Inizia subito

BlueXP classification

NetApp
August 11, 2025

Sommario

Inizia subito

Scopri di più sulla classificazione BlueXP

La classificazione BlueXP (Cloud Data Sense) è un servizio di governance dei dati per BlueXP che analizza le origini dati on-premise e cloud aziendali per mappare e classificare i dati e identificare informazioni private. In questo modo è possibile ridurre i rischi di sicurezza e conformità, ridurre i costi di storage e assistere i progetti di migrazione dei dati.

A partire dalla versione 1,31, la classificazione BlueXP è disponibile come funzionalità di base con BlueXP . Non sono previsti costi aggiuntivi. Non è richiesta alcuna licenza di classificazione o abbonamento. + se si utilizza la versione legacy 1,30 o precedente, tale versione è disponibile fino alla scadenza dell'abbonamento. "Vedere un elenco delle funzioni obsolete".

Caratteristiche

La classificazione BlueXP utilizza l'intelligenza artificiale (ai), l'elaborazione del linguaggio naturale (NLP) e l'apprendimento automatico (ML) per comprendere il contenuto che esegue la scansione al fine di estrarre le entità e classificare il contenuto di conseguenza. Ciò consente alla classificazione BlueXP di fornire le seguenti aree di funzionalità.

"Scopri di più sui casi di utilizzo per la classificazione BlueXP".

Mantenere la conformità

La classificazione BlueXP offre diversi strumenti che possono aiutare a soddisfare le tue esigenze di conformità. È possibile utilizzare la classificazione BlueXP per:

- Identificare le informazioni personali identificabili (PII).
- Identificare un'ampia gamma di informazioni personali sensibili come richiesto dalle normative sulla privacy GDPR, CCPA, PCI e HIPAA.
- Rispondere alle richieste di accesso dei soggetti dati (DSAR) in base al nome o all'indirizzo e-mail.

Rafforzare la sicurezza

La classificazione BlueXP è in grado di identificare i dati potenzialmente a rischio per l'accesso a scopi criminali. È possibile utilizzare la classificazione BlueXP per:

- Identificare tutti i file e le directory (condivisioni e cartelle) con autorizzazioni aperte che sono esposte all'intera organizzazione o al pubblico.
- Identificare i dati sensibili che risiedono al di fuori della posizione iniziale dedicata.
- Rispettare le policy di conservazione dei dati.
- Utilizzare *Policies* per rilevare automaticamente i nuovi problemi di sicurezza, in modo che il personale addetto alla sicurezza possa intervenire immediatamente.

Ottimizzare l'utilizzo dello storage

La classificazione BlueXP offre strumenti che possono aiutare con il TCO (Total Cost of Ownership) dello storage. È possibile utilizzare la classificazione BlueXP per:

- Aumenta l'efficienza dello storage identificando dati duplicati o non correlati al business.
- Risparmia i costi dello storage identificando i dati inattivi che puoi tierare per uno storage a oggetti meno costoso. "Scopri di più sul tiering dei sistemi Cloud Volumes ONTAP". "Scopri di più sul tiering dei sistemi ONTAP on-premise".

Ambienti di lavoro e origini dati supportati

La classificazione BlueXP può analizzare e analizzare dati strutturati e non strutturati provenienti dai seguenti tipi di ambienti di lavoro e origini dati:

Ambienti di lavoro

- Amazon FSX per ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP (implementato in AWS, Azure o GCP)
- Cluster ONTAP on-premise
- StorageGRID

Origini dati

- Condivisioni di file NetApp
- Database:
  - Amazon Relational Database Service (Amazon RDS)
  - MongoDB
  - MySQL
  - Oracle
  - PostgreSQL
  - SAP HANA
  - SQL Server (MSSQL)

La classificazione BlueXP supporta le versioni NFS 3.x, 4.0 e 4.1 e CIFS 1.x, 2.0, 2.1 e 3.0.

Costo

La classificazione BlueXP è gratuita. Non è richiesta alcuna licenza di classificazione o abbonamento a pagamento.

Costi delle infrastrutture

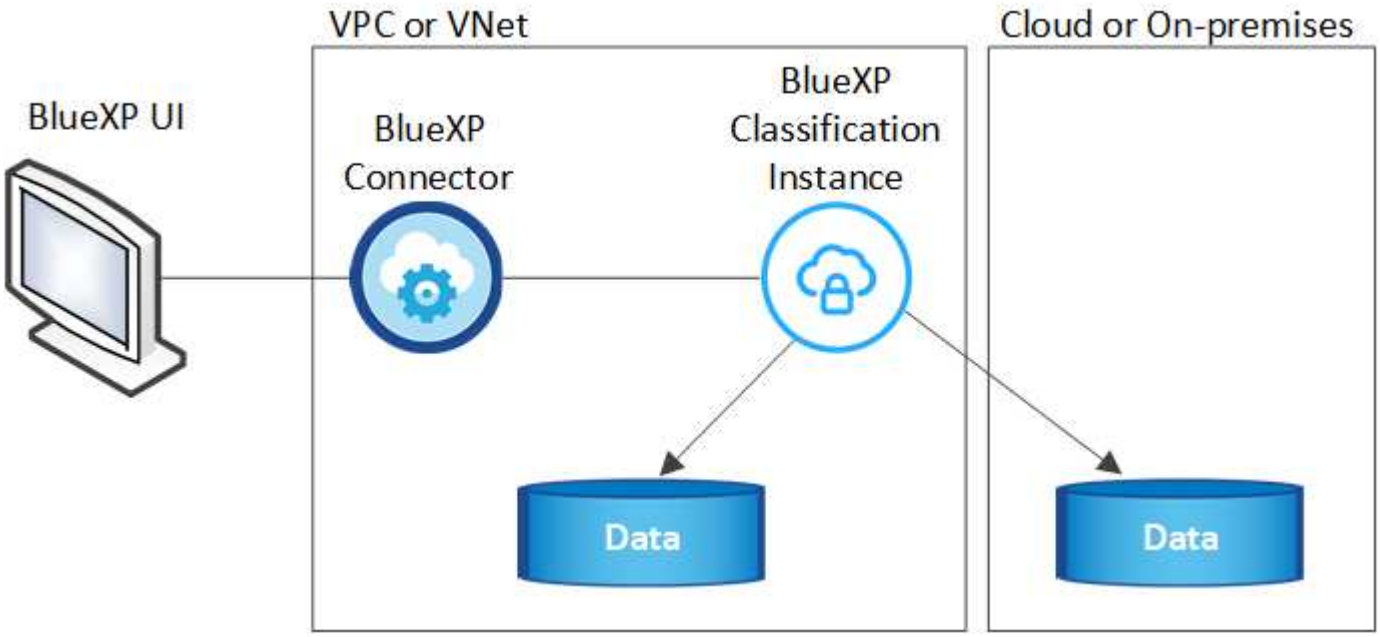
- L'installazione della classificazione BlueXP nel cloud richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del provider di cloud in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider. L'installazione della classificazione BlueXP su un sistema on-premise non richiede alcun costo.
- La classificazione BlueXP richiede l'implementazione di un connettore BlueXP. In molti casi si dispone già di un connettore a causa di altri servizi e storage utilizzati in BlueXP. L'istanza del connettore comporta addebiti da parte del cloud provider in cui viene implementata. Vedere "tipo di istanza implementata per ciascun cloud provider". L'installazione del connettore su un sistema on-premise non richiede alcun costo.

Costi di trasferimento dei dati

I costi di trasferimento dei dati dipendono dalla configurazione. Se l'istanza di classificazione BlueXP e l'origine dati si trovano nella stessa zona di disponibilità e nella stessa regione, non ci sono costi di trasferimento dei dati. Ma se l'origine dei dati, ad esempio un sistema Cloud Volumes ONTAP, si trova in una zona o regione di disponibilità *diversa*, i costi di trasferimento dei dati verranno addebitati dal provider cloud. Per ulteriori informazioni, consulta i seguenti xref:./* "AWS: Prezzi di Amazon Elastic Compute Cloud (Amazon EC2)" * "Microsoft Azure: Dettagli sui prezzi della larghezza di banda" * "Google Cloud: Prezzi del servizio di trasferimento dello storage"

L'istanza di classificazione BlueXP

Quando si implementa la classificazione BlueXP nel cloud, BlueXP implementa l'istanza nella stessa sottorete del connettore. "Scopri di più sui connettori."



Tenere presente quanto segue sull'istanza predefinita:

- In AWS, la classificazione BlueXP viene eseguita su un "m6i.4xlarge instance" Con un disco GP2 da 500 GiB. L'immagine del sistema operativo è Amazon Linux 2. Una volta implementato in AWS, è possibile scegliere una dimensione di istanza inferiore se si esegue la scansione di una piccola quantità di dati.
- In Azure, la classificazione BlueXP viene eseguita su a "Standard_D16s_v3 VM" con un disco da 500 GiB. L'immagine del sistema operativo è Ubuntu 22,04.
- Nella GCP, la classificazione BlueXP viene eseguita su un "n2-standard-16 VM" con un disco persistente standard GiB 500. L'immagine del sistema operativo è Ubuntu 22,04.
- Nelle regioni in cui l'istanza predefinita non è disponibile, la classificazione BlueXP viene eseguita su un'istanza alternativa. "Vedere i tipi di istanza alternativi".
- L'istanza è denominata *CloudCompliance* con un hash generato (UUID) concatenato ad essa. Ad esempio: *CloudCompliance-16b6564-38ad-4080-9a92-36f5fd2f71c7*
- Per ogni connettore viene implementata una sola istanza di classificazione BlueXP.

Puoi anche implementare la classificazione BlueXP su un host Linux on-premise o su un host nel tuo cloud provider preferito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di

installazione scelto. Gli aggiornamenti del software di classificazione BlueXP sono automatizzati finché l'istanza ha accesso a Internet.

L'istanza deve rimanere sempre in esecuzione perché la classificazione BlueXP esegue continuamente la scansione dei dati.

Distribuire su diversi tipi di istanza

Esaminare le seguenti specifiche per i tipi di istanza:

Dimensioni del sistema	Specifiche	Limitazioni
Extra large	32 CPU, 128 GB di RAM, 1 TiB SSD	Scansione di fino a 500 milioni di file.
Grande (impostazione predefinita)	16 CPU, 64 GB di RAM, SSD da 500 GiB	Scansione di fino a 250 milioni di file.

Quando implementi la classificazione BlueXP in Azure o GCP, invia un'email ng-contact-data-sense@netapp.com per assistenza se desideri utilizzare un tipo di istanza più piccolo.

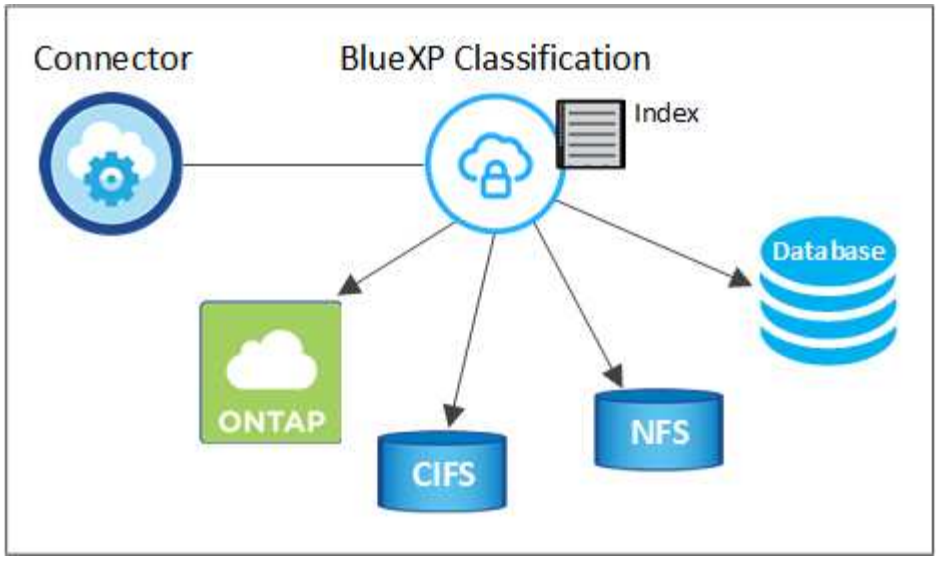
Come funziona la scansione della classificazione BlueXP

A un livello elevato, la scansione di classificazione BlueXP funziona come segue:

1. Si implementa un'istanza della classificazione BlueXP in BlueXP.
2. È possibile abilitare la mappatura di alto livello (denominata *Mapping only* Scans) o la scansione di alto livello (denominata *Map & Classify* Scans) su una o più origini dati.
3. La classificazione BlueXP esegue la scansione dei dati utilizzando un processo di apprendimento ai.
4. Utilizza le dashboard e i tool di reporting forniti per aiutarti nelle tue attività di compliance e governance.

Una volta attivata la classificazione BlueXP e selezionati i repository da analizzare (volumi, schemi di database o altri dati utente), viene avviata immediatamente la scansione dei dati per identificare i dati personali e sensibili. Nella maggior parte dei casi, è consigliabile concentrarsi sulla scansione dei dati di produzione in tempo reale anziché su backup, mirror o siti DR. Quindi, la classificazione BlueXP mappa i dati dell'organizzazione, categorizza ogni file e identifica ed estrae entità e modelli predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili, categorie di dati e tipi di file.

La classificazione BlueXP si connette ai dati come qualsiasi altro client montando volumi NFS e CIFS. Ai volumi NFS viene automaticamente eseguito l'accesso in sola lettura, mentre è necessario fornire le credenziali Active Directory per eseguire la scansione dei volumi CIFS.



Dopo la scansione iniziale, la classificazione BlueXP esegue la scansione continua dei dati in modo round robin per rilevare le modifiche incrementali. Per questo motivo è importante mantenere in esecuzione l'istanza.

È possibile abilitare e disabilitare le scansioni a livello di volume o a livello di schema del database.

La BlueXP classification non impone limiti alla quantità di dati che può analizzare. Ogni connettore supporta la scansione e la visualizzazione di 500 TiB di dati. Per analizzare più di 500 TiB di dati, "installare un altro connettore" Poi "distribuire un'altra istanza di classificazione" . + L'interfaccia utente BlueXP visualizza i dati di un singolo connettore. Per suggerimenti sulla visualizzazione dei dati di più connettori, vedere "Utilizzare più connettori" .

Qual è la differenza tra le scansioni di mappatura e classificazione

È possibile eseguire due tipi di scansioni nella classificazione BlueXP :

- **Le scansioni solo mappatura** forniscono solo una panoramica di alto livello dei vostri dati e vengono eseguite su origini dati selezionate. Le scansioni di sola mappatura richiedono meno tempo delle scansioni di mappatura e classificazione perché non accedono ai file per visualizzare i dati al loro interno. Si consiglia di eseguire questa operazione inizialmente per identificare le aree di ricerca e quindi eseguire una scansione Map & Classify su tali aree.
- **Le scansioni Map & Classify** forniscono una scansione profonda dei vostri dati.

Per informazioni dettagliate sulle differenze tra le scansioni Mapping e Classification, vedere "Qual è la differenza tra le scansioni di mappatura e classificazione?".

Informazioni classificate dalla classificazione BlueXP

La classificazione BlueXP raccoglie, indicizza e assegna categorie ai seguenti dati:

- **Metadati standard** sui file: Il tipo di file, le sue dimensioni, le date di creazione e modifica, e così via.
- **Dati personali**: Informazioni personali identificabili (PII) quali indirizzi e-mail, numeri di identificazione o numeri di carta di credito, che la classificazione BlueXP identifica utilizzando parole, stringhe e modelli specifici nei file. "Scopri di più sui dati personali".
- **Dati personali sensibili**: Tipi speciali di dati personali sensibili (SPII), quali dati sanitari, origine etnica o opinioni politiche, come definito dal regolamento generale sulla protezione dei dati (GDPR) e da altre

normative sulla privacy. "Scopri di più sui dati personali sensibili".

- **Categorie**: La classificazione BlueXP prende i dati sottoposti a scansione e li divide in diversi tipi di categorie. Le categorie sono argomenti basati sull'analisi ai del contenuto e dei metadati di ciascun file. "Scopri di più sulle categorie".
- **Tipi**: La classificazione BlueXP prende i dati sottoposti a scansione e li suddivide in base al tipo di file. "Scopri di più sui tipi".
- **Riconoscimento delle entità dei nomi**: La classificazione BlueXP utilizza l'intelligenza artificiale per estrarre i nomi naturali delle persone dai documenti. "Scopri come rispondere alle richieste di accesso ai soggetti dati".

Panoramica delle reti

La classificazione BlueXP implementa un singolo server, o cluster, ovunque tu scelga, nel cloud o on-premise. I server si connettono alle origini dati tramite protocolli standard e indicizzano i risultati in un cluster Elasticsearch, anch'esso distribuito sugli stessi server. In questo modo è possibile supportare ambienti multicloud, multicloud, cloud privato e on-premise.

BlueXP implementa l'istanza di classificazione BlueXP con un gruppo di protezione che abilita le connessioni HTTP in entrata dall'istanza del connettore.

Quando si utilizza BlueXP in modalità SaaS, la connessione a BlueXP viene fornita tramite HTTPS e i dati privati inviati tra il browser e l'istanza di classificazione BlueXP vengono protetti con la crittografia end-to-end tramite TLS 1,2, il che significa che NetApp e terze parti non possono leggerli.

Le regole in uscita sono completamente aperte. L'accesso a Internet è necessario per installare e aggiornare il software di classificazione BlueXP e per inviare metriche di utilizzo.

Se hai requisiti di rete rigorosi, "Scopri gli endpoint che BlueXP classifica a contatto con".

Accedi BlueXP classification

È possibile accedere al servizio BlueXP classification tramite NetApp BlueXP.

Per accedere a BlueXP, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per un accesso cloud NetApp utilizzando il tuo indirizzo email e una password. "Scopri di più sull'accesso a BlueXP".

Attività specifiche richiedono ruoli utente BlueXP specifici. "Scopri i ruoli di accesso BlueXP per tutti i servizi".

Prima di iniziare

- "Dovresti aggiungere un connettore BlueXP ."
- "Scopri quale stile di distribuzione BlueXP classification è più adatto al tuo carico di lavoro."

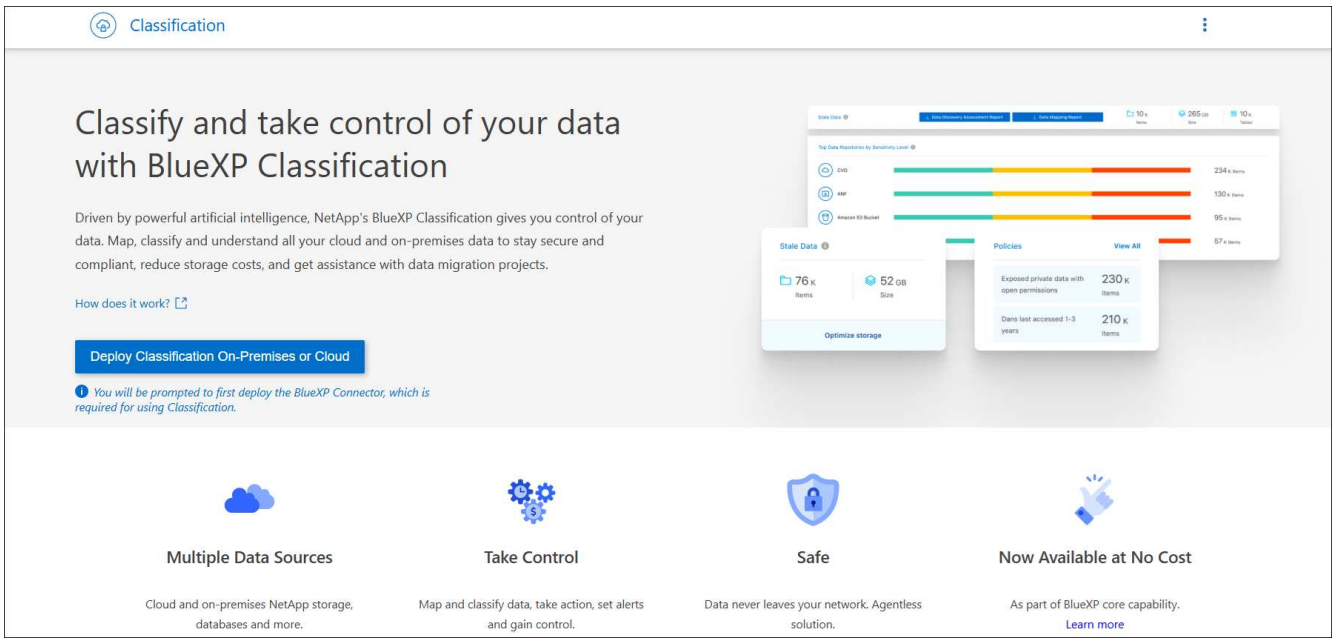
Fasi

1. In un browser web, vai a "Console BlueXP" .

   Viene visualizzata la pagina di accesso a NetApp BlueXP.

2. Sign in a BlueXP.
3. Dal menu di navigazione a sinistra BlueXP , seleziona **Governance** > **Classificazione**.
4. Se è la prima volta che accedi BlueXP classification, verrà visualizzata la pagina di destinazione.

Seleziona **Distribuisci classificazione in locale o nel cloud** per iniziare a distribuire la tua istanza di classificazione. Per ulteriori informazioni, vedere "Quale implementazione della classificazione BlueXP dovresti utilizzare?"



In caso contrario, viene visualizzata la Dashboard BlueXP classification .

Implementare la classificazione BlueXP

Quale implementazione della classificazione BlueXP dovresti utilizzare?

Puoi implementare la classificazione BlueXP in modi diversi. Scopri quale metodo soddisfa le tue esigenze.

La classificazione BlueXP può essere implementata nei seguenti modi:

- "Implementazione nel cloud con BlueXP". BlueXP implementerà l'istanza di classificazione BlueXP nella stessa rete di provider cloud del connettore BlueXP.
- "Installazione su un host Linux con accesso a Internet". Installare la classificazione BlueXP su un host Linux nella rete o su un host Linux nel cloud che dispone di accesso a Internet. Questo tipo di installazione può essere una buona opzione se preferisci analizzare i sistemi ONTAP in loco utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma non è un requisito.
- "Installazione su un host Linux in un sito locale senza accesso a Internet", Nota anche come *private mode.* questo tipo di installazione, che utilizza uno script di installazione, non ha connettività al livello SaaS di BlueXP .

Sia l'installazione su un host Linux con accesso a Internet che l'installazione in loco su un host Linux senza accesso a Internet utilizzano uno script di installazione. Lo script inizia controllando se il sistema e l'ambiente soddisfano i prerequisiti. Se i prerequisiti vengono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti.

Fare riferimento a. "Verificare che l'host Linux sia pronto per installare la classificazione BlueXP".

Implementare la classificazione BlueXP nel cloud utilizzando BlueXP

Completare alcuni passaggi per implementare la classificazione BlueXP nel cloud. BlueXP implementerà l'istanza di classificazione BlueXP nella stessa rete di provider cloud del connettore BlueXP.

Nota: È anche possibile "Installare la classificazione BlueXP su un host Linux con accesso a Internet". Questo tipo di installazione può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP on-premise utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.

Creare un connettore

Se non si dispone già di un connettore, crearne uno. Vedere "Creazione di un connettore in AWS", "Creazione di un connettore in Azure", o. "Creazione di un connettore in GCP".

Puoi anche farlo "Installare il connettore on-premise" Su un host Linux nella rete o su un host Linux nel cloud.

Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti. Ciò include l'accesso a Internet in uscita per l'istanza, la connettività tra il connettore e la classificazione BlueXP sulla porta 443 e altro ancora. Consulta l'elenco completo.

Implementare la classificazione BlueXP

Avviare l'installazione guidata per implementare l'istanza di classificazione BlueXP nel cloud.

Creare un connettore

Se non disponi già di un connettore, crea un connettore nel tuo cloud provider. Vedere "Creazione di un connettore in AWS" oppure "Creazione di un connettore in Azure", o. "Creazione di un connettore in GCP". Nella maggior parte dei casi, probabilmente si dispone di un connettore configurato prima di tentare di attivare la classificazione BlueXP, perché la maggior parte "Le funzionalità di BlueXP richiedono un connettore", ma in alcuni casi è necessario impostarne uno ora.

Esistono alcuni scenari in cui è necessario utilizzare un connettore implementato in uno specifico cloud provider:

- Quando esegui la scansione dei dati in Cloud Volumes ONTAP in AWS o in un bucket Amazon FSX per ONTAP, utilizzi un connettore in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un connettore in Azure.
    - Per Azure NetApp Files, deve essere implementato nella stessa regione dei volumi che si desidera

sottoporre a scansione.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un connettore in GCP.

È possibile eseguire la scansione dei sistemi ONTAP on-premise, delle condivisioni di file NetApp e dei database utilizzando uno di questi connettori cloud.

Nota: È anche possibile "Installare il connettore on-premise" Su un host Linux nella rete o nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Come puoi vedere, potrebbero esserci alcune situazioni in cui devi utilizzare "Connettori multipli".

La BlueXP classification non impone limiti alla quantità di dati che può analizzare. Ogni connettore supporta la scansione e la visualizzazione di 500 TiB di dati. Per analizzare più di 500 TiB di dati, "installare un altro connettore" Poi "distribuire un'altra istanza di classificazione" . + L'interfaccia utente BlueXP visualizza i dati di un singolo connettore. Per suggerimenti sulla visualizzazione dei dati di più connettori, vedere "Utilizzare più connettori" .

Supporto per le regioni governative

La classificazione BlueXP è supportata quando il connettore viene implementato in un'area governativa (AWS GovCloud, Azure Gov o Azure DoD). Se implementato in questo modo, la classificazione BlueXP presenta le seguenti restrizioni:

"Ulteriori informazioni sull'implementazione del connettore in un'area pubblica".

Esaminare i prerequisiti

Esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata prima di implementare la classificazione BlueXP nel cloud. Quando si implementa la classificazione BlueXP nel cloud, si trova nella stessa subnet del connettore.

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint. Il proxy deve essere non trasparente. I proxy trasparenti non sono attualmente supportati.

Esaminare la tabella appropriata riportata di seguito a seconda che si stia implementando la classificazione BlueXP in AWS, Azure o GCP.

Endpoint richiesti per AWS

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce l'accesso a immagini, manifesti e modelli software.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	Abilita la classificazione BlueXP per accedere e scaricare manifesti e modelli e per inviare registri e metriche.

Endpoint richiesti per Azure

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.

Endpoint richiesti per GCP

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.

Endpoint	Scopo
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.

Assicurarsi che BlueXP disponga delle autorizzazioni necessarie

Assicurarsi che BlueXP disponga delle autorizzazioni per distribuire risorse e creare gruppi di sicurezza per l'istanza BlueXP classification .

- "Autorizzazioni di Google Cloud"
- "Autorizzazioni AWS"
- "Autorizzazioni di Azure"

Assicurarsi che BlueXP Connector possa accedere alla classificazione BlueXP

Garantire la connettività tra il connettore e l'istanza di classificazione BlueXP. Il gruppo di protezione per il connettore deve consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Questa connessione consente l'implementazione dell'istanza di classificazione BlueXP e consente di visualizzare le informazioni nelle schede Compliance e Governance. La classificazione BlueXP è supportata nelle regioni governative di AWS e Azure.

Per le implementazioni di AWS e AWS GovCloud sono richieste regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per il connettore in AWS" per ulteriori informazioni.

Per le implementazioni di Azure e Azure Government sono richieste regole aggiuntive per i gruppi di sicurezza in entrata e in uscita. Vedere "Regole per il connettore in Azure" per ulteriori informazioni.

Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP

L'istanza di classificazione BlueXP deve rimanere attiva per eseguire una scansione continua dei dati.

Garantire la connettività del browser Web alla classificazione BlueXP

Una volta attivata la classificazione BlueXP, assicurarsi che gli utenti accedano all'interfaccia BlueXP da un host che dispone di una connessione all'istanza di classificazione BlueXP.

L'istanza di classificazione BlueXP utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili a Internet. Di conseguenza, il browser Web utilizzato per accedere a BlueXP deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da una connessione diretta al provider cloud (ad esempio, una VPN) o da un host all'interno della stessa rete dell'istanza di classificazione BlueXP.

Controllare i limiti della vCPU

Assicurati che il limite vCPU del tuo cloud provider consenta l'implementazione di un'istanza con il numero necessario di core. È necessario verificare il limite vCPU per la famiglia di istanze pertinente nella regione in cui è in esecuzione BlueXP. "Vedere i tipi di istanza richiesti".

Per ulteriori informazioni sui limiti delle vCPU, consultare i seguenti collegamenti:

- "Documentazione AWS: Quote di servizio Amazon EC2"
- "Documentazione di Azure: Quote vCPU delle macchine virtuali"
- "Documentazione di Google Cloud: Quote delle risorse"

Implementare la classificazione BlueXP nel cloud

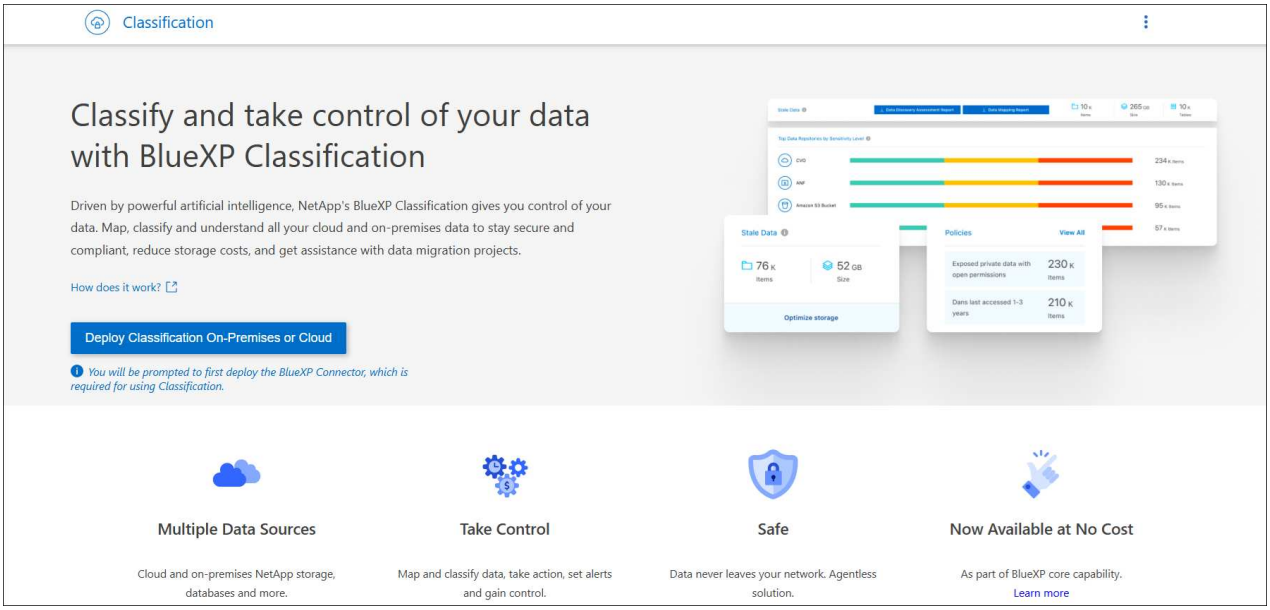
Seguire questi passaggi per implementare un'istanza della classificazione BlueXP nel cloud. Il connettore implementerà l'istanza nel cloud, quindi installerà il software di classificazione BlueXP su tale istanza.

Nelle regioni in cui il tipo di istanza predefinito non è disponibile, la classificazione BlueXP viene eseguita su un "tipo di istanza alternativo".

Implementazione in AWS

Fasi

1. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Distribuisci classificazione in locale o nel cloud**.



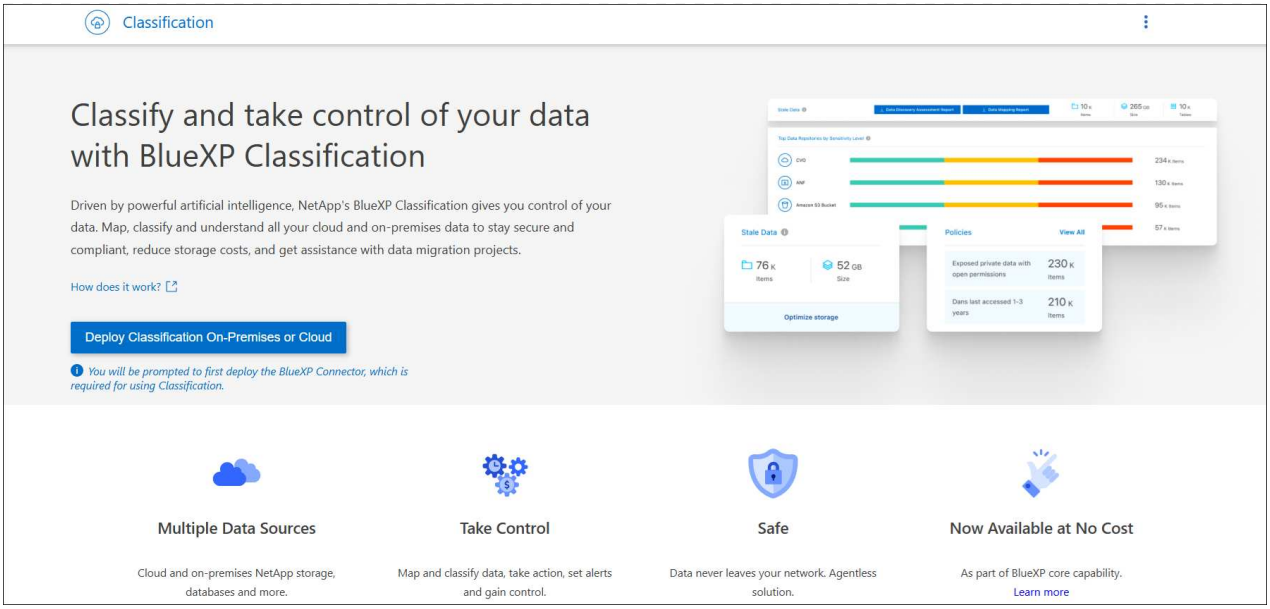
3. Dalla pagina *Installazione*, seleziona **Distribuisci > Distribuisci** per utilizzare la dimensione dell'istanza "Grande" e avviare la procedura guidata di distribuzione nel cloud.
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

5. Una volta distribuita l'istanza e installata la BlueXP classification , selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

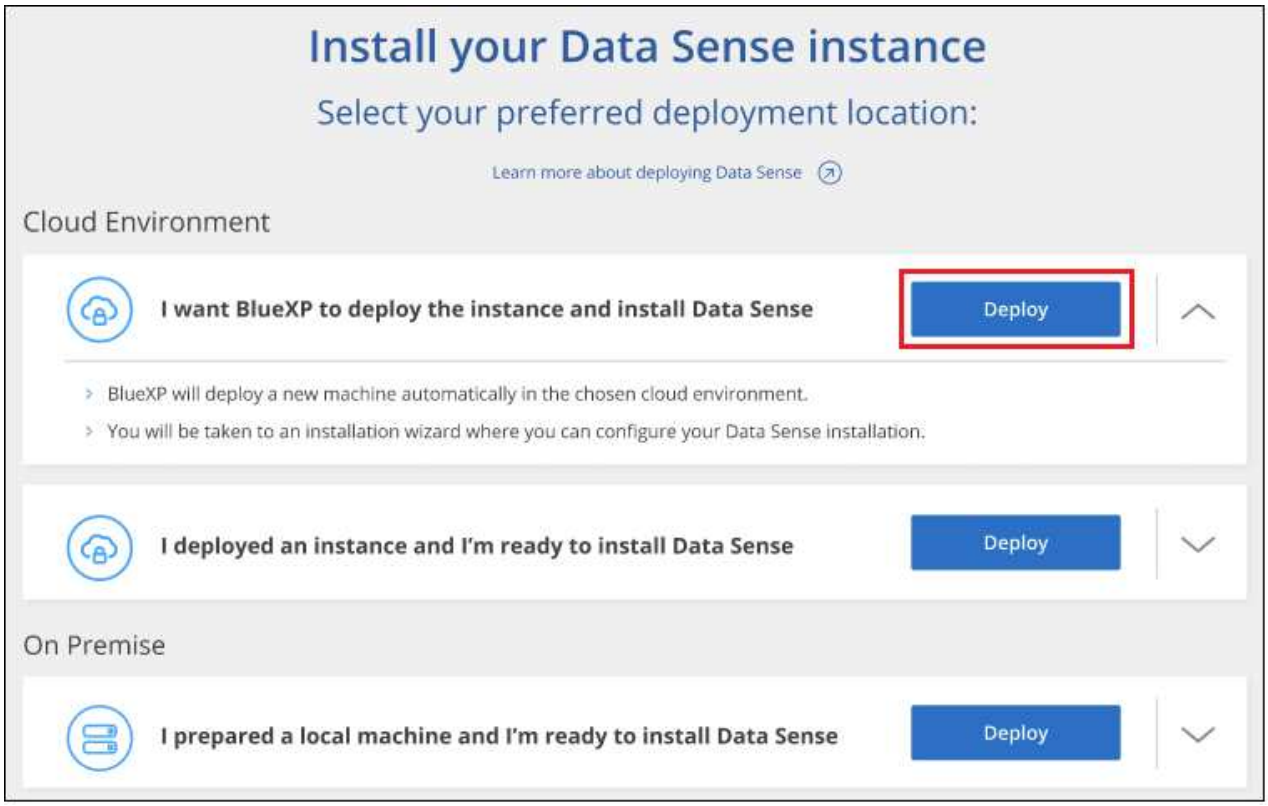
Implementazione in Azure

Fasi

1. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Distribuisci classificazione in locale o nel cloud**.



3. Selezionare **Distribuisci** per avviare la procedura guidata di distribuzione nel cloud.



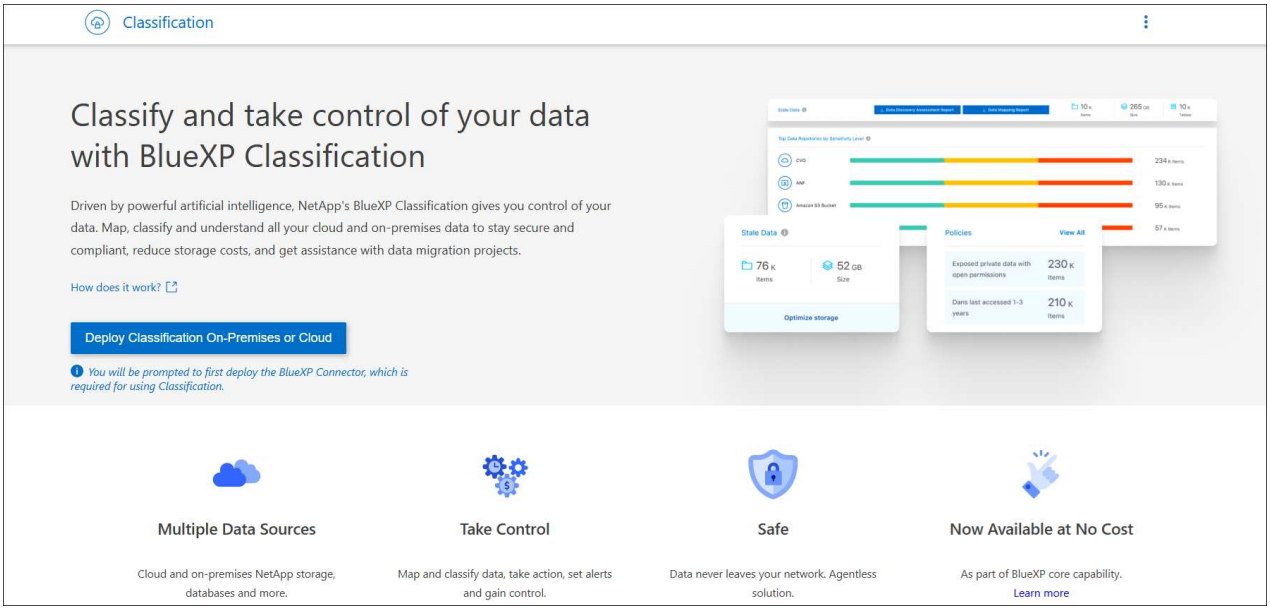
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

5. Una volta distribuita l'istanza e installata la BlueXP classification , selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

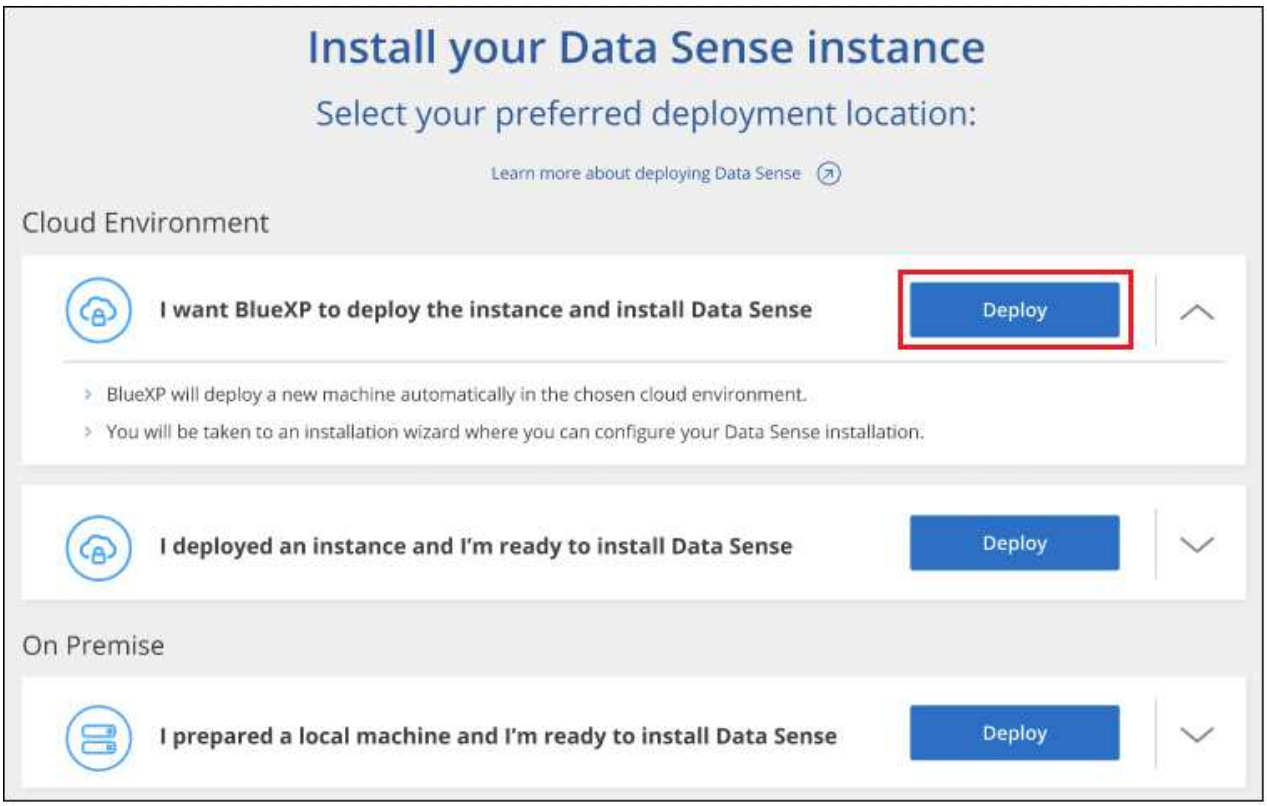
Implementazione in Google Cloud

Fasi

1. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
2. Selezionare **Distribuisci classificazione in locale o nel cloud**.



3. Selezionare **Distribuisci** per avviare la procedura guidata di distribuzione nel cloud.



4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

5. Una volta distribuita l'istanza e installata la BlueXP classification , selezionare **Continua alla configurazione** per andare alla pagina *Configurazione*.

Risultato

BlueXP implementa l'istanza di classificazione BlueXP nel tuo cloud provider.

Gli aggiornamenti al software di classificazione BlueXP Connector e BlueXP sono automatizzati purché le istanze dispongano di connettività Internet.

Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione.

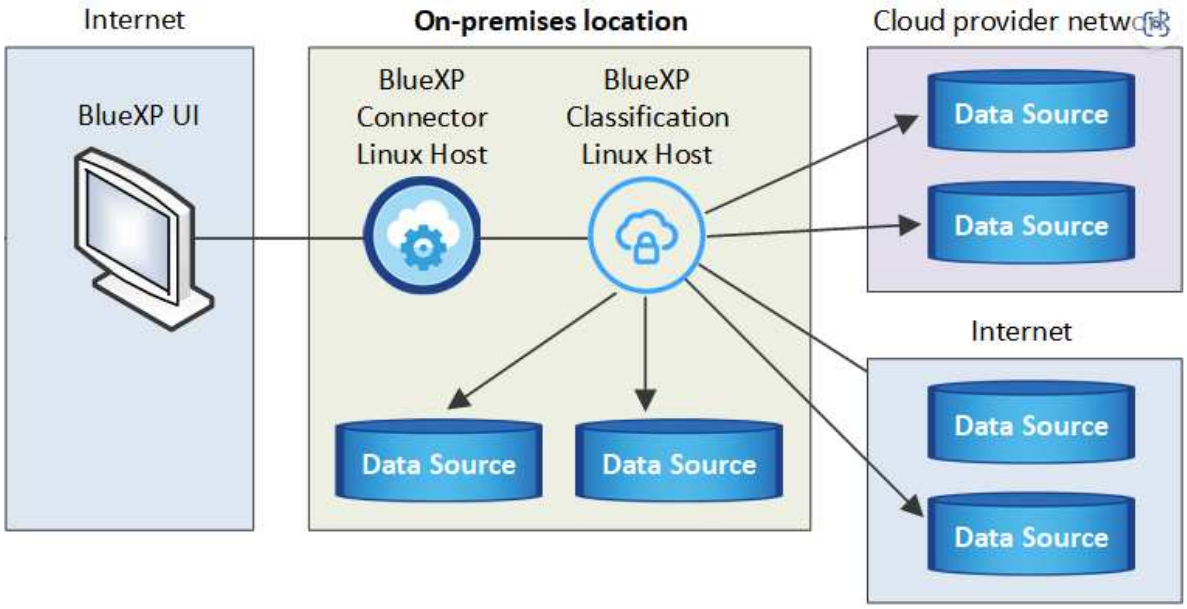
Installare la classificazione BlueXP su un host con accesso a Internet

Completare alcuni passaggi per installare la classificazione BlueXP su un host Linux nella rete o su un host Linux nel cloud con accesso a Internet. Come parte di questa installazione, sarà necessario implementare manualmente l'host Linux nella rete o nel cloud.

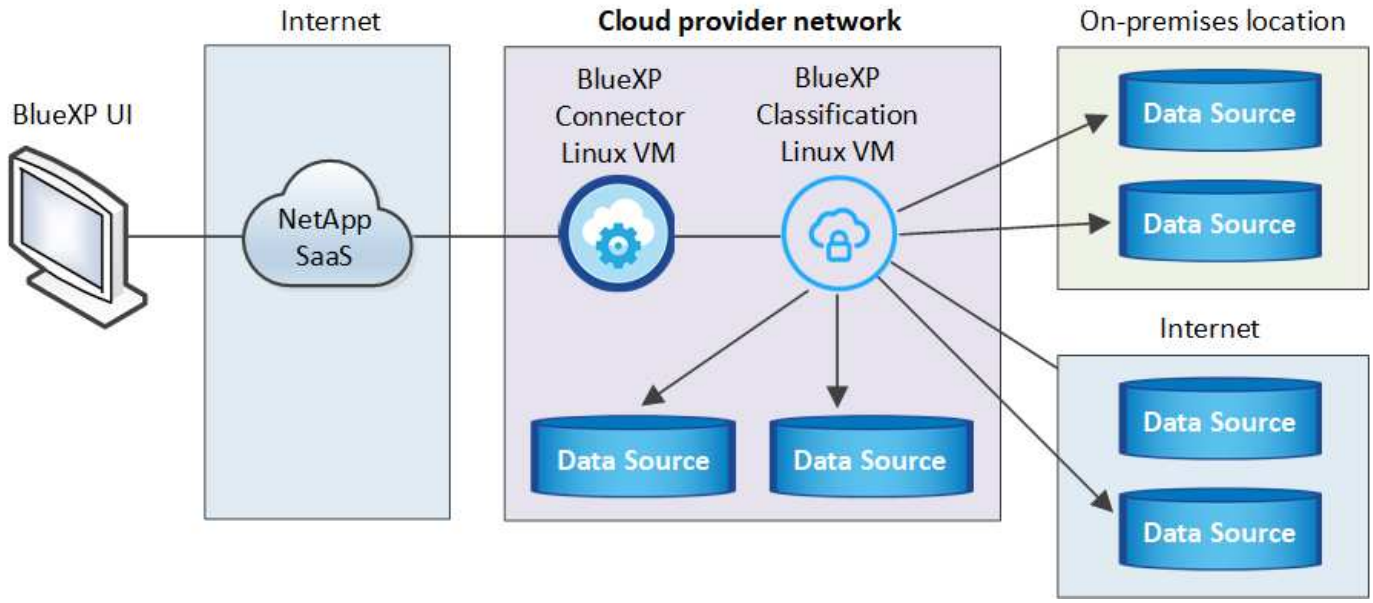
L'installazione in sede può essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP in sede utilizzando un'istanza di classificazione BlueXP che si trova anche in loco, ma questo non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente dal metodo di installazione scelto.

Lo script di installazione della classificazione BlueXP inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti richiesti. Se tutti i prerequisiti sono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti. "Scopri come verificare se il tuo host Linux è pronto per installare la classificazione BlueXP".

L'installazione tipica su un host Linux *in sede* ha i seguenti componenti e connessioni.



L'installazione tipica su un host Linux *nel cloud* ha i seguenti componenti e connessioni.



Per le versioni legacy 1,30 e precedenti, se devi installare la classificazione BlueXP su host multipli, fai riferimento a. "Installare la classificazione BlueXP su host multipli senza accesso a Internet".

È anche possibile "Installare la classificazione BlueXP in un sito on-premise che non dispone di accesso a Internet".

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.

1 Creare un connettore

Se non si dispone già di un connettore, "Implementare il connettore on-premise" Su un host Linux nella rete o su un host Linux nel cloud.

Puoi anche creare un connettore con il tuo cloud provider. Vedere "Creazione di un connettore in AWS", "Creazione di un connettore in Azure", o. "Creazione di un connettore in GCP".

2 Esaminare i prerequisiti

Assicurarsi che l'ambiente soddisfi i prerequisiti. Ciò include l'accesso a Internet in uscita per l'istanza, la connettività tra il connettore e la classificazione BlueXP sulla porta 443 e altro ancora. Consulta l'elenco completo.

È inoltre necessario un sistema Linux che soddisfi i requisiti di requisiti seguenti.

3 Scarica e implementa la classificazione BlueXP

Scarica il software di classificazione Cloud BlueXP dal sito di supporto NetApp e copia il file di installazione sull'host Linux che intendi utilizzare. Quindi, avviare l'installazione guidata e seguire le istruzioni per implementare l'istanza di classificazione BlueXP.

Creare un connettore

Prima di installare e utilizzare la classificazione BlueXP, è necessario un connettore BlueXP. Nella maggior parte dei casi, probabilmente si dispone di un connettore configurato prima di tentare di attivare la classificazione BlueXP, perché la maggior parte "Le funzionalità di BlueXP richiedono un connettore", ma in alcuni casi è necessario impostarne uno ora.

Per crearne uno nel tuo ambiente di cloud provider, consulta la sezione "Creazione di un connettore in AWS", "Creazione di un connettore in Azure", o. "Creazione di un connettore in GCP".

Esistono alcuni scenari in cui è necessario utilizzare un connettore implementato in uno specifico cloud provider:

- Quando esegui la scansione dei dati in Cloud Volumes ONTAP in AWS o in Amazon FSX per ONTAP, utilizza un connettore in AWS.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in Azure o in Azure NetApp Files, si utilizza un connettore in Azure.

  Per Azure NetApp Files, deve essere implementato nella stessa regione dei volumi che si desidera sottoporre a scansione.

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un connettore in GCP.

I sistemi ONTAP on-premise, le condivisioni dei file NetApp e gli account dei database possono essere sottoposti a scansione utilizzando uno qualsiasi di questi connettori cloud.

Nota: È anche possibile "Implementare il connettore on-premise" Su un host Linux nella rete o su un host Linux nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Quando si installa la classificazione BlueXP, è necessario l'indirizzo IP o il nome host del sistema di connessione. Queste informazioni saranno disponibili se il connettore è stato installato nella propria sede. Se il connettore è implementato nel cloud, è possibile trovare queste informazioni dalla console BlueXP: Fare clic sull'icona della Guida, selezionare **Support** e fare clic su **BlueXP Connector**.

Preparare il sistema host Linux

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via. L'host Linux può trovarsi nella rete o nel cloud.

Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP. Il sistema di classificazione BlueXP deve rimanere attivo per eseguire una scansione continua dei dati.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.
- Quando crei il sistema host on-premise, puoi scegliere tra queste dimensioni di sistema in base alle dimensioni del set di dati che intendi eseguire la scansione della classificazione BlueXP.

Dimensioni del sistema	CPU	RAM (la memoria di swap deve essere disattivata)	Disco
Molto grande	32 CPU	128 GB DI RAM	• 1 TiB SSD su /, o 100 GiB disponibile su /opz • 895 GiB disponibile su /var/lib/docker • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**
Grande	16 CPU	64 GB DI RAM	• SSD da 500 GiB su /, o 100 GiB disponibile su /opz • 395 GiB disponibile su /var/lib/docker o per Podman /var/lib/containers o per Podman /var/lib/containers • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
  - **Tipo di istanza di Amazon Elastic Compute Cloud (Amazon EC2)**: Si consiglia "m6i.4XLarge". "Vedere altri tipi di istanze AWS".
  - **Dimensione delle macchine virtuali Azure**: Si consiglia "Standard_D16s_v3". "Vedere altri tipi di istanze di Azure".
  - **Tipo di macchina GCP**: Si consiglia "n2-standard-16". "Vedere altri tipi di istanze GCP".
- **UNIX folder permissions**: Sono richieste le seguenti autorizzazioni minime per UNIX:

Cartella	Permessi minimi
/tmp	`rwxrwxrwt`
/opz	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operativo**:
  - I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:
    - Red Hat Enterprise Linux versione 7,8 e 7,9
    - Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)

        - Ubuntu 24,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
    - I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
        - Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
    - Le estensioni vettoriali avanzate (AVX2) devono essere abilitate sul sistema host.
- **Red Hat Subscription Management**: L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
- **Software aggiuntivo**: È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:
    - A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
        - Docker Engine versione 19.3.1 o superiore. "Visualizzare le istruzioni di installazione".
        - Podman versione 4 o superiore. Per installare Podman, immettere (`sudo yum install podman netavark -y`).
- Python versione 3,6 o superiore. "Visualizzare le istruzioni di installazione".
    - **Considerazioni NTP**: NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
- **Considerazioni su Firewalld**: Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare altri host di classificazione BlueXP come nodi scanner, aggiungere queste regole al sistema primario in questo momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.

L'indirizzo IP del sistema host di classificazione BlueXP non può essere modificato dopo l'installazione.

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a Internet in uscita per contattare i seguenti endpoint.

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://github.com/docker https://download.docker.com	Fornisce pacchetti prerequisiti per l'installazione di docker.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fornisce pacchetti prerequisiti per l'installazione di Ubuntu.

Verificare che tutte le porte richieste siano attivate

Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

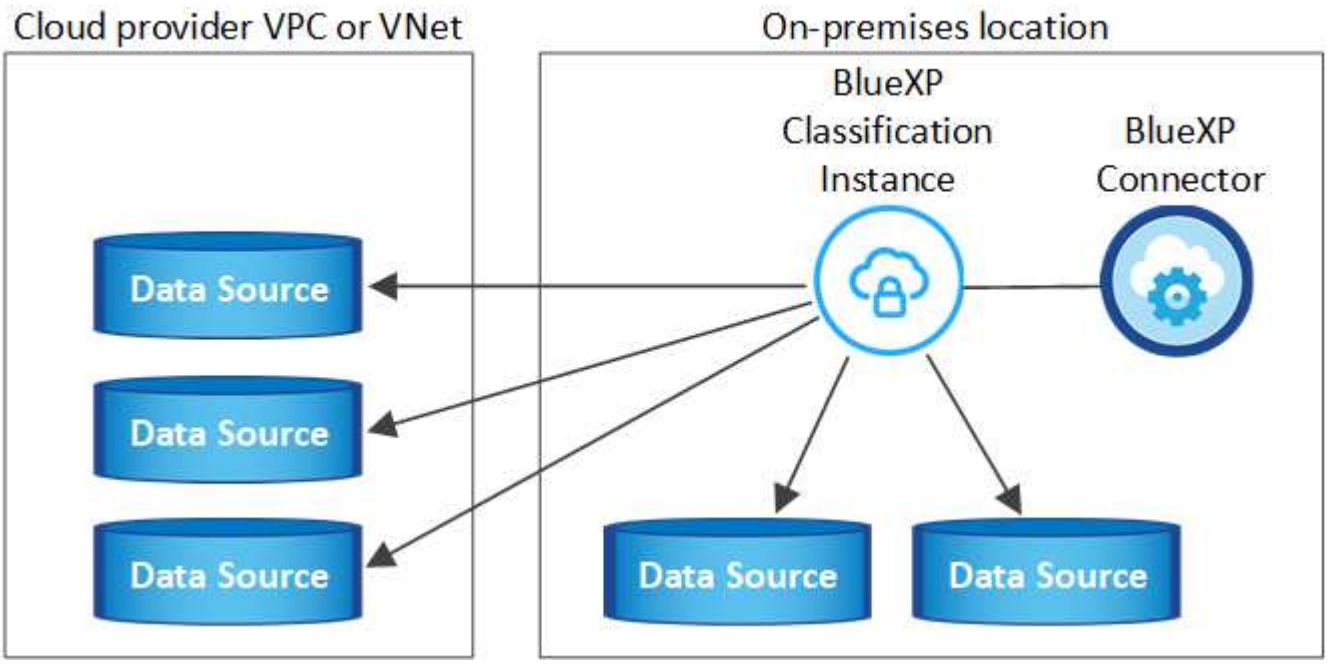
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80. 9000	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080 sia aperta in modo da visualizzare l'avanzamento dell'installazione in BlueXP. Se si utilizza un firewall sull'host Linux, è necessaria la porta 9000 per i processi interni all'interno di un server Ubuntu.

Tipo di connessione	Porte	Descrizione
Connettore <> ONTAP cluster (NAS)	443 (TCP)	BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti: • L'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal firewall predefinito o dalle regole di routing. • Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443. Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questo criterio predefinito è stato modificato o se è stato creato un criterio firewall personalizzato, è necessario associare il protocollo HTTPS a tale criterio e abilitare l'accesso dall'host del connettore.
Classificazione BlueXP <> cluster ONTAP	• Per NFS - 111 (TCP/UDP) e 2049 (TCP/UDP) • Per CIFS - 139 (TCP/UDP) e 445 (TCP/UDP)	La classificazione BlueXP richiede una connessione di rete a ogni subnet Cloud Volumes ONTAP o sistema ONTAP on-premise. I firewall o le regole di routing per Cloud Volumes ONTAP devono consentire le connessioni in entrata dall'istanza di classificazione BlueXP. Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP: • Per NFS - 111 e 2049 • Per CIFS - 139 e 445 I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.

Tipo di connessione	Porte	Descrizione
Classificazione BlueXP <> Active Directory	389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)	È necessario che sia già stata configurata una Active Directory per gli utenti della società. Inoltre, la classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS. È necessario disporre delle informazioni per Active Directory: • DNS Server IP Address (Indirizzo IP server DNS) o Multiple IP Address (indirizzi IP multipli) • Nome utente e password del server • Domain Name (Nome di Active Directory) (Nome di dominio) • Se si utilizza o meno LDAP sicuro (LDAPS) • Porta server LDAP (generalmente 389 per LDAP e 636 per LDAP sicuro)

Installare la classificazione BlueXP sull'host Linux

Per le configurazioni tipiche, il software viene installato su un singolo sistema host. Consulta questa procedura.



Vedere Preparazione del sistema host Linux e. Verifica dei prerequisiti Per l'elenco completo dei requisiti prima di implementare la classificazione BlueXP.

Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

La classificazione BlueXP non è attualmente in grado di eseguire la scansione dei bucket S3, Azure NetApp Files o FSX per ONTAP quando il software è installato on-premise. In questi casi, è necessario implementare un connettore separato e un'istanza della classificazione BlueXP nel cloud e. "Passare da un connettore all'altro" per le diverse origini dati.

Installazione a host singolo per configurazioni tipiche

Esaminare i requisiti e seguire questi passaggi quando si installa il software di classificazione BlueXP su un singolo host on-premise.

"Guarda questo video" Per vedere come installare la classificazione BlueXP .

Tenere presente che tutte le attività di installazione vengono registrate durante l'installazione della classificazione BlueXP. In caso di problemi durante l'installazione, è possibile visualizzare il contenuto del registro di controllo dell'installazione. È scritto a. `/opt/netapp/install_logs/`. "Per ulteriori informazioni, fare clic qui".

Prima di iniziare

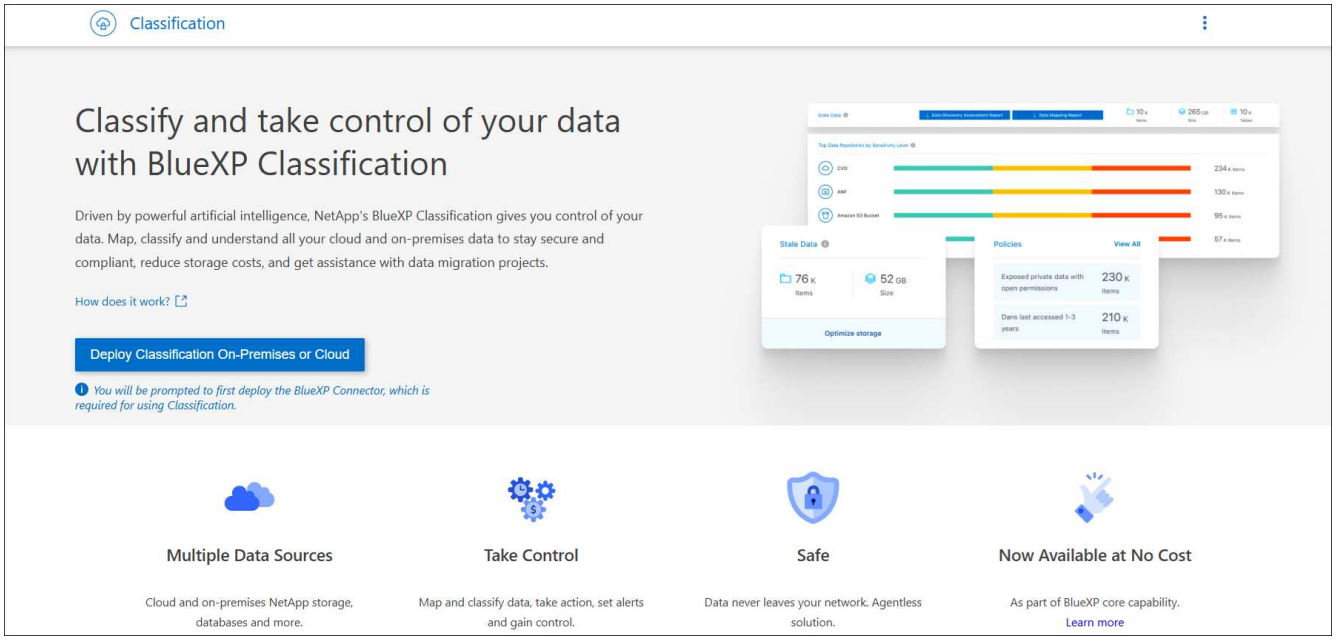
- Verificare che il sistema Linux soddisfi i requisiti requisiti dell'host.
- Verificare che sul sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.
- Se si utilizza un proxy per l'accesso a Internet:
  - Sono necessarie le informazioni sul server proxy (indirizzo IP o nome host, porta di connessione, schema di connessione: https o http, nome utente e password).
  - Se il proxy sta eseguendo l'intercettazione TLS, è necessario conoscere il percorso del sistema Linux di classificazione BlueXP in cui sono memorizzati i certificati della CA TLS.
  - Il proxy deve essere non trasparente. BlueXP classificaiton attualmente non supporta proxy trasparenti.
  - L'utente deve essere un utente locale. Gli utenti di dominio non sono supportati.
- Verificare che l'ambiente offline soddisfi i requisiti permessi e connettività.

Fasi

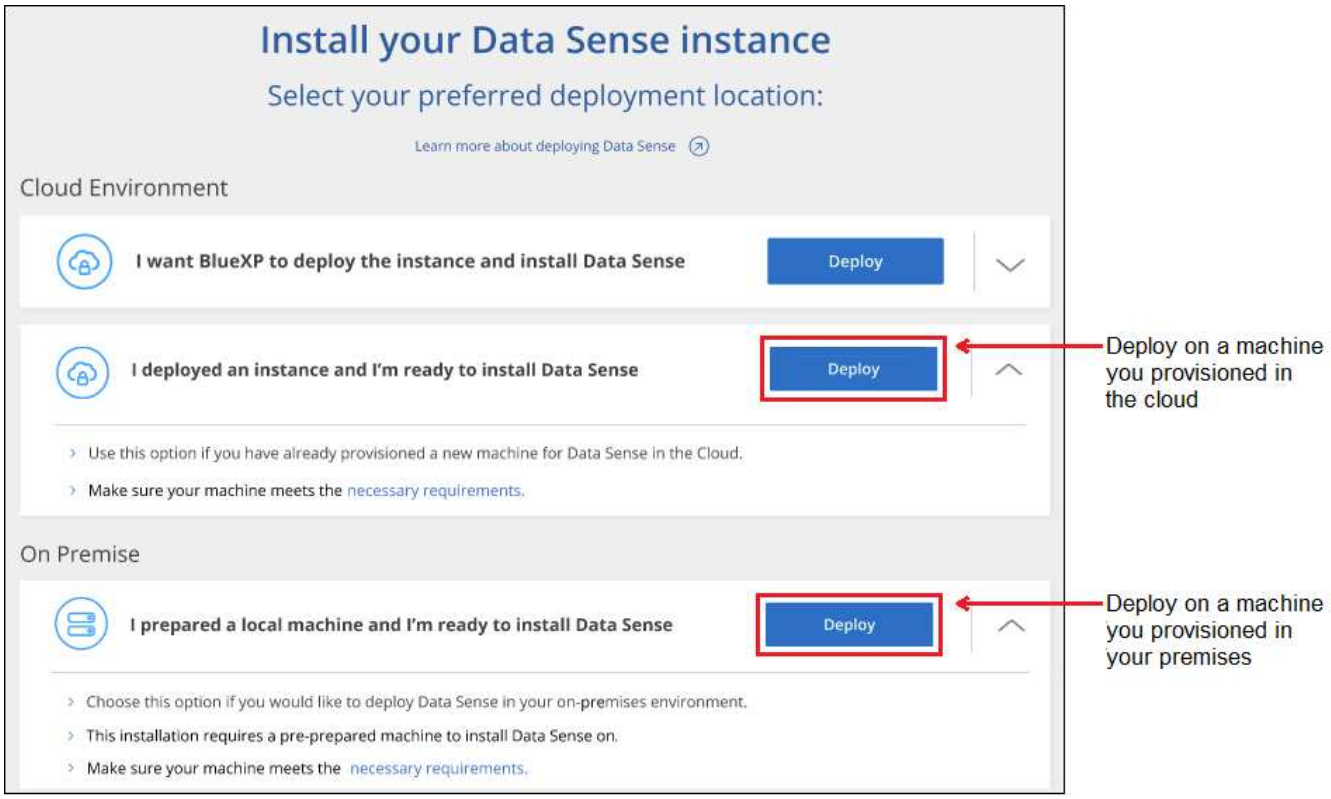
1. Scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiare il file del programma di installazione sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Decomprimere il file del programma di installazione sul computer host, ad esempio:

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. In BlueXP, selezionare **Governance > Classification**.
5. Selezionare **Distribuisci classificazione in locale o nel cloud**.



6. A seconda che si stia installando la classificazione BlueXP su un'istanza preparata nel cloud o su un'istanza preparata in sede, fare clic sul pulsante **Deploy** appropriato per avviare l'installazione della classificazione BlueXP.



7. Viene visualizzata la finestra di dialogo *Deploy Data Sense on Premise*. Copiare il comando fornito (ad esempio: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) e incollarlo in un file di testo per poterlo utilizzare in un secondo momento. Quindi fare clic su **Chiudi** per chiudere la finestra di dialogo.
8. Sul computer host, immettere il comando copiato e seguire una serie di prompt oppure fornire il comando completo che include tutti i parametri richiesti come argomenti della riga di comando.

   Si noti che il programma di installazione esegue un controllo preliminare per assicurarsi che i requisiti di

sistema e di rete siano stati impostati per una corretta installazione. "Guarda questo video" comprendere i messaggi e le implicazioni del controllo preliminare.

Inserire i parametri come richiesto:	Immettere il comando completo:
a. Incollare il comando copiato dal punto 7: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` Se si esegue l'installazione su un'istanza cloud (non on-premise), aggiungere `--manual-cloud-install <cloud_provider>`. b. Immettere l'indirizzo IP o il nome host del computer host di classificazione BlueXP in modo che sia possibile accedervi dal sistema di connettori. c. Inserire l'indirizzo IP o il nome host del computer host BlueXP Connector in modo che sia possibile accedervi dal sistema di classificazione BlueXP. d. Inserire i dettagli del proxy come richiesto. Se il connettore BlueXP utilizza già un proxy, non è necessario inserire nuovamente queste informazioni, poiché la classificazione BlueXP utilizzerà automaticamente il proxy utilizzato dal connettore.	In alternativa, è possibile creare l'intero comando in anticipo, fornendo i parametri host e proxy necessari: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy-user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

Valori variabili:

- *Account_id* = ID account NetApp
- *Client_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client se non è già presente)
- *User_token* = token di accesso utente JWT
- *Ds_host* = indirizzo IP o nome host del sistema Linux di classificazione BlueXP.
- *Cm_host* = indirizzo IP o nome host del sistema BlueXP Connector.
- *Cloud_provider* = durante l'installazione su un'istanza di cloud, immettere "AWS", "Azure" o "Gcp" a seconda del provider di cloud.
- *Proxy_host* = IP o nome host del server proxy se l'host si trova dietro un server proxy.
- *Porta_proxy* = porta per la connessione al server proxy (impostazione predefinita: 80).
- *Schema_proxy* = Schema di connessione: https o http (http predefinito).
- *Proxy_user* = utente autenticato per la connessione al server proxy, se è richiesta l'autenticazione di base. L'utente deve essere un utente locale - gli utenti di dominio non sono supportati.
- *Proxy_password* = Password per il nome utente specificato.
- *Ca_cert_dir* = percorso del sistema Linux di classificazione BlueXP contenente bundle di certificati CA TLS aggiuntivi. Richiesto solo se il proxy sta eseguendo l'intercettazione TLS.

Risultato

Il programma di installazione della classificazione BlueXP installa i pacchetti, registra l'installazione e installa la classificazione BlueXP. L'installazione può richiedere da 10 a 20 minuti.

Se la connessione tra il computer host e l'istanza del connettore avviene tramite la porta 8080, l'avanzamento dell'installazione viene visualizzato nella scheda classificazione BlueXP in BlueXP.

Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione.

Installare la classificazione BlueXP su un host Linux senza accesso Internet

Completa alcuni passaggi per installare la classificazione BlueXP su un host Linux in un sito on-premise che non dispone di accesso a Internet, anche noto come *private mode*. Questo tipo di installazione, che utilizza uno script di installazione, non ha connettività al livello SaaS di BlueXP .

"Scopri le diverse modalità di implementazione per la classificazione BlueXP Connector e BlueXP".

È anche possibile "Implementare la classificazione BlueXP in un sito on-premise con accesso a Internet".

Lo script di installazione della classificazione BlueXP inizia verificando se il sistema e l'ambiente soddisfano i prerequisiti richiesti. Se tutti i prerequisiti sono soddisfatti, viene avviata l'installazione. Se si desidera verificare i prerequisiti indipendentemente dall'esecuzione dell'installazione di classificazione BlueXP, è possibile scaricare un pacchetto software separato che esegue solo i prerequisiti. "Scopri come verificare se il tuo host Linux è pronto per installare la classificazione BlueXP".

> Per le versioni legacy 1,30 e precedenti, se devi installare la classificazione BlueXP su host multipli, fai riferimento a. "Installare la classificazione BlueXP su host multipli senza accesso a Internet".

Origini dati supportate

Quando viene installata la modalità privata (talvolta chiamata sito "offline" o "dark"), la classificazione BlueXP può eseguire la scansione dei dati solo da origini dati locali al sito on-premise. Al momento, la classificazione BlueXP è in grado di eseguire la scansione delle seguenti origini dati **locali**:

- Sistemi ONTAP on-premise
- Schemi di database

Quando la classificazione BlueXP viene implementata in modalità privata, al momento non è disponibile alcun supporto per la scansione degli account Cloud Volumes ONTAP, Azure NetApp Files o FSX per ONTAP.

Limitazioni

La maggior parte delle funzionalità di classificazione BlueXP funziona quando viene implementato in un sito senza accesso a Internet. Tuttavia, alcune funzioni che richiedono l'accesso a Internet non sono supportate, ad esempio:

- Impostazione dei ruoli BlueXP per diversi utenti (ad esempio, account Admin o Compliance Viewer)
- Copia e sincronizzazione dei file di origine utilizzando la copia e la sincronizzazione BlueXP
- Aggiornamenti software automatici da BlueXP

Sia il connettore BlueXP che la classificazione BlueXP richiederanno aggiornamenti manuali periodici per abilitare nuove funzionalità. La versione della classificazione BlueXP è disponibile nella parte inferiore delle pagine dell'interfaccia utente di classificazione BlueXP. Controllare "Classificazione BlueXP - Note di rilascio" per vedere le nuove funzionalità di ciascuna release e se si desidera. Quindi, seguire i passaggi da a. "Aggiornare BlueXP Connector" e. Aggiorna il software di classificazione BlueXP.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle sezioni rimanenti per ottenere dettagli completi.

Installare il connettore BlueXP

Se non si dispone già di un connettore installato in modalità privata, "Implementare il connettore" Su un host Linux.

Esaminare i prerequisiti di classificazione di BlueXP

Assicurarsi che il sistema Linux soddisfi i requisiti requisiti dell'host, che abbia installato tutto il software necessario e che il tuo ambiente offline soddisfi i requisiti permessi e connettività.

Scarica e implementa la classificazione BlueXP

Scaricare il software di classificazione BlueXP dal NetApp Support Site e copiare il file di installazione sull'host Linux che si desidera utilizzare. Quindi, avviare l'installazione guidata e seguire le istruzioni per implementare l'istanza di classificazione BlueXP.

Installare il connettore BlueXP

Se BlueXP Connector non è già installato in modalità privata, "Implementare il connettore" Su un host Linux nel tuo sito offline.

Preparare il sistema host Linux

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.
- Quando crei il sistema host on-premise, puoi scegliere tra queste dimensioni di sistema in base alle dimensioni del set di dati che intendi eseguire la scansione della classificazione BlueXP.

Dimensioni del sistema	CPU	RAM (la memoria di swap deve essere disattivata)	Disco
Molto grande	32 CPU	128 GB DI RAM	• 1 TiB SSD su /, o 100 GiB disponibile su /opz • 895 GiB disponibile su /var/lib/docker • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**
Grande	16 CPU	64 GB DI RAM	• SSD da 500 GiB su /, o 100 GiB disponibile su /opz • 395 GiB disponibile su /var/lib/docker o per Podman /var/lib/containers o per Podman /var/lib/containers • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
  - **Tipo di istanza di Amazon Elastic Compute Cloud (Amazon EC2)**: Si consiglia "m6i.4XLarge". "Vedere altri tipi di istanze AWS".
  - **Dimensione delle macchine virtuali Azure**: Si consiglia "Standard_D16s_v3". "Vedere altri tipi di istanze di Azure".
  - **Tipo di macchina GCP**: Si consiglia "n2-standard-16". "Vedere altri tipi di istanze GCP".
- **UNIX folder permissions**: Sono richieste le seguenti autorizzazioni minime per UNIX:

Cartella	Permessi minimi
/tmp	`rwxrwxrwt`
/opz	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operativo**:
  - I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:
    - Red Hat Enterprise Linux versione 7,8 e 7,9
    - Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)

        - Ubuntu 24,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
    - I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
        - Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
    - Le estensioni vettoriali avanzate (AVX2) devono essere abilitate sul sistema host.
- **Red Hat Subscription Management**: L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
- **Software aggiuntivo**: È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:
    - A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
        - Docker Engine versione 19.3.1 o superiore. "Visualizzare le istruzioni di installazione".
        - Podman versione 4 o superiore. Per installare Podman, immettere (`sudo yum install podman netavark -y`).
- Python versione 3,6 o superiore. "Visualizzare le istruzioni di installazione".
    - **Considerazioni NTP**: NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
- **Considerazioni su Firewalld**: Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.

L'indirizzo IP del sistema host di classificazione BlueXP non può essere modificato dopo l'installazione.

Verificare i prerequisiti di classificazione di BlueXP e BlueXP

Esaminare i seguenti prerequisiti per assicurarsi di disporre di una configurazione supportata prima di implementare la classificazione BlueXP.

- Assicurarsi che il connettore disponga delle autorizzazioni per distribuire le risorse e creare gruppi di protezione per l'istanza di classificazione BlueXP. Le autorizzazioni BlueXP più recenti sono disponibili in "Le policy fornite da NetApp".
- Assicurarsi che sia possibile mantenere in esecuzione la classificazione BlueXP. L'istanza di classificazione BlueXP deve rimanere attiva per eseguire una scansione continua dei dati.

- Garantire la connettività del browser Web alla classificazione BlueXP. Una volta attivata la classificazione BlueXP, assicurarsi che gli utenti accedano all'interfaccia BlueXP da un host che dispone di una connessione all'istanza di classificazione BlueXP.

  L'istanza di classificazione BlueXP utilizza un indirizzo IP privato per garantire che i dati indicizzati non siano accessibili ad altri. Di conseguenza, il browser Web utilizzato per accedere a BlueXP deve disporre di una connessione a tale indirizzo IP privato. Tale connessione può provenire da un host che si trova all'interno della stessa rete dell'istanza di classificazione BlueXP.

Verificare che tutte le porte richieste siano attivate

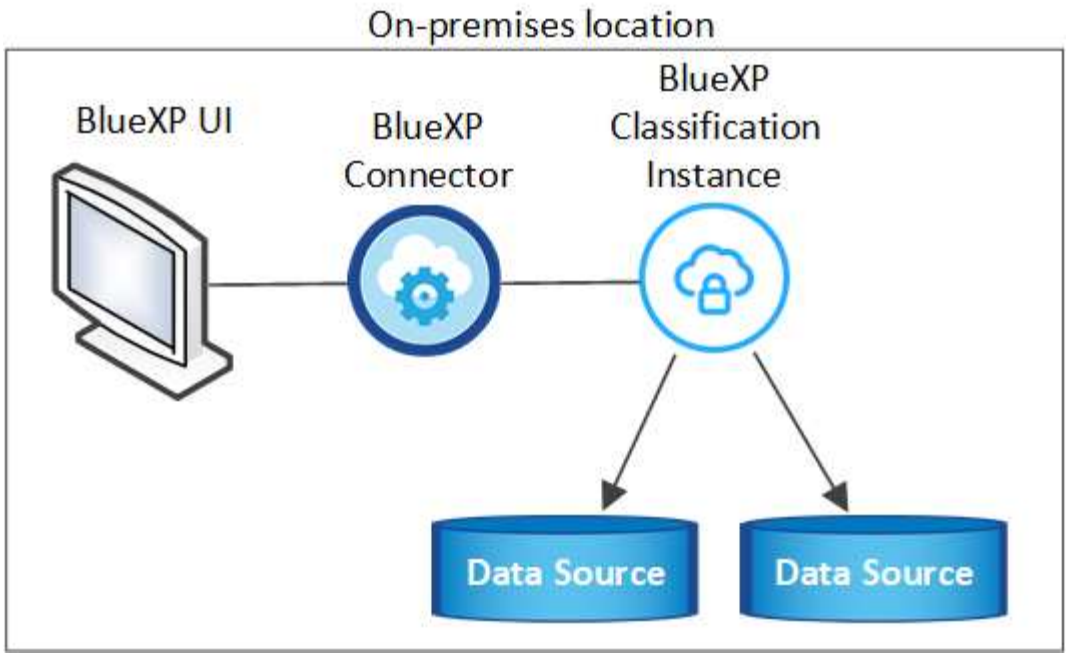
Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) E 80. 9000	Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulle porte 6000 e 443 da e verso l'istanza di classificazione BlueXP. • È necessaria la porta 6000 per fare in modo che la licenza BYOL di classificazione BlueXP funzioni in un sito oscuro. • La porta 8080 dovrebbe essere aperta in modo da poter vedere l'avanzamento dell'installazione in BlueXP. • Se si utilizza un firewall sull'host Linux, è necessaria la porta 9000 per i processi interni all'interno di un server Ubuntu.
Connettore <> ONTAP cluster (NAS)	443 (TCP)	BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, questi devono soddisfare i seguenti requisiti: • L'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal gruppo di sicurezza predefinito. • Il cluster ONTAP deve consentire l'accesso HTTPS in entrata attraverso la porta 443. Il criterio firewall predefinito "mgmt" consente l'accesso HTTPS in entrata da tutti gli indirizzi IP. Se questo criterio predefinito è stato modificato o se è stato creato un criterio firewall personalizzato, è necessario associare il protocollo HTTPS a tale criterio e abilitare l'accesso dall'host del connettore.

Tipo di connessione	Porte	Descrizione
Classificazione BlueXP <> cluster ONTAP	• Per NFS - 111 (TCP/UDP) e 2049 (TCP/UDP) • Per CIFS - 139 (TCP/UDP) e 445 (TCP/UDP)	La classificazione BlueXP richiede una connessione di rete a ogni subnet Cloud Volumes ONTAP o sistema ONTAP on-premise. I gruppi di protezione per Cloud Volumes ONTAP devono consentire le connessioni in entrata dall'istanza di classificazione BlueXP. Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP: • Per NFS - 111 e 2049 • Per CIFS - 139 e 445 I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
Classificazione BlueXP <> Active Directory	389 (TCP E UDP), 636 (TCP), 3268 (TCP) E 3269 (TCP)	È necessario che sia già stata configurata una Active Directory per gli utenti della società. Inoltre, la classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS. È necessario disporre delle informazioni per Active Directory: • DNS Server IP Address (Indirizzo IP server DNS) o Multiple IP Address (indirizzi IP multipli) • Nome utente e password del server • Domain Name (Nome di Active Directory) (Nome di dominio) • Se si utilizza o meno LDAP sicuro (LDAPS) • Porta server LDAP (generalmente 389 per LDAP e 636 per LDAP sicuro)
Se un firewall utilizzato su un host Linux	9000	Necessario per i processi interni all'interno di un server Ubuntu.

Installare la classificazione BlueXP sull'host Linux on-premise

Per le configurazioni tipiche, il software viene installato su un singolo sistema host.



Installazione a host singolo per configurazioni tipiche

Seguire questi passaggi quando si installa il software di classificazione BlueXP su un singolo host on-premise in un ambiente offline.

Tenere presente che tutte le attività di installazione vengono registrate durante l'installazione della classificazione BlueXP. In caso di problemi durante l'installazione, è possibile visualizzare il contenuto del registro di controllo dell'installazione. È scritto a. `/opt/netapp/install_logs/`. "Per ulteriori informazioni, fare clic qui".

Prima di iniziare

- Verificare che il sistema Linux soddisfi i requisiti requisiti dell'host.
- Verificare di aver installato i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.
- Verificare che l'ambiente offline soddisfi i requisiti permessi e connettività.

Fasi

1. Su un sistema configurato tramite Internet, scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è denominato **DataSense-offline-bundle-<version>.tar.gz**.
2. Copiare il pacchetto di installazione sull'host Linux che si intende utilizzare in modalità privata.
3. Decomprimere il pacchetto di installazione sul computer host, ad esempio:

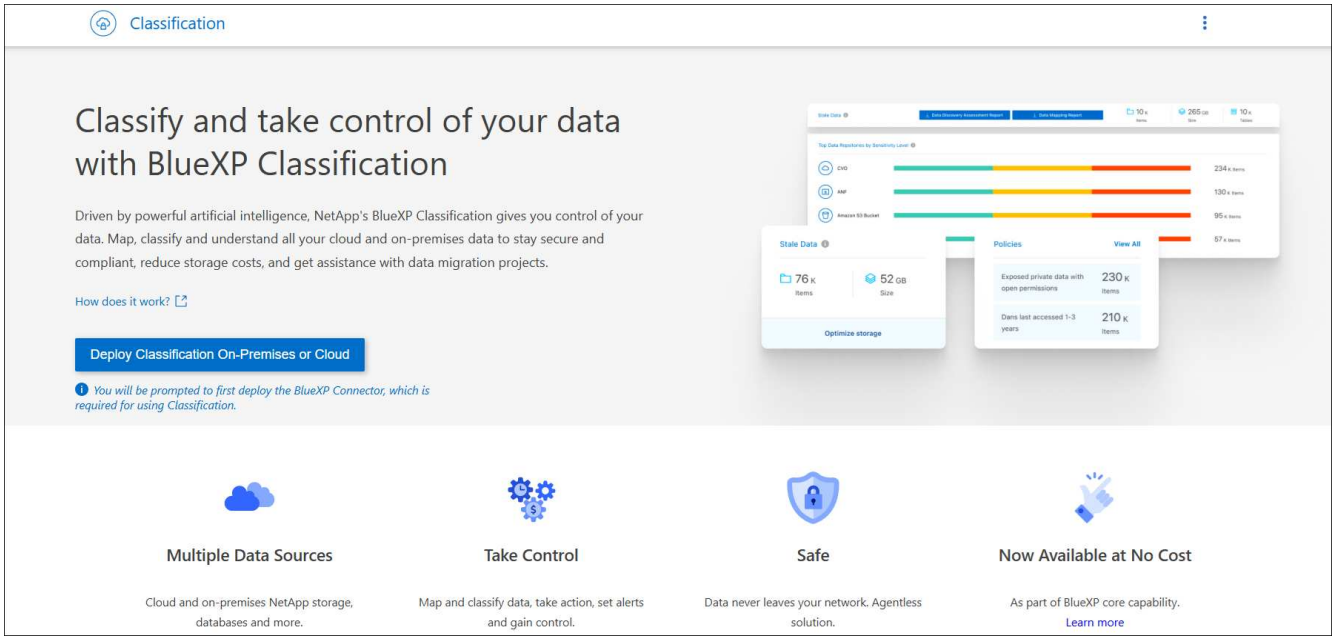
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   In questo modo si estraggono il software richiesto e il file di installazione **cc_onrem_installer.tar.gz**.

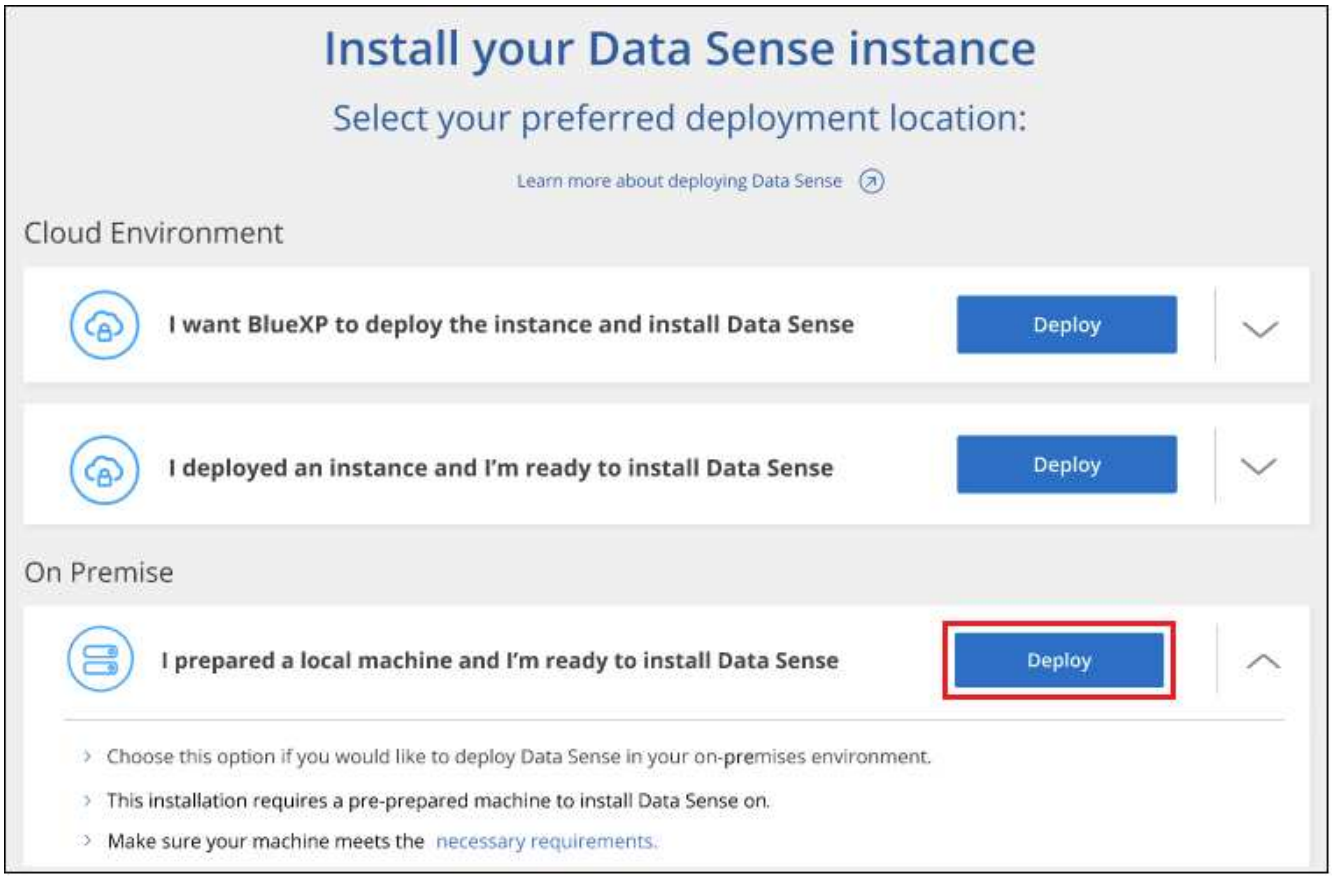
4. Decomprimere il file di installazione sul computer host, ad esempio:

```
tar -xzf cc_onprem_installer.tar.gz
```

5. Avviare BlueXP e selezionare **Governance > Classification**.
6. Selezionare **Distribuisci classificazione in locale o nel cloud**.



7. Fare clic su **Deploy** per avviare l'installazione on-premise.



8. Viene visualizzata la finestra di dialogo *Deploy Data Sense on Premise*. Copiare il comando fornito (ad esempio: `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) e incollarlo in un file di testo per poterlo utilizzare in un secondo momento. Quindi fare clic su **Chiudi** per chiudere la finestra di dialogo.
9. Sul computer host, immettere il comando copiato e seguire una serie di prompt oppure fornire il comando completo che include tutti i parametri richiesti come argomenti della riga di comando.

   Tenere presente che il programma di installazione esegue una pre-verifica per assicurarsi che i requisiti di sistema e di rete siano stati soddisfatti per una corretta installazione.

Inserire i parametri come richiesto:	**Immettere il comando completo:**
a. Incollare le informazioni copiate dal passaggio 8: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. Immettere l'indirizzo IP o il nome host del computer host di classificazione BlueXP in modo che sia possibile accedervi dal sistema di connettori. c. Inserire l'indirizzo IP o il nome host del computer host BlueXP Connector in modo che sia possibile accedervi dal sistema di classificazione BlueXP.	In alternativa, è possibile creare l'intero comando in anticipo, fornendo i parametri host necessari: `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

   Valori variabili:

   - *Account_id* = ID account NetApp
   - *Client_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client se non è già presente)
   - *User_token* = token di accesso utente JWT
   - *Ds_host* = indirizzo IP o nome host del sistema di classificazione BlueXP.
   - *Cm_host* = indirizzo IP o nome host del sistema BlueXP Connector.

Risultato

Il programma di installazione della classificazione BlueXP installa i pacchetti, registra l'installazione e installa la classificazione BlueXP. L'installazione può richiedere da 10 a 20 minuti.

Se la connessione tra il computer host e l'istanza del connettore avviene tramite la porta 8080, l'avanzamento dell'installazione viene visualizzato nella scheda classificazione BlueXP in BlueXP.

Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare il locale "Cluster ONTAP on-premise" e. "database" che si desidera acquisire.

Aggiornare il software di classificazione BlueXP

Poiché il software di classificazione BlueXP viene aggiornato regolarmente con nuove funzionalità, è necessario iniziare una routine per verificare periodicamente la presenza di nuove versioni per assicurarsi di utilizzare il software e le funzionalità più recenti. Sarà necessario aggiornare manualmente il software di

classificazione BlueXP perché non è disponibile alcuna connessione a Internet per eseguire l'aggiornamento automaticamente.

Prima di iniziare

- Si consiglia di aggiornare il software BlueXP Connector alla versione più recente disponibile. "Consultare la procedura di aggiornamento del connettore".
- A partire dalla classificazione BlueXP versione 1.24, è possibile eseguire aggiornamenti a qualsiasi versione futura del software.

  Se il software di classificazione BlueXP esegue una versione precedente alla 1.24, è possibile aggiornare solo una versione principale alla volta. Ad esempio, se è installata la versione 1.21.x, è possibile eseguire l'aggiornamento solo alla versione 1.22.x. Se si dispone di alcune versioni principali, sarà necessario aggiornare il software più volte.

Fasi

1. Su un sistema configurato tramite Internet, scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è denominato **DataSense-offline-bundle-<version>.tar.gz**.
2. Copiare il bundle software sull'host Linux in cui è installata la classificazione BlueXP nel sito buio.
3. Decomprimere il bundle software sul computer host, ad esempio:

   ```
   tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   In questo modo si estrae il file di installazione **cc_onrem_installer.tar.gz**.

4. Decomprimere il file di installazione sul computer host, ad esempio:

   ```
   tar -xzf cc_onprem_installer.tar.gz
   ```

   In questo modo si estrae lo script di aggiornamento **start_darksite_upgrade.sh** e qualsiasi software di terze parti richiesto.

5. Eseguire lo script di aggiornamento sul computer host, ad esempio:

   ```
   start_darksite_upgrade.sh
   ```

Risultato

Il software di classificazione BlueXP viene aggiornato sull'host. L'aggiornamento può richiedere da 5 a 10 minuti.

Per verificare che il software sia stato aggiornato, controllare la versione nella parte inferiore delle pagine dell'interfaccia utente di classificazione di BlueXP.

Verificare che l'host Linux sia pronto per installare la classificazione BlueXP

Prima di installare manualmente la classificazione BlueXP su un host Linux, eseguire uno script sull'host per verificare che tutti i prerequisiti siano presenti per l'installazione

della classificazione BlueXP . È possibile eseguire questo script su un host Linux nella rete o su un host Linux nel cloud. L'host può essere connesso a Internet, oppure può risiedere in un sito che non dispone di accesso a Internet (un *sito scuro*).

Esiste anche uno script di test prerequisito che fa parte dello script di installazione della classificazione BlueXP. Lo script qui descritto è stato progettato specificamente per gli utenti che desiderano verificare l'host Linux indipendentemente dall'esecuzione dello script di installazione della classificazione BlueXP.

Per iniziare

Eseguire le seguenti operazioni.

1. Se necessario, installare un connettore BlueXP, se non ne è già installato uno. È possibile eseguire lo script di test senza aver installato un connettore, ma lo script verifica la connettività tra il connettore e il computer host di classificazione BlueXP, pertanto si consiglia di disporre di un connettore.
2. Preparare il computer host e verificare che soddisfi tutti i requisiti.
3. Abilitare l'accesso a Internet in uscita dal computer host di classificazione BlueXP.
4. Verificare che tutte le porte richieste siano attivate su tutti i sistemi.
5. Scaricare ed eseguire lo script del test dei prerequisiti.

Creare un connettore

Prima di installare e utilizzare la classificazione BlueXP, è necessario un connettore BlueXP. Tuttavia, è possibile eseguire lo script Prerequisiti senza un connettore.

È possibile "Installare il connettore on-premise" Su un host Linux nella rete o su un host Linux nel cloud. Alcuni utenti che intendono installare BlueXP classification on-premise possono anche scegliere di installare il connettore on-premise.

Per creare un connettore nel tuo ambiente di cloud provider, consulta "Creazione di un connettore in AWS", "Creazione di un connettore in Azure", o. "Creazione di un connettore in GCP".

Quando si esegue lo script Prerequisiti, è necessario l'indirizzo IP o il nome host del sistema di connessione. Queste informazioni saranno disponibili se il connettore è stato installato nella propria sede. Se il connettore è implementato nel cloud, è possibile trovare queste informazioni dalla console BlueXP: Fare clic sull'icona della Guida, selezionare **Support** e fare clic su **BlueXP Connector**.

Verificare i requisiti dell'host

Il software di classificazione BlueXP deve essere eseguito su un host che soddisfi requisiti specifici del sistema operativo, requisiti di RAM, requisiti software e così via.

- La classificazione BlueXP non è supportata su un host condiviso con altre applicazioni: L'host deve essere un host dedicato.
- Quando crei il sistema host on-premise, puoi scegliere tra queste dimensioni di sistema in base alle dimensioni del set di dati che intendi eseguire la scansione della classificazione BlueXP.

Dimensioni del sistema	CPU	RAM (la memoria di swap deve essere disattivata)	Disco
Molto grande	32 CPU	128 GB DI RAM	• 1 TiB SSD su /, o 100 GiB disponibile su /opz • 895 GiB disponibile su /var/lib/docker • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**
Grande	16 CPU	64 GB DI RAM	• SSD da 500 GiB su /, o 100 GiB disponibile su /opz • 395 GiB disponibile su /var/lib/docker o per Podman /var/lib/containers o per Podman /var/lib/containers • 5 GiB ON /tmp • **Per Podman, 5 GB su /tmp** • **Per Podman, 30 GB su /var/tmp**

- Quando si implementa un'istanza di calcolo nel cloud per l'installazione della classificazione BlueXP, si consiglia di utilizzare un sistema che soddisfi i requisiti di sistema "grandi" indicati in precedenza:
  - **Tipo di istanza di Amazon Elastic Compute Cloud (Amazon EC2)**: Si consiglia "m6i.4XLarge". "Vedere altri tipi di istanze AWS".
  - **Dimensione delle macchine virtuali Azure**: Si consiglia "Standard_D16s_v3". "Vedere altri tipi di istanze di Azure".
  - **Tipo di macchina GCP**: Si consiglia "n2-standard-16". "Vedere altri tipi di istanze GCP".
- **UNIX folder permissions**: Sono richieste le seguenti autorizzazioni minime per UNIX:

Cartella	Permessi minimi
/tmp	`rwxrwxrwt`
/opz	`rwxr-xr-x`
/var/lib/docker	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- **Sistema operativo**:
  - I seguenti sistemi operativi richiedono l'utilizzo del motore dei container Docker:
    - Red Hat Enterprise Linux versione 7,8 e 7,9
    - Ubuntu 22,04 (richiede la classificazione BlueXP versione 1,23 o superiore)

        - Ubuntu 24,04 (richiede la classificazione BlueXP versione 1,23 o superiore)
    - I seguenti sistemi operativi richiedono l'utilizzo del motore del container Podman e richiedono la classificazione BlueXP versione 1,30 o superiore:
        - Red Hat Enterprise Linux versione 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 e 9.6.
    - Le estensioni vettoriali avanzate (AVX2) devono essere abilitate sul sistema host.
- **Red Hat Subscription Management**: L'host deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.
- **Software aggiuntivo**: È necessario installare il seguente software sull'host prima di installare la classificazione BlueXP:
    - A seconda del sistema operativo in uso, è necessario installare uno dei motori container:
        - Docker Engine versione 19.3.1 o superiore. "Visualizzare le istruzioni di installazione".
        - Podman versione 4 o superiore. Per installare Podman, immettere (`sudo yum install podman netavark -y`).
- Python versione 3,6 o superiore. "Visualizzare le istruzioni di installazione".
    - **Considerazioni NTP**: NetApp consiglia di configurare il sistema di classificazione BlueXP per utilizzare un servizio NTP (Network Time Protocol). L'ora deve essere sincronizzata tra il sistema di classificazione BlueXP e il sistema del connettore BlueXP.
- **Considerazioni su Firewalld**: Se si intende utilizzare `firewalld`, Si consiglia di abilitarla prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Se si prevede di utilizzare altri host di classificazione BlueXP come nodi scanner (in un modello distribuito), aggiungere queste regole al sistema primario in questo momento:

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Devi riavviare Docker o Podman ogni volta che abiliti o aggiorni il sistema `firewalld` impostazioni.

Abilitare l'accesso a Internet in uscita dalla classificazione BlueXP

La classificazione BlueXP richiede l'accesso a Internet in uscita. Se la rete fisica o virtuale utilizza un server proxy per l'accesso a Internet, assicurarsi che l'istanza di classificazione BlueXP disponga dell'accesso a

Internet in uscita per contattare i seguenti endpoint.

Questa sezione non è necessaria per i sistemi host installati in siti senza connettività Internet.

Endpoint	Scopo
https://api.bluexp.netapp.com	Comunicazione con il servizio BlueXP, che include gli account NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicazione con il sito Web BlueXP per l'autenticazione utente centralizzata.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Fornisce accesso a immagini software, manifesti, modelli e per inviare registri e metriche.
https://support.compliance.api.bluexp.netapp.com/	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://github.com/docker https://download.docker.com	Fornisce pacchetti prerequisiti per l'installazione di docker.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fornisce pacchetti prerequisiti per l'installazione di Ubuntu.

Verificare che tutte le porte richieste siano attivate

Assicurarsi che tutte le porte richieste siano aperte per la comunicazione tra il connettore, la classificazione BlueXP, Active Directory e le origini dati.

Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80. 9000	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080 sia aperta in modo da visualizzare l'avanzamento dell'installazione in BlueXP. Se si utilizza un firewall sull'host Linux, è necessaria la porta 9000 per i processi interni all'interno di un server Ubuntu.
Connettore <> ONTAP cluster (NAS)	443 (TCP)	BlueXP rileva i cluster ONTAP utilizzando HTTPS. Se si utilizzano criteri firewall personalizzati, l'host del connettore deve consentire l'accesso HTTPS in uscita attraverso la porta 443. Se il connettore si trova nel cloud, tutte le comunicazioni in uscita sono consentite dal firewall predefinito o dalle regole di routing.

Eseguire lo script dei prerequisiti di classificazione BlueXP

Seguire questa procedura per eseguire lo script dei prerequisiti di classificazione BlueXP.

"Guarda questo video" Per vedere come eseguire lo script Prerequisites e interpretare i risultati.

Prima di iniziare

- Verificare che il sistema Linux soddisfi i requisiti requisiti dell'host.
- Verificare che sul sistema siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sul sistema Linux.

Fasi

1. Scaricare lo script dei prerequisiti di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è denominato **standalone-pre-requisito-tester-<version>**.
2. Copiare il file sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Assegnare le autorizzazioni per eseguire lo script.

   ```
   chmod +x standalone-pre-requisite-tester-v1.25.0
   ```

4. Eseguire lo script utilizzando il seguente comando.

   ```
   ./standalone-pre-requisite-tester-v1.25.0 <--darksite>
   ```

   Aggiungere l'opzione "--darksite" solo se si esegue lo script su un host che non dispone di accesso a Internet. Alcuni test dei prerequisiti vengono ignorati quando l'host non è connesso a Internet.

5. Lo script richiede l'indirizzo IP del computer host di classificazione BlueXP.
   - Inserire l'indirizzo IP o il nome host.
6. Lo script chiede se si dispone di un connettore BlueXP installato.
   - Immettere **N** se non si dispone di un connettore installato.
   - Inserire **Y** se si dispone di un connettore installato. Quindi, immettere l'indirizzo IP o il nome host del connettore BlueXP in modo che lo script di test possa verificare questa connettività.
7. Lo script esegue una serie di test sul sistema e visualizza i risultati man mano che procede. Al termine, scrive un log della sessione in un file denominato `prerequisites-test-<timestamp>.log` nella directory `/opt/netapp/install_logs`.

Risultato

Se tutti i test dei prerequisiti sono stati eseguiti correttamente, è possibile installare la classificazione BlueXP sull'host quando si è pronti.

Se sono stati rilevati problemi, questi vengono classificati come "consigliati" o "richiesti" per essere risolti. I problemi consigliati in genere sono elementi che rallenterebbero le attività di classificazione e scansione di BlueXP. Questi elementi non devono essere corretti, ma è possibile che si desideri affrontarli.

In caso di problemi "obbligatori", è necessario risolvere i problemi ed eseguire nuovamente lo script di test Prerequisiti.

Attivare la scansione sulle origini dati

Panoramica delle origini dati di scansione con classificazione BlueXP

La classificazione BlueXP esegue la scansione dei dati nei repository (volumi, schemi di database o altri dati utente) scelti per identificare i dati personali e sensibili. Quindi, la classificazione BlueXP mappa i dati organizzativi, categorizza ogni file e identifica gli schemi predefiniti nei dati. Il risultato della scansione è un indice di informazioni personali, informazioni personali sensibili, categorie di dati e tipi di file.

Dopo la scansione iniziale, la classificazione BlueXP esegue la scansione continua dei dati in modo round robin per rilevare le modifiche incrementali. Per questo motivo è importante mantenere in esecuzione l'istanza.

È possibile attivare e disattivare le scansioni a livello di volume o a livello di schema del database.

Qual è la differenza tra le scansioni di mappatura e classificazione

È possibile eseguire due tipi di scansioni nella classificazione BlueXP :

- **Le scansioni solo mappatura** forniscono solo una panoramica di alto livello dei vostri dati e vengono eseguite su origini dati selezionate. Le scansioni di sola mappatura richiedono meno tempo rispetto alle scansioni di mappatura e classificazione, poiché non accedono ai file per visualizzare i dati all'interno. Si consiglia di eseguire questa operazione inizialmente per identificare le aree di ricerca e quindi eseguire una scansione Map & Classify su tali aree.
- **Le scansioni Map & Classify** forniscono una scansione profonda dei vostri dati.

La tabella seguente mostra alcune delle differenze:

Funzione	Mappatura e classificazione delle scansioni	Scansioni di sola mappatura
Velocità di scansione	Lento	Veloce
Prezzi	Gratuito	Gratuito
Capacità	Limitato a 500 TiB*	Limitato a 500 TiB*
Elenco dei tipi di file e della capacità utilizzata	Sì	Sì
Numero di file e capacità utilizzata	Sì	Sì
Età e dimensioni dei file	Sì	Sì
Possibilità di eseguire un "Report di mappatura dei dati"	Sì	Sì
Pagina di analisi dei dati per visualizzare i dettagli del file	Sì	No
Cercare i nomi all'interno dei file	Sì	No
Creare "ricerche salvate" che forniscono risultati di ricerca personalizzati	Sì	No
Possibilità di eseguire altri report	Sì	No
Possibilità di visualizzare i metadati dei file*	No	Sì

{asterisco} include::_include/connector-limit.adoc[]

*I seguenti metadati vengono estratti dai file durante le scansioni di mappatura:

- Ambiente di lavoro
- Tipo di ambiente di lavoro
- Repository di storage
- Tipo di file
- Capacità utilizzata
- Numero di file
- Dimensione del file
- Creazione di file
- Ultimo accesso al file
- Ultima modifica al file
- Ora di rilevamento file
- Estrazione delle autorizzazioni

Differenze del dashboard di governance:

Funzione	Mappa e classifica	Mappa
Dati obsoleti	Sì	Sì
Dati non aziendali	Sì	Sì
File duplicati	Sì	Sì
Ricerche salvate predefinite	Sì	No
Ricerche salvate predefinite	Sì	Sì
Rapporto DDA	Sì	Sì
Rapporto di mappatura	Sì	Sì
Rilevamento del livello di sensibilità	Sì	No
Dati sensibili con autorizzazioni estese	Sì	No
Autorizzazioni aperte	Sì	Sì
Età dei dati	Sì	Sì
Dimensioni dei dati	Sì	Sì
Categorie	Sì	No
Tipi di file	Sì	Sì

Differenze del dashboard di conformità:

Funzione	Mappa e classifica	Mappa
Informazioni personali	Sì	No
Informazioni personali sensibili	Sì	No
Report di valutazione sui rischi legati alla privacy	Sì	No
Report HIPAA	Sì	No
Report PCI DSS	Sì	No

Differenze tra i filtri di analisi:

Funzione	Mappa e classifica	Mappa
Ricerche salvate	Sì	Sì
Tipo di ambiente di lavoro	Sì	Sì
Ambiente di lavoro	Sì	Sì
Repository di storage	Sì	Sì
Tipo di file	Sì	Sì
Dimensione del file	Sì	Sì
Ora di creazione	Sì	Sì
Tempo scoperto	Sì	Sì
Ultima modifica	Sì	Sì
Ultimo accesso	Sì	Sì
Autorizzazioni aperte	Sì	Sì
Percorso directory file	Sì	Sì
Categoria	Sì	No
Livello di sensibilità	Sì	No
Numero di identificatori	Sì	No
Dati personali	Sì	No
Dati personali sensibili	Sì	No
Soggetto interessato	Sì	No
Duplicati	Sì	Sì
Stato di classificazione	Sì	Lo stato è sempre "informazioni riservate"
Evento di analisi della scansione	Sì	Sì
Hash file	Sì	Sì
Numero di utenti con accesso	Sì	Sì
Autorizzazioni utente/gruppo	Sì	Sì
Proprietario del file	Sì	Sì
Tipo di directory	Sì	Sì

Con quale rapidità la classificazione BlueXP esegue la scansione dei dati

La velocità di scansione è influenzata dalla latenza di rete, dalla latenza del disco, dalla larghezza di banda della rete, dalle dimensioni dell'ambiente e dalle dimensioni della distribuzione dei file.

- Quando si eseguono scansioni di sola mappatura, la classificazione BlueXP può eseguire la scansione tra

100-150 tibs di dati al giorno.

- Quando si eseguono scansioni mappa e classificazione, la classificazione BlueXP può eseguire la scansione tra 15-40 tibs di dati al giorno.

Esegui la scansione dei volumi Azure NetApp Files con classificazione BlueXP

Completa alcuni passaggi per iniziare a utilizzare la classificazione BlueXP per Azure NetApp Files.

Individuare il sistema Azure NetApp Files che si desidera sottoporre a scansione

Se il sistema Azure NetApp Files che si desidera sottoporre a scansione non è già in BlueXP come ambiente di lavoro, è possibile aggiungerlo all'area di lavoro in questo momento.

"Scopri come scoprire il sistema Azure NetApp Files in BlueXP".

Distribuire l'istanza di classificazione BlueXP

"Implementare la classificazione BlueXP" se non è già stata implementata un'istanza.

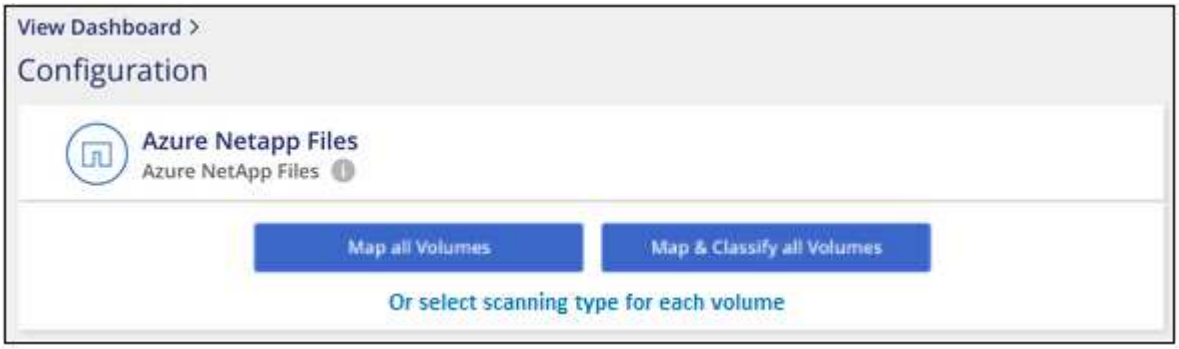
La classificazione BlueXP deve essere implementata nel cloud durante la scansione dei volumi Azure NetApp Files e deve essere implementata nella stessa regione dei volumi che si desidera sottoporre a scansione.

Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi Azure NetApp Files.

Abilita la classificazione BlueXP nei tuoi ambienti di lavoro

È possibile attivare la classificazione BlueXP sui volumi Azure NetApp Files.

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.
2. Dal menu classificazione BlueXP , selezionare **Configurazione**.



3. Selezionare la modalità di scansione dei volumi in ciascun ambiente di lavoro. "Scopri le scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, selezionare **Mappa tutti i volumi**.
   - Per mappare e classificare tutti i volumi, selezionare **Mappa e classifica tutti i volumi**.
   - Per personalizzare la scansione per ciascun volume, selezionare **o selezionare il tipo di scansione per ciascun volume**, quindi scegliere i volumi che si desidera mappare e/o classificare.

     Per ulteriori informazioni, vedere Abilitare e disabilitare le scansioni di conformità sui volumi .

4. Nella finestra di dialogo di conferma, selezionare **approva** per avviare la scansione dei volumi con la classificazione BlueXP .

Risultato

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la classificazione BlueXP completa le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore. È possibile tenere traccia dell'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando poi la **Configurazione ambiente di lavoro**. L'avanzamento di ogni scansione viene visualizzato come barra di avanzamento. È inoltre possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file sottoposti a scansione rispetto al totale dei file nel volume.

- Per impostazione predefinita, se la classificazione di BlueXP non dispone delle autorizzazioni di scrittura in CIFS o di scrittura in NFS, il sistema non esegue la scansione dei file nei volumi perché la classificazione di BlueXP non può riportare l'ultimo tempo di accesso alla data e ora originale. Se non si ha cura di ripristinare l'ultimo tempo di accesso, fare clic su **o selezionare il tipo di scansione per ciascun volume**. La pagina risultante dispone di un'impostazione che è possibile attivare in modo che la classificazione BlueXP scansiona i volumi indipendentemente dalle autorizzazioni.
- La classificazione BlueXP esegue la scansione di una sola condivisione file in un volume. Se si dispone di più condivisioni nei volumi, sarà necessario eseguire la scansione di tali condivisioni separatamente come gruppo di condivisioni. "Per ulteriori informazioni su questa limitazione di classificazione di BlueXP, vedere".

Verificare che la classificazione BlueXP abbia accesso ai volumi

Assicurarsi che la classificazione BlueXP possa accedere ai volumi controllando la rete, i gruppi di sicurezza e le policy di esportazione. È necessario fornire la classificazione BlueXP con le credenziali CIFS in modo che possa accedere ai volumi CIFS.

Per Azure NetApp Files, la classificazione BlueXP può eseguire la scansione solo dei volumi che si trovano nella stessa regione di BlueXP.

Fasi

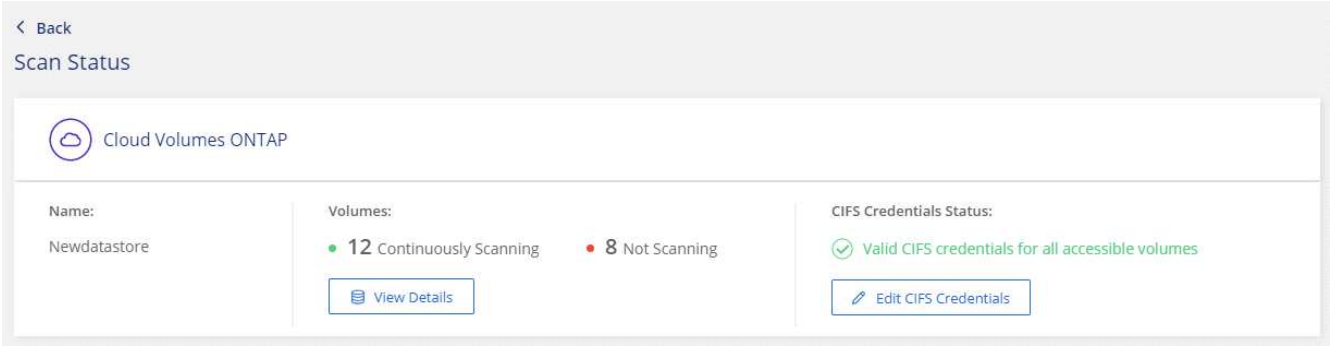
1. Assicurarsi che sia presente una connessione di rete tra l'istanza di classificazione BlueXP e ciascuna rete che include volumi per Azure NetApp Files.
2. Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
   - Per NFS: Porte 111 e 2049.
   - Per CIFS – porte 139 e 445.
3. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.
   a. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
5. Dal menu classificazione BlueXP , selezionare **Configurazione**.

a. Per ogni ambiente di lavoro, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS sul sistema.

   Le credenziali possono essere di sola lettura, ma fornendo credenziali di amministratore si garantisce che la classificazione BlueXP possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza di classificazione BlueXP.

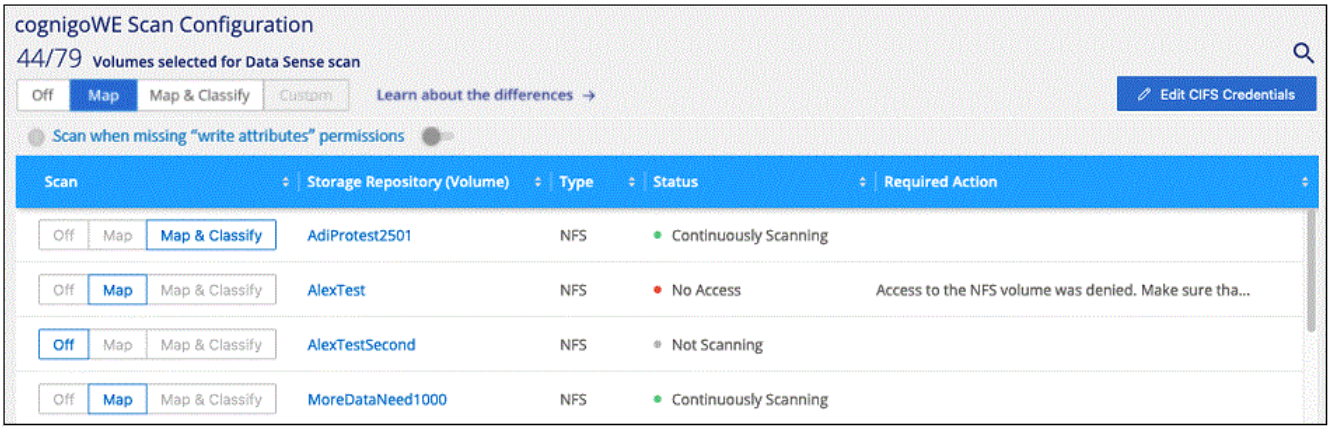
   Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory come parte di un gruppo padre nell'organizzazione che disponga delle autorizzazioni per tutti i file.

   Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.



6. Nella pagina Configuration (Configurazione), selezionare **View Details** (Visualizza dettagli) per controllare lo stato di ogni volume CIFS e NFS e correggere eventuali errori.

Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.

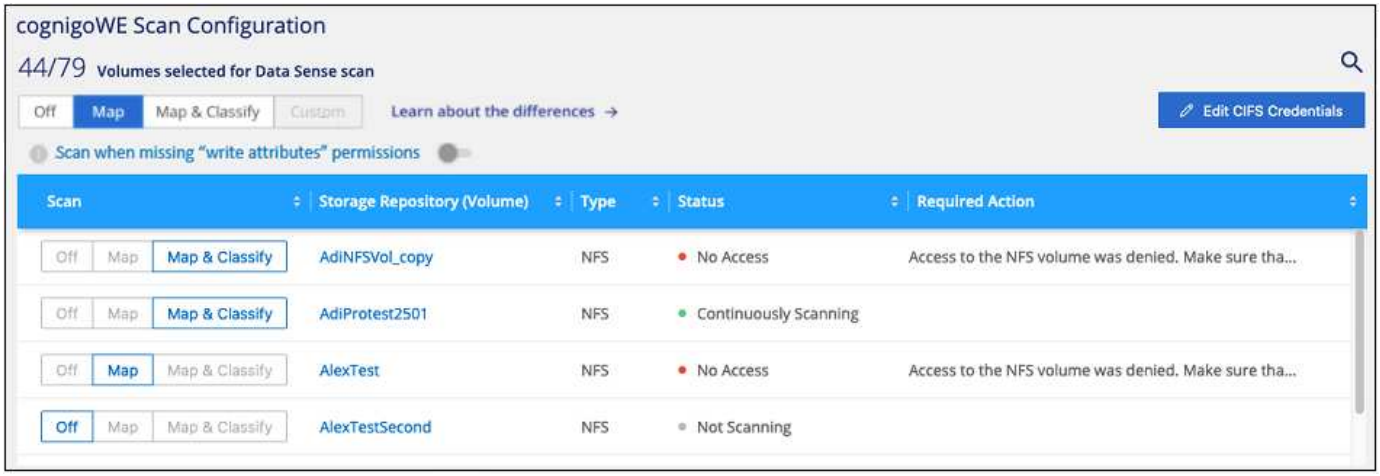


Abilitare e disabilitare le scansioni di conformità sui volumi

È possibile avviare o interrompere scansioni di sola mappatura, o scansioni di mappatura e classificazione, in un ambiente di lavoro in qualsiasi momento dalla pagina di configurazione. È inoltre possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa. Si consiglia di eseguire la scansione di tutti i volumi.

I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo se è stata impostata l'impostazione **Map** o **Map & Classify** nell'area di intestazione. Se l'opzione è impostata su **Custom** o **Off** nell'area heading, è necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto nell'ambiente di lavoro.

Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione di BlueXP non dispone di permessi di scrittura in CIFS o di permessi di scrittura in NFS, il sistema non eseguirà la scansione dei file perché la classificazione di BlueXP non può riportare l'"ultimo tempo di accesso" all'indicatore data e ora originale. Se non si ha alcun problema se l'ultimo tempo di accesso viene reimpostato, attivare l'interruttore per eseguire la scansione di tutti i file, indipendentemente dalle autorizzazioni. "Scopri di più".



Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Effettuare una delle seguenti operazioni:
   - Per attivare le scansioni di sola mappatura su un volume, nell'area del volume selezionare **Mappa**. Per attivare su tutti i volumi, nell'area intestazione selezionare **Mappa**.
   - Per abilitare la scansione completa su un volume, nell'area del volume selezionare **Mappa e Classifica**. Per attivare su tutti i volumi, nell'area intestazione selezionare **Mappa e Classifica**.
   - Per disattivare la scansione su un volume, nell'area del volume selezionare **Off**. Per disattivare la scansione su tutti i volumi, nell'area di intestazione selezionare **Off**.

Esegui la scansione di Amazon FSX per volumi ONTAP con classificazione BlueXP

Completa alcuni passaggi per iniziare a eseguire la scansione di Amazon FSX per il volume ONTAP con classificazione BlueXP.

Prima di iniziare

- È necessario un connettore attivo in AWS per implementare e gestire la classificazione BlueXP.
- Il gruppo di protezione selezionato durante la creazione dell'ambiente di lavoro deve consentire il traffico dall'istanza di classificazione BlueXP. È possibile trovare il gruppo di protezione associato utilizzando l'ENI connesso al file system FSX per ONTAP e modificarlo utilizzando la console di gestione AWS.

  "Gruppi di sicurezza AWS per istanze Linux"

  "Gruppi di sicurezza AWS per le istanze di Windows"

  "AWS Elastic Network Interface (ENI)"

- Assicurarsi che le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.

Distribuire l'istanza di classificazione BlueXP

"Implementare la classificazione BlueXP" se non è già stata implementata un'istanza.

È necessario implementare la classificazione BlueXP nella stessa rete AWS del connettore per AWS e dei volumi FSX che si desidera sottoporre a scansione.

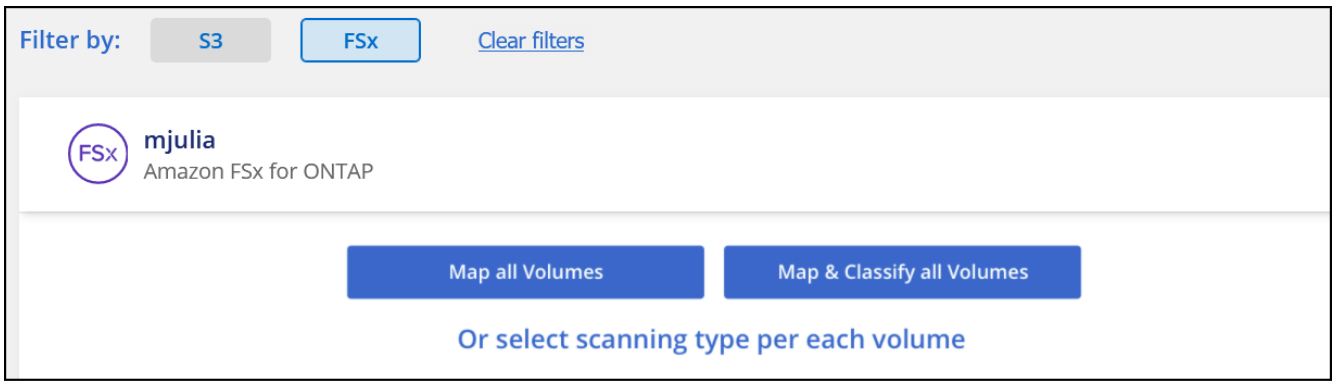
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi FSX.

Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Abilita la classificazione BlueXP nei tuoi ambienti di lavoro

È possibile attivare la classificazione BlueXP per FSX per volumi ONTAP.

1. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
2. Dal menu classificazione BlueXP , selezionare **Configurazione**.



3. Selezionare la modalità di scansione dei volumi in ciascun ambiente di lavoro. "Scopri le scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, fare clic su **Map All Volumes** (Mappa tutti i volumi).

- Per mappare e classificare tutti i volumi, fare clic su **Map & Classify All Volumes** (Mappa e classificazione di tutti i volumi).
- Per personalizzare la scansione per ciascun volume, fare clic su **o selezionare il tipo di scansione per ciascun volume**, quindi scegliere i volumi da mappare e/o classificare.

4. Nella finestra di dialogo di conferma, fare clic su **approva** per avviare la scansione dei volumi con la classificazione BlueXP.

Risultato

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati saranno disponibili nella dashboard Compliance non appena la classificazione BlueXP completa le scansioni iniziali. Il tempo necessario dipende dalla quantità di dati, che potrebbe essere di pochi minuti o ore. È possibile tenere traccia dell'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando poi la **Configurazione ambiente di lavoro**. L'avanzamento di ogni scansione viene visualizzato come barra di avanzamento. È inoltre possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file sottoposti a scansione rispetto al totale dei file nel volume.

- Per impostazione predefinita, se la classificazione di BlueXP non dispone delle autorizzazioni di scrittura in CIFS o di scrittura in NFS, il sistema non esegue la scansione dei file nei volumi perché la classificazione di BlueXP non può riportare l'ultimo tempo di accesso alla data e ora originale. Se non si ha cura di ripristinare l'ultimo tempo di accesso, fare clic su **o selezionare il tipo di scansione per ciascun volume**. La pagina risultante dispone di un'impostazione che è possibile attivare in modo che la classificazione BlueXP scansiona i volumi indipendentemente dalle autorizzazioni.
- La classificazione BlueXP esegue la scansione di una sola condivisione file in un volume. Se si dispone di più condivisioni nei volumi, sarà necessario eseguire la scansione di tali condivisioni separatamente come gruppo di condivisioni. "Per ulteriori informazioni su questa limitazione di classificazione di BlueXP, vedere".

Verificare che la classificazione BlueXP abbia accesso ai volumi

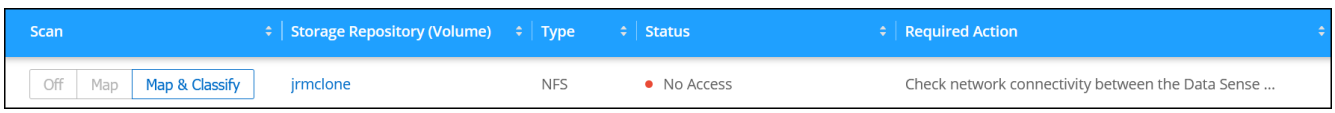
Assicurarsi che la classificazione BlueXP possa accedere ai volumi controllando la rete, i gruppi di sicurezza e le policy di esportazione.

È necessario fornire la classificazione BlueXP con le credenziali CIFS in modo che possa accedere ai volumi CIFS.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Nella pagina Configurazione, selezionare **Visualizza dettagli** per controllare lo stato e correggere eventuali errori.

   Ad esempio, l'immagine seguente mostra che la classificazione BlueXP di un volume non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



3. Assicurarsi che sia presente una connessione di rete tra l'istanza di classificazione BlueXP e ciascuna rete che include volumi per FSX per ONTAP.

Per FSX per ONTAP, la classificazione BlueXP può eseguire la scansione dei volumi solo nella stessa regione di BlueXP.

4. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
5. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.

   a. Dal menu classificazione BlueXP , selezionare **Configurazione**.
   b. Per ogni ambiente di lavoro, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS sul sistema.

      Le credenziali possono essere di sola lettura, ma fornendo credenziali di amministratore si garantisce che la classificazione BlueXP possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza di classificazione BlueXP.

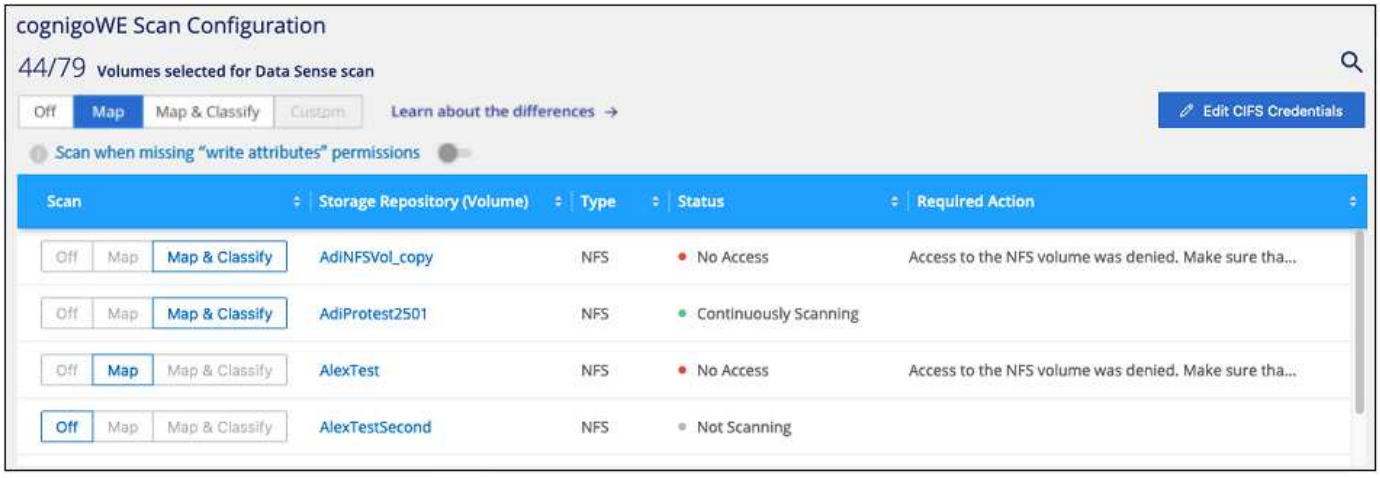
      Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory come parte di un gruppo padre nell'organizzazione che disponga delle autorizzazioni per tutti i file.

   Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.

Abilitare e disabilitare le scansioni di conformità sui volumi

È possibile avviare o interrompere scansioni di sola mappatura, o scansioni di mappatura e classificazione, in un ambiente di lavoro in qualsiasi momento dalla pagina di configurazione. È inoltre possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa. Si consiglia di eseguire la scansione di tutti i volumi.

Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione di BlueXP non dispone di permessi di scrittura in CIFS o di permessi di scrittura in NFS, il sistema non eseguirà la scansione dei file perché la classificazione di BlueXP non può riportare l'"ultimo tempo di accesso" all'indicatore data e ora originale. Se non si ha alcun problema se l'ultimo tempo di accesso viene reimpostato, attivare l'interruttore per eseguire la scansione di tutti i file, indipendentemente dalle autorizzazioni. "Scopri di più".



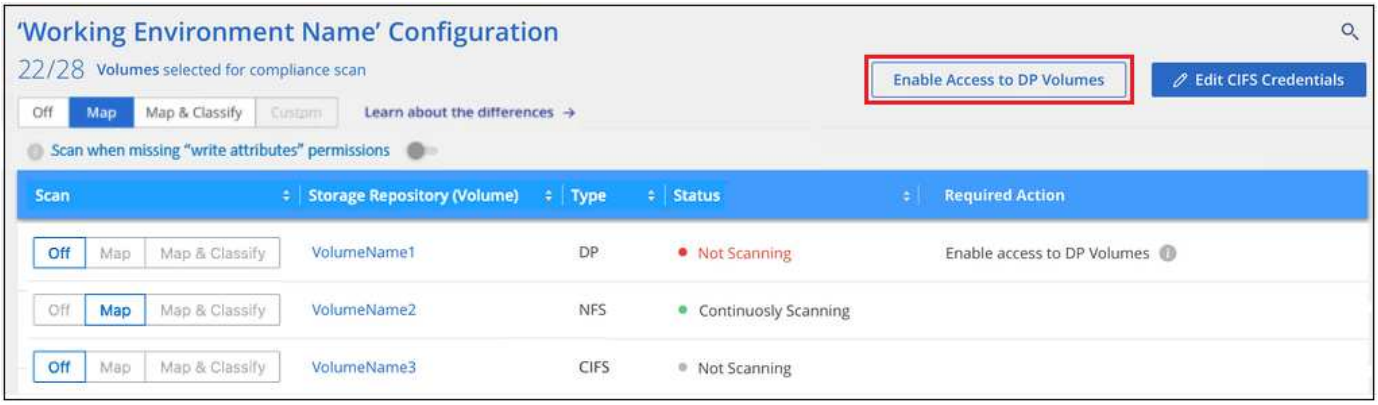
1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Nella pagina di configurazione, individuare l'ambiente di lavoro con i volumi da sottoporre a scansione.
3. Effettuare una delle seguenti operazioni:
   - Per attivare le scansioni di sola mappatura su un volume, nell'area del volume selezionare **Mappa**. Oppure, per attivare su tutti i volumi, nell'area di intestazione, selezionare **Mappa**. Per abilitare la scansione completa su un volume, nell'area del volume selezionare **Mappa e Classifica**. Oppure, per attivare su tutti i volumi, nell'area di intestazione, selezionare **Mappa e Classifica**.
   - Per disattivare la scansione su un volume, nell'area del volume selezionare **Off**. Per disattivare la scansione su tutti i volumi, nell'area di intestazione selezionare **Off**.

> I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo se è stata impostata l'impostazione **Map** o **Map & Classify** nell'area di intestazione. Se l'opzione è impostata su **Custom** o **Off** nell'area heading, è necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto nell'ambiente di lavoro.

Eseguire la scansione dei volumi di protezione dei dati

Per impostazione predefinita, i volumi di protezione dei dati (DP) non vengono sottoposti a scansione perché non sono esposti esternamente e la classificazione BlueXP non può accedervi. Questi sono i volumi di destinazione per le operazioni SnapMirror da un file system FSX per ONTAP.

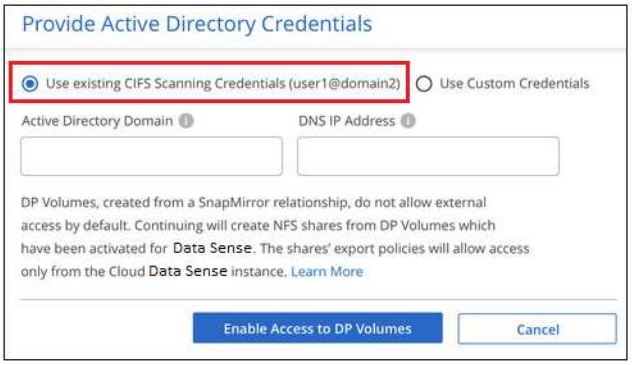
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

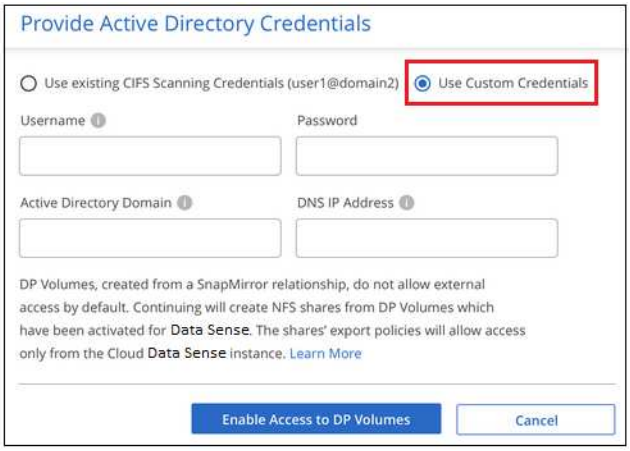


Fasi

Se si desidera eseguire la scansione di questi volumi di protezione dei dati:

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Selezionare **Abilita accesso ai volumi DP** nella parte superiore della pagina.
3. Leggere il messaggio di conferma e selezionare nuovamente **Abilita accesso ai volumi DP**.
   - I volumi creati inizialmente come volumi NFS nel file system FSX di origine per ONTAP sono abilitati.
   - I volumi creati inizialmente come volumi CIFS nel file system FSX di origine per ONTAP richiedono l'immissione delle credenziali CIFS per eseguire la scansione di tali volumi DP. Se sono già state immesse le credenziali Active Directory in modo che la classificazione BlueXP possa eseguire la scansione dei volumi CIFS, è possibile utilizzare tali credenziali oppure specificare un set diverso di credenziali Admin.





4. Attivare ciascun volume DP che si desidera sottoporre a scansione.

Risultato

Una volta attivata, la classificazione BlueXP crea una condivisione NFS da ogni volume DP attivato per la scansione. I criteri di esportazione delle condivisioni consentono l'accesso solo dall'istanza di classificazione BlueXP.

Se non si dispone di volumi di protezione dati CIFS quando è stato attivato l'accesso ai volumi DP e successivamente ne sono stati aggiunti altri, il pulsante **Enable Access to CIFS DP** (Abilita accesso a CIFS DP) viene visualizzato nella parte superiore della pagina di configurazione. Selezionare questo pulsante e aggiungere le credenziali CIFS per abilitare l'accesso a questi volumi DP CIFS.

Le credenziali Active Directory vengono registrate solo nella VM storage del primo volume CIFS DP, pertanto tutti i volumi DP presenti nella SVM verranno sottoposti a scansione. Tutti i volumi che risiedono su altre SVM non avranno le credenziali di Active Directory registrate, pertanto tali volumi DP non verranno sottoposti a scansione.

Esegui la scansione di Cloud Volumes ONTAP e dei volumi ONTAP on-premise con classificazione BlueXP

Completare alcuni passaggi per iniziare la scansione dei volumi Cloud Volumes ONTAP e ONTAP on-premise utilizzando la classificazione BlueXP.

Prerequisiti

Prima di attivare la classificazione BlueXP , assicurarsi di disporre di una configurazione supportata.

- Se si esegue la scansione di sistemi Cloud Volumes ONTAP e ONTAP in sede accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" o "in una sede on-premise con accesso a internet".
- Se si esegue la scansione di sistemi ONTAP interni installati in un sito oscuro che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

Abilitare la scansione della classificazione BlueXP negli ambienti di lavoro

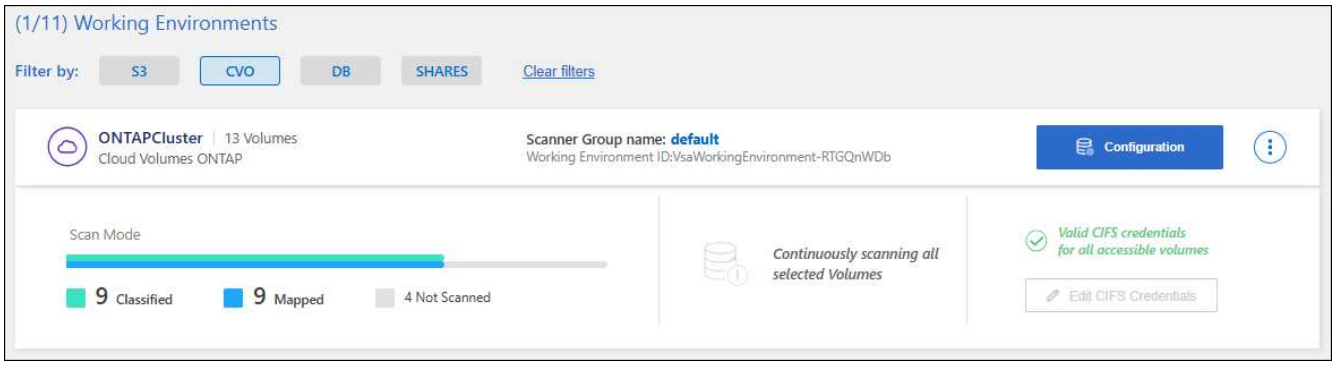
Puoi abilitare la scansione della classificazione BlueXP sui sistemi Cloud Volumes ONTAP in qualsiasi cloud

provider supportato e sui cluster ONTAP on-premise.

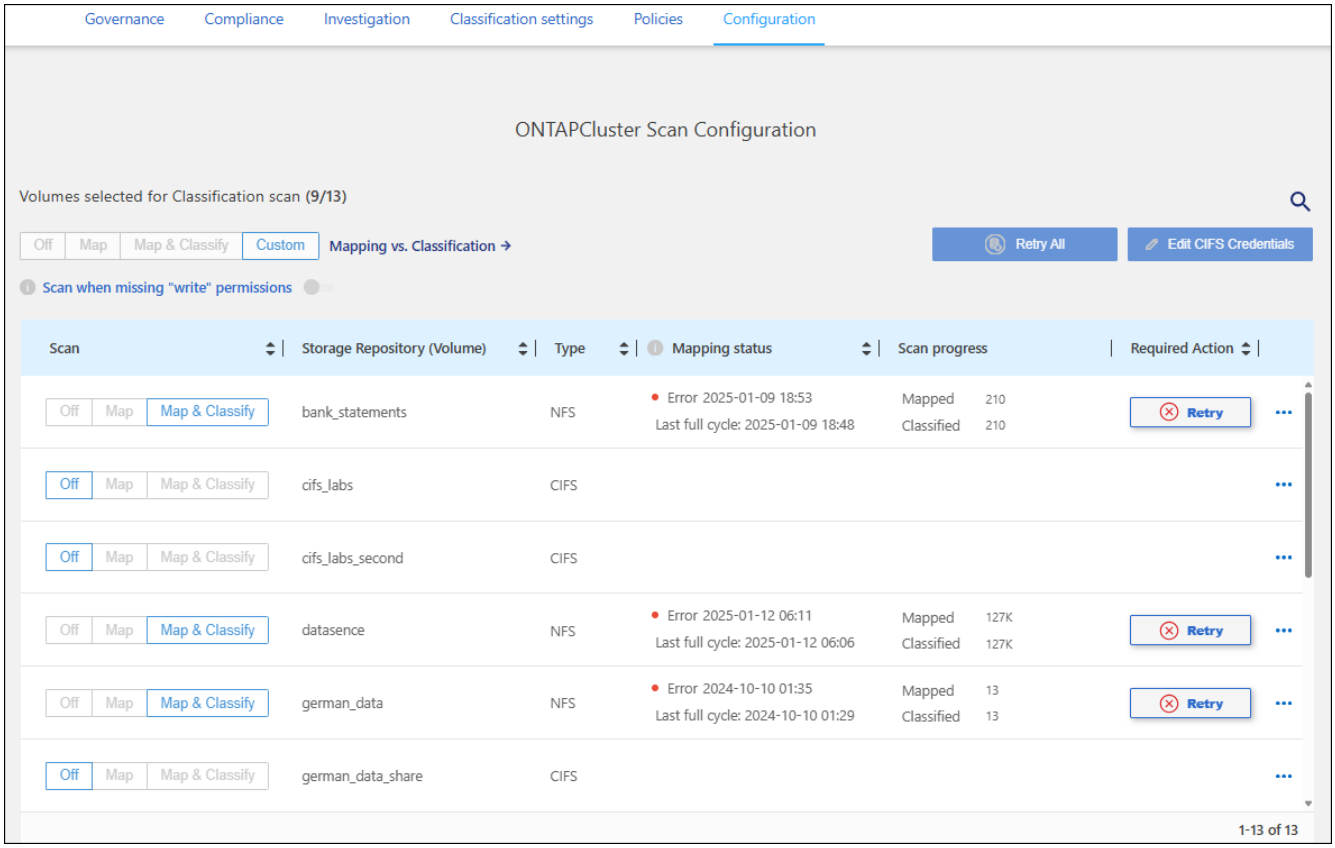
Fasi

1. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
2. Dal menu classificazione BlueXP , selezionare **Configurazione**.

   La pagina di configurazione mostra più ambienti di lavoro.



3. Scegliere un ambiente di lavoro e selezionare **Configurazione**.



4. Se non si ha interesse se l'ultima ora di accesso è stata reimpostata, ATTIVARE l'opzione **scansione quando mancano le autorizzazioni di "scrittura attributi"** e tutti i file vengono sottoposti a scansione indipendentemente dalle autorizzazioni.

   Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione BlueXP non dispone di autorizzazioni di scrittura degli attributi in

CIFS o di scrittura in NFS, il sistema non classificherà i file perché la classificazione BlueXP non può ripristinare l'ora dell'ultimo accesso all'indicatore di data e ora originale. "Scopri di più".

5. Selezionare la modalità di scansione dei volumi in ciascun ambiente di lavoro. "Scopri le scansioni di mappatura e classificazione":
   - Per mappare tutti i volumi, selezionare **Mappa**.
   - Per mappare e classificare tutti i volumi, selezionare **Mappa e Classifica**.
   - Per personalizzare la scansione di ciascun volume, selezionare **personalizzato**, quindi scegliere i volumi che si desidera mappare e/o classificare.
6. Nella finestra di dialogo di conferma, selezionare **approva** per avviare la scansione dei volumi con la classificazione BlueXP .

Risultato

La classificazione BlueXP avvia la scansione dei volumi selezionati nell'ambiente di lavoro. I risultati iniziano a comparire nel dashboard conformità non appena la classificazione BlueXP inizia la scansione. Il tempo necessario per il completamento dipende dalla quantità di dati — può essere di pochi minuti o ore.

> La classificazione BlueXP esegue la scansione di una sola condivisione file in un volume. Se si dispone di più condivisioni nei volumi, sarà necessario eseguire la scansione di tali condivisioni separatamente come gruppo di condivisioni. "Per ulteriori informazioni su questa limitazione di classificazione di BlueXP, vedere".

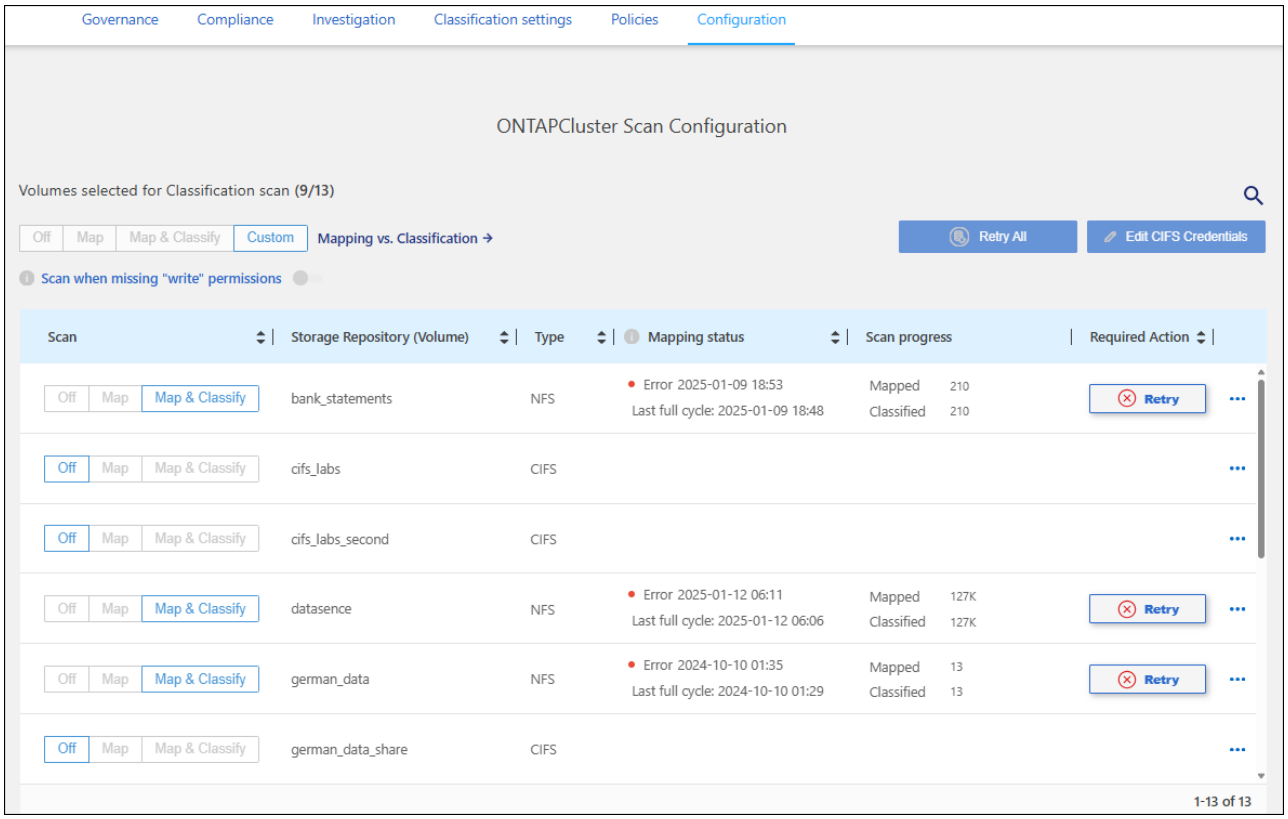
Verificare che la classificazione BlueXP abbia accesso ai volumi

Assicurarsi che la classificazione BlueXP possa accedere ai volumi controllando la rete, i gruppi di sicurezza e le policy di esportazione. È necessario fornire la classificazione BlueXP con le credenziali CIFS in modo che possa accedere ai volumi CIFS.

Fasi

1. Assicurarsi che sia presente una connessione di rete tra l'istanza di classificazione BlueXP e ciascuna rete che include volumi per cluster Cloud Volumes ONTAP o ONTAP on-premise.
2. Assicurarsi che il gruppo di protezione per Cloud Volumes ONTAP consenta il traffico in entrata dall'istanza di classificazione BlueXP.

   È possibile aprire il gruppo di protezione per il traffico dall'indirizzo IP dell'istanza di classificazione BlueXP oppure aprire il gruppo di protezione per tutto il traffico dall'interno della rete virtuale.
3. Assicurarsi che i criteri di esportazione dei volumi NFS includano l'indirizzo IP dell'istanza di classificazione BlueXP in modo che possa accedere ai dati di ciascun volume.
4. Se si utilizza CIFS, fornire la classificazione BlueXP con le credenziali Active Directory in modo che possa eseguire la scansione dei volumi CIFS.
   a. Dal menu di navigazione sinistro di BlueXP , selezionare **Governance > classificazione**.
   b. Dal menu classificazione BlueXP , selezionare **Configurazione**.



c. Per ogni ambiente di lavoro, selezionare **Modifica credenziali CIFS** e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS sul sistema.

   Le credenziali possono essere di sola lettura, ma fornendo credenziali di amministratore si garantisce che la classificazione BlueXP possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza di classificazione BlueXP.

   Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory come parte di un gruppo padre nell'organizzazione che disponga delle autorizzazioni per tutti i file.

Dopo aver immesso le credenziali, viene visualizzato un messaggio che indica che tutti i volumi CIFS sono stati autenticati correttamente.

5. Nella pagina Configuration (Configurazione), selezionare **Configuration** (Configurazione) per controllare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

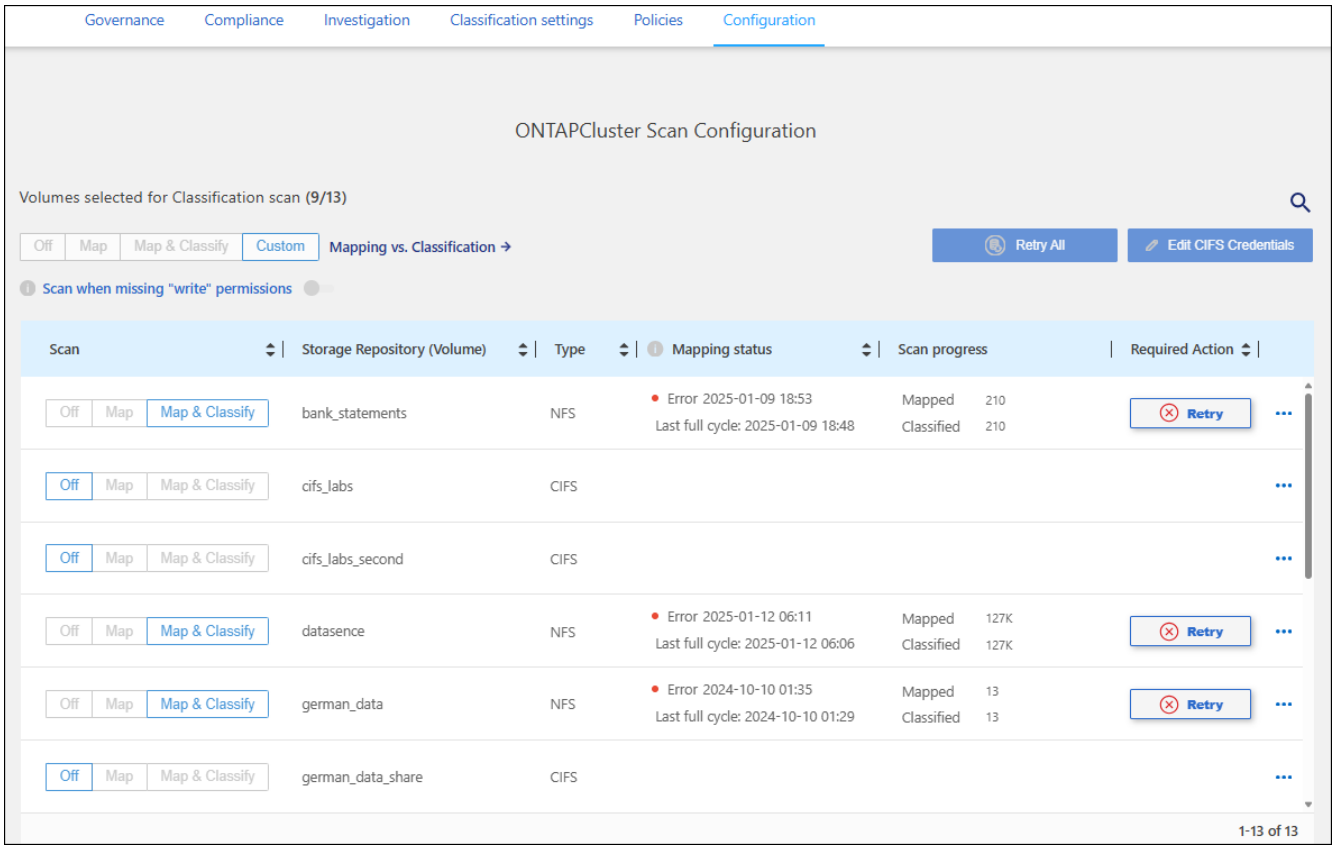
Disattivare le scansioni di conformità sui volumi

È possibile avviare o interrompere scansioni di sola mappatura, o scansioni di mappatura e classificazione, in un ambiente di lavoro in qualsiasi momento dalla pagina di configurazione. È inoltre possibile passare da scansioni di sola mappatura a scansioni di mappatura e classificazione e viceversa. Si consiglia di eseguire la scansione di tutti i volumi.

I nuovi volumi aggiunti all'ambiente di lavoro vengono sottoposti automaticamente a scansione solo se è stata impostata l'impostazione **Map** o **Map & Classify** nell'area di intestazione. Quando l'opzione è impostata su **personalizzato** o **Off** nell'area di intestazione, è necessario attivare la mappatura e/o la scansione completa su ogni nuovo volume aggiunto nell'ambiente di lavoro.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Selezionare il pulsante **Configurazione** per l'ambiente di lavoro che si desidera modificare.



3. Effettuare una delle seguenti operazioni:
   - Per disattivare la scansione su un volume, nell'area del volume selezionare **Off**.
   - Per disattivare la scansione su tutti i volumi, nell'area di intestazione selezionare **Off**.

Eseguire la scansione degli schemi del database con classificazione BlueXP

Completare alcuni passaggi per avviare la scansione degli schemi di database con la classificazione BlueXP.

Esaminare i prerequisiti

Prima di attivare la classificazione BlueXP, verificare di disporre di una configurazione supportata.

Database supportati

La classificazione BlueXP può eseguire la scansione degli schemi dai seguenti database:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle

- PostgreSQL
- SAP HANA
- SQL Server (MSSQL)

La funzione di raccolta delle statistiche **deve essere abilitata** nel database.

Requisiti del database

Qualsiasi database con connettività all'istanza di classificazione BlueXP può essere sottoposto a scansione, indipendentemente dalla posizione in cui è ospitato. Per connettersi al database sono necessarie solo le seguenti informazioni:

- Indirizzo IP o nome host
- Porta
- Nome del servizio (solo per l'accesso ai database Oracle)
- Credenziali che consentono l'accesso in lettura agli schemi

  Quando si sceglie un nome utente e una password, è importante sceglierne uno che disponga delle autorizzazioni di lettura complete per tutti gli schemi e le tabelle che si desidera sottoporre a scansione. Si consiglia di creare un utente dedicato per il sistema di classificazione BlueXP con tutte le autorizzazioni necessarie.

Nota: per MongoDB, è necessario un ruolo Admin di sola lettura.

Distribuire l'istanza di classificazione BlueXP

Distribuire la classificazione BlueXP se non è già stata implementata un'istanza.

Se si eseguono scansioni di schemi di database accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" oppure "Implementare la classificazione BlueXP in una posizione on-premise con accesso a Internet".

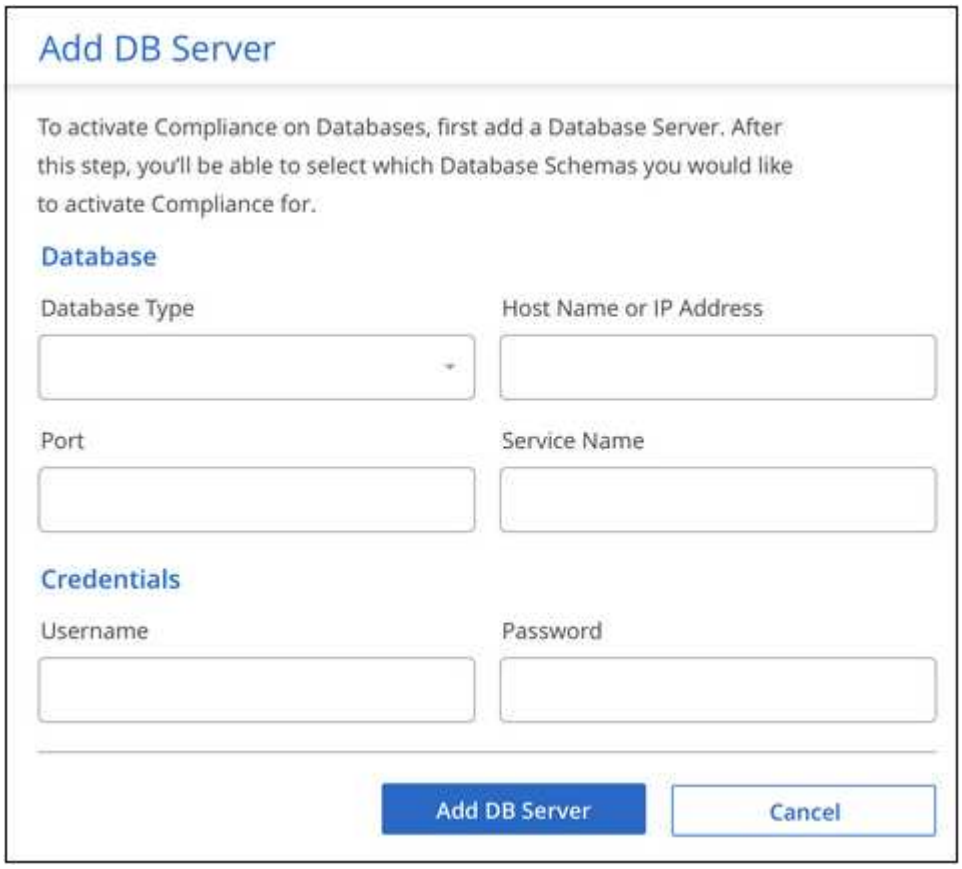
Se si eseguono scansioni di schemi di database installati in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

Aggiungere il server database

Aggiungere il server di database in cui risiedono gli schemi.

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Nella pagina Configurazione, selezionare **Aggiungi ambiente di lavoro** > **Aggiungi server database**.
3. Inserire le informazioni richieste per identificare il server di database.
   a. Selezionare il tipo di database.
   b. Immettere la porta e il nome host o l'indirizzo IP per la connessione al database.
   c. Per i database Oracle, immettere il nome del servizio.
   d. Inserire le credenziali in modo che la classificazione BlueXP possa accedere al server.

e. Fare clic su **Add DB Server** (Aggiungi server DB).



Il database viene aggiunto all'elenco degli ambienti di lavoro.

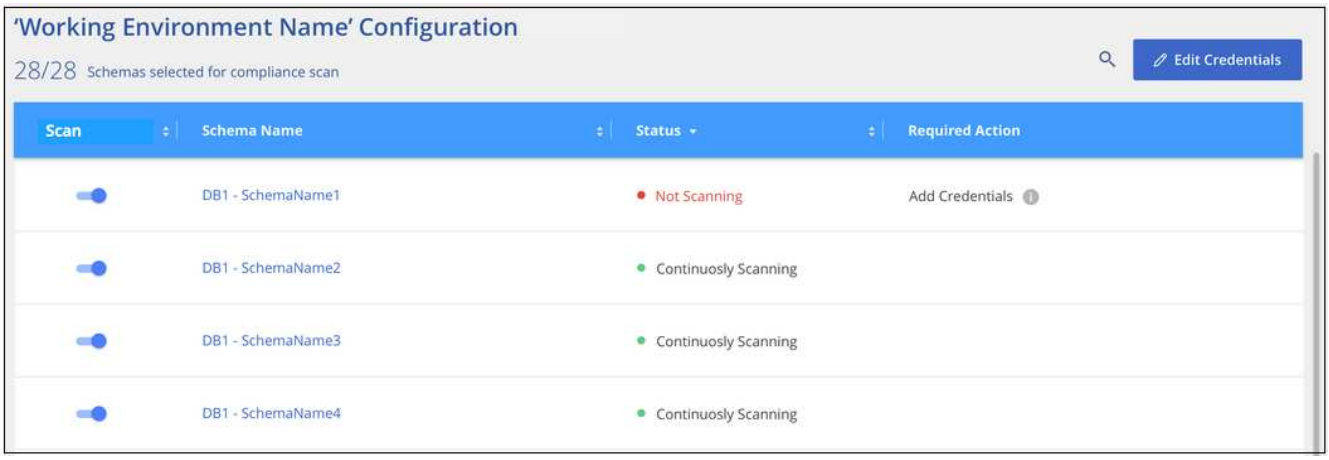
Abilitare e disabilitare le scansioni di conformità sugli schemi di database

È possibile interrompere o avviare la scansione completa degli schemi in qualsiasi momento.

Non è disponibile alcuna opzione per selezionare le scansioni di sola mappatura per gli schemi di database.

1. Nella pagina Configurazione, selezionare il pulsante **Configurazione** per il database che si desidera configurare.

2. Selezionare gli schemi da sottoporre a scansione spostando il dispositivo di scorrimento verso destra.



Risultato

La classificazione BlueXP avvia la scansione degli schemi di database abilitati. È possibile tenere traccia dell'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando poi la **Configurazione ambiente di lavoro**. L'avanzamento di ogni scansione viene visualizzato come barra di avanzamento. È inoltre possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file sottoposti a scansione rispetto al totale dei file nel volume. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

La classificazione BlueXP analizza i database una volta al giorno; i database non vengono sottoposti a scansione continua come altre origini dati.

Eseguire la scansione delle condivisioni di file con classificazione BlueXP

Per analizzare le condivisioni file, è necessario prima creare un gruppo di condivisioni file nella BlueXP classification. I gruppi di condivisioni file sono per le condivisioni NFS o CIFS (SMB) ospitate in locale o nel cloud.

La scansione dei dati da condivisioni di file non NetApp non è supportata nella versione principale della classificazione BlueXP.

Prerequisiti

Prima di attivare la classificazione BlueXP, verificare di disporre di una configurazione supportata.

- Le condivisioni possono essere ospitate ovunque, anche nel cloud o on-premise. È possibile eseguire la scansione delle condivisioni CIFS di sistemi storage NetApp 7-Mode meno recenti come condivisioni di file.
  - La BlueXP classification non è in grado di estrarre le autorizzazioni o l'"ultimo orario di accesso" dai sistemi 7-Mode.
  - A causa di un problema noto tra alcune versioni di Linux e le condivisioni CIFS sui sistemi 7-Mode, è necessario configurare la condivisione in modo che utilizzi solo SMBv1 con autenticazione NTLM abilitata.
- È necessario disporre di una connettività di rete tra l'istanza di classificazione BlueXP e le condivisioni.
- È possibile aggiungere una condivisione DFS (Distributed file System) come normale condivisione CIFS. Poiché la BlueXP classification non è a conoscenza del fatto che la condivisione è basata su più server/volumi combinati in un'unica condivisione CIFS, potrebbero essere visualizzati errori di autorizzazione o connettività relativi alla condivisione quando il messaggio si applica in realtà solo a una

delle cartelle/condivisioni che si trova su un server/volume diverso.

- Per le condivisioni CIFS (SMB), assicurarsi di disporre delle credenziali Active Directory che forniscono l'accesso in lettura alle condivisioni. Le credenziali di amministratore sono preferite nel caso in cui la classificazione BlueXP debba eseguire la scansione di qualsiasi dato che richieda autorizzazioni elevate.

  Per assicurarsi che gli "ultimi accessi" dei file non vengano modificati dalle scansioni BlueXP classification , si consiglia che l'utente disponga delle autorizzazioni di scrittura degli attributi in CIFS o di autorizzazioni di scrittura in NFS. Se possibile, configurare l'utente di Active Directory come parte di un gruppo padre nell'organizzazione che disponga delle autorizzazioni per tutti i file.

- Tutte le condivisioni file CIFS in un gruppo devono utilizzare le stesse credenziali di Active Directory.
- È possibile combinare condivisioni NFS e CIFS (utilizzando Kerberos o NTLM). È necessario aggiungere le condivisioni al gruppo separatamente. In altre parole, è necessario completare il processo due volte, una per protocollo.
  - Non è possibile creare un gruppo di condivisioni file che combini i tipi di autenticazione CIFS (Kerberos e NTLM).
- Se si utilizza CIFS con autenticazione Kerberos, assicurarsi che l'indirizzo IP fornito sia accessibile al servizio BlueXP classification . Le condivisioni file non possono essere aggiunte se l'indirizzo IP non è raggiungibile.

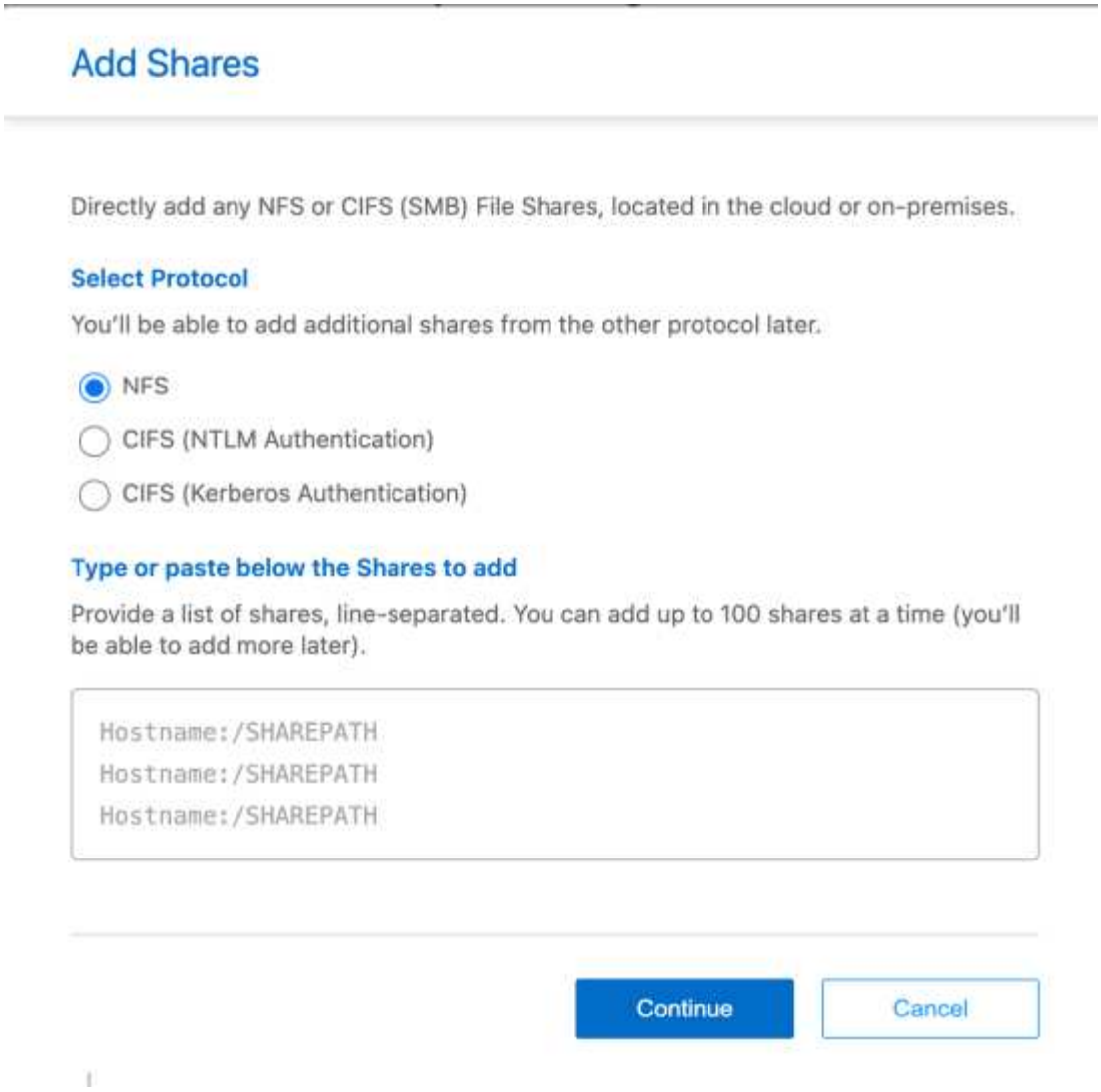
Crea un gruppo di condivisione file

Quando aggiungi condivisioni di file al gruppo, devi utilizzare il formato `<host_name>:/<share_path>` .

+ È possibile aggiungere le condivisioni file singolarmente oppure immettere un elenco separato da righe delle condivisioni file che si desidera analizzare. È possibile aggiungere fino a 100 condivisioni alla volta.

Fasi

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla pagina Configurazione, selezionare **Aggiungi ambiente di lavoro** > **Aggiungi gruppo condivisioni file**.
3. Nella finestra di dialogo Aggiungi gruppo di condivisioni file, immetti il nome per il gruppo di condivisioni, quindi seleziona **Continua**.
4. Selezionare il protocollo per le condivisioni file che si desidera aggiungere.



Se si aggiungono condivisioni CIFS con autenticazione NTLM, immettere le credenziali di Active Directory per accedere ai volumi CIFS. Sebbene siano supportate le credenziali di sola lettura, si consiglia di fornire l'accesso completo con credenziali di amministratore. Selezionare Salva.

1. Aggiungere le condivisioni di file che si desidera analizzare (una condivisione di file per riga). Quindi seleziona **Continua**.
2. Viene visualizzata una finestra di dialogo di conferma del numero di condivisioni aggiunte.

   Se la finestra di dialogo elenca le condivisioni che non è stato possibile aggiungere, acquisire queste informazioni in modo da risolvere il problema. Se il problema riguarda una convenzione di denominazione, puoi aggiungere nuovamente la condivisione con un nome corretto.

3. Configurare la scansione sul volume:
   - Per attivare le scansioni di sola mappatura sulle condivisioni di file, selezionare **Mappa**.
   - Per abilitare le scansioni complete sulle condivisioni di file, selezionare **Mappa e Classifica**.
   - Per disattivare la scansione sulle condivisioni file, selezionare **Off**.

Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la BlueXP classification non dispone di autorizzazioni per gli attributi di scrittura in CIFS o di autorizzazioni per la scrittura in NFS, il sistema non eseguirà la scansione dei file perché la BlueXP classification non può ripristinare l'orario dell'ultimo accesso al timestamp originale. + Se si imposta **Scansione in caso di autorizzazioni per gli attributi di scrittura mancanti** su **Attivato**, la scansione reimposta l'orario dell'ultimo accesso e analizza tutti i file indipendentemente dalle autorizzazioni. + Per ulteriori informazioni sull'orario dell'ultimo accesso, vedere xref:./"Metadati raccolti dalle origini dei dati nella classificazione BlueXP " .

Risultato

La BlueXP classification avvia la scansione dei file nelle condivisioni file aggiunte. Puoi Tenere traccia dell'avanzamento della scansione e visualizza i risultati della scansione nella **Dashboard**.

Se la scansione non viene completata correttamente per una configurazione CIFS con autenticazione Kerberos, controllare la scheda **Configurazione** per eventuali errori.

Modifica un gruppo di condivisione file

Dopo aver creato un gruppo di condivisioni file, è possibile modificare il protocollo CIFS o aggiungere e rimuovere condivisioni file.

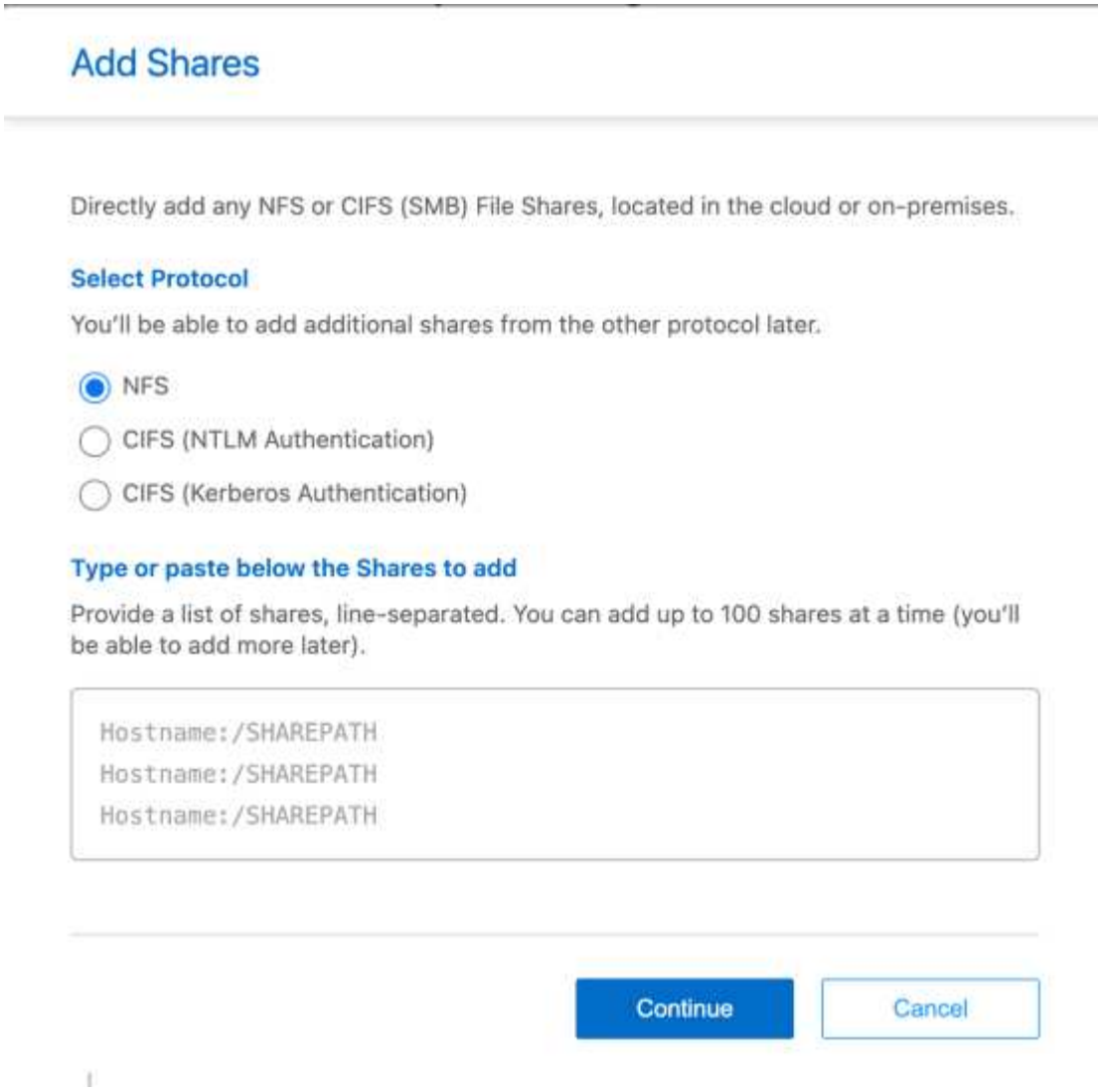
Modifica la configurazione del protocollo CIFS

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla pagina Configurazione, seleziona il gruppo di condivisioni file che desideri modificare.
3. Selezionare **Modifica credenziali CIFS**.

4. Selezionare il metodo di autenticazione: **NTLM** o **Kerberos**.
5. Immettere **Nome utente** e **Password** di Active Directory.
6. Selezionare **Salva** per completare il processo.

Aggiungere condivisioni di file alle scansioni di conformità

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Dalla pagina Configurazione, seleziona il gruppo di condivisioni file che desideri modificare.
3. Seleziona **+ Aggiungi azioni**.
4. Selezionare il protocollo per le condivisioni file che si desidera aggiungere.



Se aggiungi condivisioni di file a un protocollo già configurato, non sono necessarie modifiche.

Se si aggiungono condivisioni di file con un secondo protocollo, assicurarsi di aver configurato correttamente l'autenticazione come dettagliato in "prerequisiti" .

5. Aggiungi le condivisioni di file che desideri scansionare (una condivisione di file per riga) utilizzando il formato `<host_name>:/<share_path>` .
6. Selezionare **Continua** per completare l'aggiunta delle condivisioni file.

Rimuovere una condivisione di file dalle scansioni di conformità

1. Dal menu classificazione BlueXP , selezionare **Configurazione**.
2. Selezionare l'ambiente di lavoro da cui si desidera rimuovere le condivisioni di file.
3. Selezionare **Configurazione**.
4. Nella pagina Configurazione, selezionare azioni ••• per la condivisione file che si desidera rimuovere.
5. Dal menu azioni, selezionare **Rimuovi condivisione**.

Tenere traccia dell'avanzamento della scansione

È possibile tenere traccia dell'avanzamento della scansione iniziale.

1. Selezionare il menu **Configurazione**.
2. Selezionare **Configurazione dell'ambiente di lavoro**.

   L'avanzamento di ogni scansione viene visualizzato come barra di avanzamento.

3. Passare il mouse sulla barra di avanzamento per visualizzare il numero di file sottoposti a scansione rispetto al totale dei file nel volume.

Eseguire la scansione dei dati StorageGRID con classificazione BlueXP

Completare alcuni passaggi per avviare la scansione dei dati all'interno di StorageGRID direttamente con la classificazione BlueXP .

Consulta i requisiti delle StorageGRID

Prima di attivare la classificazione BlueXP, verificare di disporre di una configurazione supportata.

- Per connettersi al servizio di storage a oggetti, è necessario disporre dell'URL dell'endpoint.
- È necessario disporre della chiave di accesso e della chiave segreta di StorageGRID in modo che la classificazione BlueXP possa accedere ai bucket.

Distribuire l'istanza di classificazione BlueXP

Distribuire la classificazione BlueXP se non è già stata implementata un'istanza.

Se si esegue la scansione di dati da StorageGRID accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" o "Implementare la classificazione BlueXP in una posizione on-premise con accesso a Internet".

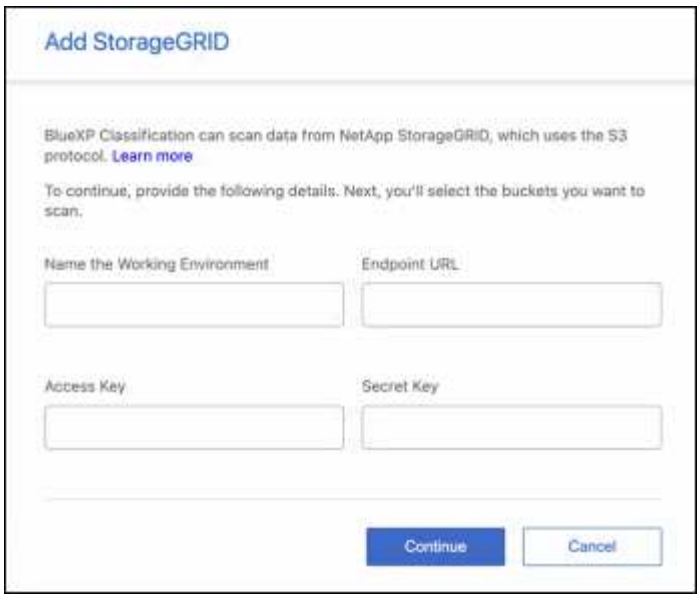
Se si esegue la scansione di dati da StorageGRID installati in un sito oscuro che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

Aggiungere il servizio StorageGRID alla classificazione BlueXP

Aggiungere il servizio StorageGRID.

Fasi

1. Dal menu classificazione BlueXP , selezionare l'opzione **Configurazione**.
2. Nella pagina Configurazione, selezionare **Aggiungi ambiente di lavoro** > **Aggiungi StorageGRID**.
3. Nella finestra di dialogo Aggiungi servizio StorageGRID, immettere i dettagli per il servizio StorageGRID e fare clic su **continua**.
   a. Immettere il nome che si desidera utilizzare per l'ambiente di lavoro. Questo nome deve riflettere il nome del servizio StorageGRID a cui si sta effettuando la connessione.
   b. Inserire l'URL dell'endpoint per accedere al servizio di storage a oggetti.
   c. Immettere la chiave di accesso e la chiave segreta in modo che la classificazione BlueXP possa accedere ai bucket in StorageGRID.



Risultato

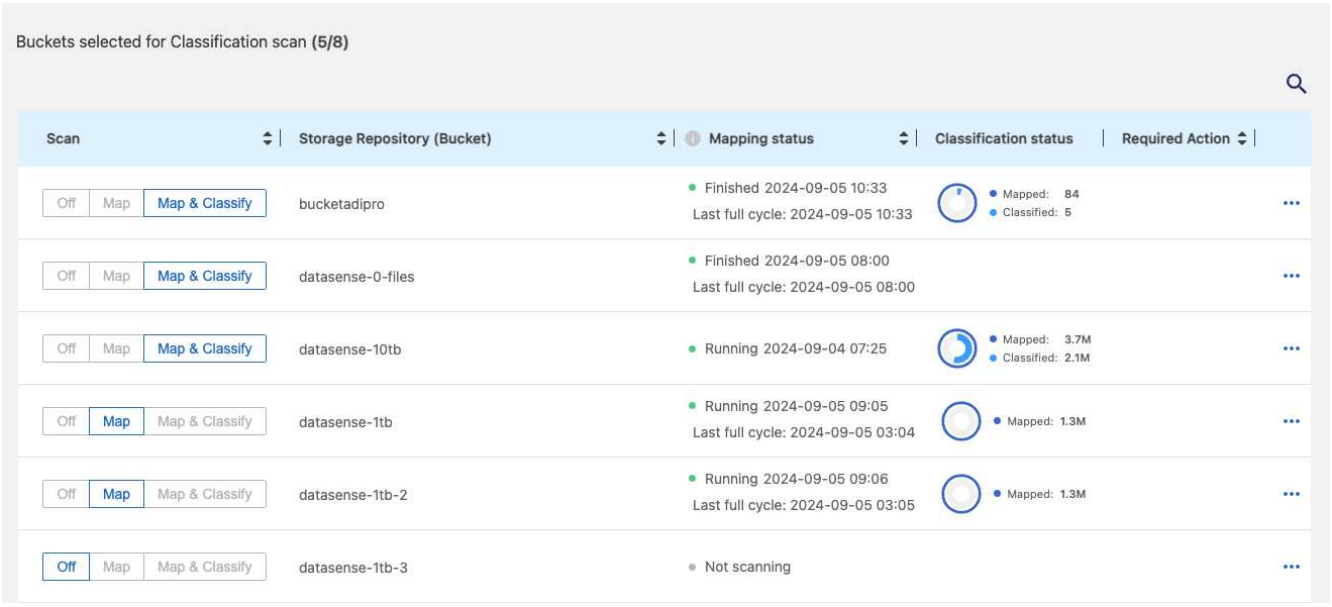
StorageGRID viene aggiunto all'elenco degli ambienti di lavoro.

Abilitare e disabilitare le scansioni di conformità sui bucket StorageGRID

Dopo aver attivato la classificazione BlueXP su StorageGRID, il passaggio successivo consiste nel configurare i bucket che si desidera analizzare. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

Fasi

1. Nella pagina di configurazione, individuare l'ambiente di lavoro StorageGRID.
2. Nella sezione ambiente di lavoro StorageGRID, selezionare **Configurazione**.



3. Per attivare o disattivare la scansione, completare una delle seguenti operazioni:
   - Per attivare le scansioni di sola mappatura su un bucket, selezionare **Mappa**.

- Per abilitare le scansioni complete su un bucket, selezionare **Mappa e Classifica**.
- Per disattivare la scansione su un bucket, selezionare **Off**.

Risultato

La classificazione BlueXP avvia la scansione dei bucket attivati. È possibile tenere traccia dell'avanzamento della scansione iniziale accedendo al menu **Configurazione** e selezionando poi la **Configurazione ambiente di lavoro**. L'avanzamento di ogni scansione viene visualizzato come barra di avanzamento. È inoltre possibile passare il mouse sulla barra di avanzamento per visualizzare il numero di file sottoposti a scansione rispetto al totale dei file nel volume. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Integra Active Directory con la classificazione BlueXP

È possibile integrare un Active Directory globale con la classificazione BlueXP per migliorare i risultati che BlueXP fornisce in relazione ai proprietari dei file e agli utenti e ai gruppi che hanno accesso ai file.

Quando si impostano determinate origini dati (elencate di seguito), è necessario immettere le credenziali Active Directory per consentire alla classificazione BlueXP di eseguire la scansione dei volumi CIFS. Questa integrazione fornisce la classificazione BlueXP con i dettagli relativi al proprietario del file e alle autorizzazioni per i dati che risiedono in tali origini dati. L'Active Directory immesso per tali origini dati potrebbe differire dalle credenziali di Active Directory globali inserite qui. La classificazione BlueXP cerca in tutte le Active Directory integrate i dettagli relativi all'utente e alle autorizzazioni.

Questa integrazione fornisce informazioni aggiuntive nelle seguenti posizioni della classificazione BlueXP:

- È possibile utilizzare il "Proprietario del file" "filtro" e visualizzare i risultati nei metadati del file nel riquadro delle indagini. Al posto del proprietario del file che contiene il SID (Security identifier), viene inserito il nome utente effettivo.

  Puoi anche visualizzare maggiori dettagli sul proprietario del file: nome dell'account, indirizzo email e nome dell'account SAM, oppure visualizzare gli elementi di proprietà di quell'utente.

- È possibile visualizzare "autorizzazioni complete per i file" per ogni file e directory quando si fa clic sul pulsante "Visualizza tutte le autorizzazioni".
- In "Dashboard di governance", Il pannello Open Permissions (autorizzazioni aperte) mostra un livello di dettaglio maggiore sui dati.

> I SID degli utenti locali e i SID dei domini sconosciuti non vengono convertiti nel nome utente effettivo.

Origini dati supportate

L'integrazione di Active Directory con la classificazione BlueXP consente di identificare i dati dalle seguenti origini dati:

- Sistemi ONTAP on-premise
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX per ONTAP

- Account OneDrive e account SharePoint (per versioni legacy 1,30 e precedenti)

Non è disponibile alcun supporto per l'identificazione delle informazioni relative a utenti e autorizzazioni da schemi di database, account Google Drive, account Amazon S3 o storage a oggetti che utilizzano il protocollo S3 (Simple Storage Service).

Connettersi al server Active Directory

Dopo aver implementato la classificazione BlueXP e aver attivato la scansione sulle origini dati, è possibile integrare la classificazione BlueXP con Active Directory. È possibile accedere ad Active Directory utilizzando un indirizzo IP del server DNS o un indirizzo IP del server LDAP.

Le credenziali di Active Directory possono essere di sola lettura, ma fornendo credenziali di amministratore si garantisce che la classificazione BlueXP possa leggere tutti i dati che richiedono autorizzazioni elevate. Le credenziali vengono memorizzate nell'istanza di classificazione BlueXP.

Per le condivisioni di file/volumi CIFS, se vuoi essere sicuro che i file "ultimi tempi di accesso" siano invariati dalle scansioni della classificazione di BlueXP, consigliamo all'utente di disporre dell'autorizzazione attributi di scrittura. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory di un gruppo principale dell'organizzazione che dispone delle autorizzazioni per tutti i file.

Requisiti

- È necessario che sia già stata configurata una Active Directory per gli utenti della società.
- È necessario disporre delle informazioni per Active Directory:
  - Indirizzo IP del server DNS o indirizzi IP multipli

    oppure

  Indirizzo IP del server LDAP o indirizzi IP multipli
  - User Name (Nome utente) e Password per accedere al server
  - Domain Name (Nome di Active Directory) (Nome di dominio)
  - Se si utilizza o meno LDAP sicuro (LDAPS)
  - Porta server LDAP (generalmente 389 per LDAP e 636 per LDAP sicuro)
- Le seguenti porte devono essere aperte per la comunicazione in uscita dall'istanza di classificazione BlueXP:

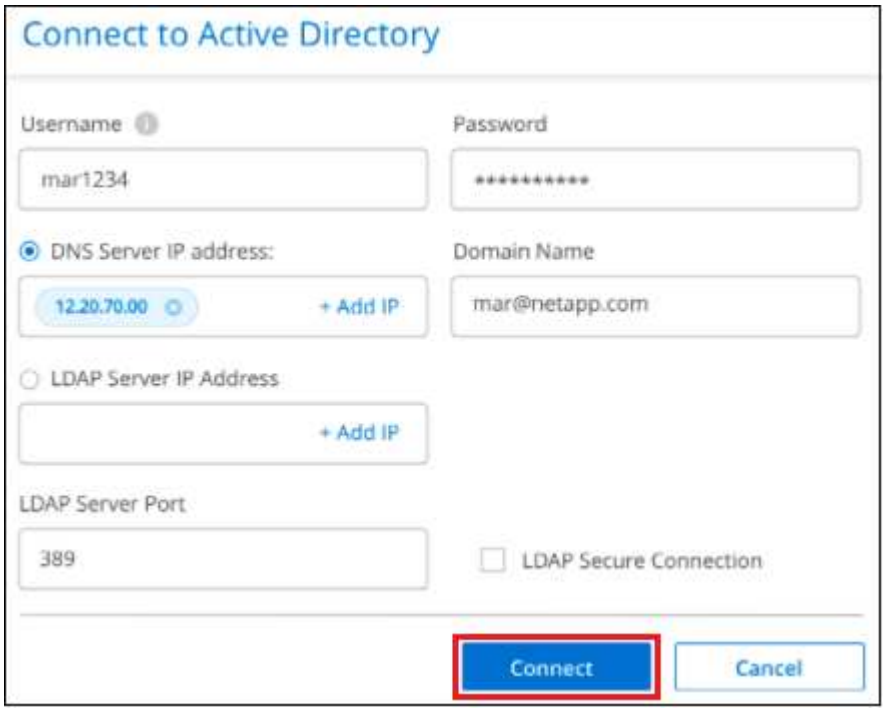
Protocollo	Porta	Destinazione	Scopo
TCP E UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP su SSL
TCP	3268	Active Directory	Catalogo globale
TCP	3269	Active Directory	Catalogo globale su SSL

Fasi

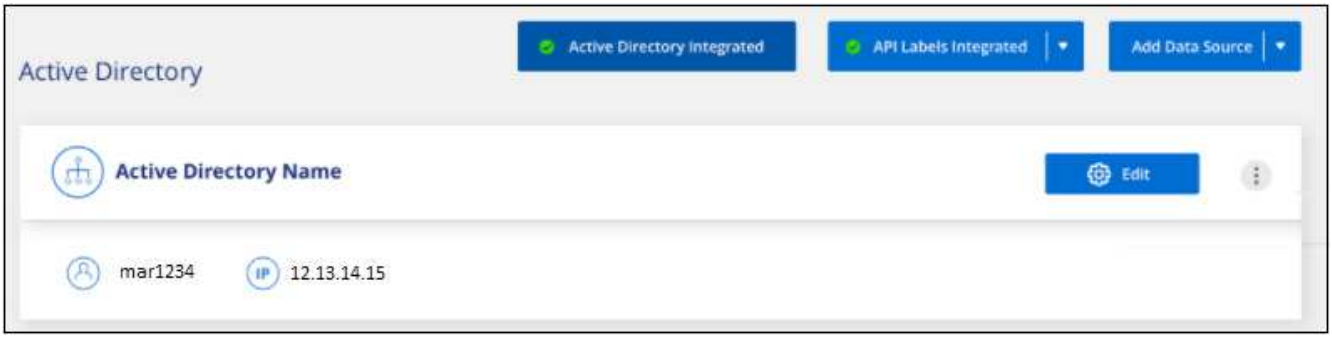
1. Dalla pagina di configurazione della classificazione BlueXP, fare clic su **Add Active Directory** (Aggiungi Active Directory).

2. Nella finestra di dialogo connessione ad Active Directory, immettere i dettagli di Active Directory e fare clic su **Connetti**.

   Se necessario, è possibile aggiungere più indirizzi IP facendo clic su **Add IP** (Aggiungi indirizzo IP).



   La classificazione BlueXP si integra con Active Directory e viene aggiunta una nuova sezione alla pagina di configurazione.



Gestire l'integrazione di Active Directory

Se è necessario modificare i valori dell'integrazione di Active Directory, fare clic sul pulsante **Edit** (Modifica) e apportare le modifiche.

È inoltre possibile eliminare l'integrazione selezionando il pulsante quindi **Rimuovi Active Directory**.

Informazioni sul copyright

Informazioni sul marchio commerciale