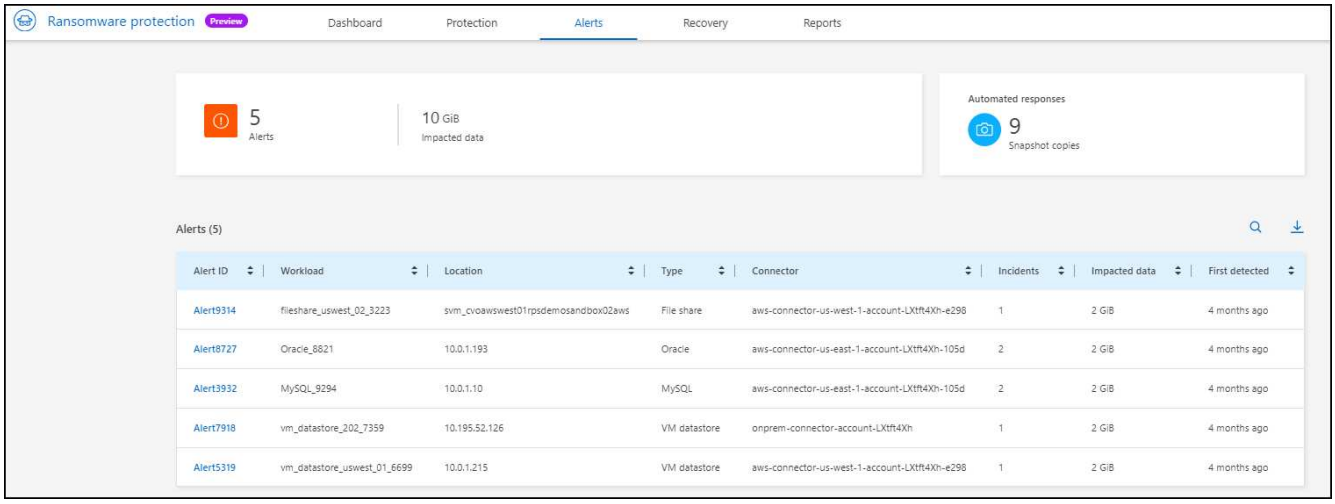
6. Continuare con Contrassegna gli incidenti ransomware come pronti per il recovery (dopo la neutralizzazione degli incidenti).

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

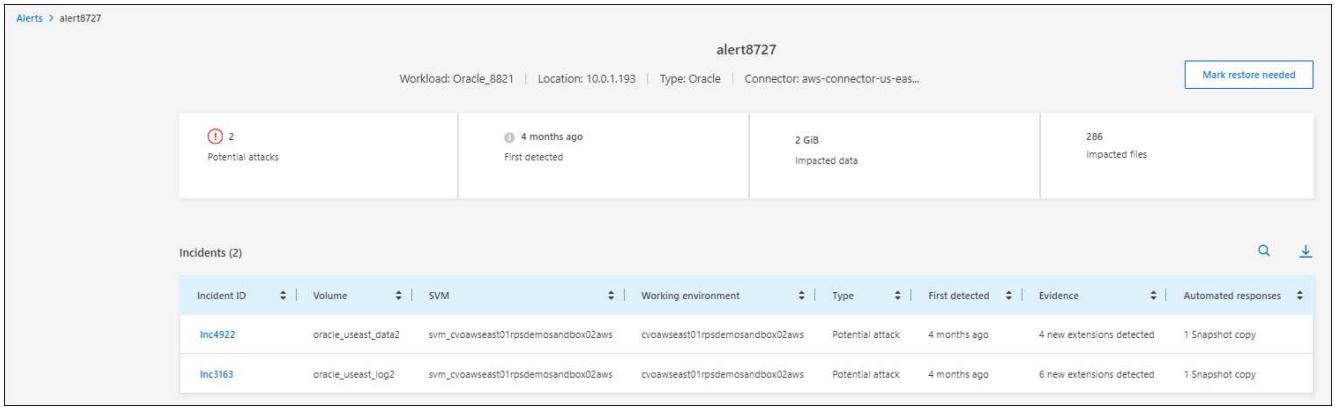
Una volta mitigato l'attacco e sei pronto a ripristinare i carichi di lavoro, dovresti comunicare con il tuo team di amministrazione dello storage che i dati sono pronti per il recovery, in modo che possano avviare il processo di recovery.

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)

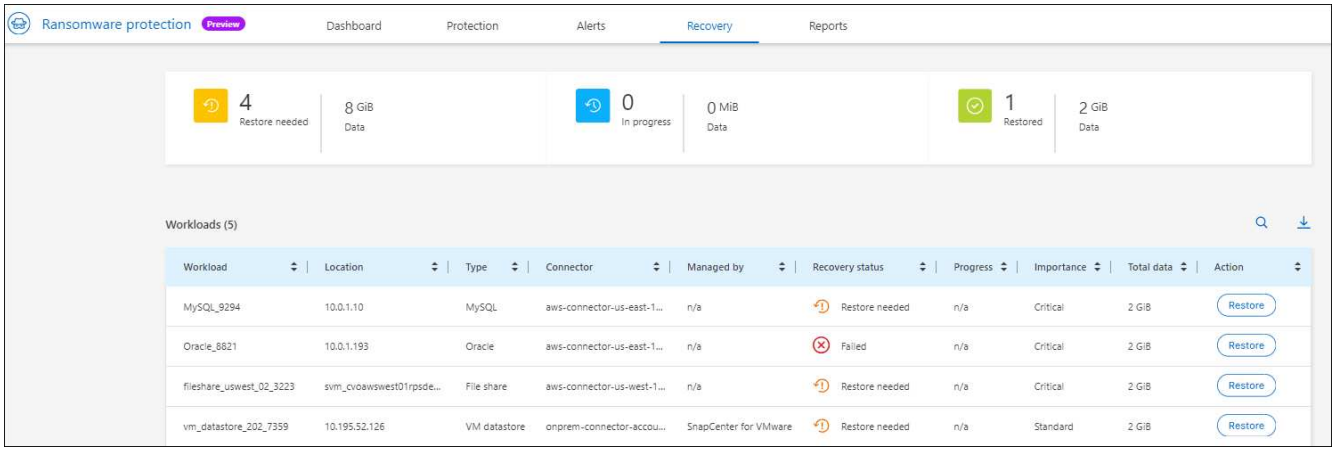
Dopo che i carichi di lavoro sono stati contrassegnati come "pronti per il recovery", la protezione dal ransomware di BlueXP consiglia un recovery point effettivo (RPA) e orchestra il workflow per un recovery resistente ai crash.

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

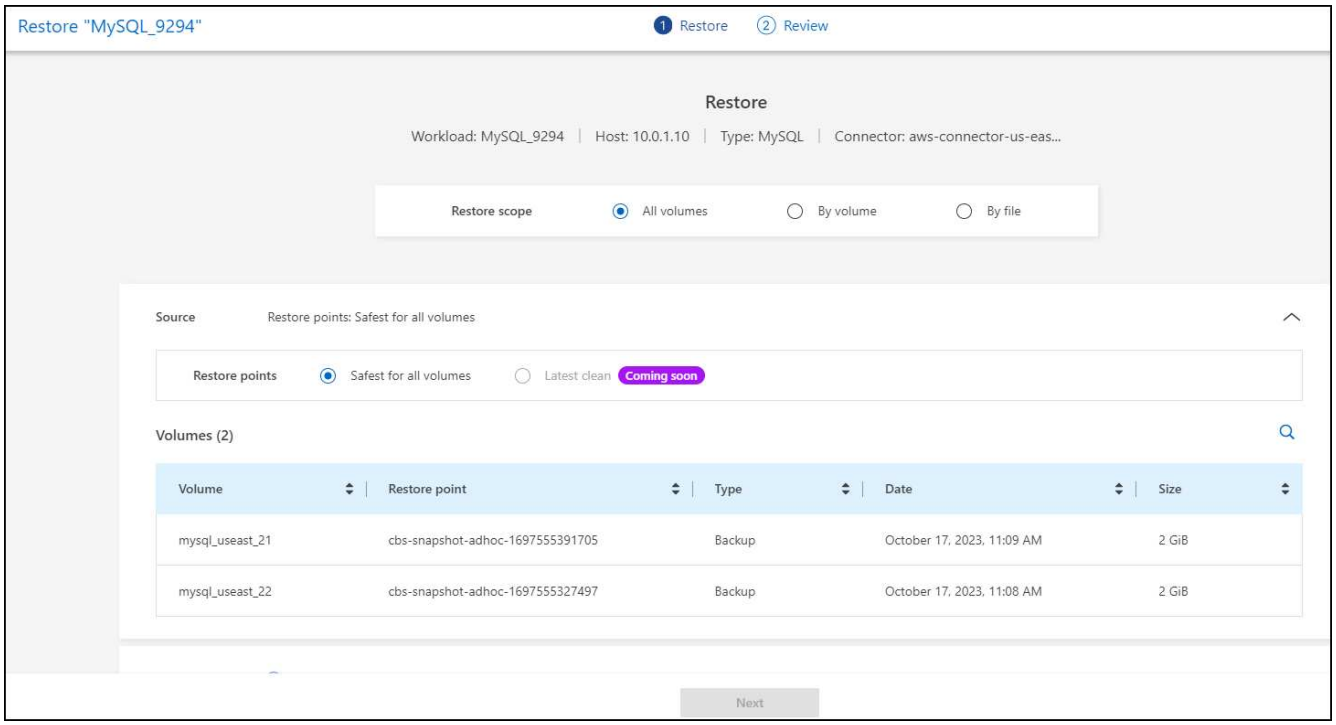
1. Dal menu di protezione dal ransomware BlueXP, seleziona **Recovery**.
2. Esaminare le informazioni sul carico di lavoro nella pagina **Ripristino**.
3. Seleziona un carico di lavoro in stato "Ripristino necessario".
4. Per ripristinare, selezionare **Ripristina**.
5. **Ripristina ambito**: Selezionare 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.

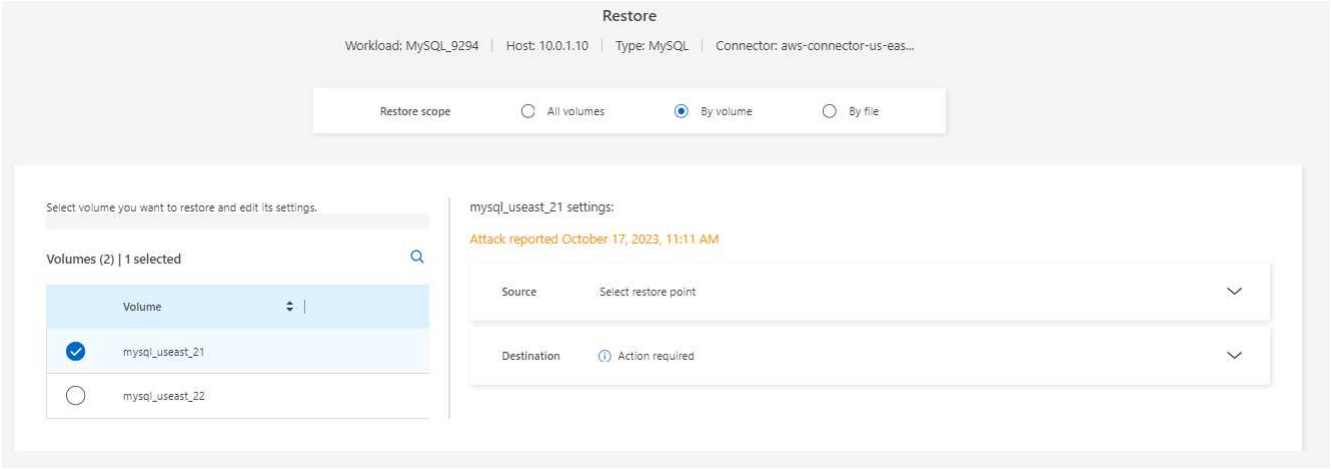
> Il nome del nuovo volume viene visualizzato come prefisso + nome del volume originale + nome del backup + data di backup.

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.

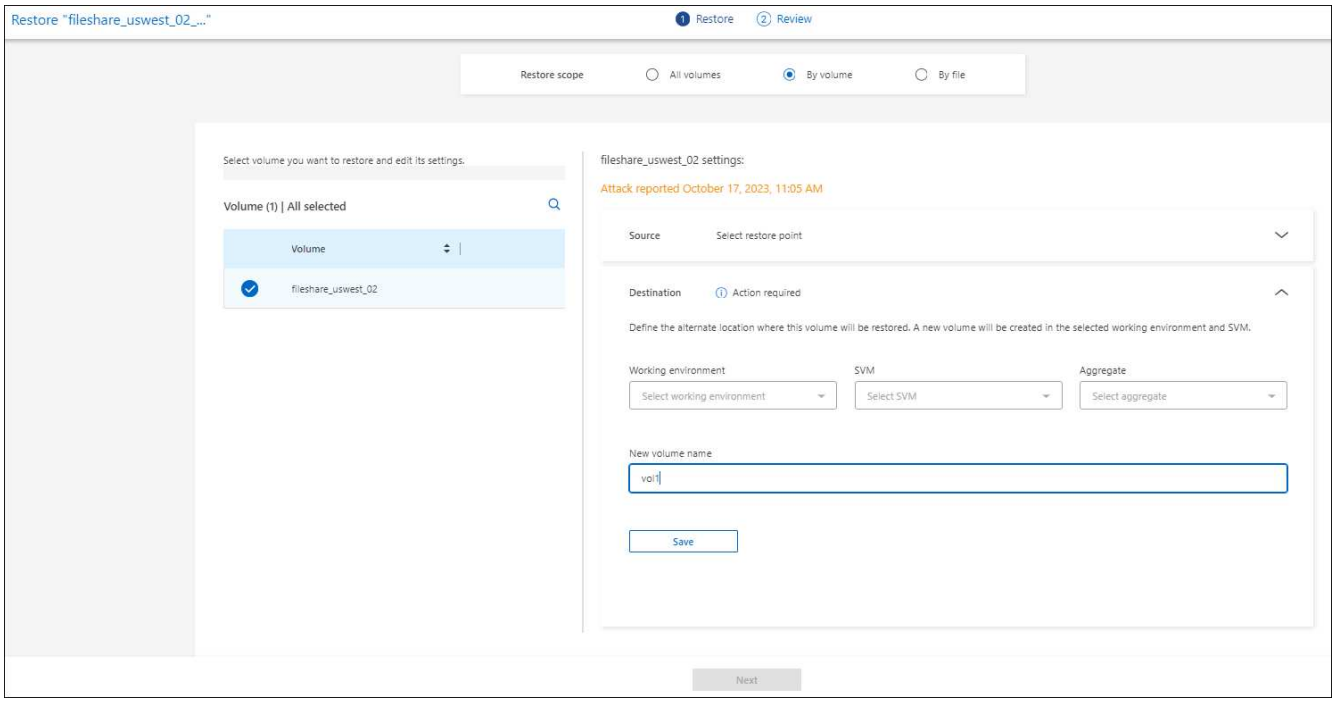
   b. Selezionare l'ambiente di lavoro.
   c. Selezionare la VM di storage.
   d. Facoltativamente, immettere il percorso.

      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.

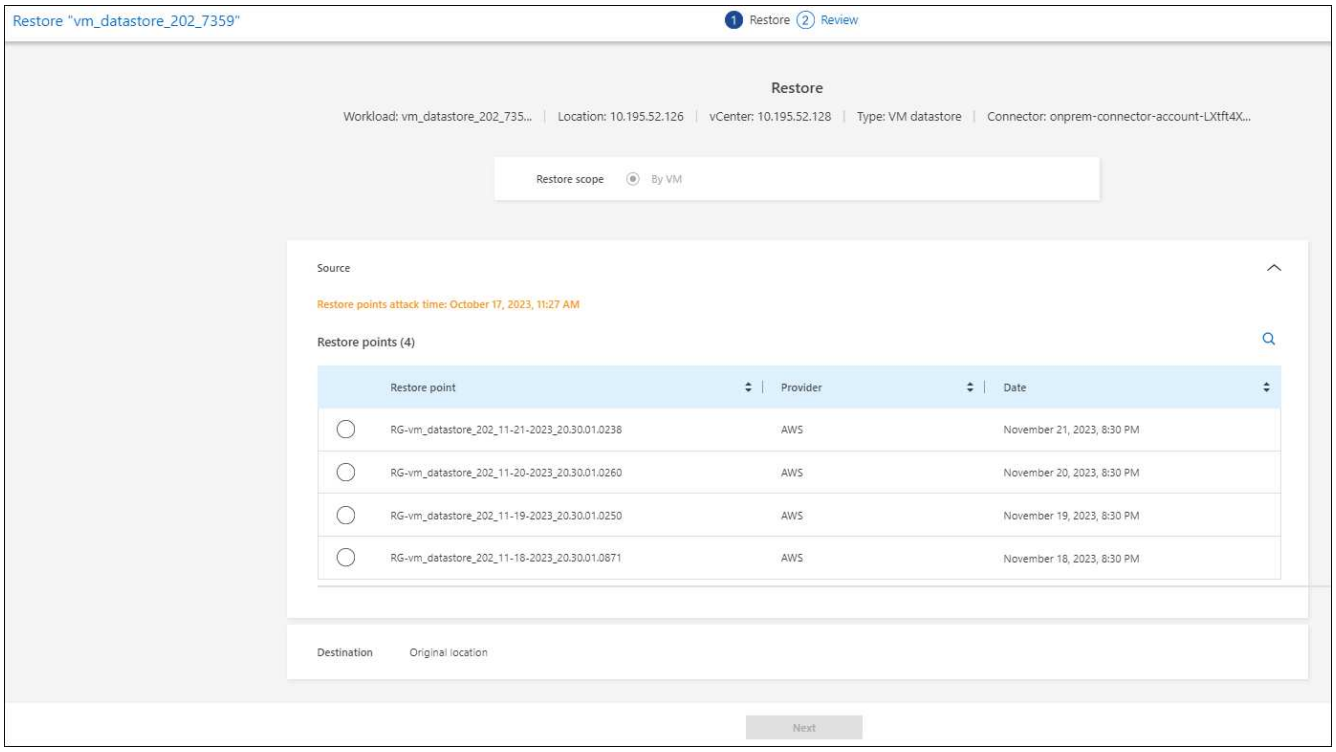
> Se non si specifica un percorso per il ripristino, i file verranno ripristinati in un nuovo volume nella directory di livello superiore.

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.

Conoscenza e supporto

Registrati per ricevere assistenza

È necessaria la registrazione del supporto per ricevere supporto tecnico specifico per BlueXP e le relative soluzioni e servizi storage. È inoltre necessaria la registrazione del supporto per abilitare i flussi di lavoro chiave per i sistemi Cloud Volumes ONTAP.

La registrazione per il supporto non attiva il supporto NetApp per un file service provider cloud. Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Panoramica sulla registrazione del supporto

Esistono due forme di registrazione per attivare i diritti di supporto:

- Registrazione dell'abbonamento al supporto per l'ID account BlueXP (il numero di serie a 20 cifre 960xxxxxxxxx nella pagina Support Resources di BlueXP).

  Questa funzione funge da unico ID di abbonamento al supporto per qualsiasi servizio all'interno di BlueXP. Ogni abbonamento al supporto a livello di account BlueXP deve essere registrato.

- Registrazione dei numeri di serie Cloud Volumes ONTAP associati a un abbonamento nel mercato del provider cloud (si tratta di numeri di serie 909201xxxxxxxx a 20 cifre).

  Questi numeri seriali sono comunemente denominati *numeri seriali PAYGO* e vengono generati da BlueXP al momento dell'implementazione di Cloud Volumes ONTAP.

La registrazione di entrambi i tipi di numeri di serie offre funzionalità come l'apertura di ticket di supporto e la generazione automatica dei casi. La registrazione viene completata aggiungendo account del sito di supporto NetApp a BlueXP come descritto di seguito.

Registrare l'account BlueXP per il supporto NetApp

Per registrarsi al supporto e attivare i diritti di supporto, un utente del proprio account BlueXP deve associare un account del sito di supporto NetApp al proprio account di accesso BlueXP. La modalità di registrazione al supporto NetApp dipende dal fatto che si disponga già di un account NetApp Support Site (NSS).

Cliente esistente con un account NSS

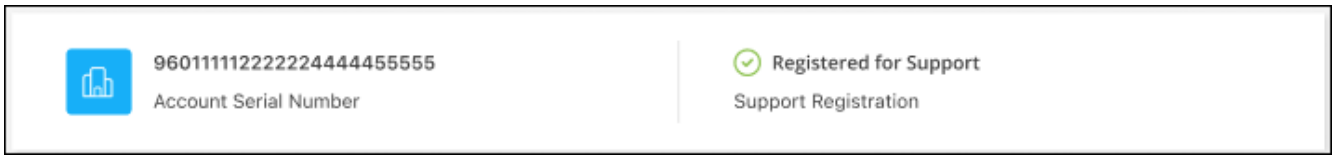
Se sei un cliente NetApp con un account NSS, devi semplicemente registrarti per ricevere supporto tramite BlueXP.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona Impostazioni e selezionare **credenziali**.

2. Selezionare **User Credentials** (credenziali utente).
3. Selezionare **Aggiungi credenziali NSS** e seguire la richiesta di autenticazione del sito di supporto NetApp.
4. Per confermare che la procedura di registrazione è stata eseguita correttamente, selezionare l'icona Guida e selezionare **supporto**.

   La pagina **risorse** dovrebbe mostrare che il tuo account è registrato per il supporto.



   Si noti che gli altri utenti di BlueXP non visualizzeranno lo stesso stato di registrazione del supporto se non hanno associato un account del sito di supporto NetApp al proprio login BlueXP. Tuttavia, ciò non significa che il tuo account BlueXP non sia registrato per il supporto. Se un utente dell'account ha seguito questa procedura, l'account è stato registrato.

Cliente esistente ma nessun account NSS

Se sei un cliente NetApp con licenze e numeri di serie esistenti ma *no* account NSS, devi creare un account NSS e associarlo al tuo login BlueXP.

Fasi

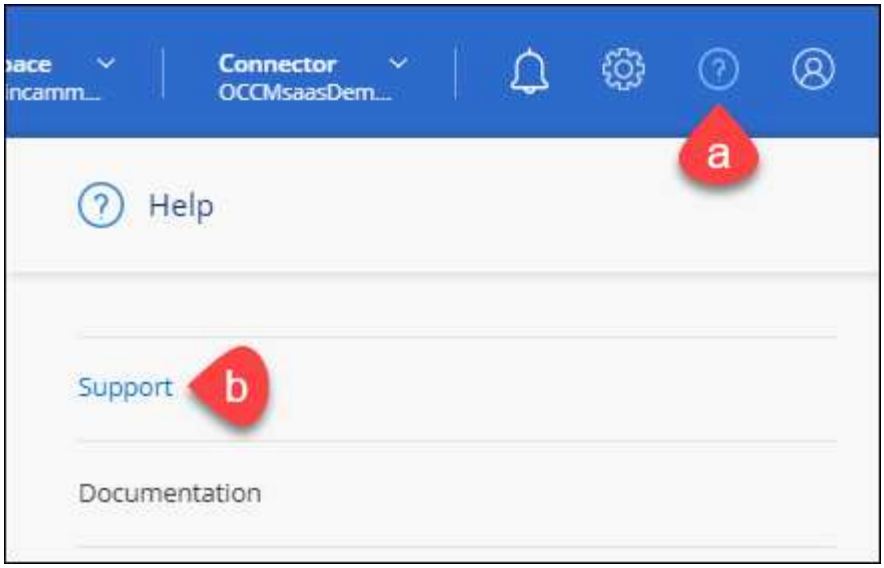
1. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account BlueXP (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.
2. Associare il nuovo account NSS al login BlueXP completando la procedura riportata sotto Cliente esistente con un account NSS.

Novità di NetApp

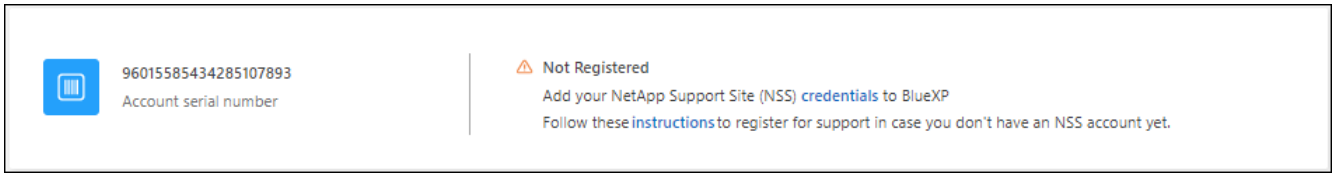
Se sei nuovo di NetApp e non disponi di un account NSS, segui i passaggi riportati di seguito.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Individuare il numero di serie dell'ID account nella pagina Support Registration (registrazione supporto).



3. Selezionare "Sito per la registrazione del supporto NetApp" E selezionare **non sono un cliente NetApp registrato**.
4. Compilare i campi obbligatori (con asterischi rossi).
5. Nel campo **Product Line**, selezionare **Cloud Manager**, quindi selezionare il provider di fatturazione appropriato.
6. Copia il numero di serie del tuo account dal punto 2 precedente, completa il controllo di sicurezza, quindi conferma di aver letto la Global Data Privacy Policy di NetApp.

   Viene immediatamente inviata un'e-mail alla casella di posta fornita per finalizzare questa transazione sicura. Controllare le cartelle di spam se l'e-mail di convalida non arriva in pochi minuti.

7. Confermare l'azione dall'interno dell'e-mail.

   La conferma invia la tua richiesta a NetApp e ti consiglia di creare un account NetApp Support Site.

8. Creare un account NetApp Support Site completando il "Modulo di registrazione per l'utente del sito di supporto NetApp"
   a. Assicurarsi di selezionare il livello utente appropriato, che in genere è **cliente/utente finale NetApp**.
   b. Assicurarsi di copiare il numero di serie dell'account (960xxxx) utilizzato in precedenza per il campo del numero di serie. In questo modo, l'elaborazione dell'account sarà più rapida.

Al termine

NetApp dovrebbe contattarti durante questo processo. Si tratta di un esercizio di assunzione per i nuovi utenti.

Una volta ottenuto l'account del sito di supporto NetApp, associare l'account al login BlueXP completando la procedura indicata in Cliente esistente con un account NSS.

Associare le credenziali NSS per il supporto Cloud Volumes ONTAP

Per attivare i seguenti flussi di lavoro chiave per Cloud Volumes ONTAP, è necessario associare le credenziali del sito di supporto NetApp all'account BlueXP:

- Registrazione dei sistemi Cloud Volumes ONTAP pay-as-you-go per il supporto

  È necessario fornire l'account NSS per attivare il supporto per il sistema e accedere alle risorse di supporto tecnico di NetApp.

- Implementazione di Cloud Volumes ONTAP con la propria licenza (BYOL)

  È necessario fornire l'account NSS in modo che BlueXP possa caricare la chiave di licenza e attivare l'abbonamento per il periodo di validità dell'acquisto. Sono inclusi gli aggiornamenti automatici per i rinnovi dei termini.

- Aggiornamento del software Cloud Volumes ONTAP alla versione più recente

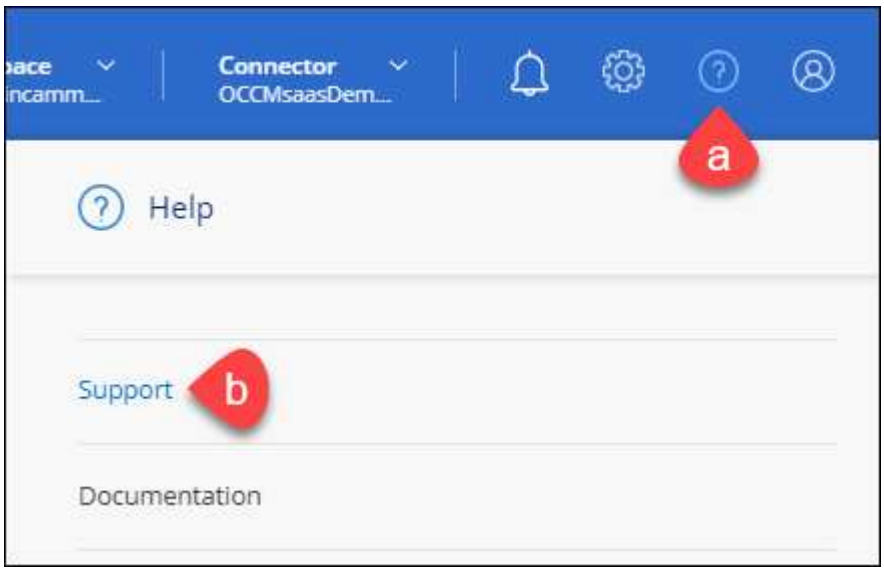
L'associazione delle credenziali NSS all'account BlueXP è diversa dall'account NSS associato a un account utente BlueXP.

Queste credenziali NSS sono associate all'ID account BlueXP specifico. Gli utenti che appartengono all'account BlueXP possono accedere a queste credenziali da **Support > NSS Management**.

- Se disponi di un account a livello di cliente, puoi aggiungere uno o più account NSS.
- Se disponi di un account partner o reseller, puoi aggiungere uno o più account NSS, ma non possono essere aggiunti insieme agli account a livello di cliente.

Fasi

1. Nella parte superiore destra della console BlueXP, selezionare l'icona della Guida e selezionare **supporto**.



2. Selezionare **Gestione NSS > Aggiungi account NSS**.
3. Quando richiesto, selezionare **continua** per essere reindirizzato a una pagina di accesso Microsoft.

   NetApp utilizza Microsoft Entra ID come provider di identità per i servizi di autenticazione specifici per il supporto e la licenza.

4. Nella pagina di accesso, fornire l'indirizzo e-mail e la password registrati del NetApp Support Site per eseguire il processo di autenticazione.

   Queste azioni consentono a BlueXP di utilizzare il tuo account NSS per download di licenze, verifica dell'aggiornamento software e registrazioni di supporto future.

   Tenere presente quanto segue:

   - L'account NSS deve essere un account a livello di cliente (non un account guest o temporaneo). Puoi avere più account NSS a livello di cliente.
   - Se si tratta di un account di livello partner, può essere presente un solo account NSS. Se si tenta di aggiungere account NSS a livello di cliente ed esiste un account a livello di partner, viene visualizzato il seguente messaggio di errore:

     "Il tipo di cliente NSS non è consentito per questo account, in quanto esistono già utenti NSS di tipo diverso."

   Lo stesso vale se si dispone di account NSS a livello di cliente preesistenti e si tenta di aggiungere un account a livello di partner.

   - Una volta effettuato l'accesso, NetApp memorizzerà il nome utente NSS.

     Si tratta di un ID generato dal sistema che viene mappato all'e-mail. Nella pagina **NSS Management**, è possibile visualizzare l'e-mail da ••• menu.

   - Se è necessario aggiornare i token delle credenziali di accesso, è disponibile anche l'opzione **Update Credentials** (Aggiorna credenziali) in ••• menu.

     Questa opzione richiede di effettuare nuovamente l'accesso. Il token per questi account scade dopo 90 giorni. Verrà inviata una notifica per avvisare l'utente.

Richiedi assistenza

NetApp fornisce supporto per BlueXP e i suoi servizi cloud in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un forum della community. La registrazione al supporto include il supporto tecnico remoto via web ticketing.

Ottieni supporto per un file service del cloud provider

Per supporto tecnico relativo a un file service di un cloud provider, alla sua infrastruttura o a una soluzione che utilizza il servizio, fare riferimento a "Guida in linea" nella documentazione BlueXP relativa a quel prodotto.

- "Amazon FSX per ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service per Google Cloud"

Per ricevere supporto tecnico specifico di BlueXP e delle relative soluzioni e servizi storage, utilizza le opzioni di supporto descritte di seguito.

Utilizzare le opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- Documentazione

  La documentazione BlueXP attualmente visualizzata.

- "Knowledge base"

  Cercare nella Knowledge base di BlueXP articoli utili per la risoluzione dei problemi.

- "Community"

  Unisciti alla community BlueXP per seguire le discussioni in corso o crearne di nuove.

Crea un caso con il supporto NetApp

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con uno specialista del supporto NetApp per risolvere eventuali problemi dopo l'attivazione del supporto.

Prima di iniziare

- Per utilizzare la funzione **creazione di un caso**, è necessario prima associare le credenziali del sito di supporto NetApp al login BlueXP. "Scopri come gestire le credenziali associate all'accesso a BlueXP".
- Se stai aprendo un caso per un sistema ONTAP con un numero di serie, il tuo account NSS deve essere associato al numero di serie di quel sistema.

Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Nella pagina **risorse**, scegliere una delle opzioni disponibili in supporto tecnico:

   a. Selezionare **Chiamateci** se si desidera parlare con qualcuno al telefono. Viene visualizzata una pagina su netapp.com che elenca i numeri di telefono che è possibile chiamare.

   b. Selezionare **Crea un caso** per aprire un ticket con uno specialista del supporto NetApp:

      - **Servizio**: Selezionare il servizio a cui è associato il problema. Ad esempio, BlueXP quando si tratta di un problema di supporto tecnico relativo a flussi di lavoro o funzionalità all'interno del servizio.
      - **Ambiente di lavoro**: Se applicabile allo storage, selezionare **Cloud Volumes ONTAP** o **on-premise** e quindi l'ambiente di lavoro associato.

        L'elenco degli ambienti di lavoro rientra nell'ambito dell'account, dell'area di lavoro e del connettore BlueXP selezionato nel banner superiore del servizio.

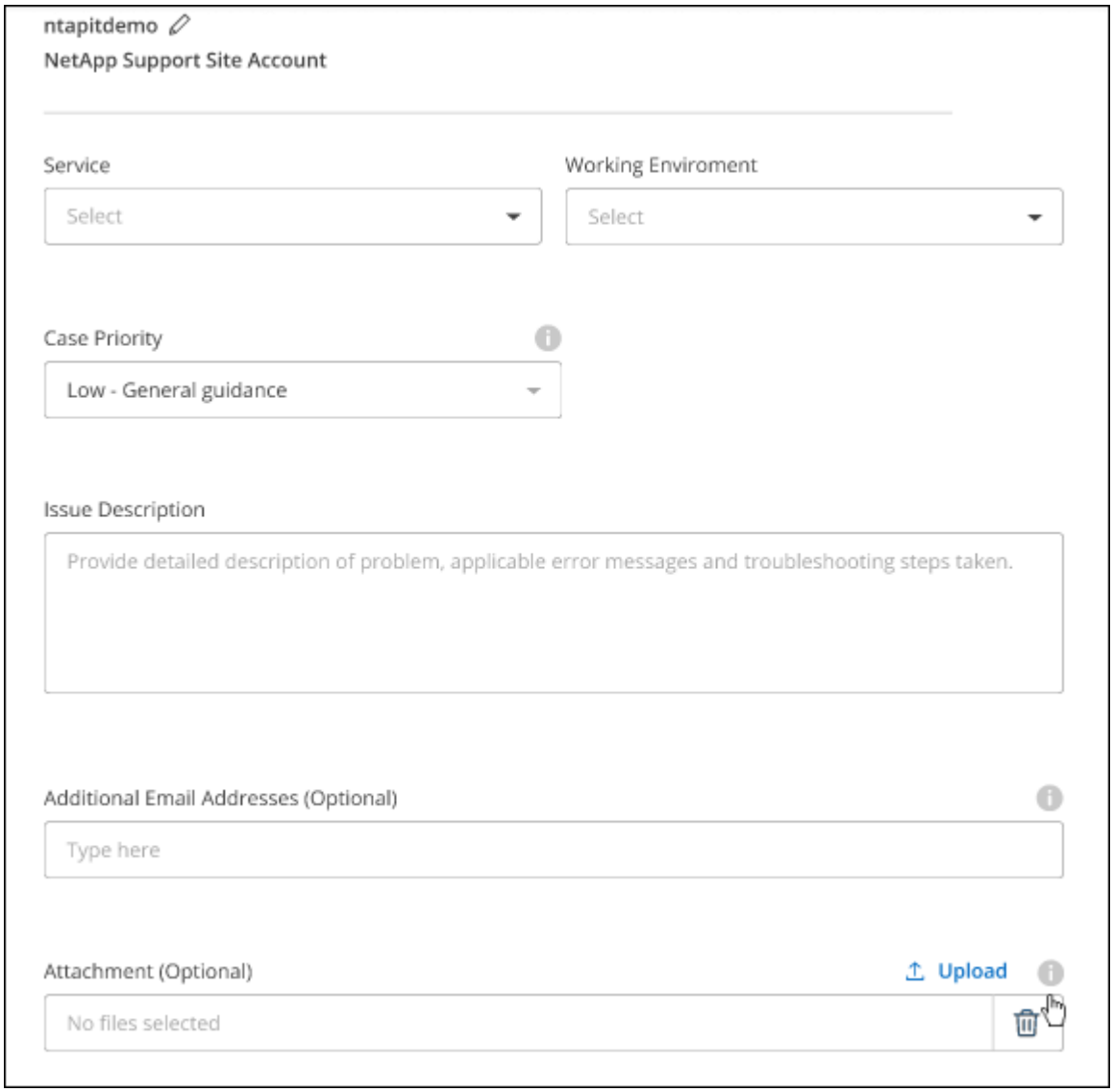
      - **Priorità caso**: Scegliere la priorità per il caso, che può essere bassa, Media, alta o critica.

        Per ulteriori informazioni su queste priorità, passare il mouse sull'icona delle informazioni accanto al nome del campo.

      - **Descrizione del problema**: Fornire una descrizione dettagliata del problema, inclusi eventuali messaggi di errore o procedure di risoluzione dei problemi che sono state eseguite.
      - **Indirizzi e-mail aggiuntivi**: Inserisci indirizzi e-mail aggiuntivi se desideri informare qualcun altro del problema.

- **Allegato (opzionale)**: Carica fino a cinque allegati, uno alla volta.

  Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Al termine

Viene visualizzata una finestra a comparsa con il numero del caso di supporto. Uno specialista del supporto NetApp esaminerà il tuo caso e ti contatterà al più presto.

Per una cronologia dei casi di supporto, selezionare **Impostazioni > Cronologia** e cercare le azioni denominate "Crea caso di supporto". Un pulsante all'estrema destra consente di espandere l'azione per visualizzare i dettagli.

È possibile che venga visualizzato il seguente messaggio di errore quando si tenta di creare un caso:

"Non sei autorizzato a creare un caso per il servizio selezionato"

Questo errore potrebbe indicare che l'account NSS e la società di registrazione a cui è associato non sono la stessa società di registrazione per il numero di serie dell'account BlueXP (ad es. 960xxxx) o il numero di serie dell'ambiente di lavoro. È possibile richiedere assistenza utilizzando una delle seguenti opzioni:

- Utilizza la chat integrata nel prodotto
- Inviare un caso non tecnico all'indirizzo https://mysupport.netapp.com/site/help

Gestire i casi di supporto (anteprima)

È possibile visualizzare e gestire i casi di supporto attivi e risolti direttamente da BlueXP. Puoi gestire i casi associati al tuo account NSS e alla tua azienda.

La gestione del caso è disponibile come anteprima. Intendiamo perfezionare questa esperienza e aggiungere miglioramenti alle prossime release. Inviaci un feedback utilizzando la chat in-product.

Tenere presente quanto segue:

- La dashboard di gestione dei casi nella parte superiore della pagina offre due visualizzazioni:
  - La vista a sinistra mostra il totale dei casi aperti negli ultimi 3 mesi dall'account NSS dell'utente fornito.
  - La vista a destra mostra il totale dei casi aperti negli ultimi 3 mesi a livello aziendale in base all'account NSS dell'utente.

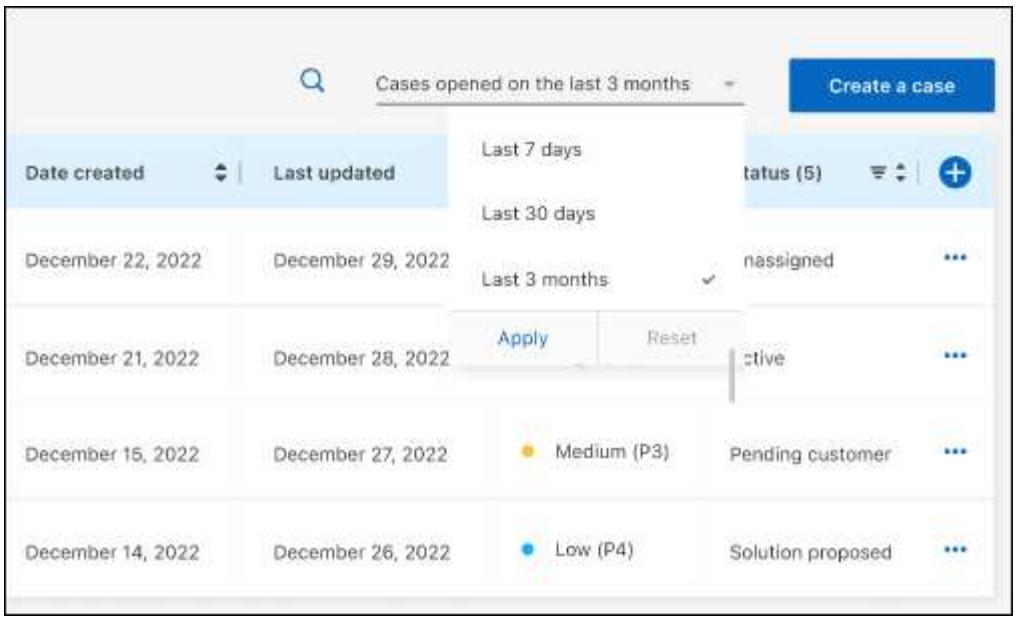
  I risultati della tabella riflettono i casi correlati alla vista selezionata.
- È possibile aggiungere o rimuovere colonne di interesse e filtrare il contenuto di colonne come priorità e Stato. Altre colonne offrono funzionalità di ordinamento.

  Per ulteriori informazioni, consulta la procedura riportata di seguito.
- A livello di caso, offriamo la possibilità di aggiornare le note del caso o chiudere un caso che non è già in stato chiuso o in attesa di chiusura.

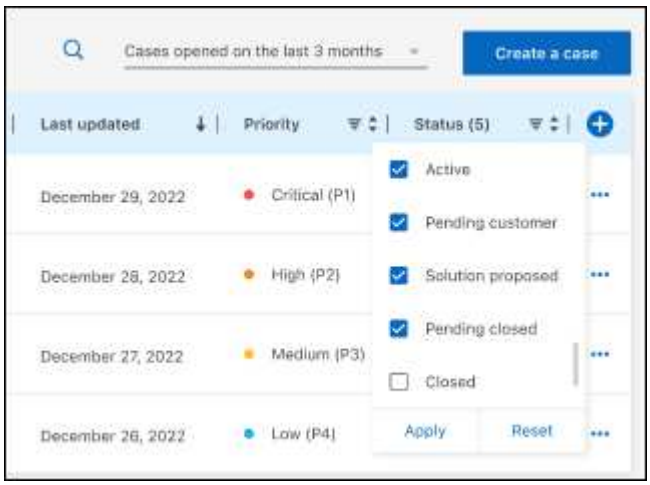
Fasi

1. In BlueXP, selezionare **Guida > supporto**.
2. Selezionare **Gestione casi** e, se richiesto, aggiungere l'account NSS a BlueXP.

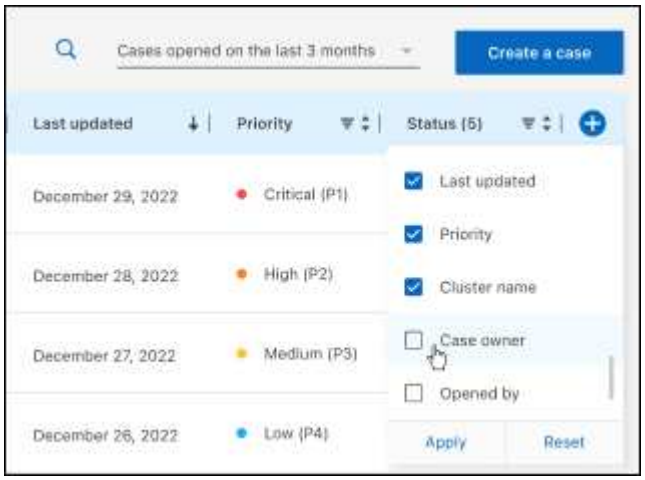
   La pagina **Gestione del caso** mostra i casi aperti relativi all'account NSS associato all'account utente BlueXP. Si tratta dello stesso account NSS visualizzato nella parte superiore della pagina **gestione NSS**.
3. Se si desidera, modificare le informazioni visualizzate nella tabella:
   - In **Organization's Cases** (casi dell'organizzazione), selezionare **View** (Visualizza) per visualizzare tutti i casi associati alla società.
   - Modificare l'intervallo di date scegliendo un intervallo di date esatto o scegliendo un intervallo di tempo diverso.



- Filtrare il contenuto delle colonne.



- Modificare le colonne visualizzate nella tabella selezionando e quindi scegliere le colonne che si desidera visualizzare.

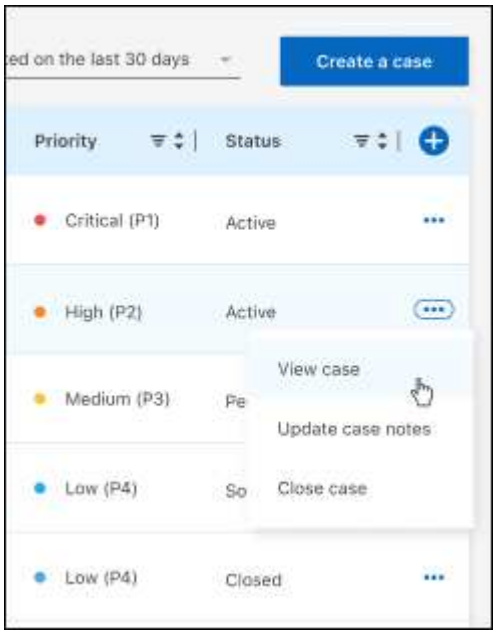


4. Gestire un caso esistente selezionando ••• e selezionando una delle opzioni disponibili:

   - **Visualizza caso**: Visualizza tutti i dettagli relativi a un caso specifico.
   - **Aggiorna note sul caso**: Fornisci ulteriori dettagli sul problema oppure seleziona **carica file** per allegare fino a un massimo di cinque file.

     Gli allegati sono limitati a 25 MB per file. Sono supportate le seguenti estensioni di file: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

   - **Chiudi caso**: Fornisci i dettagli sul motivo per cui stai chiudendo il caso e seleziona **Chiudi caso**.



Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per BlueXP"