Inizia subito

BlueXP classification

NetApp
April 03, 2024

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.

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.
- Identificare se gli identificatori univoci dei database sono presenti nei file di altri repository, creando in pratica un elenco personalizzato di "dati personali" identificati nelle scansioni di classificazione di BlueXP.
- Notifica ad alcuni utenti via email quando i file contengono determinati dati PII (si definiscono questi criteri utilizzando "Policy") in modo da poter decidere un piano d'azione.

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.
- Utilizza *Policies* per notificare automaticamente al personale addetto alla sicurezza i nuovi problemi di sicurezza in modo che possa intervenire immediatamente.
- Aggiungere tag personalizzati ai file (ad esempio, "deve essere spostato") e assegnare un utente BlueXP in modo che la persona possa possedere gli aggiornamenti dei file.
- Visualizzare e modificare "Etichette AIP (Azure Information Protection)" nei file.

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. È possibile utilizzare queste informazioni per decidere se si desidera spostare o eliminare determinati file.
- Eliminare i file che sembrano insicuri o troppo rischiosi da lasciare nel sistema storage o che sono stati identificati come duplicati. È possibile utilizzare *Policies* per eliminare automaticamente i file che corrispondono a determinati criteri.
- 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".

Accelera la migrazione dei dati

La classificazione BlueXP può essere utilizzata per eseguire la scansione dei dati on-premise prima di eseguirne la migrazione nel cloud pubblico o privato. È possibile utilizzare la classificazione BlueXP per:

- Visualizzare le dimensioni dei dati e se questi contengono informazioni riservate prima di spostarli.
- Filtrare i dati di origine (in base a oltre 25 tipi di criteri) in modo da poter spostare solo i file richiesti nella destinazione - i dati non necessari non vengono spostati.
- Sposta, copia o sincronizza automaticamente e continuamente solo i dati richiesti nel repository cloud.

Origini dati supportate

La classificazione BlueXP è in grado di eseguire la scansione e l'analisi di dati strutturati e non strutturati provenienti dai seguenti tipi di origini dati:

NetApp:

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

Non NetApp:

- Dell EMC Isilon
- Storage puro
- Nutanix
- Qualsiasi altro vendor di storage

Cloud:

- Amazon S3
- Storage Google Cloud

- OneDrive
- SharePoint Online
- SharePoint on-premise (SharePoint Server)
- Google Drive

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 e CIFS 1.x, 2,0, 2,1 e 3,0.

Costo

- Il costo per l'utilizzo della classificazione BlueXP dipende dalla quantità di dati che si sta eseguendo la scansione. I primi 1 TB di dati che la classificazione BlueXP scansiona in un'area di lavoro BlueXP sono gratuiti per 30 giorni. Sono inclusi tutti i dati provenienti da tutti gli ambienti di lavoro e le origini dati. Per continuare la scansione dei dati dopo tale data, è necessario un abbonamento a AWS, Azure o GCP Marketplace o una licenza BYOL di NetApp. Vedere "prezzi" per ulteriori informazioni.

  "Scopri come concedere in licenza la classificazione BlueXP".

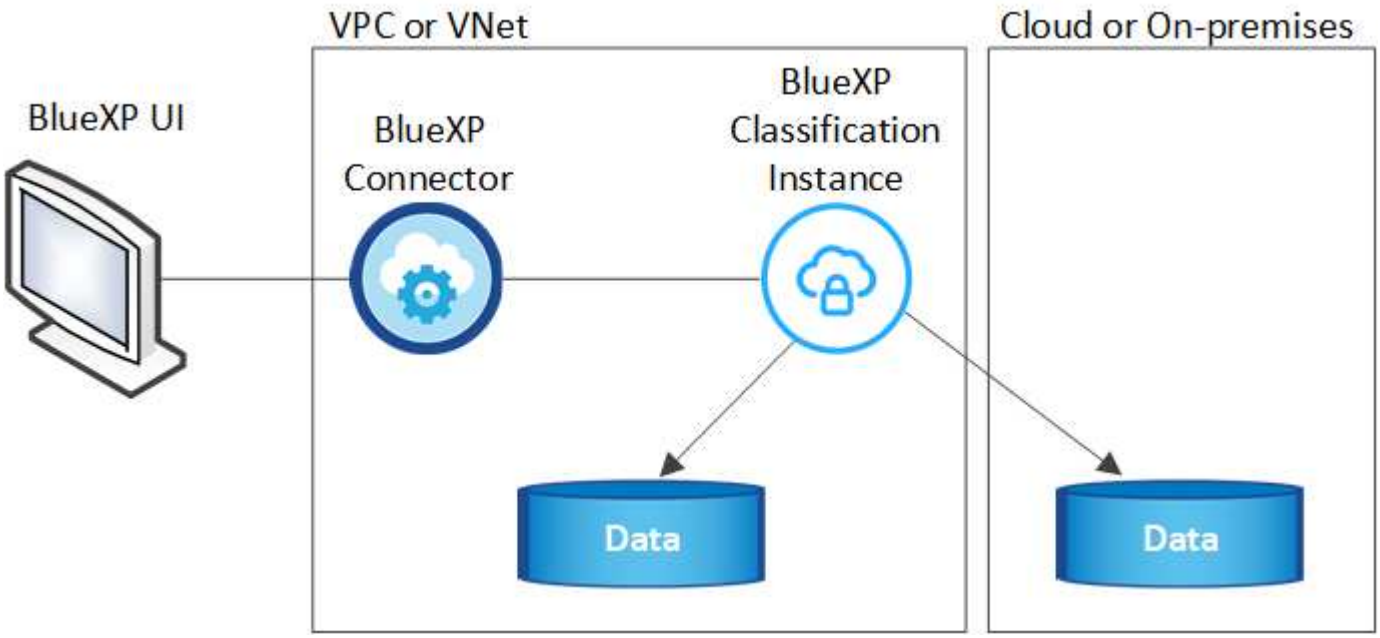
- L'installazione della classificazione BlueXP nel cloud richiede l'implementazione di un'istanza di cloud, con conseguente addebito da parte del provider di cloud in cui viene implementata. Vedere il tipo di istanza implementata per ciascun cloud provider. L'installazione della classificazione BlueXP 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. Tuttavia, se l'origine dati, come un sistema Cloud Volumes ONTAP o un bucket S3, si trova in una _area o regione di disponibilità diversa, il tuo cloud provider addebiterà i costi di trasferimento dei dati. Per ulteriori informazioni, consulta i seguenti xref:./* "AWS: Prezzi 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 un "Standard_D16s_v3 VM" Con un disco da 500 GiB. L'immagine del sistema operativo è CentOS 7.9.
- In GCP, la classificazione BlueXP viene eseguita su un "n2-standard-16 VM" Con un disco persistente standard da 500 GiB. L'immagine del sistema operativo è CentOS 7.9.
- 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 dispone di accesso a Internet.

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

Utilizzando un tipo di istanza più piccolo

È possibile implementare la classificazione BlueXP su un sistema con meno CPU e meno RAM, ma ci sono alcune limitazioni quando si utilizzano questi sistemi meno potenti.

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.
Medio	8 CPU, 32 GB di RAM, SSD da 200 GiB	Scansione più lenta e scansione di un massimo di 1 milione di file.
Piccolo	8 CPU, 16 GB di RAM, SSD da 100 GiB	Stesse limitazioni del "Medio", più la capacità di identificare "nomi dei soggetti dei dati" l'interno dei file è disattivato.

Quando si implementa la classificazione BlueXP nel cloud su AWS, è possibile scegliere un'istanza grande/media/piccola. Quando implementi la classificazione BlueXP in Azure o GCP, invia un'email ng-contact-data-sense@netapp.com per assistenza se desideri utilizzare uno di questi sistemi alternativi. Dovremo collaborare con te per implementare queste altre configurazioni cloud.

Quando si implementa la classificazione BlueXP on-premise, basta utilizzare un host Linux con specifiche alternative. Non è necessario contattare NetApp per assistenza.

Come funziona la classificazione BlueXP

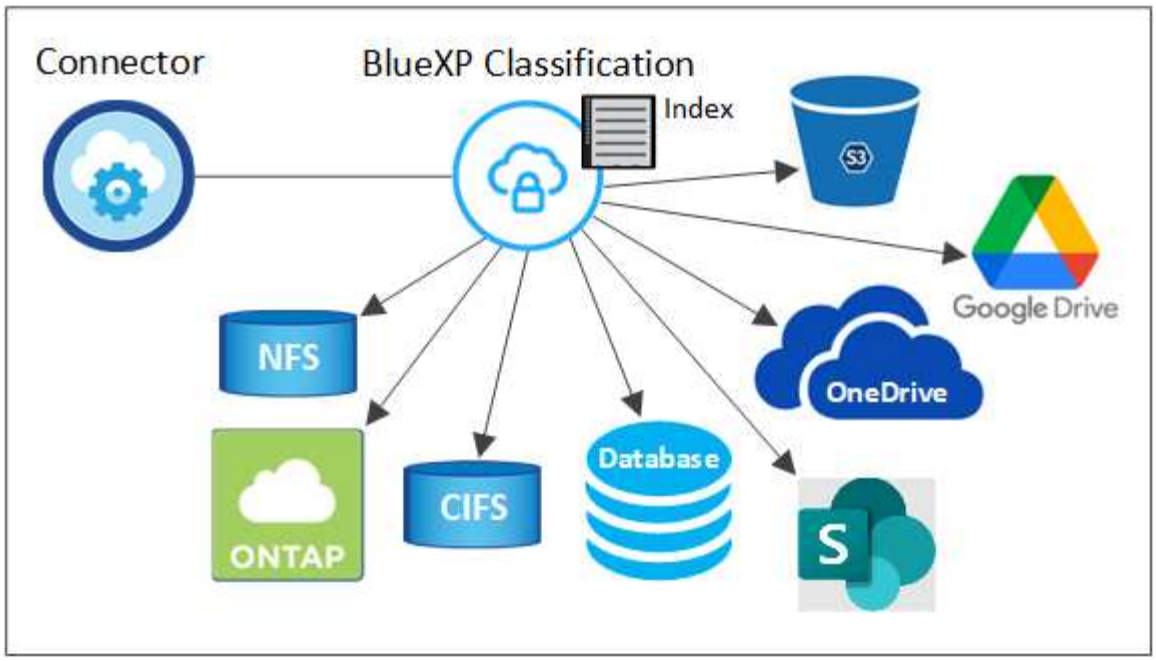
Ad alto livello, la classificazione BlueXP funziona come segue:

1. Si implementa un'istanza della classificazione BlueXP in BlueXP.
2. È possibile attivare la mappatura ad alto livello o la scansione a livello profondo 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.

Come funzionano le scansioni

Dopo aver attivato la classificazione BlueXP e selezionato i repository da analizzare (volumi, bucket, schemi di database o dati utente di OneDrive o SharePoint), 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 analizza continuamente i dati in modo round-robin per rilevare le modifiche incrementali (è per questo che è importante mantenere l'istanza in esecuzione).

È possibile attivare e disattivare le scansioni a livello di volume, a livello di bucket, a livello di schema del database, a livello di utente OneDrive e a livello di sito SharePoint.

Qual è la differenza tra le scansioni di mappatura e classificazione

La classificazione BlueXP consente di eseguire una scansione generale di "mappatura" su origini dati selezionate. La mappatura fornisce solo una panoramica di alto livello dei dati, mentre la classificazione fornisce una scansione di alto livello dei dati. Il mapping può essere eseguito sulle origini dati molto rapidamente perché non accede ai file per vedere i dati all'interno.

Molti utenti apprezzano questa funzionalità perché desiderano eseguire rapidamente la scansione dei dati per identificare le origini dati che richiedono una maggiore ricerca e quindi possono abilitare le scansioni di classificazione solo su quelle origini dati o volumi richiesti.

La tabella seguente mostra alcune delle differenze:

Funzione	Classificazione	Mappatura
Velocità di scansione	Lento	Veloce
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
Capacità 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 "policy" che forniscono risultati di ricerca personalizzati	Sì	No

Funzione	Classificazione	Mappatura
Categorizzare i dati utilizzando le etichette AIP e i tag di stato	Sì	No
Copiare, eliminare e spostare i file di origine	Sì	No
Possibilità di eseguire altri report	Sì	No

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 Mapping, la classificazione BlueXP può eseguire la scansione tra 100-150 Tibers di dati al giorno, per nodo dello scanner.
- Quando si eseguono scansioni di classificazione, la classificazione BlueXP è in grado di eseguire la scansione tra 15-40 Tibers di dati al giorno, per nodo dello scanner.

"Scopri di più sull'implementazione di più nodi scanner per la scansione dei dati".

Informazioni indicizzati dalla classificazione BlueXP

La classificazione BlueXP raccoglie, indicizza e assegna categorie ai dati (file). I dati indicizzati dalla classificazione BlueXP includono quanto segue:

Metadati standard

La classificazione BlueXP raccoglie i metadati standard relativi ai file: Il tipo di file, le dimensioni, le date di creazione e modifica e così via.

Dati personali

Informazioni personali come indirizzi e-mail, numeri di identificazione o numeri di carta di credito. "Scopri di più sui dati personali".

Dati personali sensibili

Tipi speciali di informazioni sensibili, come dati sanitari, origine etnica o opinioni politiche, come definito dal 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 entità nome

La classificazione BlueXP utilizza l'ai per estrarre i nomi delle persone fisiche dai documenti. "Scopri come rispondere alle richieste di accesso ai soggetti dati".

Panoramica delle reti

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 servita su HTTPS e i dati privati inviati tra il browser e l'istanza di classificazione BlueXP sono protetti con una crittografia end-to-end basata su TLS 1,2, il che significa che NetApp e terze parti non possono leggerla.

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".

Accesso dell'utente alle informazioni di conformità

Il ruolo assegnato a ciascun utente offre diverse funzionalità all'interno di BlueXP e all'interno della classificazione BlueXP:

- Un **account Admin** può gestire le impostazioni di conformità e visualizzare le informazioni di conformità per tutti gli ambienti di lavoro.
- Un **Workspace Admin** può gestire le impostazioni di conformità e visualizzare le informazioni di conformità solo per i sistemi ai quali è consentito l'accesso. Se un amministratore dell'area di lavoro non riesce ad accedere a un ambiente di lavoro in BlueXP, non può visualizzare alcuna informazione di conformità per l'ambiente di lavoro nella scheda di classificazione di BlueXP.
- Gli utenti con il ruolo **Compliance Viewer** possono solo visualizzare le informazioni di conformità e generare report per i sistemi ai quali sono autorizzati ad accedere. Questi utenti non possono attivare/disattivare la scansione di volumi, bucket o schemi di database. Questi utenti non possono copiare, spostare o eliminare i file.

"Scopri di più sui ruoli BlueXP" e come fare "aggiungere utenti con ruoli specifici".

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", Noto anche come *private mode.* questo tipo di installazione, che utilizza uno script di installazione, è utile per i siti protetti.

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.

1. **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.

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.

3. **Implementare la classificazione BlueXP**

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

4. **Iscriviti al servizio di classificazione BlueXP**

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento BlueXP tramite il proprio provider cloud Marketplace o una licenza BYOL di NetApp.

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 si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS, Amazon FSX per ONTAP o nei bucket AWS S3, si 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 di file non NetApp, lo storage a oggetti S3 generico, i database, le cartelle OneDrive, gli account SharePoint e gli account Google Drive possono essere sottoposti a scansione quando si utilizza 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".

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:

- Impossibile eseguire la scansione di account OneDrive, SharePoint e Google Drive.
- La funzionalità dell'etichetta AIP (Microsoft Azure Information Protection) non può essere integrata.

"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, al momento non supportiamo proxy trasparenti.

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 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 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"

Si noti che è possibile implementare la classificazione BlueXP su un'istanza in ambienti cloud AWS con meno CPU e meno RAM, ma l'utilizzo di questi sistemi presenta delle limitazioni. Vedere "Utilizzando un tipo di istanza più piccolo" per ulteriori informazioni.

Implementare la classificazione BlueXP nel cloud

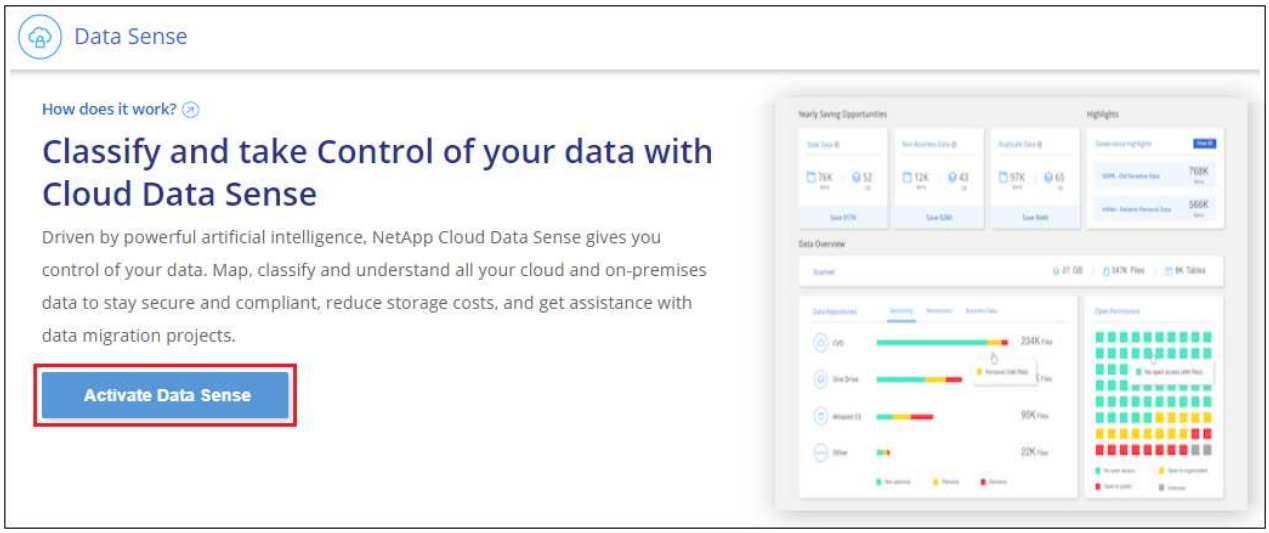
Seguire questi passaggi per implementare un'istanza della classificazione BlueXP nel cloud. Il connettore implementerà l'istanza nel cloud, quindi installerà il software di classificazione BlueXP su tale istanza.

Quando si implementa la classificazione BlueXP da un connettore BlueXP in un ambiente AWS, è possibile selezionare la dimensione predefinita dell'istanza oppure scegliere tra due tipi di istanze più piccoli. "Vedere i tipi di istanze e le limitazioni disponibili". 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 a sinistra di BlueXP, fare clic su **Governance > Classification**.



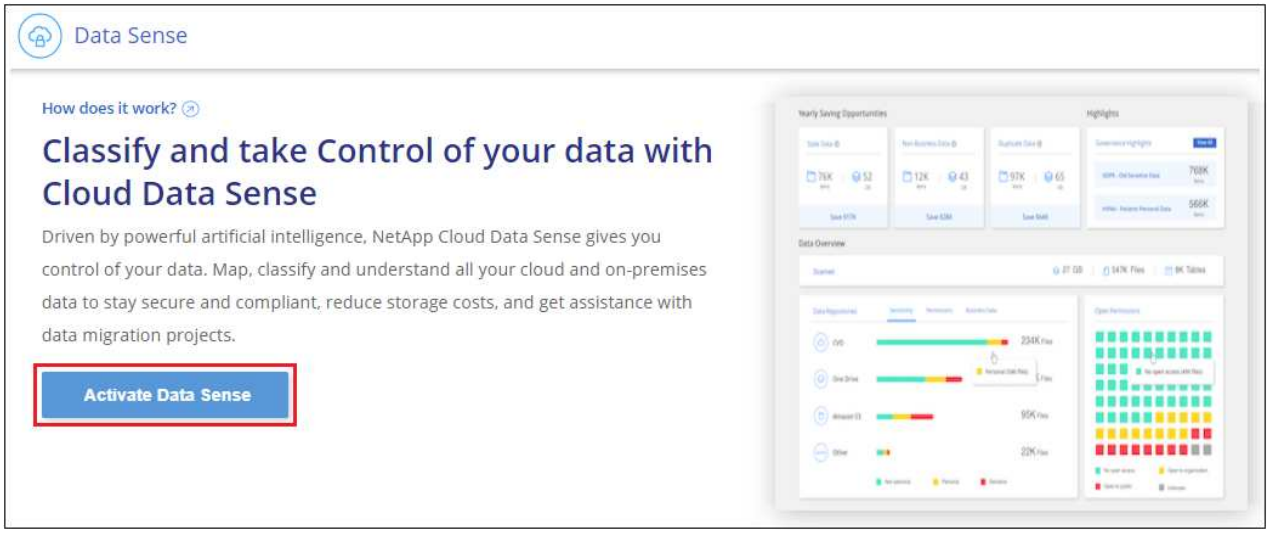
2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).
3. Dalla pagina *Installation*, fare clic su **Deploy > Deploy** per utilizzare le dimensioni dell'istanza "Large" e avviare la procedura guidata di implementazione del cloud.
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

5. Una volta implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (Configurazione).

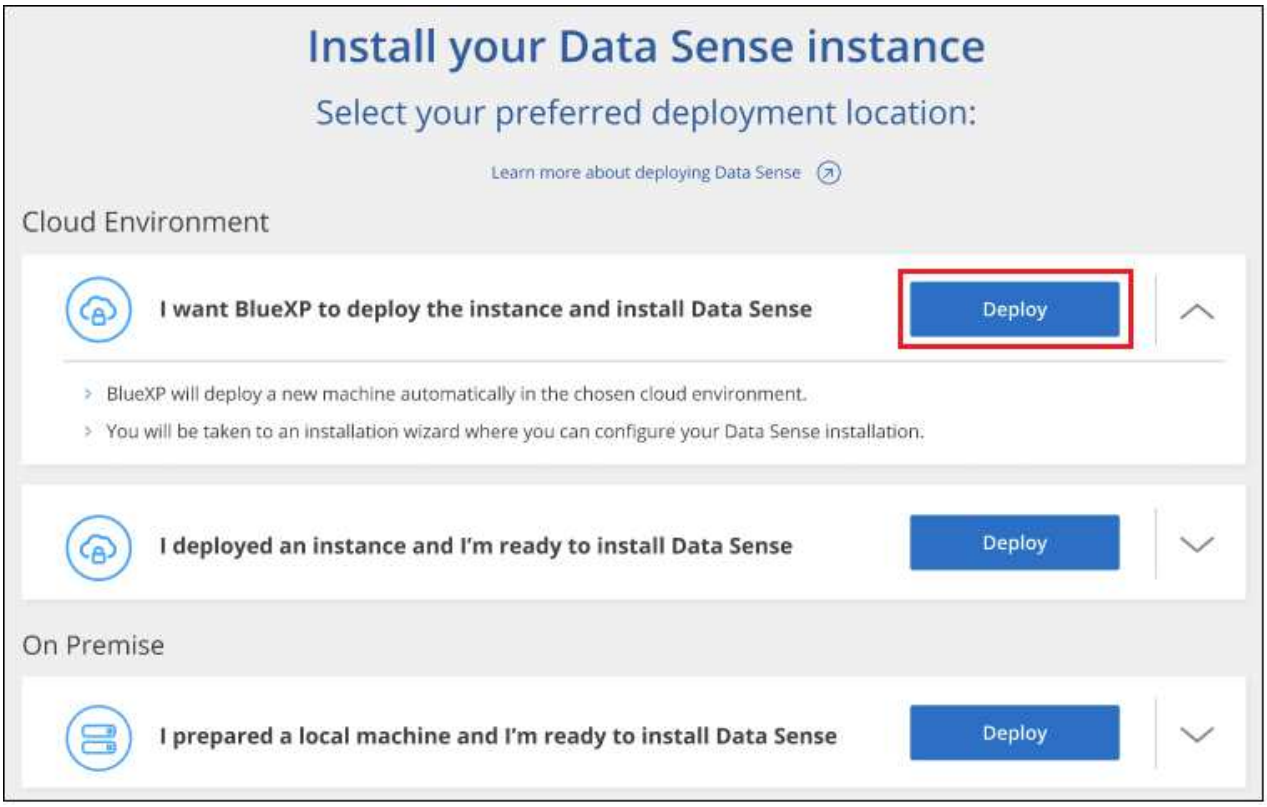
Implementazione in Azure

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



3. Fare clic su **Deploy** per avviare la procedura guidata di implementazione del cloud.



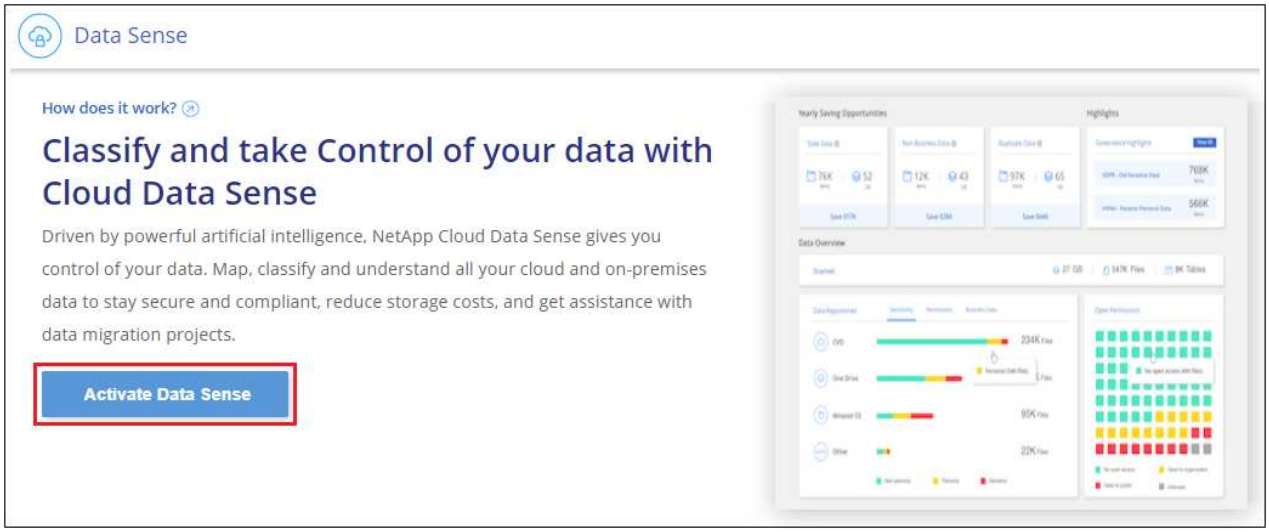
4. La procedura guidata visualizza lo stato di avanzamento durante le fasi di implementazione. In caso di problemi, il sistema si arresta e richiede l'immissione.

5. Una volta implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (Configurazione).

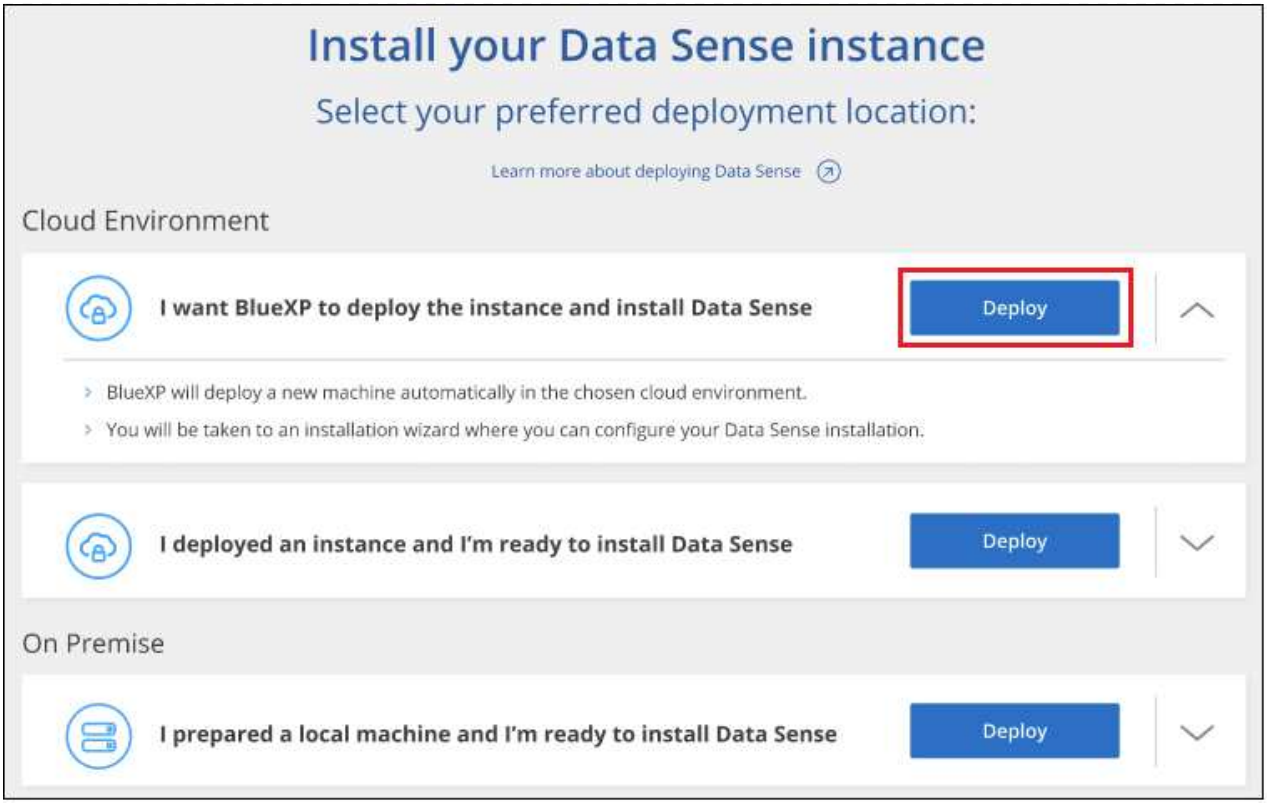
Implementazione in Google Cloud

Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification**.
2. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



3. Fare clic su **Deploy** per avviare la procedura guidata di implementazione del 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 implementata l'istanza e installata la classificazione BlueXP, fare clic su **Continue to Configuration** (continua alla configurazione) per accedere alla pagina *Configuration* (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.

Puoi anche farlo "Impostare la licenza per la classificazione BlueXP" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

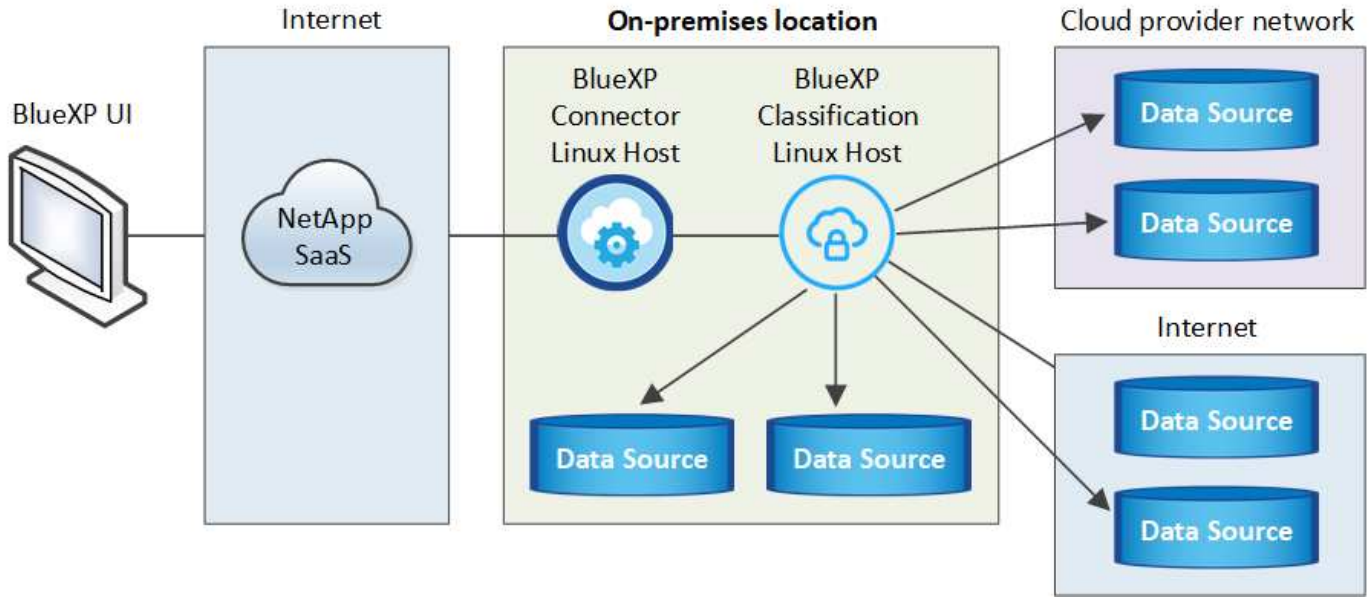
Installare la classificazione BlueXP su un host con accesso a Internet

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.

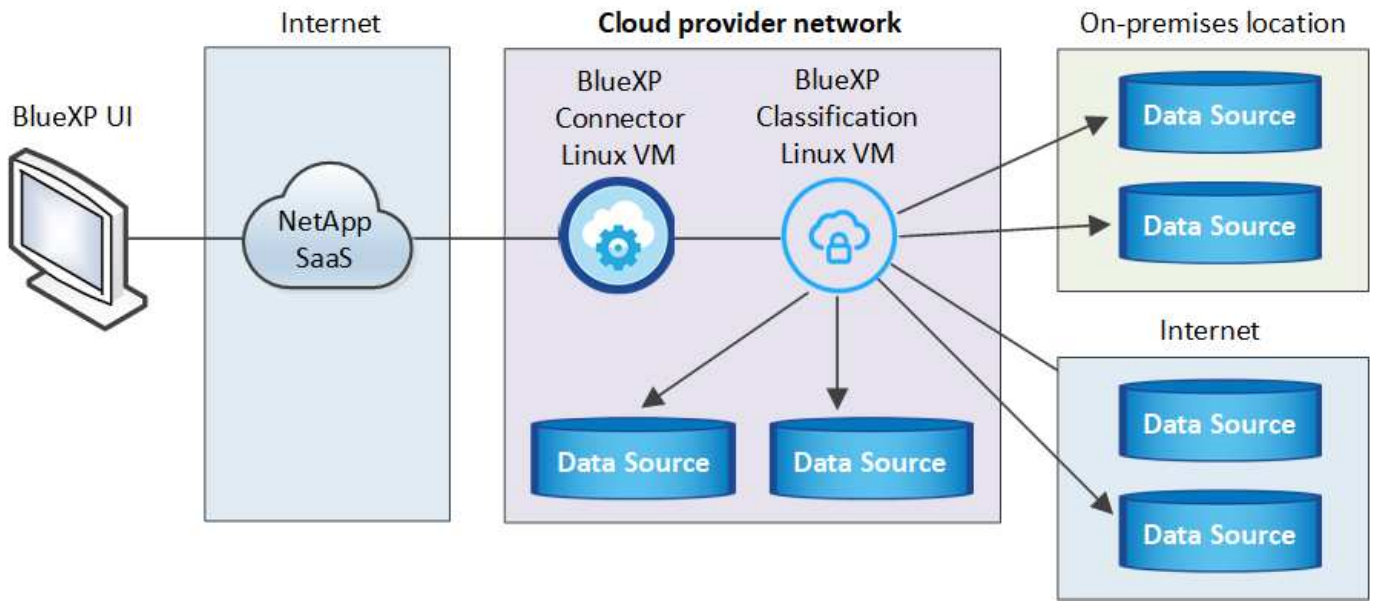
L'installazione on-premise potrebbe essere una buona opzione se si preferisce eseguire la scansione dei sistemi ONTAP on-premise utilizzando un'istanza di classificazione BlueXP che si trova anche on-premise, ma questo non è un requisito. Il software funziona esattamente allo stesso modo, indipendentemente 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 configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

Nota: È anche possibile "Installare la classificazione BlueXP in un sito on-premise che non dispone di accesso a Internet" per siti completamente sicuri.

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.

4 Iscriviti al servizio di classificazione BlueXP

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Per continuare a eseguire la scansione dei dati dopo tale data, è necessario un abbonamento al tuo provider cloud Marketplace o una licenza BYOL di NetApp.

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 si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS, Amazon FSX per ONTAP o nei bucket AWS S3, si 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 di file non NetApp, lo storage a oggetti S3 generico, i database, le cartelle OneDrive, gli account SharePoint e gli account Google Drive possono essere sottoposti a scansione utilizzando uno 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.

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

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 si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di 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 /opt 895 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Grande	16 CPU	64 GB DI RAM	500 GiB SSD ON /, OR - 100 GiB disponibile su /opt - 395 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Medio	8 CPU	32 GB DI RAM	200 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 145 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Piccolo	8 CPU	16 GB DI RAM	100 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 45 GiB disponibile su /var/lib/docker - 5 GiB su /tmp

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere "Utilizzando un tipo di istanza più piccolo" per ulteriori informazioni.

- 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 AWS 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
  - CentOS versione 7,8 e 7,9
  - Ubuntu 22,04 (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, 9,0, 9,1, 9,2 e 9,3

    Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

    - Installazione in un luogo buio
    - Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti

- **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".

      "Guarda questo video" Per una rapida dimostrazione dell'installazione di Docker su CentOS.

    - Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install 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://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Fornisce pacchetti prerequisiti per l'installazione di CentOS.
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.

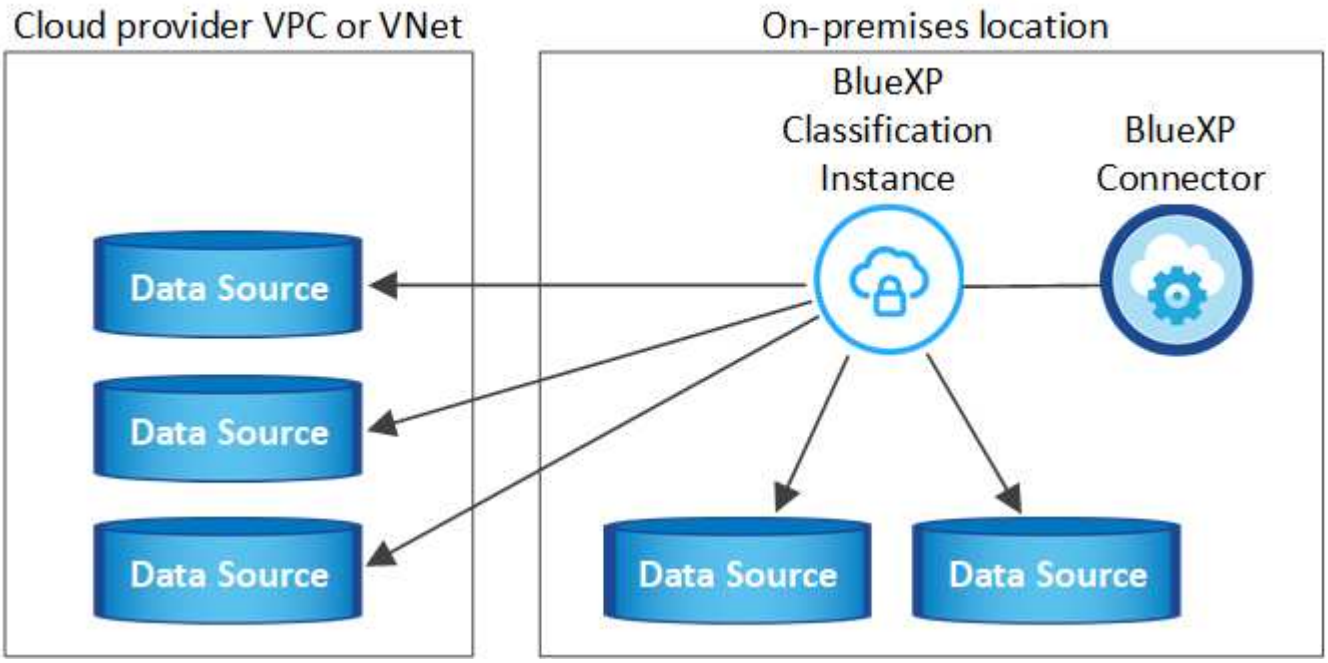
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 443 (TCP) e 80	Il firewall o le regole di routing per il connettore devono consentire il traffico in entrata e in uscita sulla porta 443 da e verso l'istanza di classificazione BlueXP. Assicurarsi che la porta 8080 sia aperta in modo da visualizzare l'avanzamento dell'installazione in BlueXP.
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)

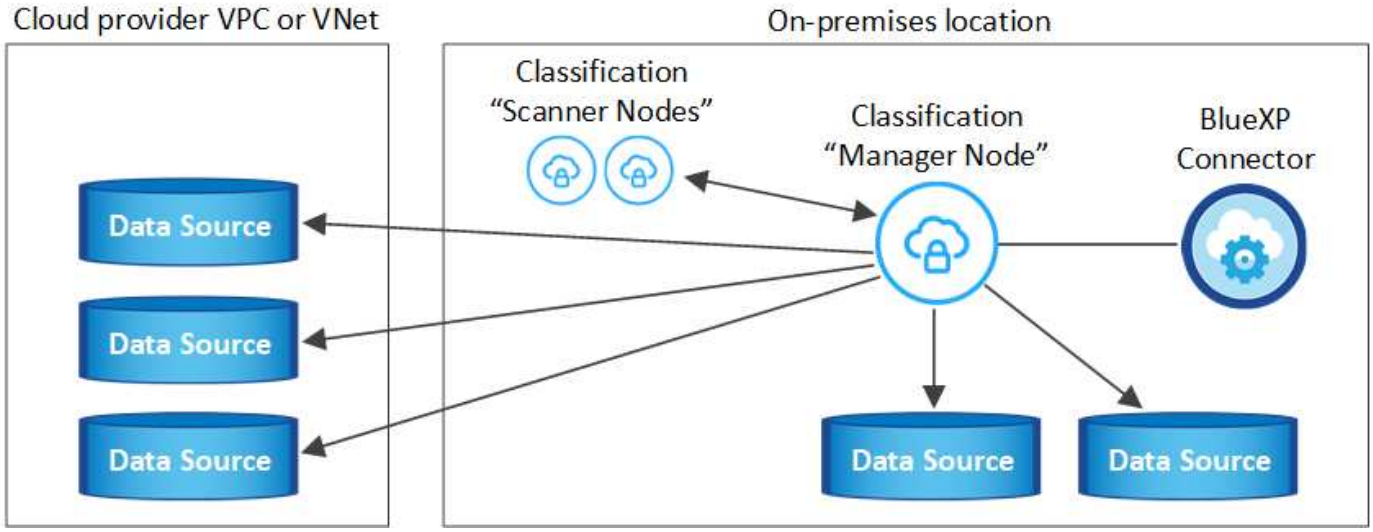
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. "Vedere i requisiti aggiuntivi per le porte".

Installare la classificazione BlueXP sull'host Linux

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



Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. 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 scoprire 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".

Di cosa hai bisogno

- 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, al momento non supportiamo proxy trasparenti.

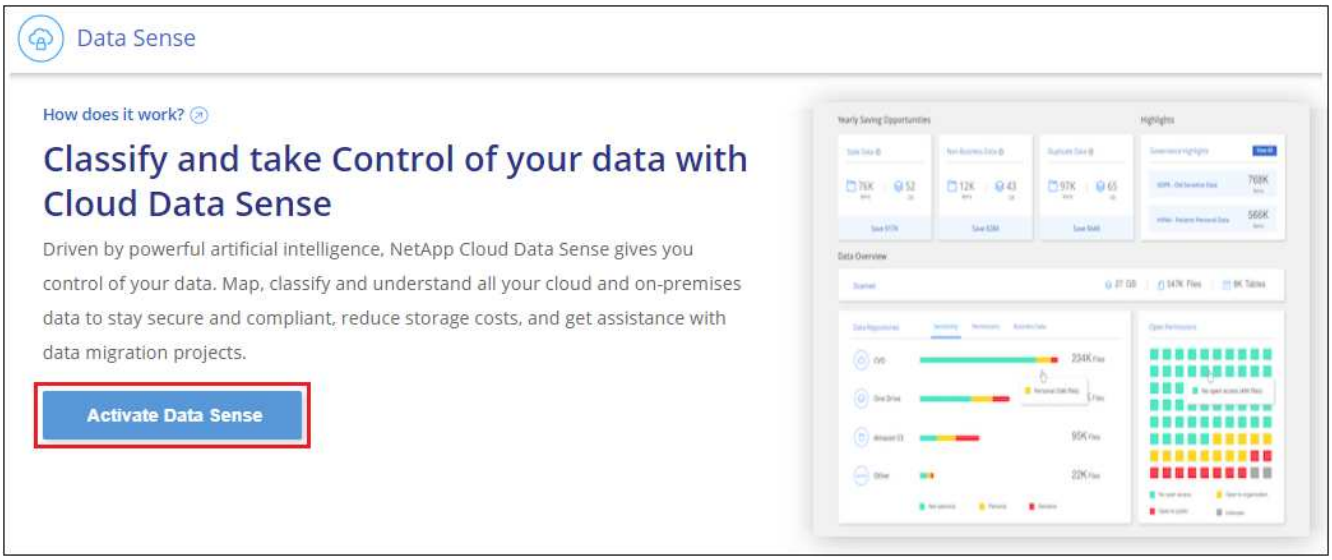
- L'utente deve essere un utente locale. Gli utenti di dominio non sono supportati.
- Verificare che l'ambiente offline soddisfi i requisiti permessi e connettività.

Fasi

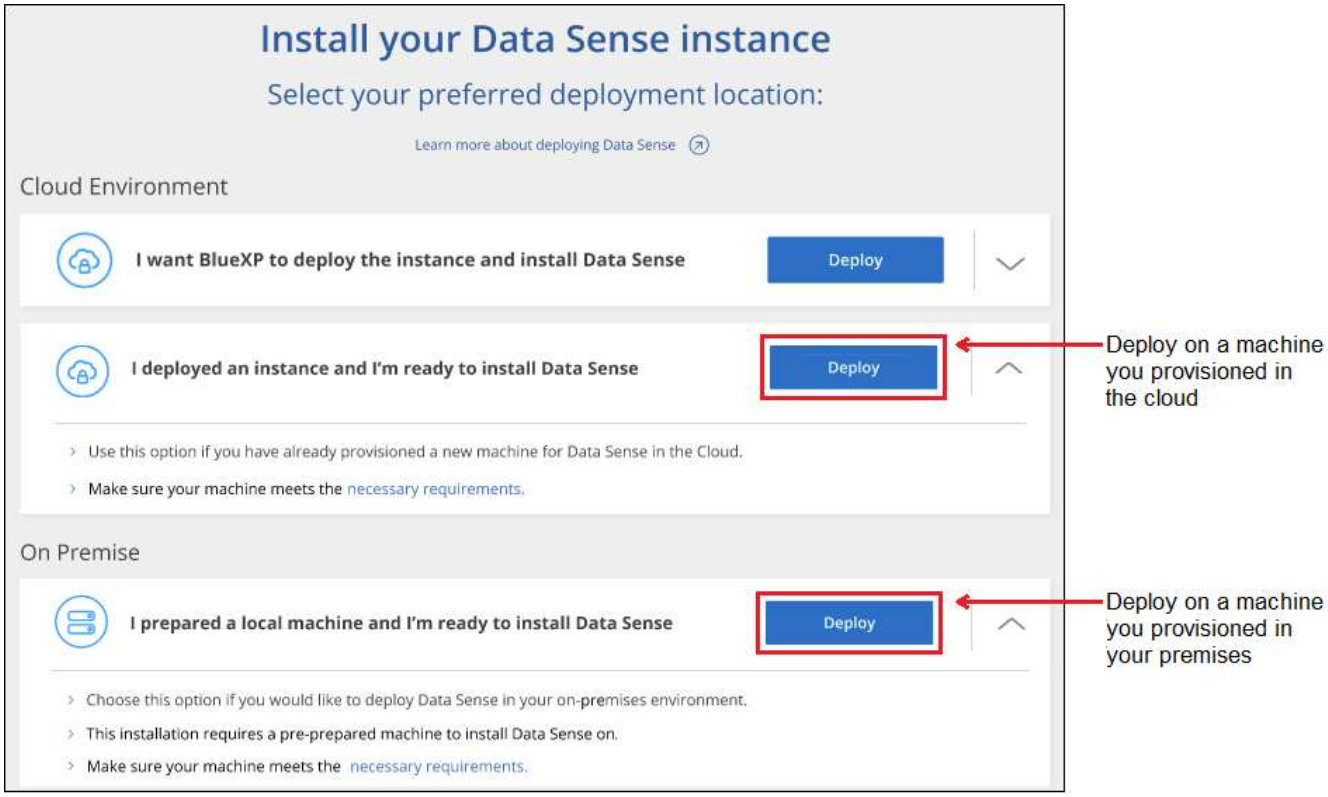
1. Scaricare il software di classificazione BlueXP dal "Sito di supporto NetApp". Il file da selezionare è **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiare il file del programma di installazione sull'host Linux che si desidera utilizzare (utilizzando `scp` o qualche altro metodo).
3. Decomprimere 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. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



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.

   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. "Guarda questo video" comprendere i messaggi di pre-controllo e le implicazioni.

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.

Puoi anche farlo "Impostare la licenza per la classificazione BlueXP" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

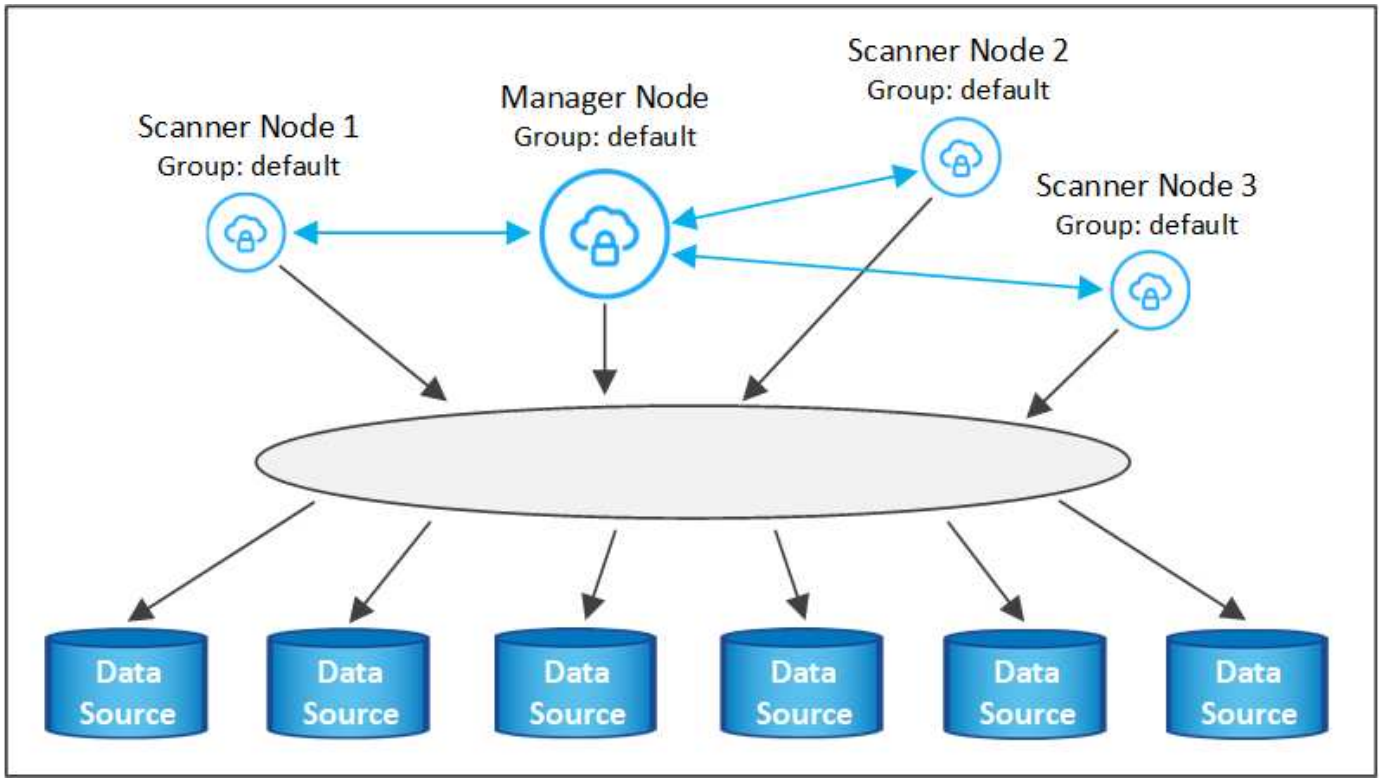
Aggiunta di nodi scanner a un'implementazione esistente

È possibile aggiungere altri nodi dello scanner se si ha bisogno di una maggiore potenza di elaborazione della scansione per eseguire la scansione delle origini dati. È possibile aggiungere i nodi dello scanner subito dopo l'installazione del nodo manager oppure aggiungere un nodo scanner in un secondo momento. Ad esempio, se si comprende che la quantità di dati in una delle origini dati è raddoppiata o triplicata dopo 6 mesi, è possibile aggiungere un nuovo nodo scanner per agevolare la scansione dei dati.

Esistono due modi per aggiungere nodi scanner aggiuntivi:

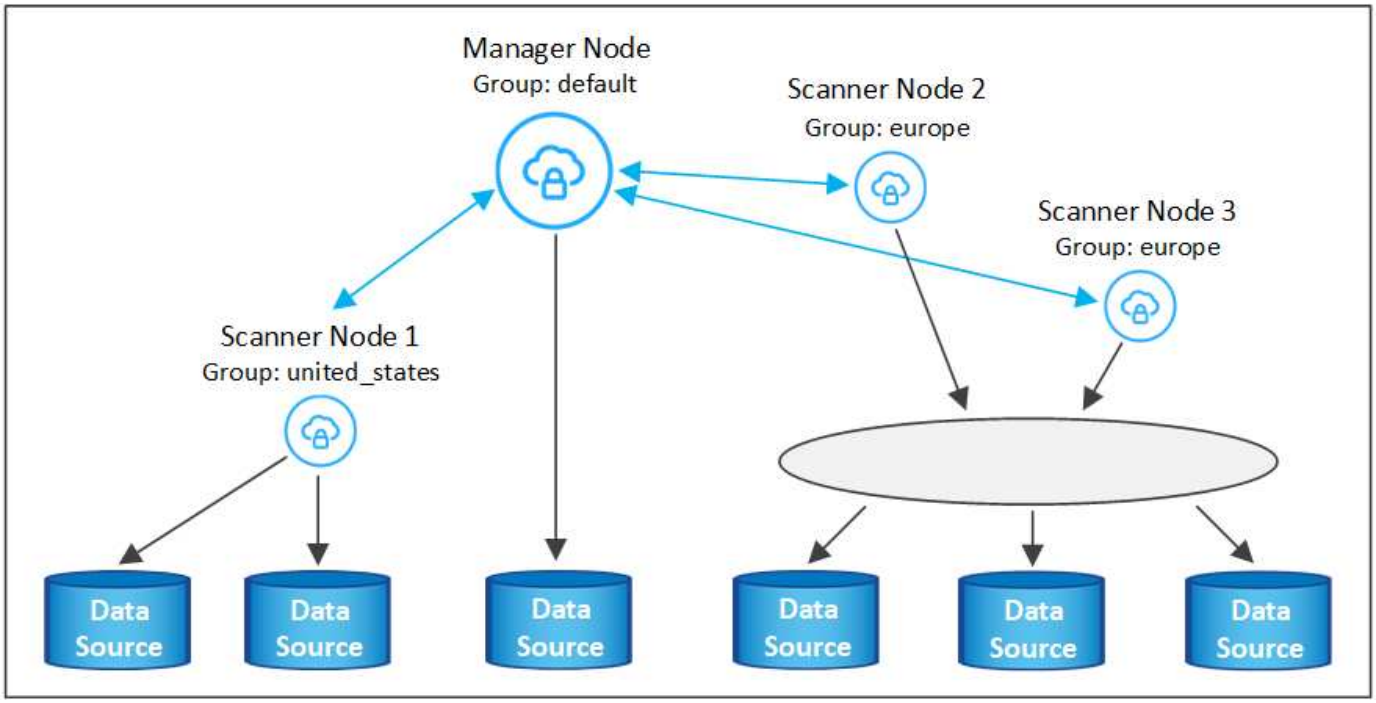
- aggiungere un nodo per facilitare la scansione di tutte le origini dati
- aggiunta di un nodo per agevolare la scansione di una specifica origine dati o di un gruppo specifico di origini dati (in genere in base alla posizione)

Per impostazione predefinita, i nuovi nodi dello scanner aggiunti vengono aggiunti al pool generale di risorse di scansione. Questo è chiamato "gruppo scanner predefinito". Nell'immagine riportata di seguito, sono presenti 1 nodo Manager e 3 nodi scanner nel gruppo "default" che sono tutti dati di scansione da tutte e 6 le origini dati.



Se si desidera eseguire la scansione di determinate origini dati da parte di nodi scanner fisicamente più vicini alle origini dati, è possibile definire un nodo scanner o un gruppo di nodi scanner per eseguire la scansione di una specifica origine dati o di un gruppo di origini dati. Nell'immagine seguente sono presenti 1 nodo Manager e 3 nodi scanner.

- Il nodo Manager si trova nel gruppo "default" e sta eseguendo la scansione di un'origine dati
- Il nodo scanner 1 si trova nel gruppo "united_states" e sta eseguendo la scansione di 2 origini dati
- I nodi scanner 2 e 3 fanno parte del gruppo "europa" e condividono le attività di scansione per 3 origini dati



I gruppi di scanner di classificazione BlueXP possono essere definiti come aree geografiche separate in cui sono memorizzati i dati. È possibile implementare più nodi scanner di classificazione BlueXP in tutto il mondo e scegliere un gruppo di scanner per ciascun nodo. In questo modo, ciascun nodo dello scanner eseguirà la scansione dei dati più vicini. Più vicino è il nodo dello scanner ai dati, meglio è perché riduce il più possibile la latenza di rete durante la scansione dei dati.

È possibile scegliere i gruppi di scanner da aggiungere alla classificazione BlueXP ed è possibile sceglierne i nomi. La classificazione BlueXP non impone l'implementazione in Europa di un nodo mappato a un gruppo di scanner denominato "europa".

Seguire questi passaggi per installare altri nodi scanner di classificazione BlueXP:

1. Preparare i sistemi host Linux che fungeranno da nodi scanner
2. Scarica il software Data Sense su questi sistemi Linux
3. Eseguire un comando sul nodo Manager per identificare i nodi scanner
4. Seguire la procedura per implementare il software sui nodi scanner (e, facoltativamente, definire un "gruppo scanner" per alcuni nodi scanner)
5. Se è stato definito un gruppo di scanner, nel nodo Manager:
    a. Aprire il file "Working_Environment_to_scanner_group_config.yml" e definire gli ambienti di lavoro che verranno sottoposti a scansione da ciascun gruppo di scanner
    b. Eseguire il seguente script per registrare queste informazioni di mappatura con tutti i nodi scanner: `update_we_scanner_group_from_config_file.sh`

Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi scanner soddisfino il requisiti dell'host.

- Verificare che sui sistemi siano installati i due pacchetti software prerequisiti (Docker Engine o Podman e Python 3).
- Assicurarsi di disporre dei privilegi di root sui sistemi Linux.
- Verificare che l'ambiente soddisfi i requisiti permessi e connettività.
- È necessario disporre degli indirizzi IP degli host del nodo scanner che si stanno aggiungendo.
- È necessario disporre dell'indirizzo IP del sistema host del nodo BlueXP Classification Manager
- È necessario disporre dell'indirizzo IP o del nome host del sistema di connessione, dell'ID account NetApp, dell'ID client del connettore e del token di accesso dell'utente. Se si intende utilizzare gruppi di scanner, è necessario conoscere l'ID dell'ambiente di lavoro per ciascuna origine dati nell'account. Per ottenere queste informazioni, vedere ***Prerequisite Steps*** di seguito.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

Porta	Protocolli	Descrizione
2377	TCP	Comunicazioni per la gestione del cluster
7946	TCP, UDP	Comunicazione tra nodi
4789	UDP	Sovrapporre il traffico di rete
50	ESP	Traffico ESP (Encrypted IPSec Overlay Network)
111	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)
2049	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)

- Se si utilizza `firewalld` Sulle macchine di classificazione BlueXP, si consiglia di attivarlo prima di installare la classificazione BlueXP. Eseguire i seguenti comandi per configurare `firewalld` In modo che sia compatibile con la classificazione BlueXP:

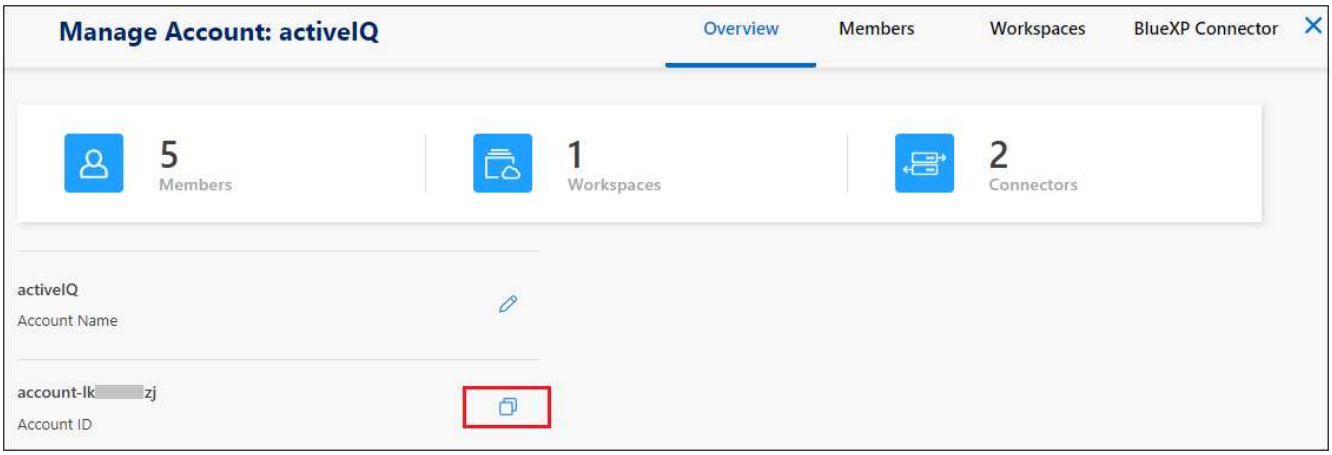
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

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

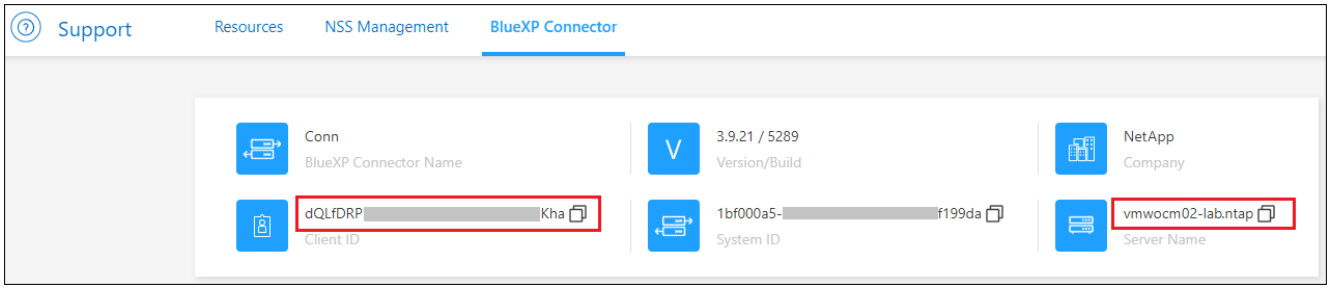
Fasi preliminari

Seguire questa procedura per ottenere l'ID account NetApp, l'ID client del connettore, il nome del server del connettore e il token di accesso dell'utente necessari per aggiungere i nodi dello scanner.

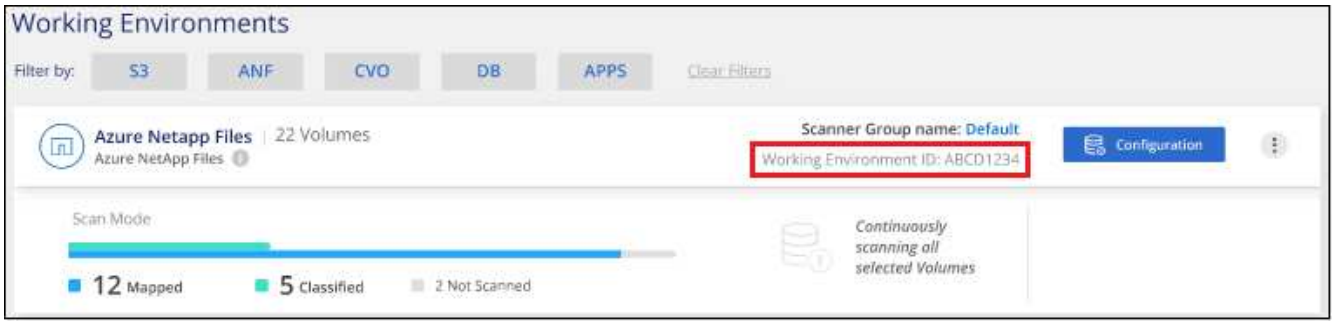
1. Dalla barra dei menu di BlueXP, fare clic su **account > Gestisci account**.



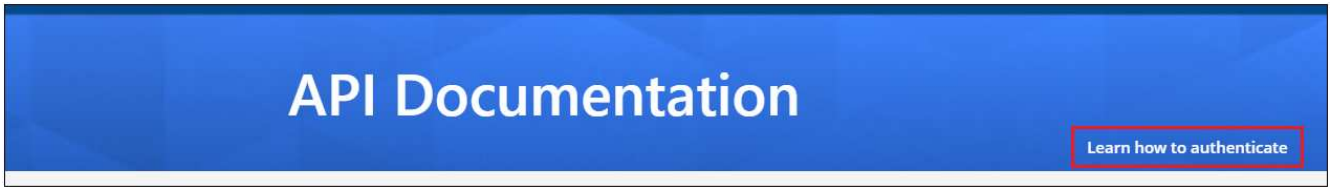
2. Copia l' *ID account*.
3. Dalla barra dei menu di BlueXP, fare clic su **Help > Support > BlueXP Connector**.



4. Copiare il connettore *ID client* e il *Nome server*.
5. Se si intende utilizzare gruppi di scanner, dalla scheda Configurazione classificazione BlueXP, copiare l'ID dell'ambiente di lavoro per ciascun ambiente di lavoro che si desidera aggiungere a un gruppo di scanner.



6. Accedere alla "API Documentation Developer Hub" E fare clic su **Scopri come autenticare**.



7. Seguire le istruzioni di autenticazione, utilizzando il nome utente e la password dell'account admin nei parametri "Username" (Nome utente) e "password".

8. Quindi, copiare il *token di accesso* dalla risposta.

Fasi

1. Nel nodo di gestione della classificazione BlueXP, eseguire lo script "add_scanner_node.sh". Ad esempio, questo comando aggiunge 2 nodi scanner:

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   Valori variabili:

   - *Account_id* = ID account NetApp
   - *Client_id* = ID client del connettore (aggiungere il suffisso "client" all'ID client copiato nei passaggi del prerequisito)
   - *Cm_host* = indirizzo IP o nome host del sistema di connessione
   - *Ds_manager_ip* = Indirizzo IP privato del sistema di nodi BlueXP Classification Manager
   - *Node_private_ip* = indirizzi IP dei sistemi a nodi scanner di classificazione BlueXP (gli IP di più nodi scanner sono separati da una virgola)
   - *User_token* = token di accesso utente JWT
2. Prima del completamento dello script add_scanner_node, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) e salvarlo in un file di testo.
3. Su **ciascun** host nodo scanner:
   a. Copiare il file di installazione di Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sul computer host (utilizzando `scp` o qualche altro metodo).
   b. Decomprimere il file di installazione.
   c. Incollare ed eseguire il comando copiato al punto 2.
   d. Se si desidera aggiungere un nodo scanner in un "gruppo scanner", aggiungere il parametro **-r <scanner_group_name>** al comando. In caso contrario, il nodo scanner viene aggiunto al gruppo "default".

      Quando l'installazione termina su tutti i nodi dello scanner e sono stati Uniti al nodo manager, termina anche lo script "add_scanner_node.sh". L'installazione può richiedere da 10 a 20 minuti.
4. Se sono stati aggiunti nodi scanner in un gruppo di scanner, tornare al nodo Manager ed eseguire le seguenti 2 operazioni:
   a. Aprire il file "/opt/netapp/config/custom_Configuration/working_environment_to_scanner_group_config.yml" e immettere la mappatura per cui i gruppi di scanner eseguiranno la scansione di specifici ambienti di lavoro. È necessario disporre dell' *ID ambiente di lavoro* per ogni origine dati. Ad esempio, le seguenti voci aggiungono 2 ambienti di lavoro al gruppo scanner "europa" e 2 al gruppo scanner "stati_uniti":

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

Tutti gli ambienti di lavoro non aggiunti all'elenco vengono sottoposti a scansione dal gruppo "predefinito". Nel gruppo "predefinito" deve essere presente almeno un nodo del gestore o dello scanner.

b. Eseguire il seguente script per registrare queste informazioni di mappatura con tutti i nodi scanner: `/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

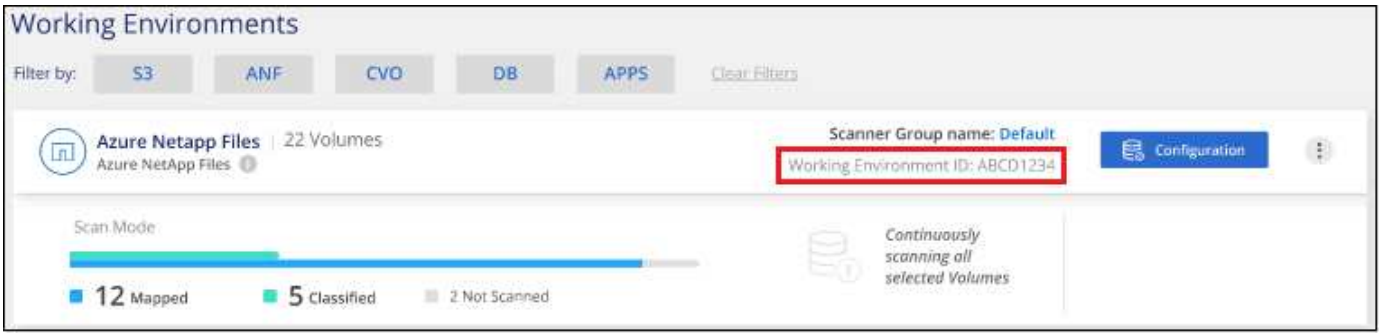
Risultato

La classificazione BlueXP viene impostata con Manager e scanner Node per eseguire la scansione di tutte le origini dati.

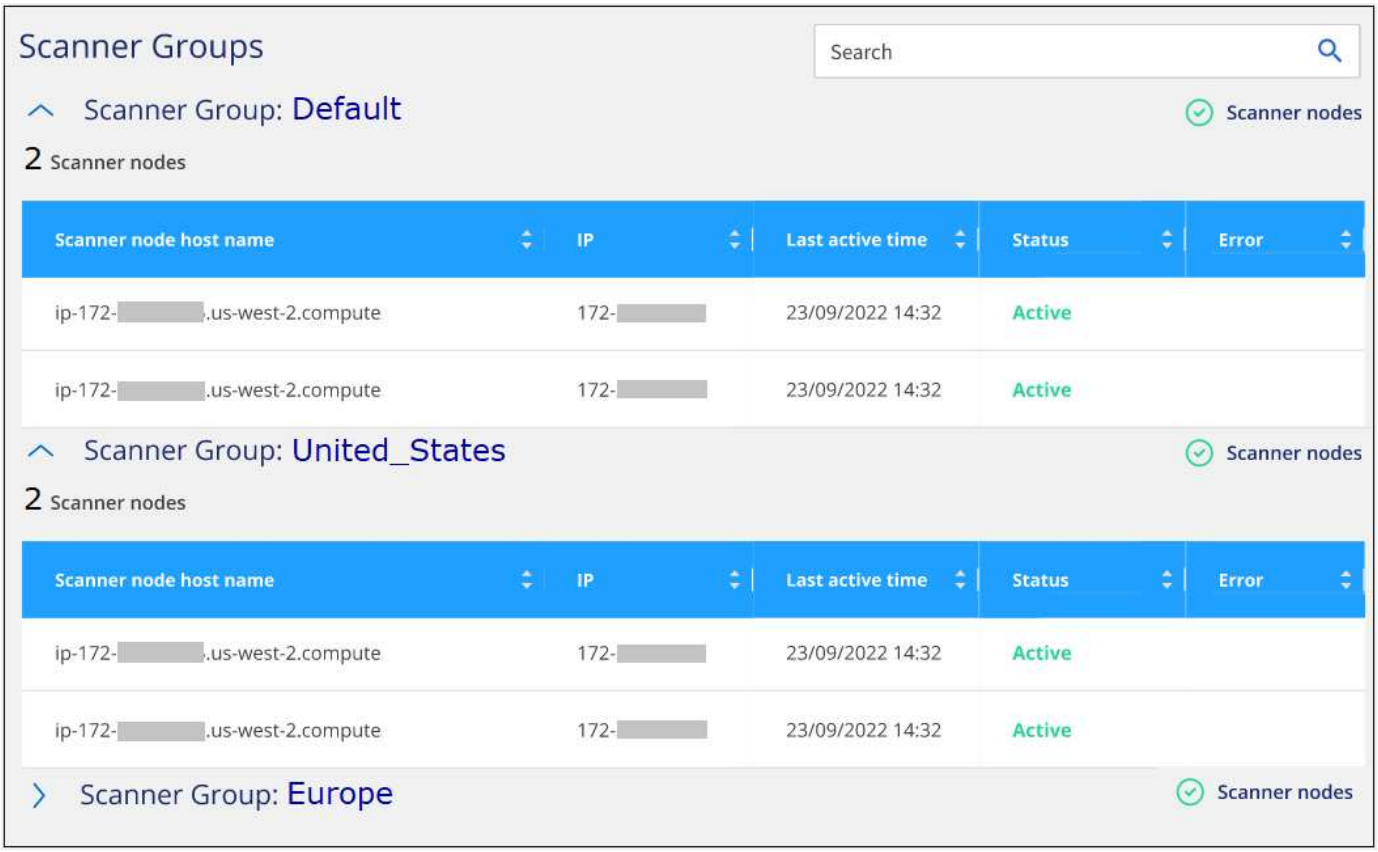
Cosa c'è di nuovo

Dalla pagina di configurazione è possibile selezionare le origini dati da sottoporre a scansione, se non è già stato fatto. Se sono stati creati gruppi scanner, ogni origine dati viene sottoposta a scansione dai nodi scanner del rispettivo gruppo.

Il nome del gruppo di scanner per ciascun ambiente di lavoro viene visualizzato nella pagina di configurazione.



È inoltre possibile visualizzare l'elenco di tutti i gruppi di scanner, l'indirizzo IP e lo stato di ciascun nodo dello scanner nel gruppo nella parte inferiore della pagina di configurazione.



È possibile "Impostare la licenza per la classificazione BlueXP" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

Installazione multi-host per configurazioni di grandi dimensioni

Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

Seguire questi passaggi quando si installa il software di classificazione BlueXP su più host on-premise contemporaneamente. Tenere presente che non è possibile utilizzare "gruppi di scanner" quando si implementano più host in questo modo.

Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi Manager e scanner soddisfino il requisiti dell'host.
- Verificare che sui sistemi siano installati i due pacchetti software prerequisiti (Docker o Podman Engine e Python 3).
- Assicurarsi di disporre dei privilegi di root sui sistemi Linux.
- Verificare che l'ambiente soddisfi i requisiti permessi e connettività.
- È necessario disporre degli indirizzi IP degli host dei nodi dello scanner che si intende utilizzare.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

Porta	Protocolli	Descrizione
2377	TCP	Comunicazioni per la gestione del cluster

Porta	Protocolli	Descrizione
7946	TCP, UDP	Comunicazione tra nodi
4789	UDP	Sovrapporre il traffico di rete
50	ESP	Traffico ESP (Encrypted IPSec Overlay Network)
111	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)
2049	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)

Fasi

1. Seguire i passi da 1 a 7 dal Installazione su host singolo sul nodo manager.
2. Come illustrato nel passaggio 8, quando richiesto dal programma di installazione, è possibile immettere i valori richiesti in una serie di prompt oppure fornire i parametri richiesti come argomenti della riga di comando al programma di installazione.

   Oltre alle variabili disponibili per un'installazione a singolo host, viene utilizzata una nuova opzione **-n <node_ip>** per specificare gli indirizzi IP dei nodi dello scanner. Gli IP di più nodi dello scanner sono separati da una virgola.

   Ad esempio, questo comando aggiunge 3 nodi scanner:
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
   -host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
   --proxy-user <proxy_user> --proxy-password <proxy_password>
   ```
3. Prima del completamento dell'installazione del nodo manager, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio, `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) e salvarlo in un file di testo.
4. Su **ciascun** host nodo scanner:
   a. Copiare il file di installazione di Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sul computer host (utilizzando `scp` o qualche altro metodo).
   b. Decomprimere il file di installazione.
   c. Incollare ed eseguire il comando copiato al punto 3.

      Una volta completata l'installazione su tutti i nodi dello scanner e collegati al nodo manager, l'installazione del nodo manager viene completata.

Risultato

Il programma di installazione della classificazione BlueXP completa l'installazione dei pacchetti e registra l'installazione. L'installazione può richiedere da 10 a 20 minuti.

Cosa c'è di nuovo

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

Puoi anche farlo "Impostare la licenza per la classificazione BlueXP" a questo punto. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

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 è perfetto per i siti sicuri.

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

Nota: 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".

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
- Account SharePoint on-premise (SharePoint Server)
- Condivisioni di file NFS o CIFS non NetApp
- Storage a oggetti che utilizza il protocollo S3 (Simple Storage Service)

Attualmente non è disponibile alcun supporto per la scansione di Cloud Volumes ONTAP, Azure NetApp Files, FSX per ONTAP, AWS S3 o Google Drive, OneDrive o SharePoint Online quando la classificazione BlueXP viene implementata in modalità privata.

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:

- Gestione delle etichette AIP (Microsoft Azure Information Protection)
- Invio di avvisi e-mail agli utenti di BlueXP quando alcuni criteri critici restituiscono risultati
- 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
- Ricezione del feedback dell'utente
- 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.

1. **Installare il connettore BlueXP**

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

2. **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.

3. **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.

4. **Iscriviti al servizio di classificazione BlueXP**

I primi 1 TB di dati che la classificazione BlueXP scansiona in BlueXP sono gratuiti per 30 giorni. Una licenza BYOL di NetApp è necessaria per continuare la scansione dei dati dopo tale data.

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 si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di 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 /opt 895 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Grande	16 CPU	64 GB DI RAM	500 GiB SSD ON /, OR - 100 GiB disponibile su /opt - 395 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Medio	8 CPU	32 GB DI RAM	200 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 145 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Piccolo	8 CPU	16 GB DI RAM	100 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 45 GiB disponibile su /var/lib/docker - 5 GiB su /tmp

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere "Utilizzando un tipo di istanza più piccolo" per ulteriori informazioni.

- 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 AWS 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
    - CentOS versione 7,8 e 7,9

        - Ubuntu 22,04 (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, 9,0, 9,1, 9,2 e 9,3

          Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

            - Installazione in un luogo buio
            - Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti
- **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".

          "Guarda questo video" Per una rapida dimostrazione dell'installazione di Docker su CentOS.

        - Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install 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.

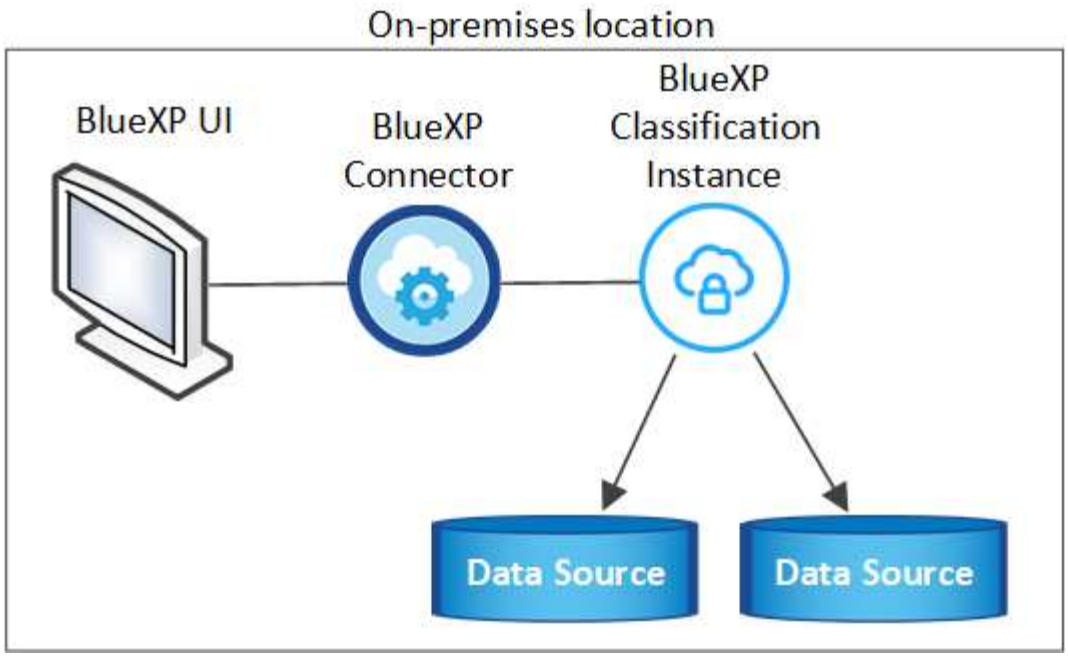
Tipo di connessione	Porte	Descrizione
Connettore <> classificazione BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) E 80	Il gruppo di sicurezza per il connettore deve consentire il traffico in entrata e in uscita sulle porte 6000 e 443 da e verso l'istanza di classificazione BlueXP. • È necessaria la porta 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.
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)

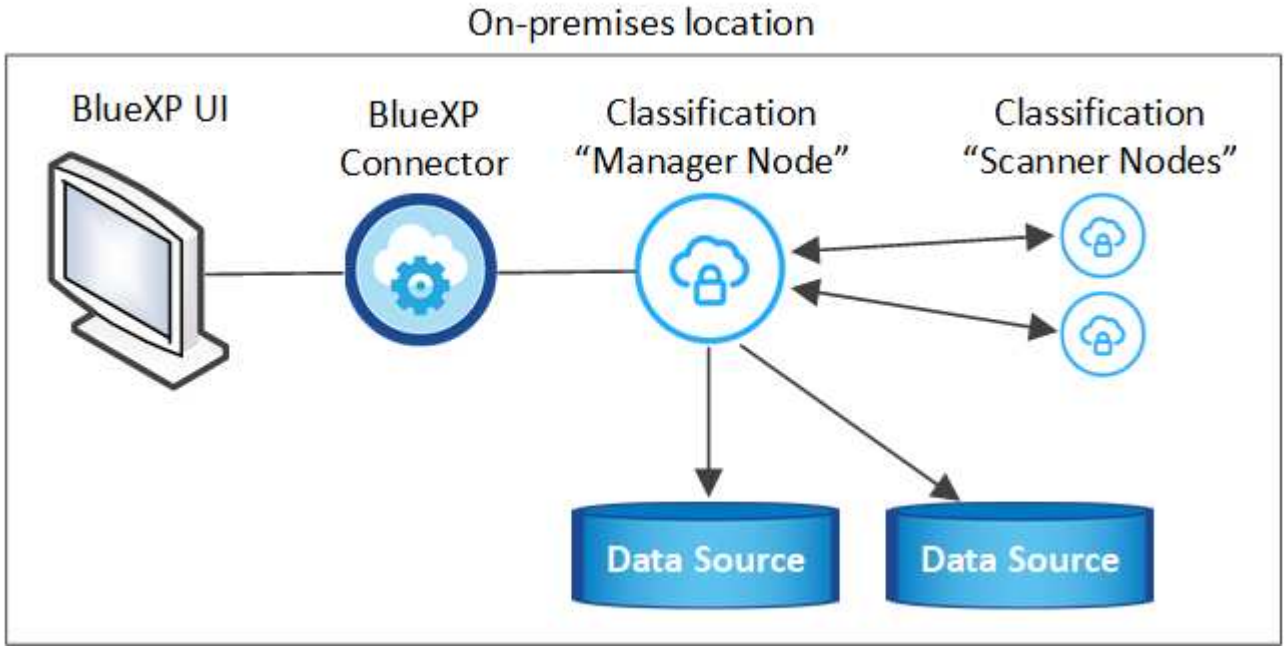
Se si utilizzano più host di classificazione BlueXP per fornire ulteriore potenza di elaborazione per eseguire la scansione delle origini dati, è necessario attivare porte/protocolli aggiuntivi. "Vedere i requisiti aggiuntivi per le porte".

Installare la classificazione BlueXP sull'host Linux on-premise

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



Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. "Consulta questa procedura".



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".

Di cosa hai bisogno

- 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:

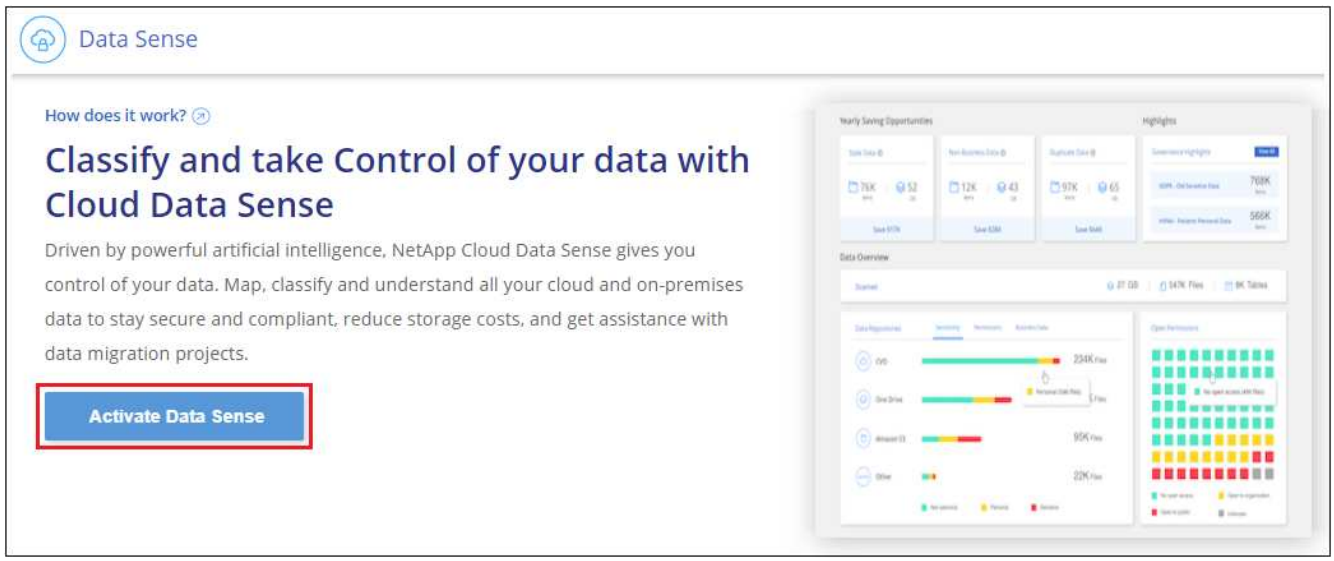
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

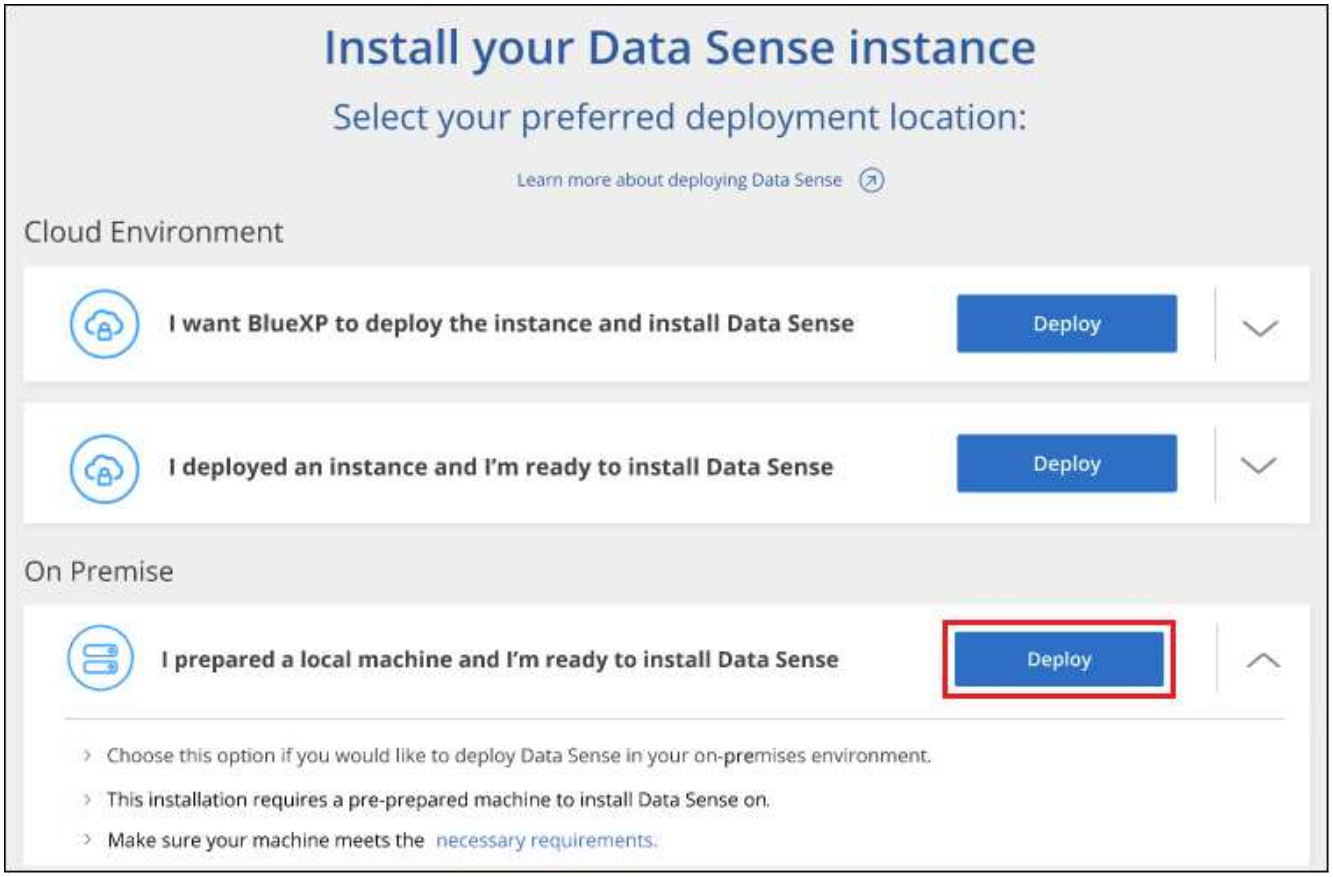
4. Decomprimere il file di installazione sul computer host, ad esempio:

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

5. Avviare BlueXP e selezionare **Governance > Classification**.
6. Fare clic su **Activate Data Sense** (attiva rilevamento dati).



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.

Puoi anche farlo "Impostare la licenza BYOL per la classificazione BlueXP" Dalla pagina del portafoglio digitale BlueXP. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

Installazione multi-host per configurazioni di grandi dimensioni

Per configurazioni molto grandi in cui si eseguono scansioni di petabyte di dati, è possibile includere più host per fornire ulteriore potenza di elaborazione. Quando si utilizzano più sistemi host, il sistema primario è denominato *nodo Manager* e i sistemi aggiuntivi che forniscono potenza di elaborazione aggiuntiva sono denominati *nodi scanner*.

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

Di cosa hai bisogno

- Verificare che tutti i sistemi Linux per i nodi Manager e scanner soddisfino il 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 sui sistemi Linux.
- Verificare che l'ambiente offline soddisfi i requisiti permessi e connettività.
- È necessario disporre degli indirizzi IP degli host dei nodi dello scanner che si intende utilizzare.
- Su tutti gli host devono essere attivati i seguenti protocolli e porte:

Porta	Protocolli	Descrizione
2377	TCP	Comunicazioni per la gestione del cluster
7946	TCP, UDP	Comunicazione tra nodi
4789	UDP	Sovrapporre il traffico di rete
50	ESP	Traffico ESP (Encrypted IPSec Overlay Network)
111	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)

Porta	Protocolli	Descrizione
2049	TCP, UDP	Server NFS per la condivisione dei file tra gli host (necessario da ciascun nodo scanner al nodo manager)

Fasi

1. Seguire i passi da 1 a 8 dal "Installazione su host singolo" sul nodo manager.
2. Come illustrato al punto 9, quando richiesto dal programma di installazione, è possibile immettere i valori richiesti in una serie di prompt oppure fornire i parametri richiesti come argomenti della riga di comando al programma di installazione.

   Oltre alle variabili disponibili per un'installazione a singolo host, viene utilizzata una nuova opzione **-n <node_ip>** per specificare gli indirizzi IP dei nodi dello scanner. Gli IP di più nodi sono separati da una virgola.

   Ad esempio, questo comando aggiunge 3 nodi scanner:
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
   -proxy --darksite
   ```
3. Prima del completamento dell'installazione del nodo manager, viene visualizzata una finestra di dialogo con il comando di installazione necessario per i nodi dello scanner. Copiare il comando (ad esempio: `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) e salvarlo in un file di testo.
4. Su **ciascun** host nodo scanner:
   a. Copiare il file del programma di installazione Data Sense (**cc_onrem_installer.tar.gz**) sul computer host.
   b. Decomprimere il file di installazione.
   c. Incollare ed eseguire il comando copiato al punto 3.

      Una volta completata l'installazione su tutti i nodi dello scanner e collegati al nodo manager, l'installazione del nodo manager viene completata.

Risultato

Il programma di installazione della classificazione BlueXP completa l'installazione dei pacchetti e registra l'installazione. L'installazione può richiedere da 15 a 25 minuti.

Cosa c'è di nuovo

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

Puoi anche farlo "Impostare la licenza BYOL per la classificazione BlueXP" Dalla pagina del portafoglio digitale BlueXP. Non ti verrà addebitato alcun costo fino al termine della prova gratuita di 30 giorni.

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.

Tenere presente che non è necessario alcun aggiornamento sui nodi dello scanner se è stata implementata la classificazione BlueXP su sistemi host multipli per la scansione di configurazioni molto grandi.

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, è possibile eseguire uno script sull'host per verificare che tutti i prerequisiti siano stati implementati 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 si costruisce il sistema host in sede, è possibile scegliere tra tre dimensioni del sistema a seconda delle dimensioni del set di dati che si prevede di sottoporre a scansione di 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 /opt 895 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Grande	16 CPU	64 GB DI RAM	500 GiB SSD ON /, OR - 100 GiB disponibile su /opt - 395 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Medio	8 CPU	32 GB DI RAM	200 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 145 GiB disponibile su /var/lib/docker - 5 GiB su /tmp
Piccolo	8 CPU	16 GB DI RAM	100 GiB SSD ON /, OR - 50 GiB disponibile su /opt - 45 GiB disponibile su /var/lib/docker - 5 GiB su /tmp

Tenere presente che esistono limitazioni quando si utilizzano sistemi di dimensioni inferiori. Vedere "Utilizzando un tipo di istanza più piccolo" per ulteriori informazioni.

- 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 AWS 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
    - CentOS versione 7,8 e 7,9

    - Ubuntu 22,04 (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, 9,0, 9,1, 9,2 e 9,3

      Tenere presente che le seguenti funzioni non sono attualmente supportate quando si utilizzano RHEL 8.x e RHEL 9.x:

      - Installazione in un luogo buio
      - Scansione distribuita, utilizzando un nodo scanner master e nodi scanner remoti
- **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".

      "Guarda questo video" Per una rapida dimostrazione dell'installazione di Docker su CentOS.

    - Podman versione 4 o superiore. Per installare Podman, aggiorna i pacchetti di sistema (`sudo yum update -y`), quindi installare Podman (`sudo yum install 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://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Fornisce pacchetti prerequisiti per l'installazione di CentOS.
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	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.

Tipo di connessione	Porte	Descrizione
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.

Di cosa hai bisogno

- 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

Introduzione alla classificazione BlueXP per Cloud Volumes ONTAP e on-premise ONTAP

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

Avvio rapido

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

1. **Individuare le origini dati da sottoporre a scansione**

Prima di poter eseguire la scansione dei volumi, è necessario aggiungere i sistemi come ambienti di lavoro in BlueXP:

- Per i sistemi Cloud Volumes ONTAP, questi ambienti di lavoro dovrebbero essere già disponibili in BlueXP
- Per sistemi ONTAP on-premise, "BlueXP deve rilevare i cluster ONTAP"

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione**

Selezionare la scheda **Configuration** (Configurazione) e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

4. **Garantire l'accesso ai volumi**

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di 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 - porte 111 e 2049.
  - Per CIFS - porte 139 e 445.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

5 Gestire i volumi che si desidera sottoporre a scansione

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

Rilevamento delle origini dati che si desidera acquisire

Se le origini dati che si desidera sottoporre a scansione non sono già presenti nell'ambiente BlueXP, è possibile aggiungerle all'area di lavoro.

I sistemi Cloud Volumes ONTAP dovrebbero essere già disponibili in Canvas in BlueXP. Per i sistemi ONTAP on-premise, è necessario disporre di "BlueXP Scopri questi cluster".

Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di sistemi Cloud Volumes ONTAP e ONTAP on-premise accessibili tramite Internet, è possibile "Implementare la classificazione BlueXP nel cloud" oppure "in una sede on-premise con accesso a internet".

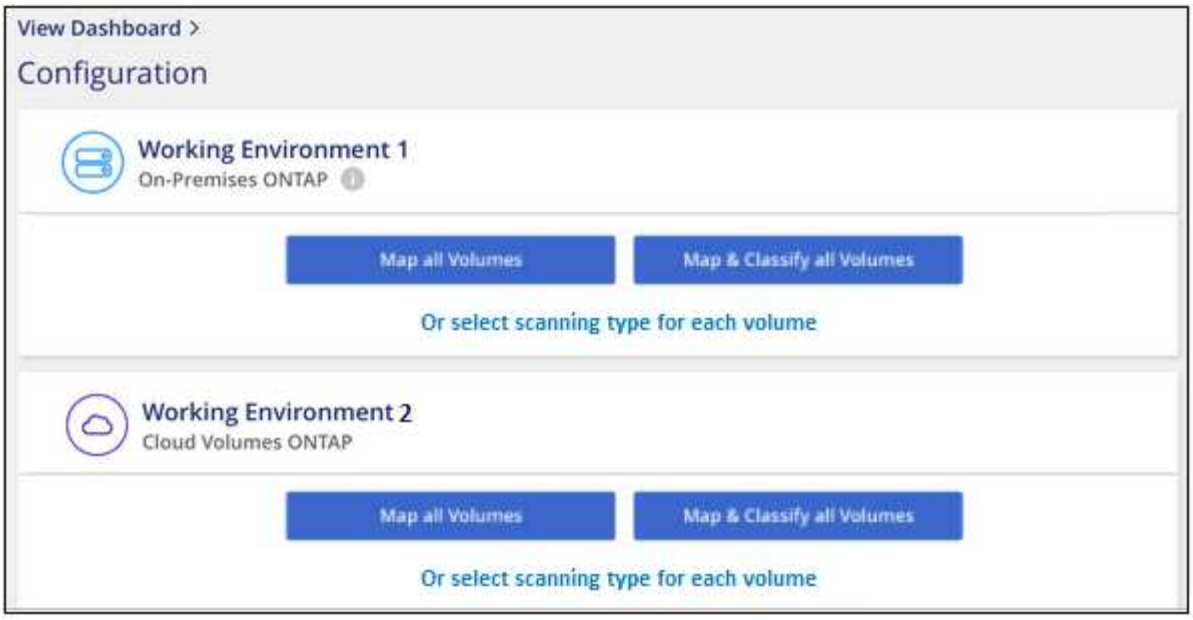
Se si esegue la scansione di sistemi ONTAP on-premise che sono stati installati in un sito buio e che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella stessa posizione on-premise.

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

Abilitazione della classificazione BlueXP negli ambienti di lavoro

Puoi abilitare la classificazione BlueXP sui sistemi Cloud Volumes ONTAP in qualsiasi cloud provider supportato e sui cluster ONTAP on-premise.

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).



2. 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.

     Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.
3. 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.

- 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.

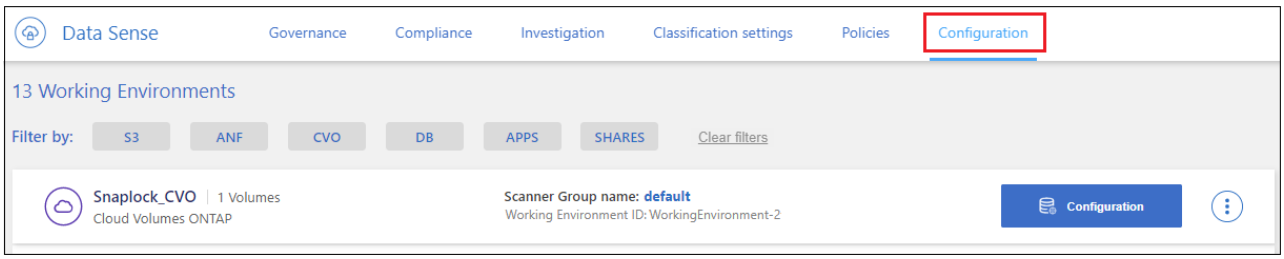
Fasi

1. 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 le seguenti porte siano aperte per l'istanza di classificazione BlueXP:
   - Per NFS - porte 111 e 2049.
   - Per CIFS - porte 139 e 445.
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 di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).

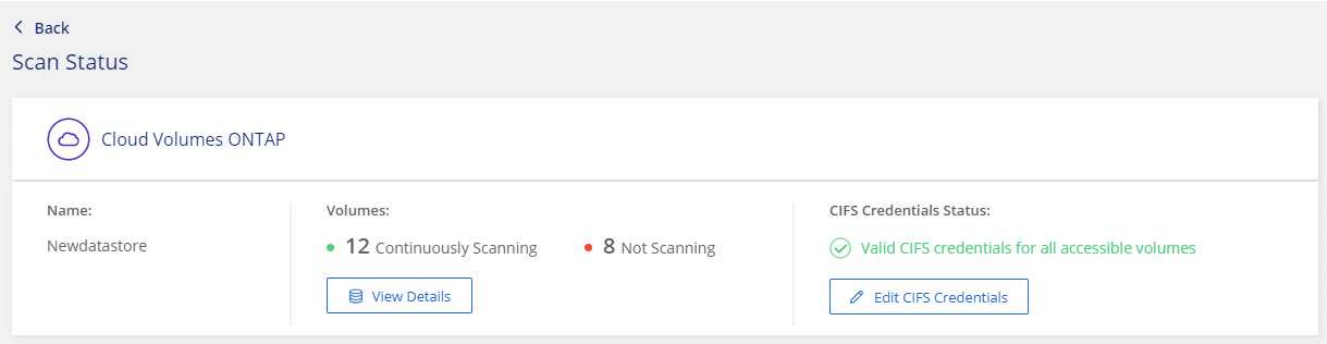


   b. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS nel sistema.

      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.

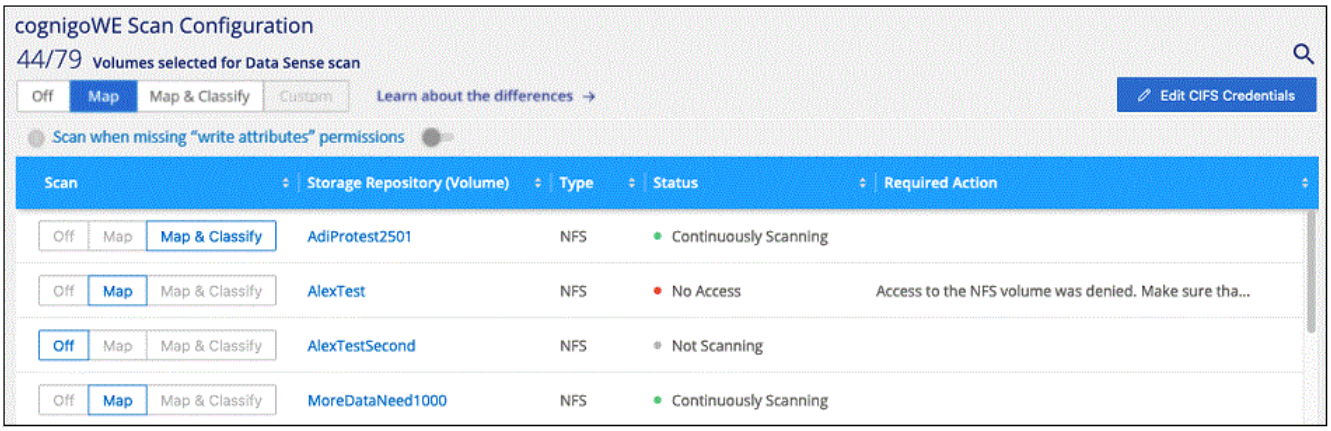
      Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory di un gruppo principale dell'organizzazione che dispone delle autorizzazioni per tutti i file.

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



6. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

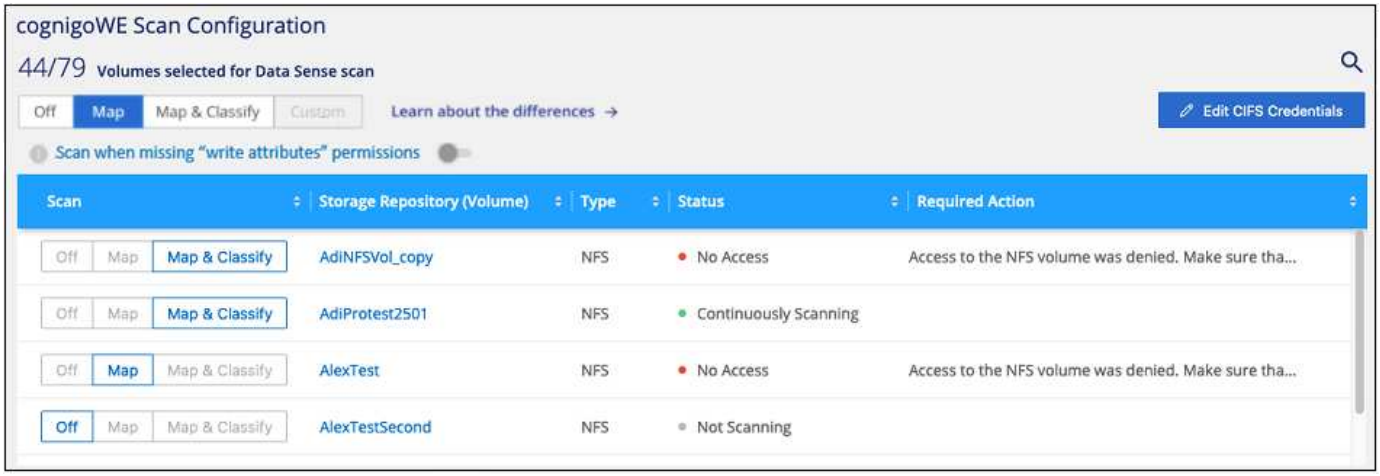
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



Attivazione e disattivazione delle scansioni di compliance 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".



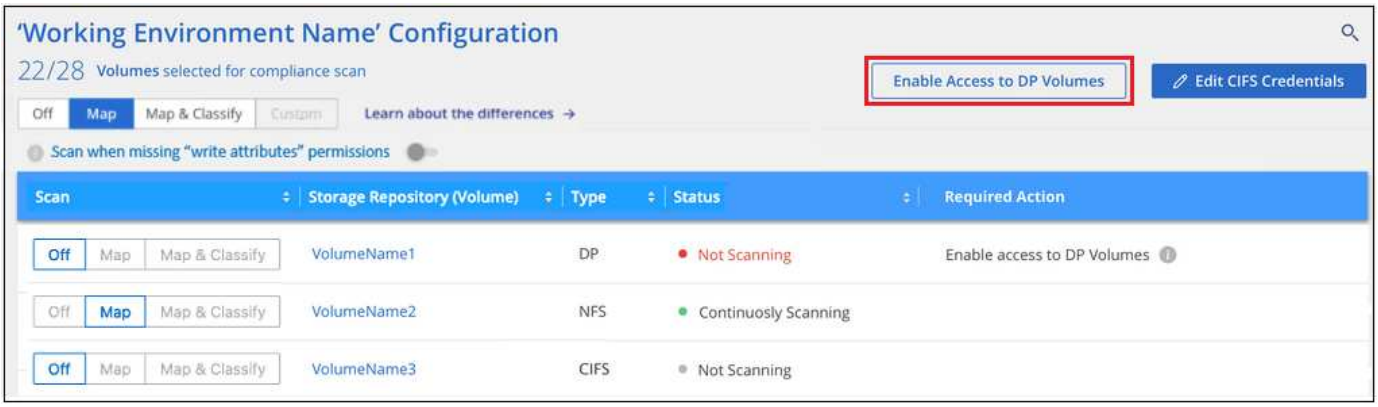
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura su un volume	Nell'area del volume, fare clic su **Map** (Mappa)
Abilitare la scansione completa su un volume	Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un volume	Nell'area del volume, fare clic su **Off**
Abilitare le scansioni di sola mappatura su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map** (Mappa)
Abilitare la scansione completa su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su tutti i volumi	Nell'area dell'intestazione, fare clic su **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.

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 sistema ONTAP on-premise o da un sistema Cloud Volumes ONTAP.

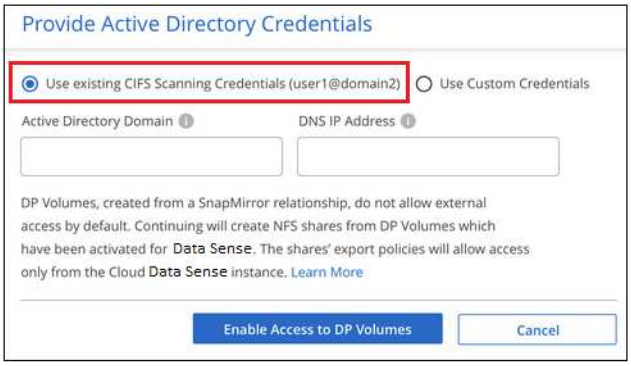
Inizialmente, l'elenco dei volumi identifica questi volumi come *Type* **DP** con *Status* **Not Scanning** e *Required Action* **Enable Access to DP Volumes**.

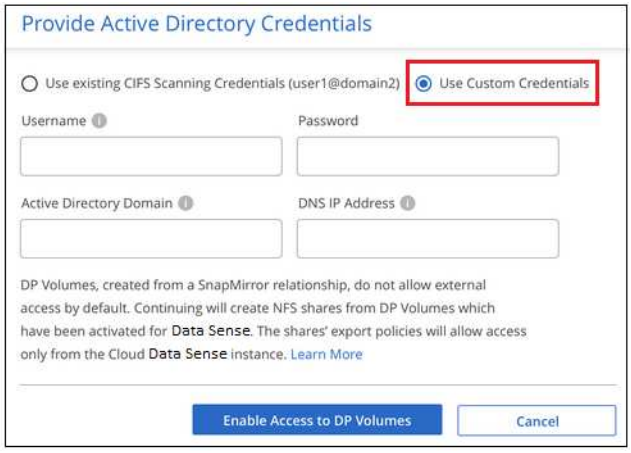


Fasi

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

1. Fare clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP) nella parte superiore della pagina.
2. Leggere il messaggio di conferma e fare nuovamente clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP).
   - I volumi creati inizialmente come volumi NFS nel sistema ONTAP di origine sono abilitati.
   - I volumi creati inizialmente come volumi CIFS nel sistema ONTAP di origine 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.





3. Attivare ciascun volume DP che si desidera sottoporre a scansione allo stesso modo in cui sono stati attivati altri volumi.

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.

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

Le credenziali di Active Directory vengono registrate solo nella VM di storage del primo volume CIFS DP, quindi tutti i volumi DP su tale 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.

Introduzione alla classificazione BlueXP per Azure NetApp Files

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

Avvio rapido

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

1 Individuare i sistemi Azure NetApp Files che si desidera sottoporre a scansione

Prima di eseguire la scansione dei volumi Azure NetApp Files, "BlueXP deve essere configurato per rilevare la configurazione".

2 Distribuire l'istanza di classificazione BlueXP

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

3 Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione

Fare clic su **Compliance**, selezionare la scheda **Configuration** e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

4 Garantire l'accesso ai volumi

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di classificazione BlueXP richiede una connessione di rete a ciascuna subnet Azure NetApp Files.
- Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS.

  Fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

5 Gestire i volumi che si desidera sottoporre a scansione

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

Rilevamento del 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".

Implementazione dell'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.

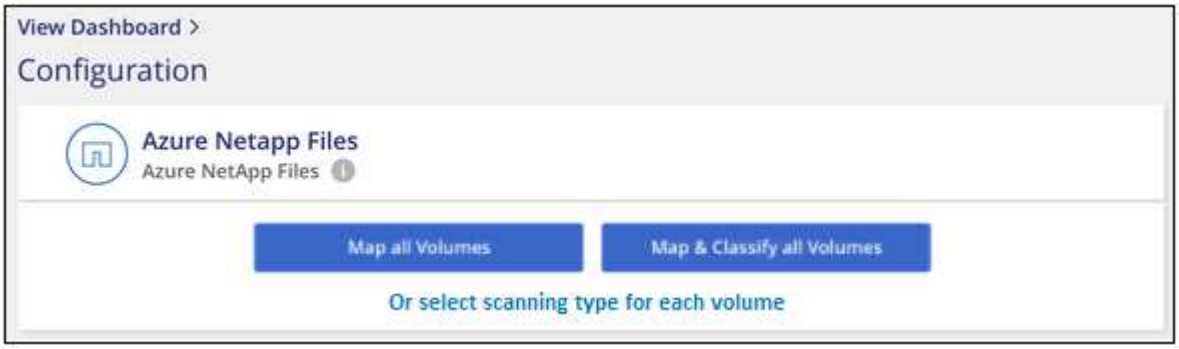
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi Azure NetApp Files.

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

Abilitazione della classificazione BlueXP negli 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** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).



2. 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.

     Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

3. 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.

- 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. Assicurarsi che sia presente una connessione di rete tra l'istanza di classificazione BlueXP e ciascuna rete che include volumi per Azure NetApp Files.

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

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.

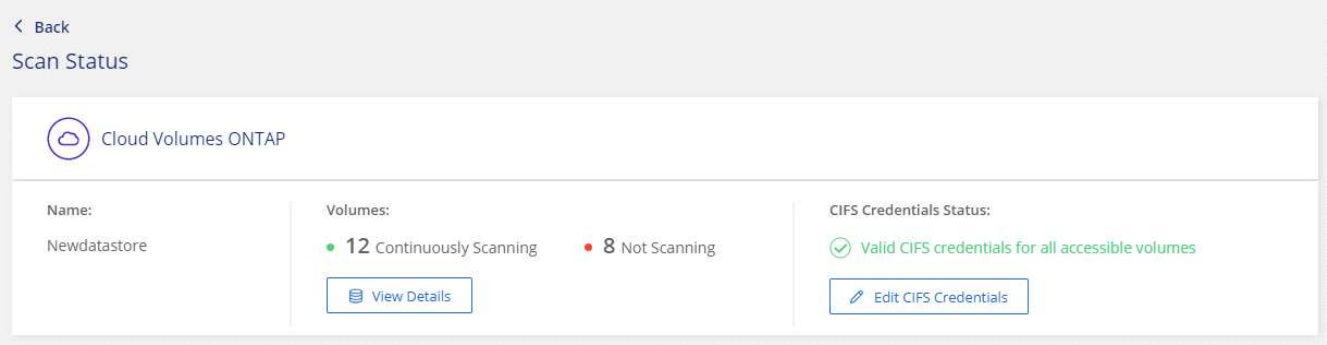
   a. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).

b. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS nel 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.

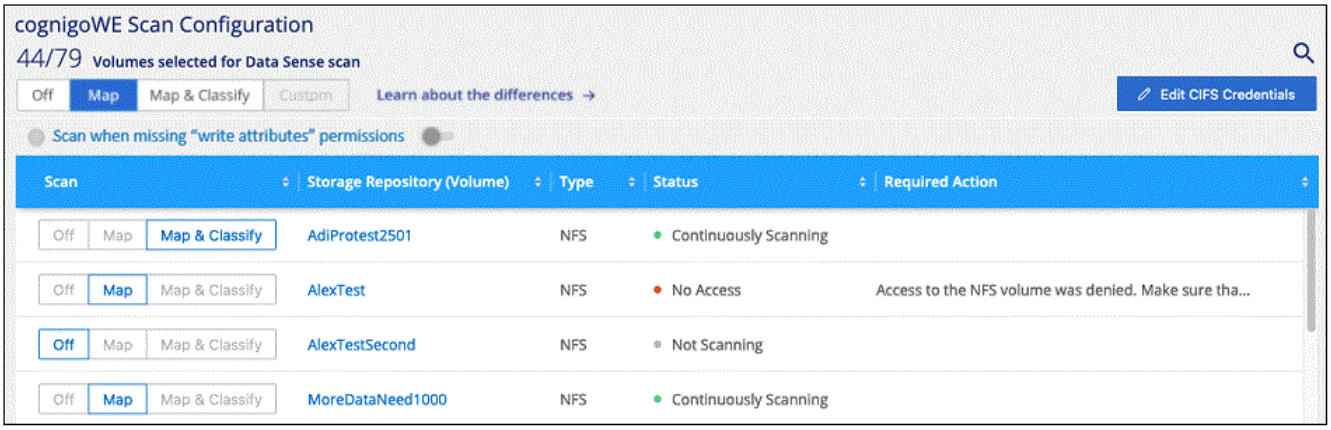
   Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory di un gruppo principale dell'organizzazione che dispone delle autorizzazioni per tutti i file.

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



5. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare lo stato di ciascun volume CIFS e NFS e correggere eventuali errori.

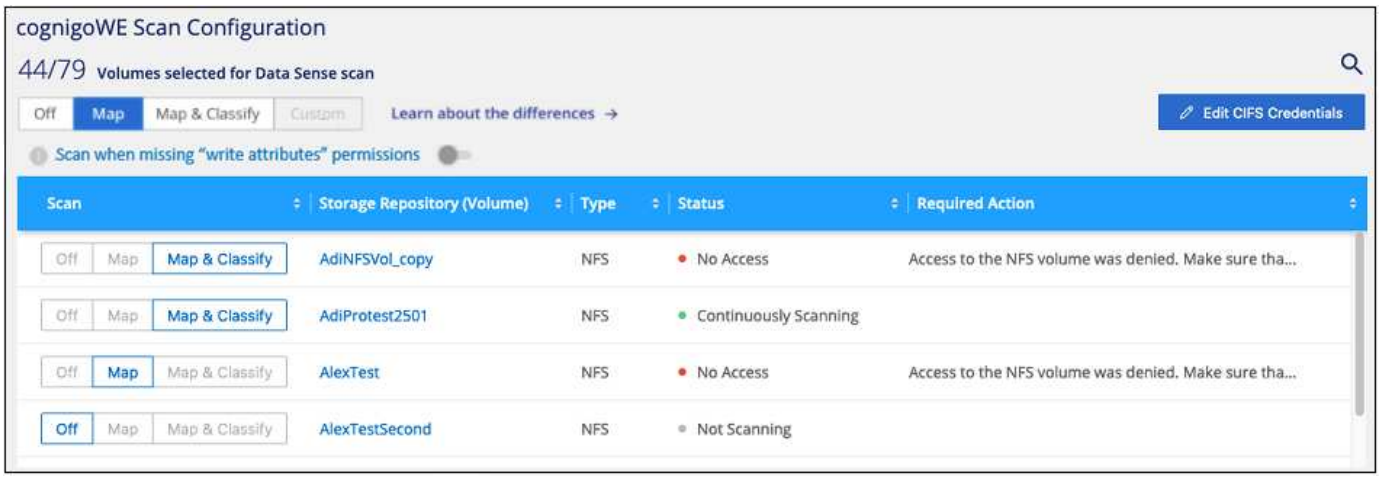
   Ad esempio, l'immagine seguente mostra quattro volumi, uno dei quali non è in grado di eseguire la scansione a causa di problemi di connettività di rete tra l'istanza di classificazione BlueXP e il volume.



Attivazione e disattivazione delle scansioni di compliance 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".



A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura su un volume	Nell'area del volume, fare clic su **Map** (Mappa)
Abilitare la scansione completa su un volume	Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un volume	Nell'area del volume, fare clic su **Off**
Abilitare le scansioni di sola mappatura su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map** (Mappa)
Abilitare la scansione completa su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su tutti i volumi	Nell'area dell'intestazione, fare clic su **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.

Inizia a utilizzare la classificazione BlueXP per Amazon FSX per ONTAP

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)"

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso per ottenere informazioni dettagliate.

1 **Scopri il file system FSX per ONTAP che desideri sottoporre a scansione**

Prima di eseguire la scansione di FSX per i volumi ONTAP, "È necessario disporre di un ambiente di lavoro FSX con volumi configurati".

2 **Distribuire l'istanza di classificazione BlueXP**

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

3 **Abilitare la classificazione BlueXP e selezionare i volumi da sottoporre a scansione**

Selezionare la scheda **Configuration** (Configurazione) e attivare le scansioni di compliance per i volumi in ambienti di lavoro specifici.

4 **Garantire l'accesso ai volumi**

Ora che la classificazione BlueXP è attivata, assicurarsi che sia in grado di accedere a tutti i volumi.

- L'istanza di classificazione BlueXP richiede una connessione di rete a ciascuna subnet FSX per ONTAP.
- 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.
- I criteri di esportazione dei volumi NFS devono consentire l'accesso dall'istanza di classificazione BlueXP.
- La classificazione BlueXP richiede le credenziali di Active Directory per eseguire la scansione dei volumi CIFS. + fare clic su **Compliance** > **Configuration** > **Edit CIFS Credentials** (Modifica credenziali CIFS) e fornire le credenziali.

5 Gestire i volumi che si desidera sottoporre a scansione

Selezionare o deselezionare i volumi da sottoporre a scansione per avviare o interrompere la scansione della classificazione BlueXP.

Rilevamento del file system FSX per ONTAP che si desidera sottoporre a scansione

Se il file system FSX per ONTAP 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 individuare o creare il file system FSX per ONTAP in BlueXP".

Implementazione dell'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.

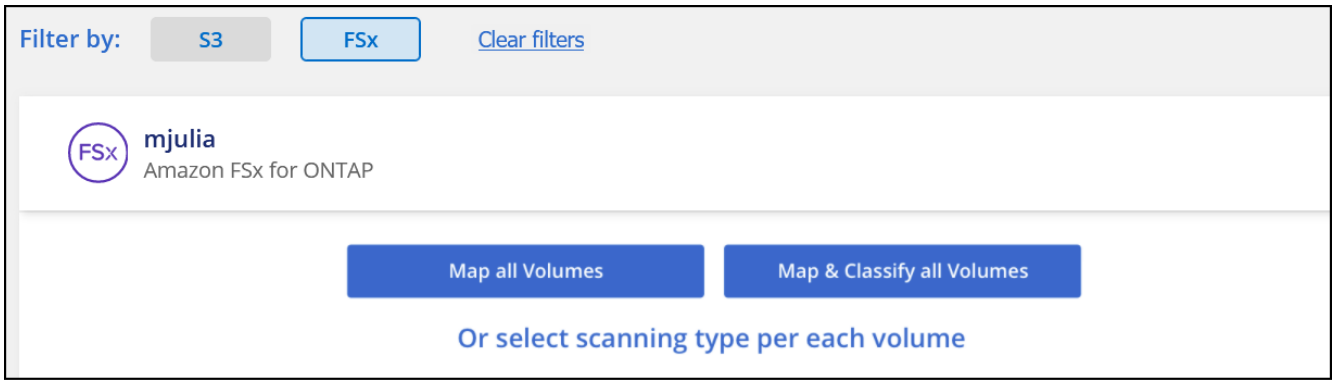
Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei volumi FSX.

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

Abilitazione della classificazione BlueXP negli ambienti di lavoro

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

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).



2. 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.

     Vedere Attivazione e disattivazione delle scansioni di compliance sui volumi per ulteriori informazioni.

3. 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.

- 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. Nella pagina *Configuration*, fare clic su **View Details** (Visualizza dettagli) per esaminare 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.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. 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.

3. 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.
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 di navigazione a sinistra di BlueXP, fare clic su **Governance > Classification** (Governance > classificazione), quindi selezionare la scheda **Configuration** (Configurazione).

   b. Per ciascun ambiente di lavoro, fare clic su **Edit CIFS Credentials** (Modifica credenziali CIFS) e immettere il nome utente e la password necessari per la classificazione BlueXP per accedere ai volumi CIFS nel 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.

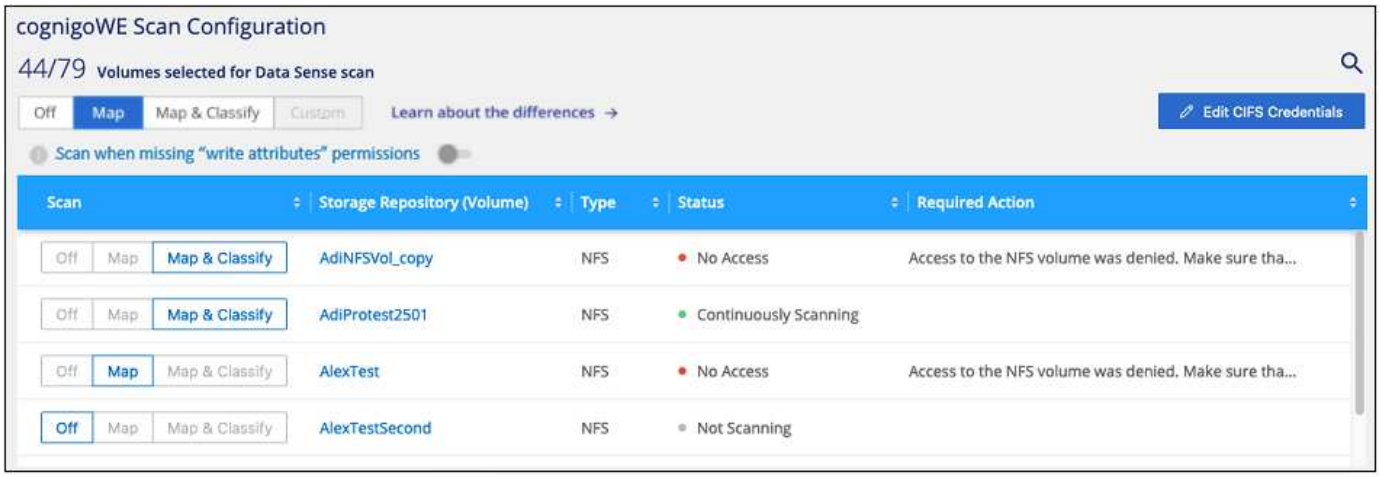
      Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. Se possibile, si consiglia di far parte dell'utente configurato con Active Directory di un gruppo principale dell'organizzazione che dispone delle autorizzazioni per tutti i file.

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

Attivazione e disattivazione delle scansioni di compliance 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".



A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura su un volume	Nell'area del volume, fare clic su **Map** (Mappa)

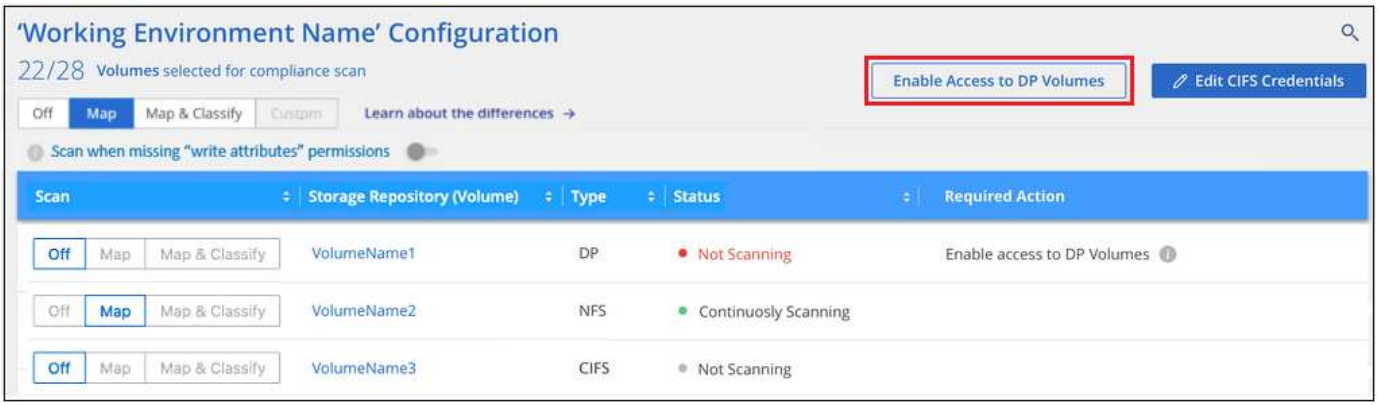
A:	Eseguire questa operazione:
Abilitare la scansione completa su un volume	Nell'area del volume, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un volume	Nell'area del volume, fare clic su **Off**
Abilitare le scansioni di sola mappatura su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map** (Mappa)
Abilitare la scansione completa su tutti i volumi	Nell'area dell'intestazione, fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su tutti i volumi	Nell'area dell'intestazione, fare clic su **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.

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**.

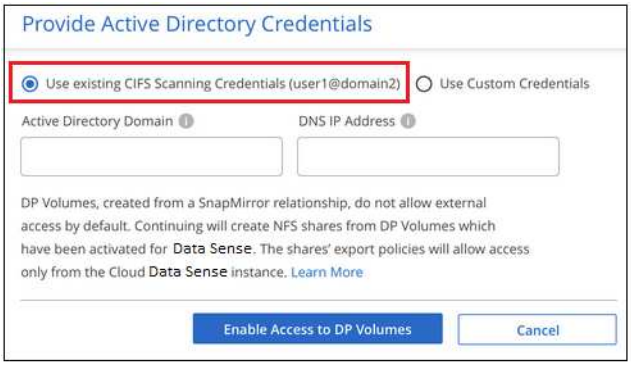


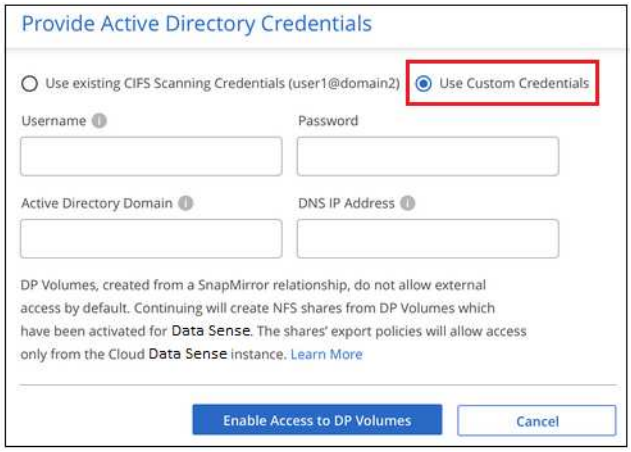
Fasi

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

1. Fare clic su **Enable Access to DP Volumes** (attiva accesso ai volumi DP) nella parte superiore della pagina.
2. Leggere il messaggio di conferma e fare nuovamente clic su **Enable Access to DP Volumes** (attiva 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.





3. Attivare ciascun volume DP che si desidera sottoporre a scansione allo stesso modo in cui sono stati attivati altri volumi.

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.

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

> Le credenziali di Active Directory vengono registrate solo nella VM di storage del primo volume CIFS DP, quindi tutti i volumi DP su tale 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.

Introduzione alla classificazione BlueXP per Amazon S3

La classificazione BlueXP consente di eseguire la scansione dei bucket Amazon S3 per identificare i dati personali e sensibili presenti nello storage a oggetti S3. La classificazione BlueXP può eseguire la scansione di qualsiasi bucket dell'account, indipendentemente dal fatto che sia stato creato per una soluzione NetApp.

Avvio rapido

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

1 **Imposta i requisiti S3 nel tuo ambiente cloud**

Assicurati che il tuo ambiente cloud sia in grado di soddisfare i requisiti per la classificazione BlueXP, inclusa la preparazione di un ruolo IAM e la configurazione della connettività dalla classificazione BlueXP a S3. Consulta l'elenco completo.

Distribuire l’istanza di classificazione BlueXP

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

Attivare la classificazione BlueXP nell’ambiente di lavoro S3

Selezionare l’ambiente di lavoro Amazon S3, fare clic su **Enable** (attiva) e selezionare un ruolo IAM che includa le autorizzazioni richieste.

Selezionare i bucket da sottoporre a scansione

Selezionare i bucket che si desidera sottoporre a scansione e la classificazione BlueXP inizierà a eseguirne la scansione.

Verifica dei prerequisiti di S3

I seguenti requisiti sono specifici per la scansione dei bucket S3.

Impostare un ruolo IAM per l’istanza di classificazione BlueXP

La classificazione BlueXP richiede autorizzazioni per connettersi ai bucket S3 del tuo account e per eseguirne la scansione. Impostare un ruolo IAM che includa le autorizzazioni elencate di seguito. BlueXP richiede di selezionare un ruolo IAM quando si attiva la classificazione BlueXP nell’ambiente di lavoro Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Fornire connettività dalla classificazione BlueXP ad Amazon S3

La classificazione BlueXP richiede una connessione ad Amazon S3. Il modo migliore per fornire tale connessione è tramite un endpoint VPC al servizio S3. Per istruzioni, vedere "Documentazione AWS: Creazione di un endpoint gateway".

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di classificazione BlueXP. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, la classificazione BlueXP non può connettersi al servizio S3.

In caso di problemi, vedere "AWS Support Knowledge Center: Perché non è possibile connettersi a un bucket S3 utilizzando un endpoint VPC gateway?"

In alternativa, è possibile stabilire la connessione utilizzando un gateway NAT.

Non puoi utilizzare un proxy per accedere a S3 tramite Internet.

Implementazione dell'istanza di classificazione BlueXP

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

È necessario implementare l'istanza utilizzando un connettore implementato in AWS in modo che BlueXP scopra automaticamente i bucket S3 in questo account AWS e li visualizzi in un ambiente di lavoro Amazon S3.

Nota: l'implementazione della classificazione BlueXP in una posizione on-premise non è attualmente supportata durante la scansione dei bucket S3.

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

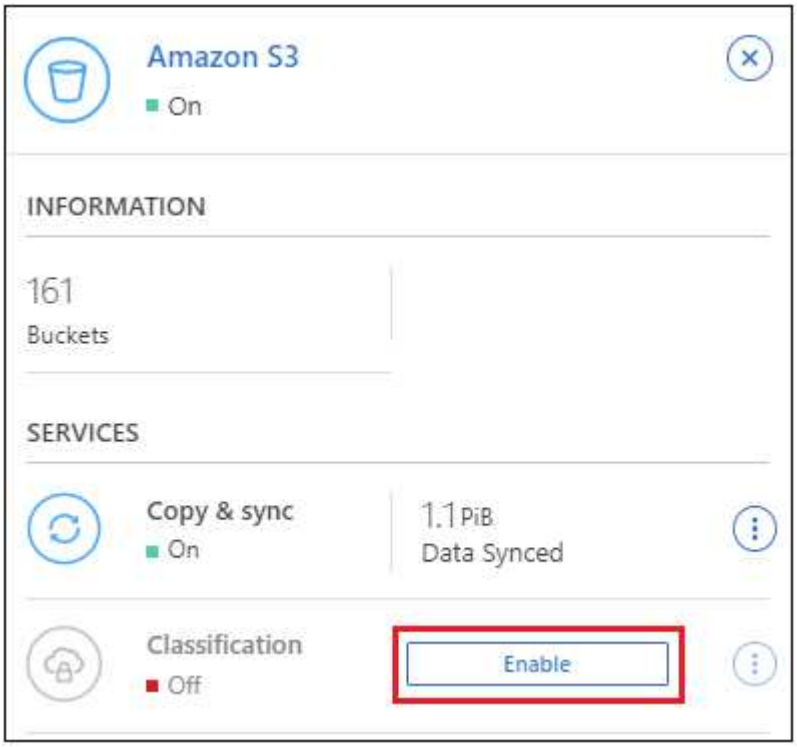
Attivazione della classificazione BlueXP nell'ambiente di lavoro S3

Abilitare la classificazione BlueXP su Amazon S3 dopo aver verificato i prerequisiti.

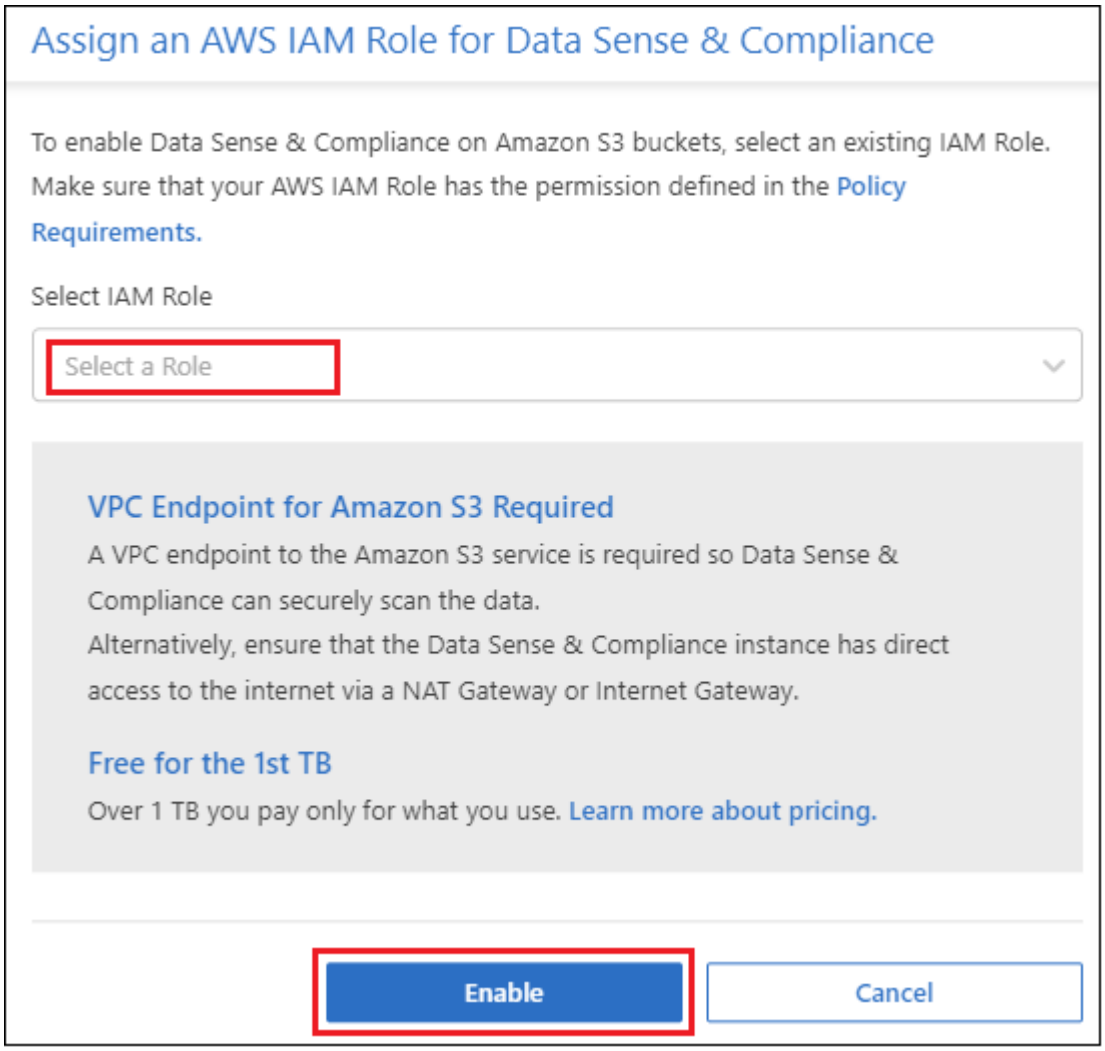
Fasi

1. Dal menu di navigazione a sinistra di BlueXP, fare clic su **Storage > Canvas**.
2. Selezionare l'ambiente di lavoro Amazon S3.

3. Nel riquadro servizi a destra, fare clic su **Enable** (attiva) accanto a **Classification** (classificazione).



4. Quando richiesto, assegnare un ruolo IAM all'istanza di classificazione BlueXP che ha le autorizzazioni richieste.



5. Fare clic su **Enable** (attiva).

> È inoltre possibile attivare le scansioni di conformità per un ambiente di lavoro dalla pagina di configurazione facendo clic su ⋮ E selezionando **Activate BlueXP classification** (attiva classificazione BlueXP).

Risultato

BlueXP assegna il ruolo IAM all'istanza.

Attivazione e disattivazione delle scansioni di compliance sui bucket S3

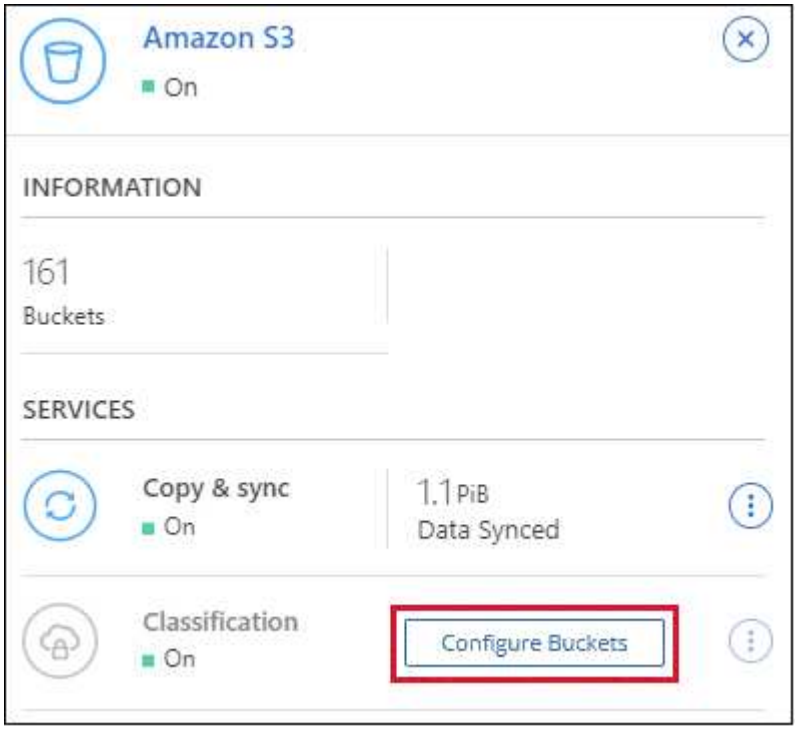
Dopo che BlueXP ha attivato la classificazione BlueXP su Amazon S3, il passaggio successivo consiste nella configurazione dei bucket che si desidera sottoporre a scansione.

Quando BlueXP viene eseguito nell'account AWS che dispone dei bucket S3 che si desidera sottoporre a scansione, rileva tali bucket e li visualizza in un ambiente di lavoro Amazon S3.

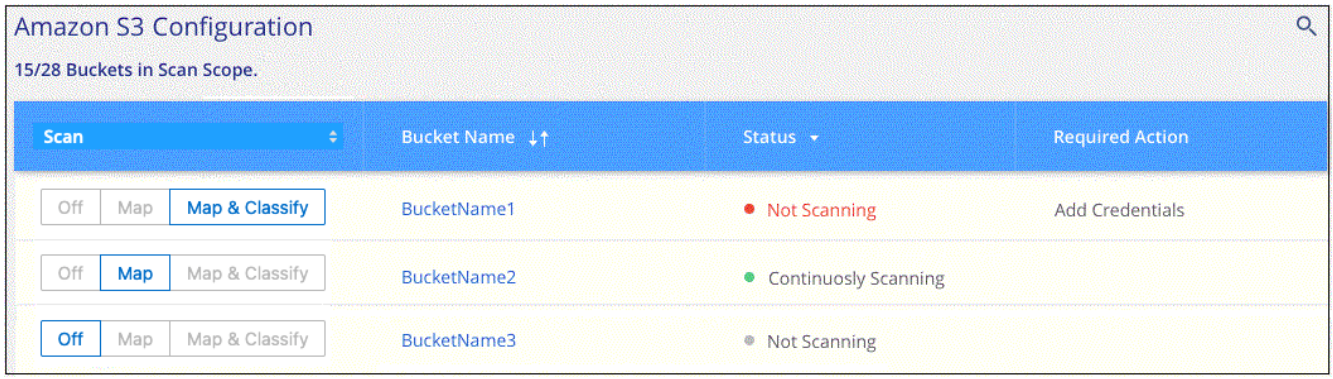
La classificazione BlueXP può anche Eseguire la scansione dei bucket S3 che si trovano in diversi account AWS.

Fasi

1. Selezionare l'ambiente di lavoro Amazon S3.
2. Nel riquadro servizi a destra, fare clic su **Configura bucket**.



3. Abilita scansioni di sola mappatura o scansioni di mappatura e classificazione sui bucket.



A:	Eseguire questa operazione:
Attivare scansioni solo mappatura su un bucket	Fare clic su **Map** (Mappa)
Abilitare scansioni complete su un bucket	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un bucket	Fare clic su **Off**

Risultato

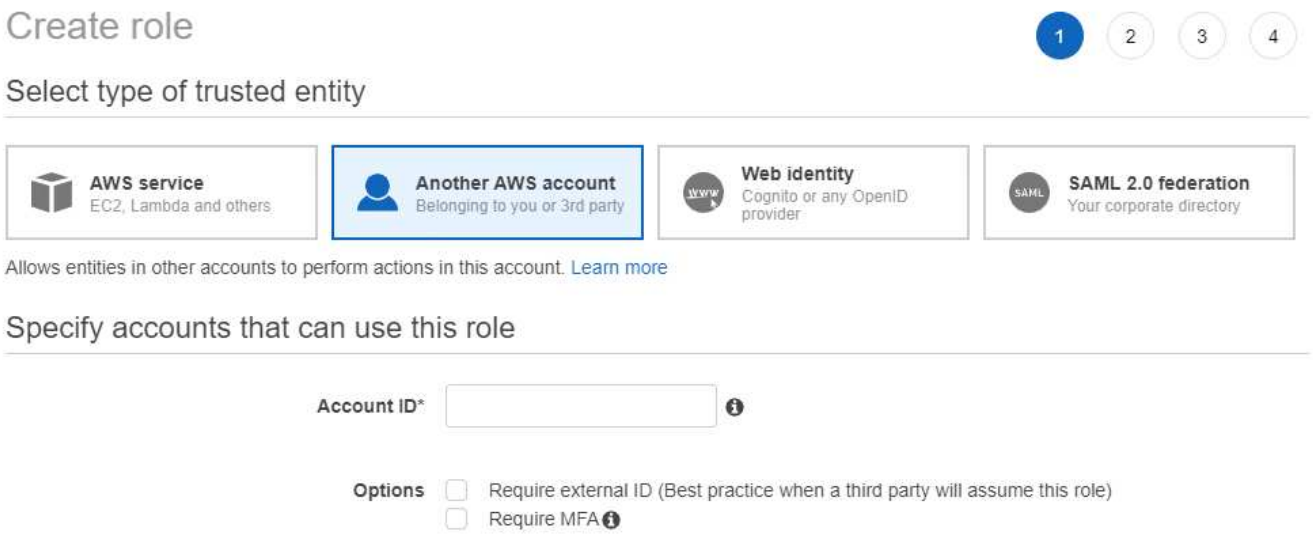
La classificazione BlueXP avvia la scansione dei bucket S3 abilitati. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Scansione dei bucket da account AWS aggiuntivi

È possibile eseguire la scansione dei bucket S3 che si trovano sotto un account AWS diverso assegnando un ruolo da tale account per accedere all'istanza di classificazione BlueXP esistente.

Fasi

1. Accedere all'account AWS di destinazione in cui si desidera eseguire la scansione dei bucket S3 e creare un ruolo IAM selezionando **un altro account AWS**.



   Assicurarsi di effettuare le seguenti operazioni:

   - Inserire l'ID dell'account in cui risiede l'istanza di classificazione BlueXP.
   - Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.
   - Allegare il criterio IAM di classificazione BlueXP. Assicurarsi che disponga delle autorizzazioni necessarie.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:PutObject"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Accedere all'account AWS di origine in cui risiede l'istanza di classificazione BlueXP e selezionare il ruolo

IAM associato all'istanza.

a. Modificare la **durata massima della sessione CLI/API** da 1 ora a 12 ore e salvare la modifica.

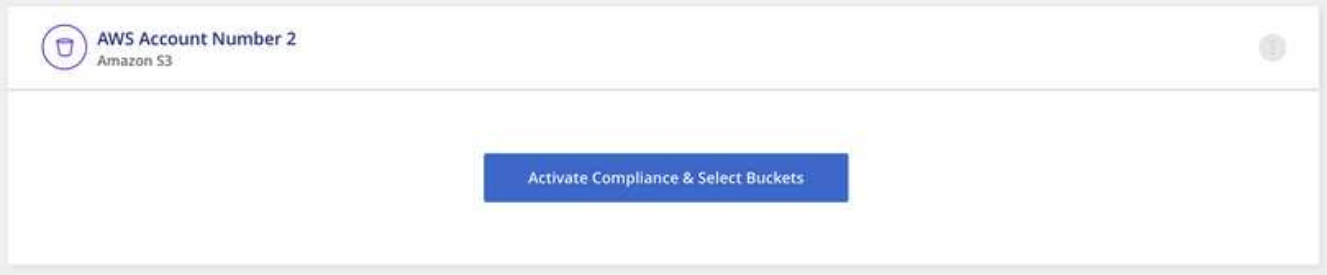
b. Fare clic su **Allega policy**, quindi su **Crea policy**.

c. Creare un criterio che includa l'azione "sts:AssumeRole" e specificare l'ARN del ruolo creato nell'account di destinazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

L'account del profilo dell'istanza di classificazione BlueXP ora ha accesso all'account AWS aggiuntivo.

3. Accedere alla pagina **Amazon S3 Configuration** (Configurazione Amazon S3) per visualizzare il nuovo account AWS. Nota: La sincronizzazione dell'ambiente di lavoro del nuovo account e la visualizzazione di queste informazioni possono richiedere alcuni minuti prima che la classificazione BlueXP venga eseguita.



4. Fare clic su **Activate BlueXP classification & Select Bucket** (attiva classificazione BlueXP e seleziona bucket) e selezionare i bucket da sottoporre a scansione.

Risultato

La classificazione BlueXP avvia la scansione dei nuovi bucket S3 abilitati.

Scansione degli schemi del database

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

Dopo aver abilitato la scansione del database, è possibile aggiungere identificatori univoci che la classificazione BlueXP identificherà in tutte le origini dati in base a colonne specifiche dei database. Questa funzione è denominata *Data Fusion*. "Scopri come aggiungere identificatori di dati personali personalizzati dai tuoi database".

Avvio rapido

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

1. **Esaminare i prerequisiti del database**

Assicurarsi che il database sia supportato e di disporre delle informazioni necessarie per la connessione al database.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Aggiungere il server database**

Aggiungere il server database a cui si desidera accedere.

4. **Selezionare gli schemi**

Selezionare gli schemi da sottoporre a scansione.

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".

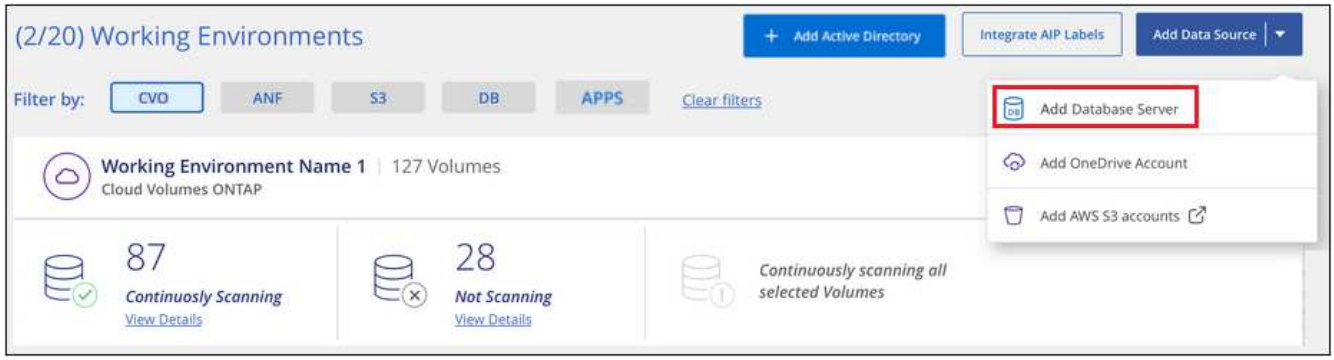
Se si eseguono scansioni di schemi di database installati in un sito buio che non dispone di accesso a Internet, è necessario "Implementare la classificazione BlueXP nella stessa posizione on-premise che non dispone di accesso a Internet". Ciò richiede anche che BlueXP Connector sia implementato nella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

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

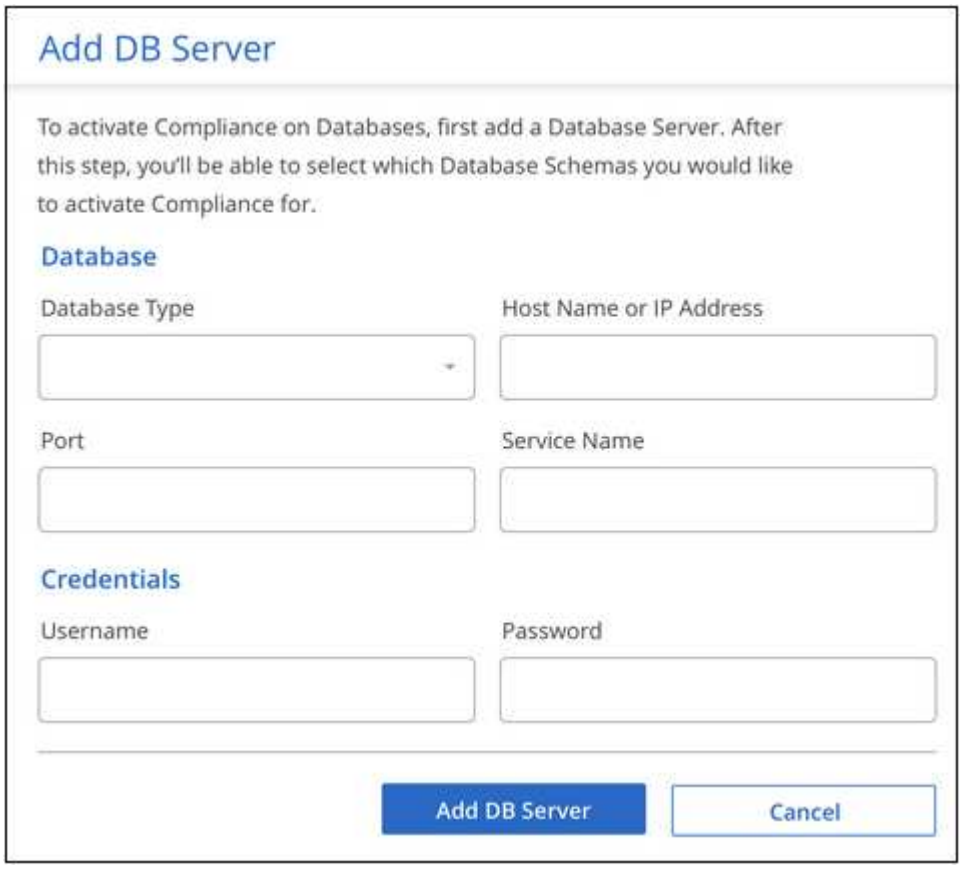
Aggiungere il server database

Aggiungere il server di database in cui risiedono gli schemi.

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Database Server** (Aggiungi server database).



2. 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.

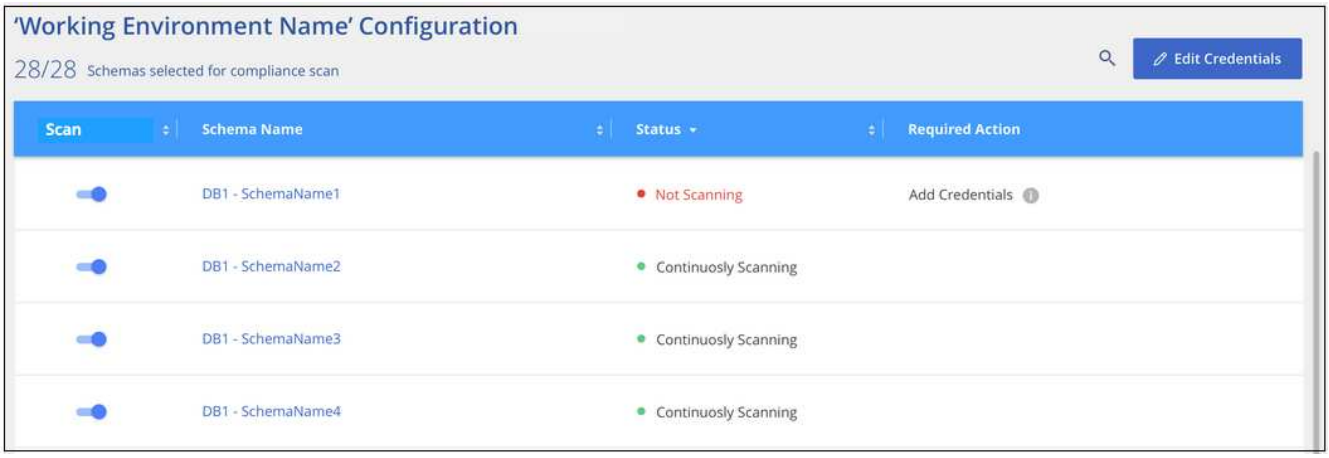
Abilitare e disabilitare le scansioni di conformità sugli schemi di database

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. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** del 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. In caso di errori, questi vengono visualizzati nella colonna Status (Stato), insieme all'azione richiesta per risolvere l'errore.

Si noti che la classificazione BlueXP esegue la scansione dei database una volta al giorno, poiché i database non vengono sottoposti a scansione continua come altre origini dati.

Scansione degli account OneDrive

Completare alcuni passaggi per avviare la scansione dei file nelle cartelle OneDrive dell'utente con la classificazione BlueXP.

Avvio rapido

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

1 **Verifica dei prerequisiti di OneDrive**

Assicurarsi di disporre delle credenziali di amministratore per accedere all'account OneDrive.

2 **Distribuire l'istanza di classificazione BlueXP**

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

3 **Aggiungere l'account OneDrive**

Utilizzando le credenziali dell'utente Admin, accedere all'account OneDrive a cui si desidera accedere in modo che venga aggiunto come nuovo ambiente di lavoro.

4 **Aggiungere gli utenti e selezionare il tipo di scansione**

Aggiungere l'elenco degli utenti dall'account OneDrive che si desidera sottoporre a scansione e selezionare il tipo di scansione. È possibile aggiungere fino a 100 utenti alla volta.

Verifica dei requisiti di OneDrive

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

- È necessario disporre delle credenziali di accesso Admin per l'account OneDrive for Business che fornisce l'accesso in lettura ai file dell'utente.
- Avrai bisogno di un elenco degli indirizzi e-mail separato da righe per tutti gli utenti di cui desideri eseguire la scansione delle cartelle di OneDrive.

Implementazione dell'istanza di classificazione BlueXP

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

La classificazione BlueXP può essere "implementato nel cloud" oppure "in una sede on-premise con accesso a internet".

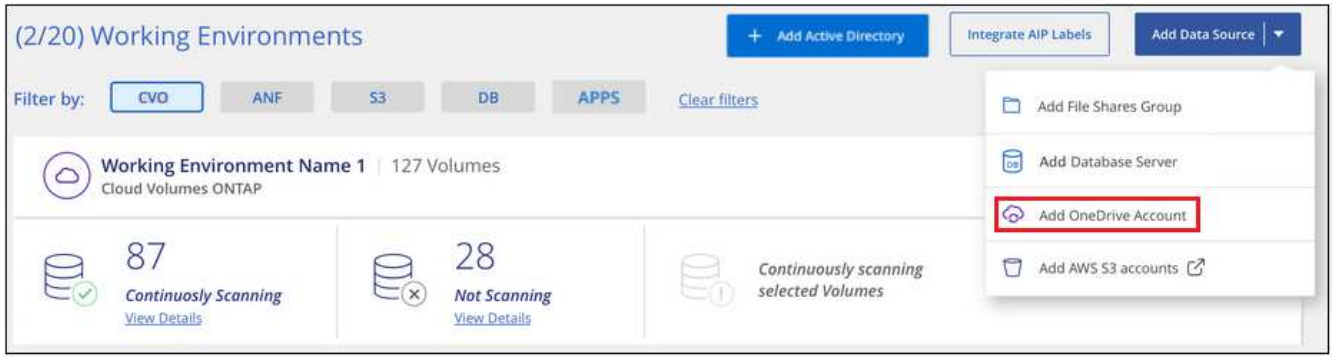
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta dell'account OneDrive

Aggiungere l'account OneDrive in cui risiedono i file utente.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add OneDrive account** (Aggiungi account OneDrive).



2. Nella finestra di dialogo Aggiungi un account OneDrive, fai clic su **Accedi a OneDrive**.
3. Nella pagina Microsoft che viene visualizzata, selezionare l'account OneDrive e immettere l'utente e la password di amministratore richiesti, quindi fare clic su **Accept** per consentire alla classificazione BlueXP di leggere i dati da questo account.

L'account OneDrive viene aggiunto all'elenco degli ambienti di lavoro.

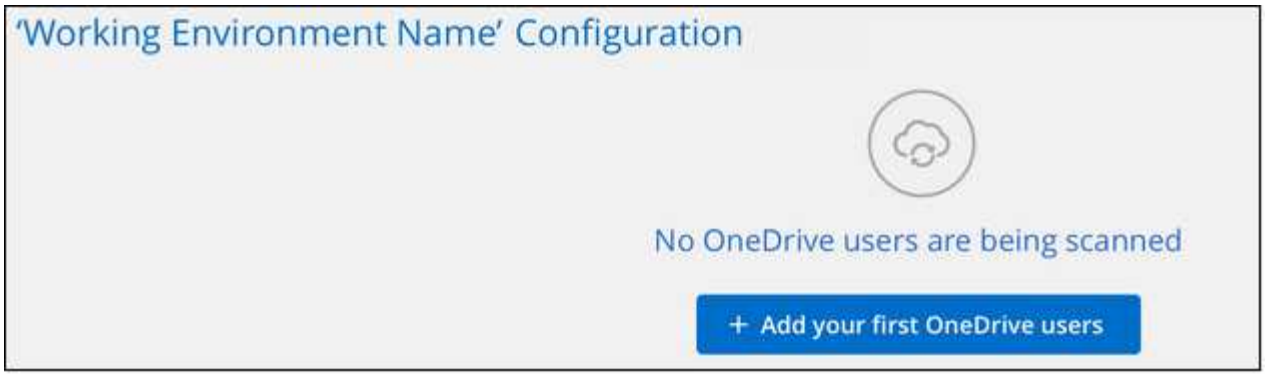
Aggiunta di utenti OneDrive alle scansioni di conformità

Puoi aggiungere singoli utenti OneDrive o tutti gli utenti OneDrive, in modo che i loro file vengano sottoposti a scansione in base alla classificazione BlueXP.

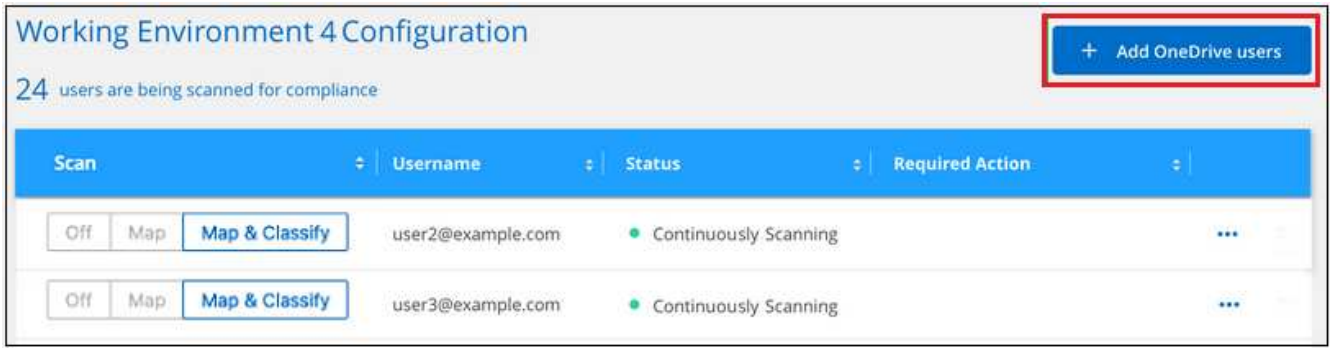
Fasi

1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account OneDrive.

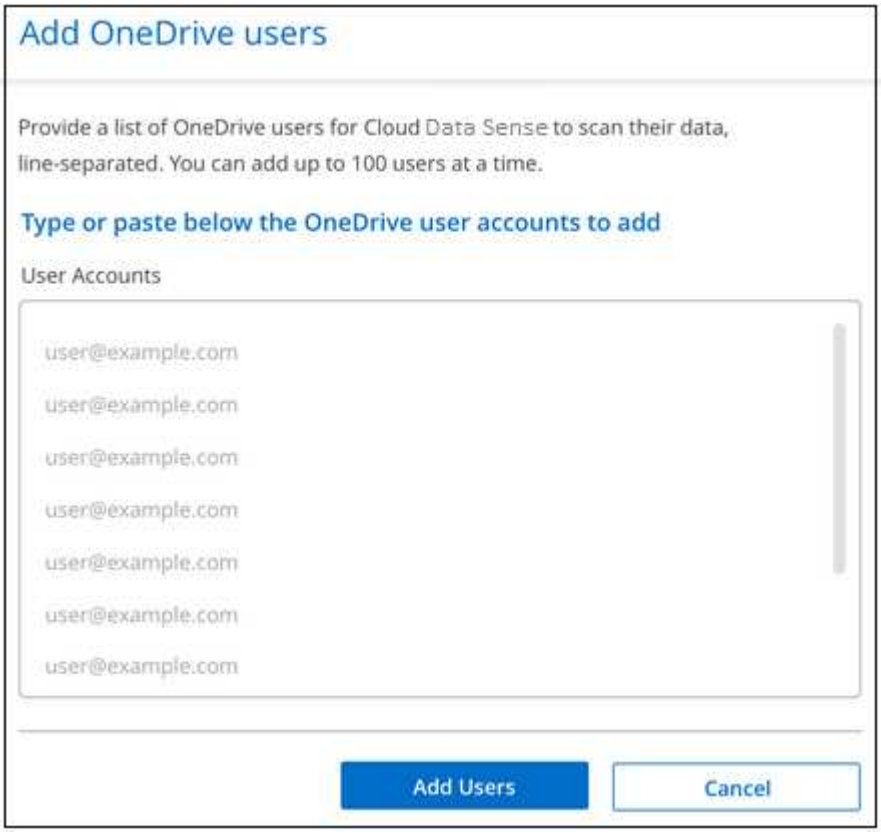
2. Se è la prima volta che si aggiungono utenti per questo account OneDrive, fare clic su **Aggiungi i primi utenti OneDrive**.



Se si aggiungono altri utenti da un account OneDrive, fare clic su **Aggiungi utenti OneDrive**.



3. Aggiungere gli indirizzi e-mail degli utenti di cui si desidera eseguire la scansione - un indirizzo e-mail per riga (fino a 100 per sessione) - e fare clic su **Aggiungi utenti**.



Una finestra di dialogo di conferma visualizza il numero di utenti aggiunti.

Se la finestra di dialogo elenca gli utenti che non possono essere aggiunti, acquisire queste informazioni in modo da poter risolvere il problema. In alcuni casi è possibile aggiungere nuovamente l'utente con un indirizzo e-mail corretto.

4. Attivare scansioni di sola mappatura o scansioni di mappatura e classificazione sui file utente.

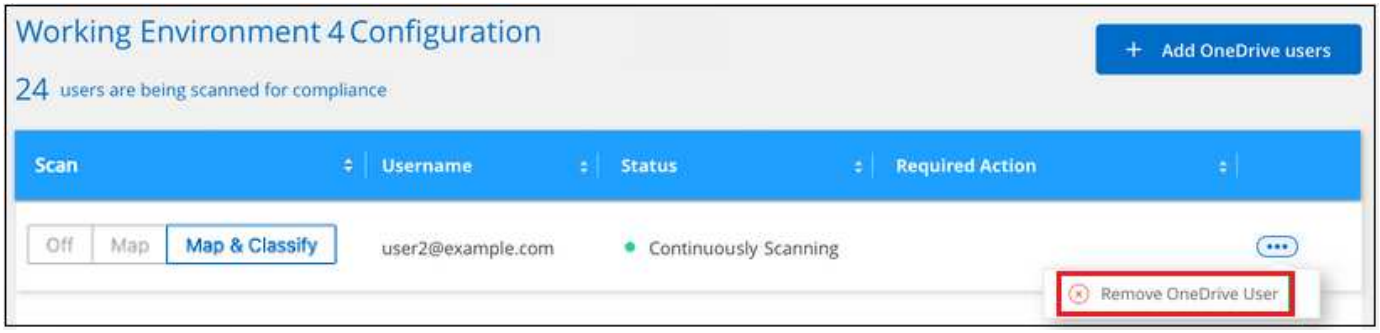
A:	Eseguire questa operazione:
Attiva scansioni solo mappatura sui file utente	Fare clic su **Map** (Mappa)
Attiva scansioni complete sui file utente	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file utente	Fare clic su **Off**

Risultato

La classificazione BlueXP avvia la scansione dei file per gli utenti aggiunti e i risultati vengono visualizzati nella dashboard e in altre posizioni.

Rimozione di un utente OneDrive dalle scansioni di conformità

Se gli utenti lasciano l'azienda o se il loro indirizzo e-mail cambia, puoi rimuovere singoli utenti di OneDrive dall'eseguire la scansione dei loro file in qualsiasi momento. Fare clic su **Remove OneDrive User** (Rimuovi utente OneDrive) dalla pagina di configurazione.



Nota: È possibile "Elimina l'intero account OneDrive dalla classificazione BlueXP" Se non si desidera più eseguire la scansione dei dati utente dall'account OneDrive.

Scansione degli account SharePoint

Completa alcuni passaggi per iniziare la scansione dei file negli account SharePoint Online e SharePoint on-premise con classificazione BlueXP.

Avvio rapido

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

1. **Esaminare i prerequisiti di SharePoint**

Assicurarsi di disporre di credenziali qualificate per accedere all'account SharePoint e di disporre degli URL dei siti SharePoint che si desidera sottoporre a scansione.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Accedere all'account SharePoint**

Utilizzando credenziali utente qualificate, accedere all'account SharePoint a cui si desidera accedere in modo che venga aggiunto come nuova origine dati/ambiente di lavoro.

4. **Aggiungere gli URL del sito SharePoint da sottoporre a scansione**

Aggiungere l'elenco degli URL del sito SharePoint che si desidera sottoporre a scansione nell'account SharePoint e selezionare il tipo di scansione. È possibile aggiungere fino a 100 URL alla volta e fino a 1,000 siti in totale per ciascun account.

Analisi dei requisiti di SharePoint

Esaminare i seguenti prerequisiti per assicurarsi di essere pronti per attivare la classificazione BlueXP su un account SharePoint.

- È necessario disporre delle credenziali di accesso dell'utente Admin per l'account SharePoint che fornisce l'accesso in lettura a tutti i siti SharePoint.

- Per SharePoint Online è possibile utilizzare un account non Admin, ma tale utente deve disporre dell'autorizzazione per accedere a tutti i siti SharePoint che si desidera sottoporre a scansione.

- Per SharePoint on-premise, è necessario anche l'URL di SharePoint Server.
- Per tutti i dati che si desidera sottoporre a scansione, è necessario disporre di un elenco degli URL del sito SharePoint separato da righe.

Implementazione dell'istanza di classificazione BlueXP

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

- Per SharePoint Online, la classificazione BlueXP può essere "implementato nel cloud".
- Per SharePoint on-premise, è possibile installare la classificazione BlueXP "in una sede on-premise con accesso a internet" oppure "in una sede on-premise che non dispone di accesso a internet".

Quando la classificazione BlueXP viene installata in un sito senza accesso a Internet, BlueXP Connector deve essere installato nello stesso sito senza accesso a Internet. "Scopri di più".

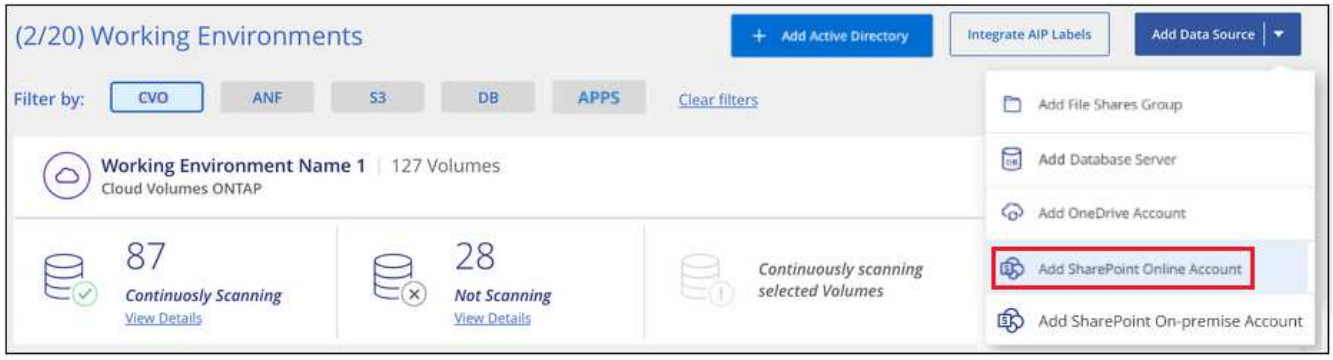
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta di un account SharePoint Online

Aggiungere l'account SharePoint Online in cui risiedono i file utente.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add SharePoint Online account** (Aggiungi account online SharePoint).



2. Nella finestra di dialogo Aggiungi un account online SharePoint, fare clic su **Accedi a SharePoint**.
3. Nella pagina Microsoft visualizzata, selezionare l'account SharePoint e immettere l'utente e la password (utente amministratore o altro utente con accesso ai siti SharePoint), quindi fare clic su **Accetta** per consentire alla classificazione BlueXP di leggere i dati da questo account.

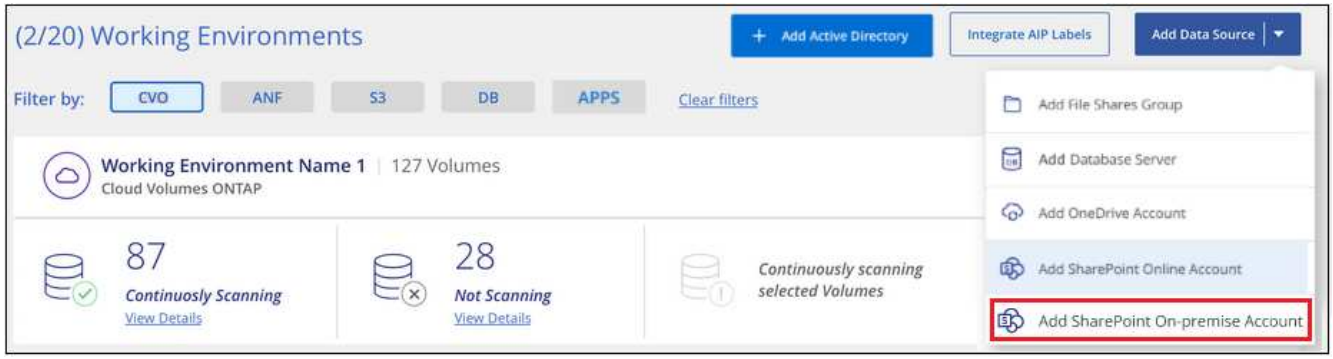
L'account SharePoint Online viene aggiunto all'elenco degli ambienti di lavoro.

Aggiunta di un account SharePoint on-premise

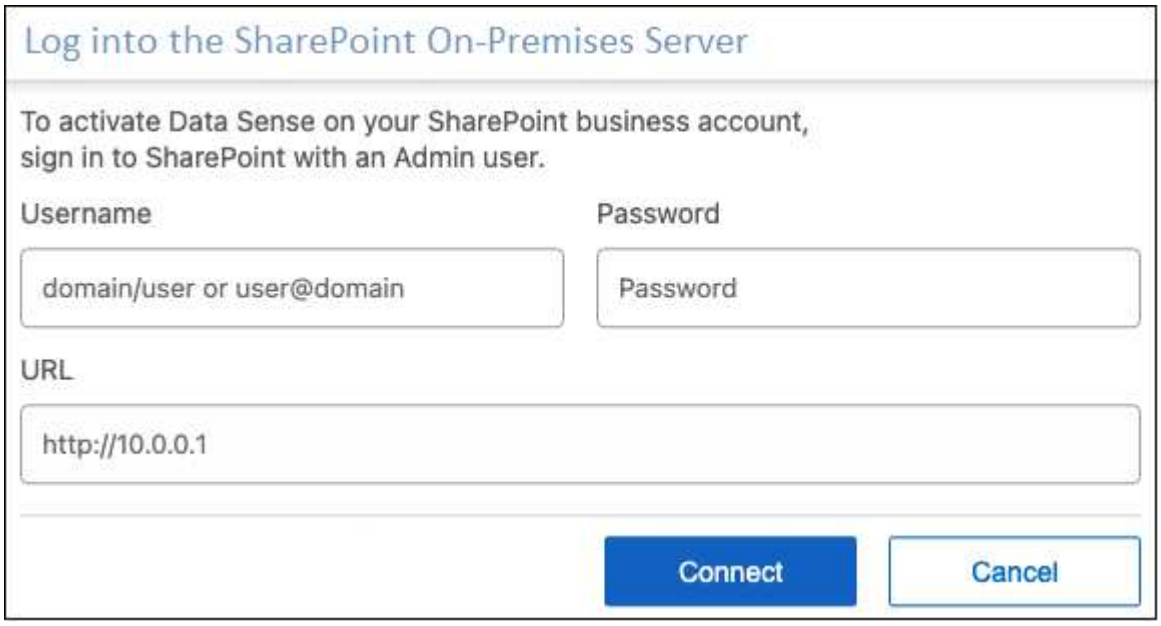
Aggiungere l'account SharePoint on-premise in cui risiedono i file utente.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add SharePoint on-premise account** (Aggiungi account SharePoint on-premise).



2. Nella finestra di dialogo Log in the SharePoint on-premise Server (Accedi al server SharePoint on-premise), immettere le seguenti informazioni:
   - Admin user in formato "dominio/utente" o "utente@dominio" e admin password
   - URL di SharePoint Server



3. Fare clic su **Connect** (Connetti).

L'account SharePoint on-premise viene aggiunto all'elenco degli ambienti di lavoro.

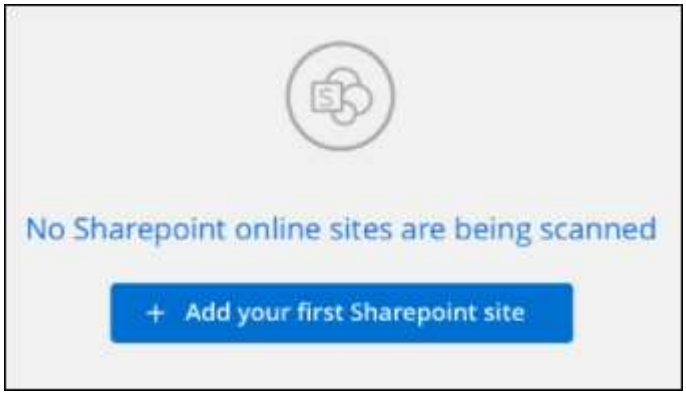
Aggiunta di siti SharePoint alle scansioni di conformità

È possibile aggiungere singoli siti SharePoint o fino a 1,000 siti SharePoint nell'account, in modo che i file associati vengano sottoposti a scansione in base alla classificazione BlueXP. La procedura è la stessa, sia che si aggiungano siti SharePoint Online o SharePoint on-premise.

Fasi

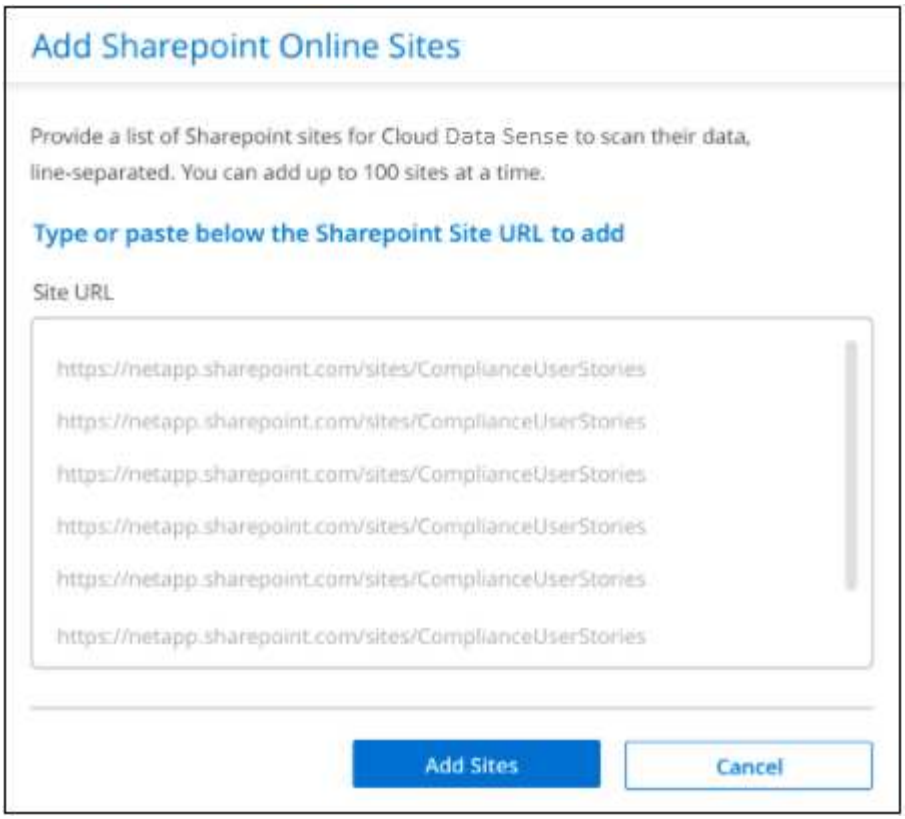
1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account SharePoint.

2. Se questa è la prima volta che si aggiungono siti per questo account SharePoint, fare clic su **Aggiungi il primo sito SharePoint**.



Se si aggiungono altri utenti da un account SharePoint, fare clic su **Aggiungi siti SharePoint**.

3. Aggiungere gli URL dei siti di cui si desidera eseguire la scansione - un URL per riga (fino a 100 per sessione) - e fare clic su **Aggiungi siti**.



Una finestra di dialogo di conferma visualizza il numero di siti aggiunti.

Se la finestra di dialogo elenca i siti che non è stato possibile aggiungere, acquisire queste informazioni in modo da risolvere il problema. In alcuni casi è possibile aggiungere nuovamente il sito con un URL corretto.

4. Se è necessario aggiungere più di 100 siti per questo account, fare clic nuovamente su **Aggiungi siti SharePoint** fino a quando non sono stati aggiunti tutti i siti per questo account (fino a un totale di 1,000 siti per ciascun account).
5. Attivare scansioni di sola mappatura o scansioni di mappatura e classificazione sui file nei siti SharePoint.

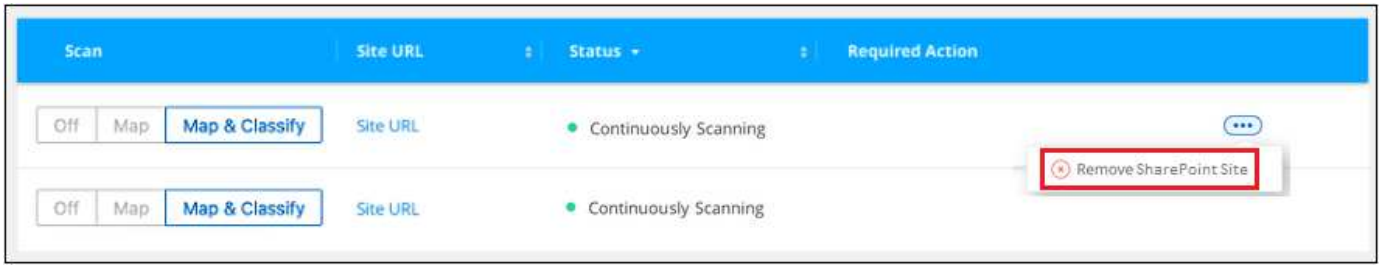
A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sui file	Fare clic su **Map** (Mappa)
Attivare scansioni complete sui file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file	Fare clic su **Off**

Risultato

La classificazione BlueXP avvia la scansione dei file nei siti SharePoint aggiunti e i risultati vengono visualizzati nella dashboard e in altre posizioni.

Rimozione di un sito SharePoint dalle scansioni di conformità

Se si rimuove un sito SharePoint in futuro o si decide di non eseguire la scansione dei file in un sito SharePoint, è possibile rimuovere singoli siti SharePoint dall'eseguire la scansione dei file in qualsiasi momento. Fai clic su **Rimuovi sito SharePoint** dalla pagina di configurazione.



Nota: È possibile "Eliminare l'intero account SharePoint dalla classificazione BlueXP" Se non si desidera più eseguire la scansione dei dati utente dall'account SharePoint.

Scansione di account Google Drive

Completare alcuni passaggi per avviare la scansione dei file utente negli account Google Drive con classificazione BlueXP.

Avvio rapido

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

1. **Esaminare i prerequisiti di Google Drive**

Assicurarsi di disporre delle credenziali di amministratore per accedere all'account Google Drive.

2. **Implementare la classificazione BlueXP**

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

3. **Accedere all'account Google Drive**

Utilizzando le credenziali dell'utente Admin, accedere all'account Google Drive a cui si desidera accedere in modo che venga aggiunto come nuova origine dati.

4. **Selezionare il tipo di scansione dei file utente**

Selezionare il tipo di scansione che si desidera eseguire sui file dell'utente; mappatura o mappatura e classificazione.

Analisi dei requisiti di Google Drive

Esaminare i seguenti prerequisiti per assicurarsi di essere pronti per attivare la classificazione BlueXP su un account Google Drive.

- È necessario disporre delle credenziali di accesso Admin per l'account Google Drive che fornisce l'accesso in lettura ai file dell'utente

Restrizioni attuali

Le seguenti funzionalità di classificazione BlueXP non sono attualmente supportate con Google Drive Files:

- Quando si visualizzano i file nella pagina Data Investigation (analisi dati), le azioni nella barra dei pulsanti non sono attive. Non è possibile copiare, spostare, eliminare, ecc. alcun file.
- Non è possibile identificare le autorizzazioni all'interno dei file in Google Drive, pertanto non vengono visualizzate informazioni sulle autorizzazioni nella pagina di analisi.

Implementazione della classificazione BlueXP

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

La classificazione BlueXP può essere "implementato nel cloud" oppure "in una sede on-premise con accesso a internet".

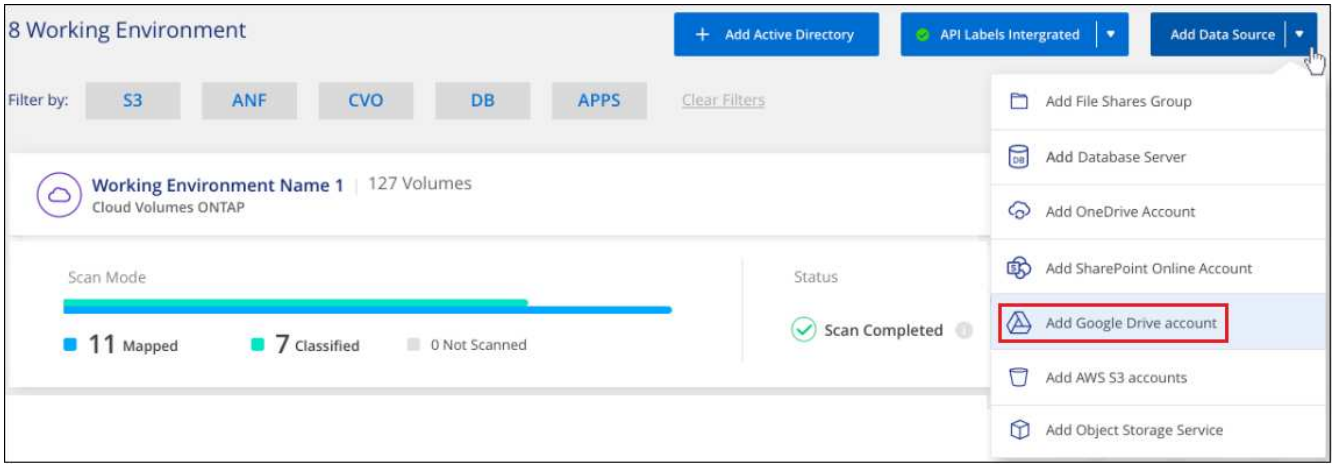
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta dell'account Google Drive

Aggiungere l'account Google Drive in cui risiedono i file utente. Se si desidera eseguire la scansione di file da più utenti, è necessario eseguire questa procedura per ciascun utente.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Google Drive account** (Aggiungi account Google Drive).



2. Nella finestra di dialogo Aggiungi un account Google Drive, fare clic su **Accedi a Google Drive**.
3. Nella pagina Google visualizzata, selezionare l'account Google Drive e immettere l'utente e la password di amministratore richiesti, quindi fare clic su **Accept** (Accetta) per consentire alla classificazione BlueXP di leggere i dati da questo account.

L'account Google Drive viene aggiunto all'elenco degli ambienti di lavoro.

Selezione del tipo di scansione per i dati dell'utente

Selezionare il tipo di scansione che verrà eseguita dalla classificazione BlueXP sui dati dell'utente.

Fasi

1. Dalla pagina *Configuration*, fare clic sul pulsante **Configuration** dell'account Google Drive.

2. Abilitare le scansioni di sola mappatura, o le scansioni di mappatura e classificazione, sui file nell'account Google Drive.

A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sui file	Fare clic su **Map** (Mappa)
Attivare scansioni complete sui file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione dei file	Fare clic su **Off**

Risultato

La classificazione BlueXP avvia la scansione dei file nell'account Google Drive aggiunto e i risultati vengono visualizzati nella dashboard e in altre posizioni.

Rimozione di un account Google Drive dalle scansioni di conformità

Poiché solo i file Google Drive di un singolo utente fanno parte di un singolo account Google Drive, se si desidera interrompere la scansione dei file dall'account Google Drive di un utente, è necessario "Eliminare l'account Google Drive dalla classificazione BlueXP".

Scansione delle condivisioni di file

Completare alcuni passaggi per avviare la scansione di condivisioni di file NFS o CIFS non NetApp direttamente con la classificazione BlueXP. Queste condivisioni di file possono risiedere on-premise o nel cloud.

Avvio rapido

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

1 **Verificare i prerequisiti per la condivisione dei file**

Per le condivisioni CIFS (SMB), assicurarsi di disporre delle credenziali per accedere alle condivisioni.

2 **Distribuire l'istanza di classificazione BlueXP**

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

3 **Creare un gruppo per conservare le condivisioni di file**

Il gruppo è un contenitore per le condivisioni di file che si desidera sottoporre a scansione e viene utilizzato come nome dell'ambiente di lavoro per tali condivisioni di file.

4 **Aggiungere le condivisioni di file al gruppo**

Aggiungere l'elenco delle condivisioni di file che si desidera acquisire e selezionare il tipo di scansione. È possibile aggiungere fino a 100 condivisioni di file alla volta.

Revisione dei requisiti di condivisione dei file

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. Nella maggior parte dei casi si tratta di condivisioni di file che risiedono su sistemi di storage non NetApp. Tuttavia, le condivisioni CIFS dei sistemi storage NetApp 7-Mode precedenti possono essere sottoposte a scansione come condivisioni di file.

  Si noti che la classificazione BlueXP non può estrarre le autorizzazioni o il "tempo di accesso ultimo" dai sistemi 7-Mode. Inoltre, a causa di un problema noto tra alcune versioni di Linux e le condivisioni CIFS su sistemi 7-Mode, è necessario configurare la condivisione in modo che utilizzi solo SMB v1 con l'autenticazione NTLM attivata.

- È necessario disporre di una connettività di rete tra l'istanza di classificazione BlueXP e le condivisioni.
- Assicurarsi che queste porte siano aperte per l'istanza di classificazione BlueXP:
  - Per NFS: Porte 111 e 2049.
  - Per CIFS – porte 139 e 445.
- È possibile aggiungere una condivisione DFS (Distributed file System) come normale condivisione CIFS. Tuttavia, poiché la classificazione BlueXP non è consapevole che la condivisione è costruita su più server/volumi combinati come una singola CIFS share, potresti ricevere errori di permessi o connettività sulla condivisione quando il messaggio si applica davvero 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.

  Se si desidera assicurarsi che i file "ultimi tempi di accesso" non vengano modificati dalle scansioni di classificazione BlueXP, si consiglia di disporre dei permessi Write Attributes in CIFS o Write Permissions in NFS. 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.

- Sarà necessario l'elenco delle condivisioni che si desidera aggiungere nel formato `<host_name>:/<share_path>`. È possibile immettere le condivisioni singolarmente oppure fornire un elenco separato da riga delle condivisioni di file che si desidera acquisire.

Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di condivisioni di file NFS o CIFS non NetApp 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 esegue la scansione di condivisioni di file NFS o CIFS non NetApp installate 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.

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

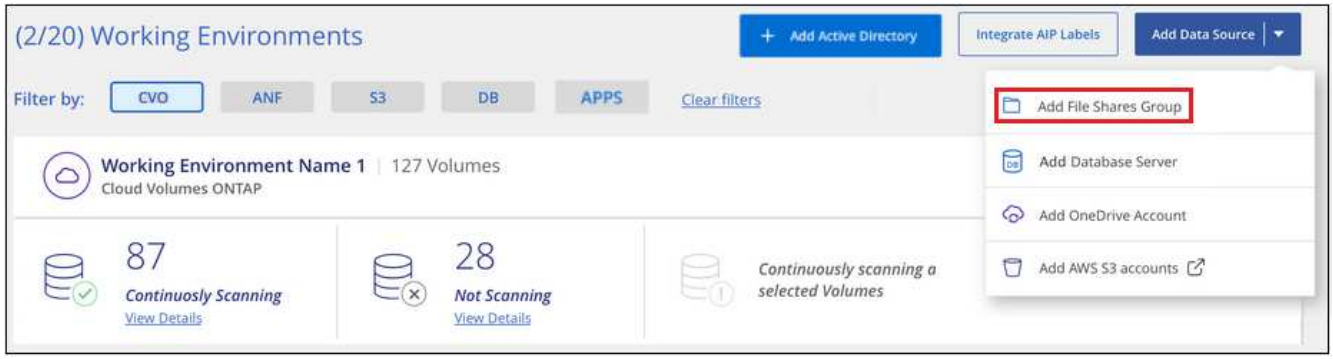
Creazione del gruppo per le condivisioni file

È necessario aggiungere un "gruppo" di condivisioni file prima di poter aggiungere le condivisioni file. Il gruppo è un contenitore per le condivisioni di file che si desidera sottoporre a scansione e il nome del gruppo viene utilizzato come nome dell'ambiente di lavoro per tali condivisioni di file.

È possibile combinare condivisioni NFS e CIFS nello stesso gruppo, tuttavia tutte le condivisioni file CIFS di un gruppo devono utilizzare le stesse credenziali Active Directory. Se si prevede di aggiungere condivisioni CIFS che utilizzano credenziali diverse, è necessario creare un gruppo separato per ogni set univoco di credenziali.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add file Shares Group** (Aggiungi gruppo condivisioni file).



2. Nella finestra di dialogo Add Files shares Group (Aggiungi gruppo condivisioni file), immettere il nome del gruppo di condivisioni e fare clic su **Continue** (continua).

Il nuovo file shares Group viene aggiunto all'elenco degli ambienti di lavoro.

Aggiunta di condivisioni di file a un gruppo

Le condivisioni di file vengono aggiunte al file shares Group in modo che i file in tali condivisioni vengano sottoposti a scansione in base alla classificazione BlueXP. Le condivisioni vengono aggiunte nel formato `<host_name>:/<share_path>`.

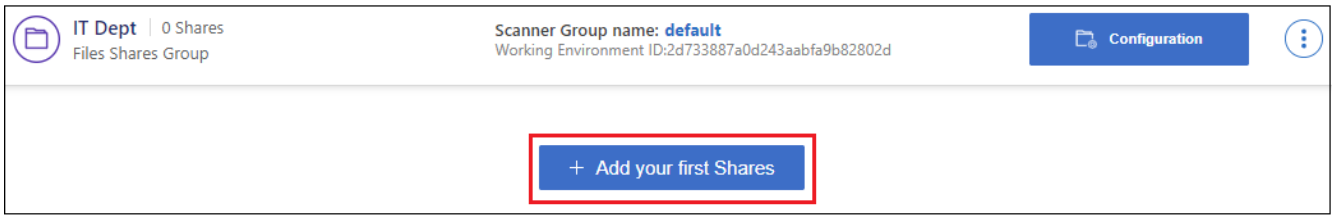
È possibile aggiungere singole condivisioni di file oppure fornire un elenco separato da righe delle condivisioni di file che si desidera sottoporre a scansione. È possibile aggiungere fino a 100 condivisioni alla volta.

Quando si aggiungono sia le condivisioni NFS che CIFS in un singolo gruppo, è necessario eseguire il processo due volte, una volta aggiunte le condivisioni NFS e quindi di nuovo le condivisioni CIFS.

Fasi

1. Dalla pagina *ambienti di lavoro*, fare clic sul pulsante **Configurazione** per il gruppo condivisioni file.

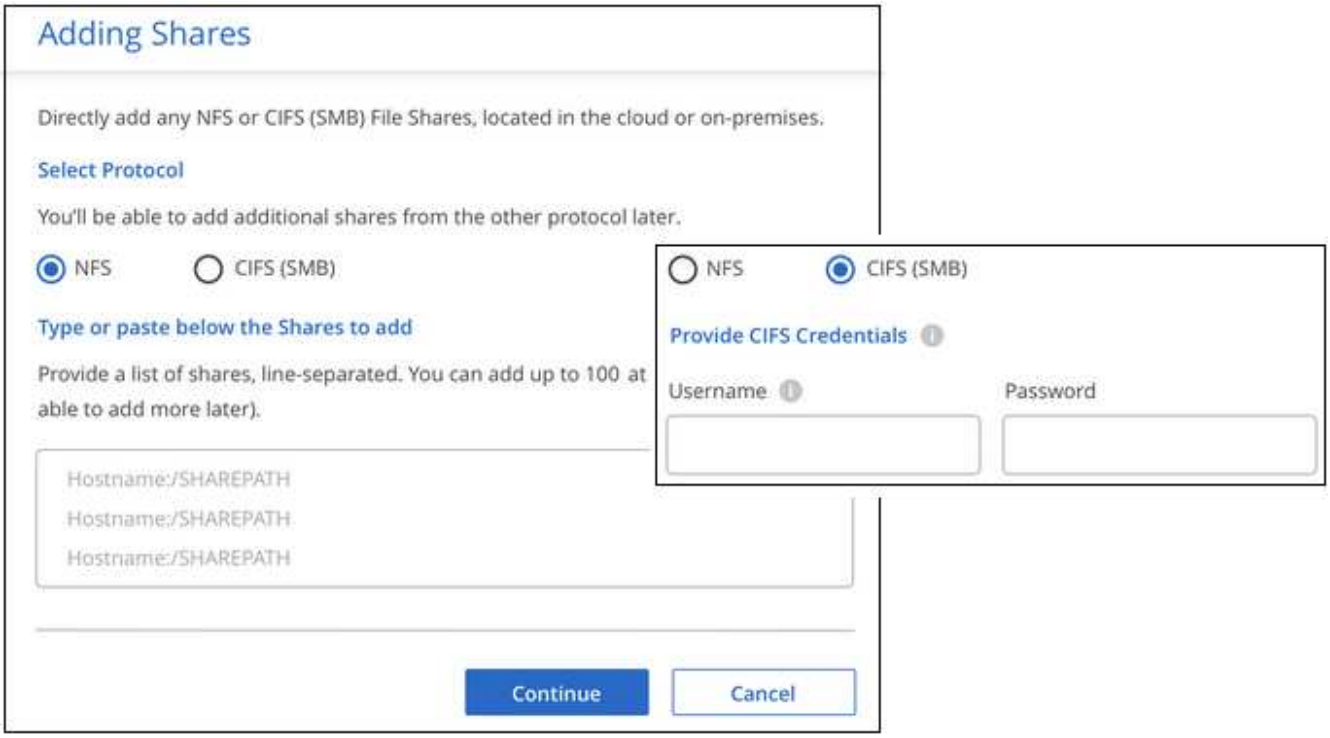
2. Se è la prima volta che si aggiungono condivisioni file per questo gruppo di condivisioni file, fare clic su **Aggiungi le prime condivisioni**.



Se si stanno aggiungendo condivisioni di file a un gruppo esistente, fare clic su **Aggiungi condivisioni**.

3. Selezionare il protocollo per le condivisioni di file che si desidera aggiungere, aggiungere le condivisioni di file che si desidera sottoporre a scansione (una condivisione di file per riga) e fare clic su **continua**.

   Quando si aggiungono condivisioni CIFS (SMB), è necessario immettere le credenziali Active Directory che forniscono l'accesso in lettura alle condivisioni. Si preferiscono le credenziali di amministratore.



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. In alcuni casi è possibile aggiungere nuovamente la condivisione con un nome host o un nome di condivisione corretto.

4. Abilitare scansioni di sola mappatura o scansioni di mappatura e classificazione su ogni condivisione di file.

A:	Eseguire questa operazione:
Abilitare le scansioni di sola mappatura sulle condivisioni di file	Fare clic su **Map** (Mappa)
Attiva scansioni complete sulle condivisioni di file	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione sulle condivisioni di file	Fare clic su **Off**

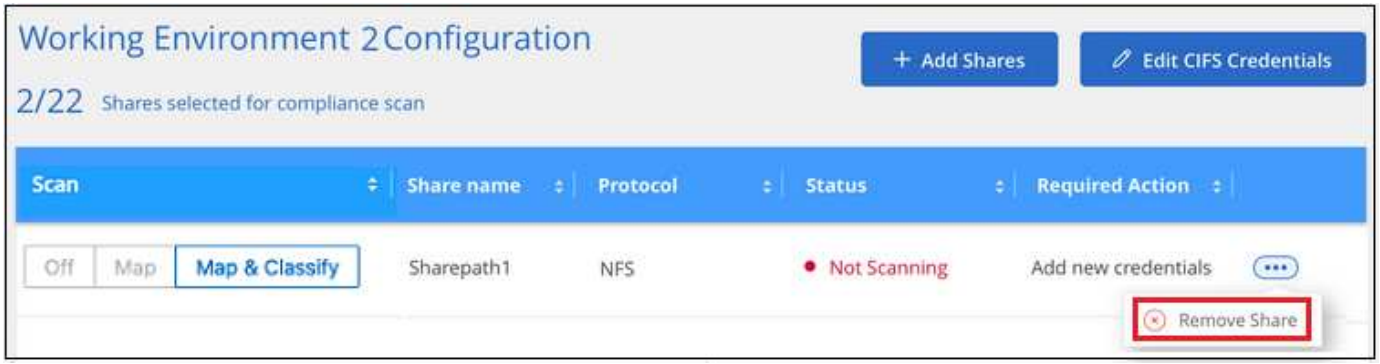
Per impostazione predefinita, lo switch nella parte superiore della pagina per le autorizzazioni **Scan when missing "write attributa" (Esegui scansione quando mancano gli attributi di scrittura)** è disattivato. Ciò significa che se la classificazione di BlueXP non dispone di permessi di scrittura in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

Risultato

La classificazione BlueXP avvia la scansione dei file nelle condivisioni di file aggiunte e i risultati vengono visualizzati nella dashboard e in altre posizioni.

Rimozione di una condivisione file dalle scansioni di conformità

Se non è più necessario eseguire la scansione di determinate condivisioni di file, è possibile rimuovere singole condivisioni di file dal fatto che i file siano sottoposti a scansione in qualsiasi momento. Fare clic su **Remove Share** (Rimuovi condivisione) dalla pagina di configurazione.



Scansione dello storage a oggetti che utilizza il protocollo S3

Completare alcuni passaggi per avviare la scansione dei dati all'interno dello storage a oggetti direttamente con la classificazione BlueXP. La classificazione BlueXP consente di eseguire la scansione dei dati da qualsiasi servizio di storage a oggetti che utilizza il protocollo S3 (Simple Storage Service). Tra cui NetApp StorageGRID, IBM Cloud Object Store, Linode, B2 Cloud Storage, Amazon S3 e molto altro ancora.

Avvio rapido

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

1. **Esaminare i prerequisiti dello storage a oggetti**

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 del provider di storage a oggetti, in modo che la classificazione BlueXP possa accedere ai bucket.

2. **Distribuire l'istanza di classificazione BlueXP**

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

3. **Aggiungere il servizio di storage a oggetti**

Aggiungere il servizio di storage a oggetti alla classificazione BlueXP.

4. **Selezionare i bucket da sottoporre a scansione**

Selezionare i bucket che si desidera sottoporre a scansione e la classificazione BlueXP inizierà a eseguirne la scansione.

Analisi dei requisiti di storage a oggetti

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 del provider di storage a oggetti, in modo che la classificazione BlueXP possa accedere ai bucket.

Implementazione dell'istanza di classificazione BlueXP

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

Se si esegue la scansione di dati dallo storage a oggetti S3 accessibile 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 esegue la scansione di dati dallo storage a oggetti S3 installato 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.

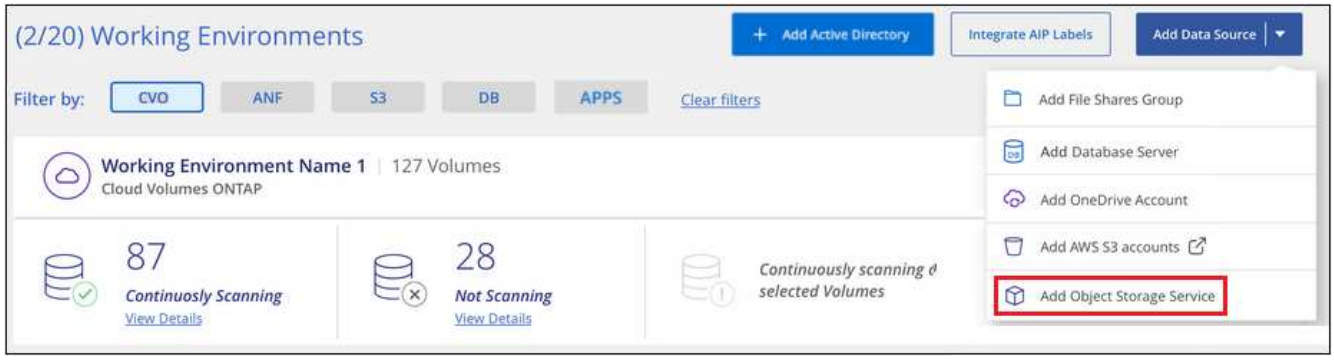
Gli aggiornamenti al software di classificazione BlueXP sono automatizzati finché l'istanza dispone di connettività Internet.

Aggiunta del servizio di storage a oggetti alla classificazione BlueXP

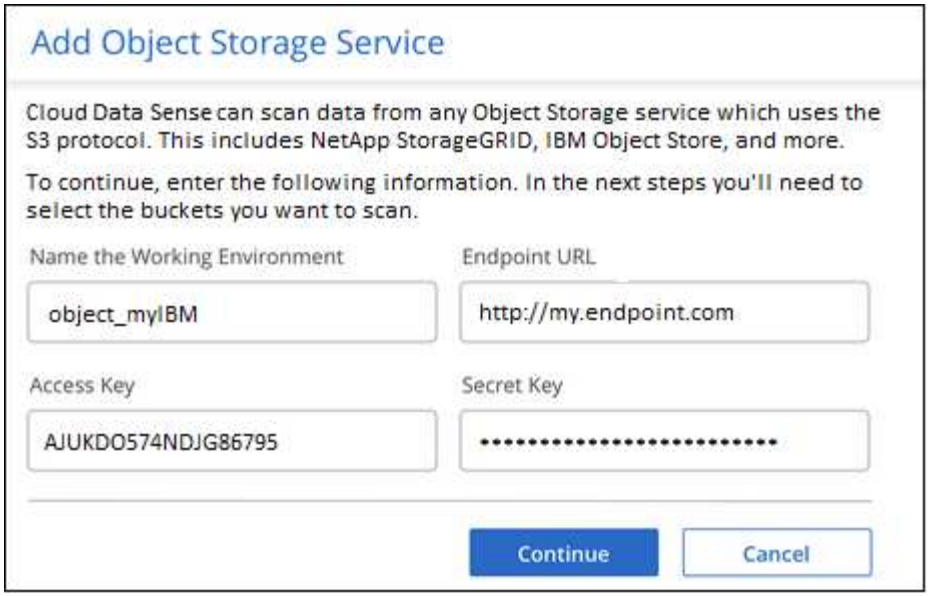
Aggiungere il servizio di storage a oggetti.

Fasi

1. Dalla pagina Working Environments Configuration (Configurazione ambienti di lavoro), fare clic su **Add Data Source** (Aggiungi origine dati) > **Add Object Storage Service** (Aggiungi servizio di storage a oggetti).



2. Nella finestra di dialogo Add Object Storage Service (Aggiungi servizio di storage a oggetti), immettere i dettagli del servizio di storage a oggetti e fare clic su **Continue** (continua).
   a. Immettere il nome che si desidera utilizzare per l'ambiente di lavoro. Questo nome deve riflettere il nome del servizio di storage a oggetti a cui ci si connette.
   b. Inserire l'URL dell'endpoint per accedere al servizio di storage a oggetti.
   c. Inserire la chiave di accesso e la chiave segreta in modo che la classificazione BlueXP possa accedere ai bucket nello storage a oggetti.



Risultato

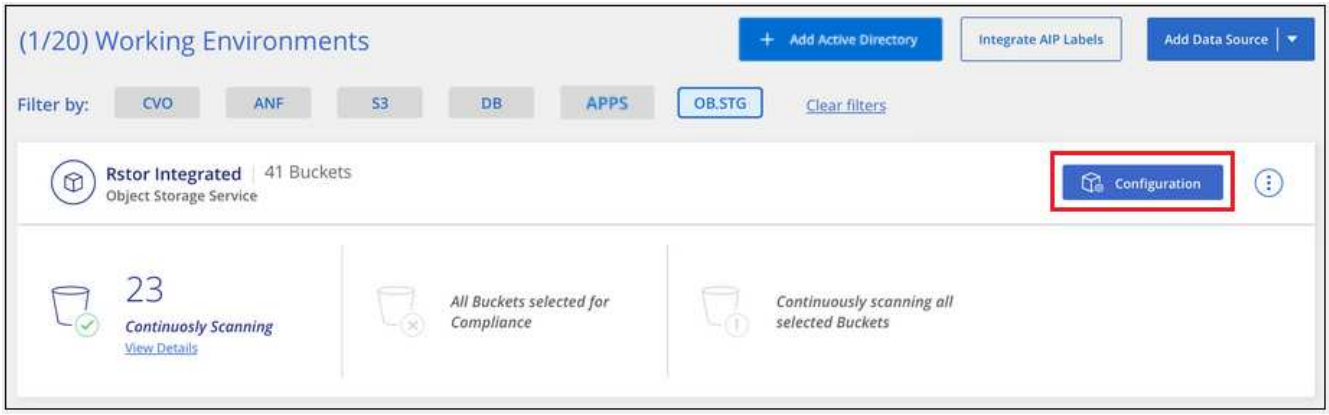
Il nuovo servizio di storage a oggetti viene aggiunto all'elenco degli ambienti di lavoro.

Attivazione e disattivazione delle scansioni di compliance nei bucket di storage a oggetti

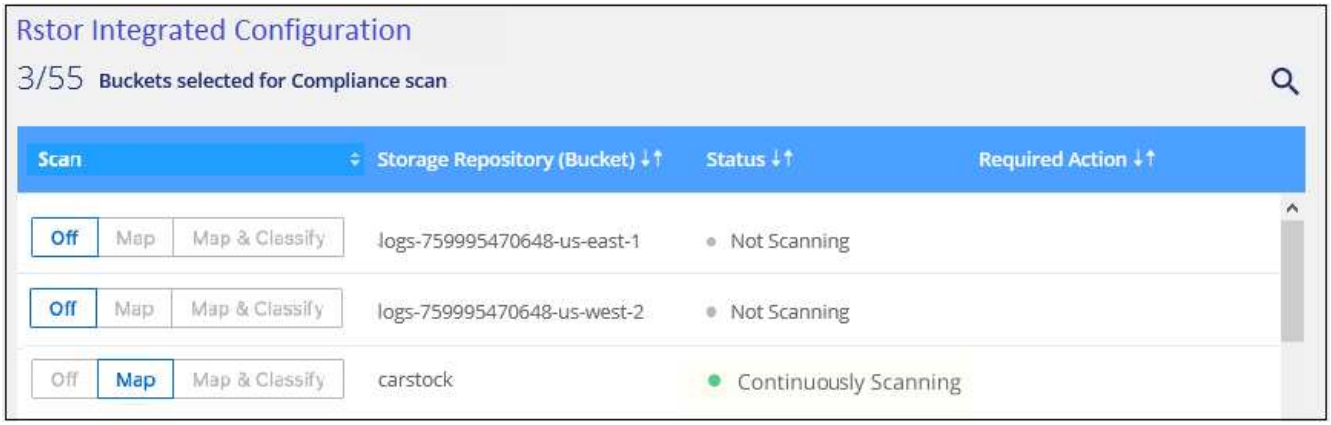
Dopo aver attivato la classificazione BlueXP sul servizio di storage a oggetti, il passaggio successivo consiste nel configurare i bucket che si desidera sottoporre a scansione. La classificazione BlueXP rileva tali bucket e li visualizza nell'ambiente di lavoro creato.

Fasi

1. Nella pagina Configuration (Configurazione), fare clic su **Configuration** (Configurazione) dall'ambiente di lavoro Object Storage Service (Servizio di archiviazione oggetti).



2. Abilita scansioni di sola mappatura o scansioni di mappatura e classificazione sui bucket.



A:	Eseguire questa operazione:
Attivare scansioni solo mappatura su un bucket	Fare clic su **Map** (Mappa)
Abilitare scansioni complete su un bucket	Fare clic su **Map & Classify** (Mappa e classificazione)
Disattivare la scansione su un bucket	Fare clic su **Off**

Risultato

La classificazione BlueXP avvia la scansione dei bucket attivati. 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 immessa per tali origini dati potrebbe essere diversa dalle credenziali globali di Active Directory 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 di analisi. Al posto del proprietario del file che contiene il SID (Security identifier), viene inserito il nome utente effettivo.
- Puoi vedere "autorizzazioni complete per i file" Per ogni file e directory quando si fa clic sul pulsante "View All Permissions" (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
- Condivisioni file CIFS non NetApp (non condivisioni file NFS)
- Account OneDrive
- Account SharePoint

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 volumi CIFS/condivisioni file, se si desidera assicurarsi che i file "ultimi tempi di accesso" siano invariati dalle scansioni di classificazione BlueXP, si consiglia di disporre dell'autorizzazione Write Attributes. 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

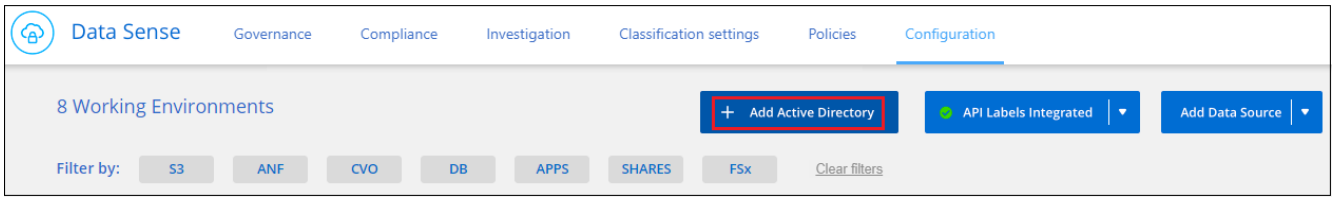
    oppure

  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

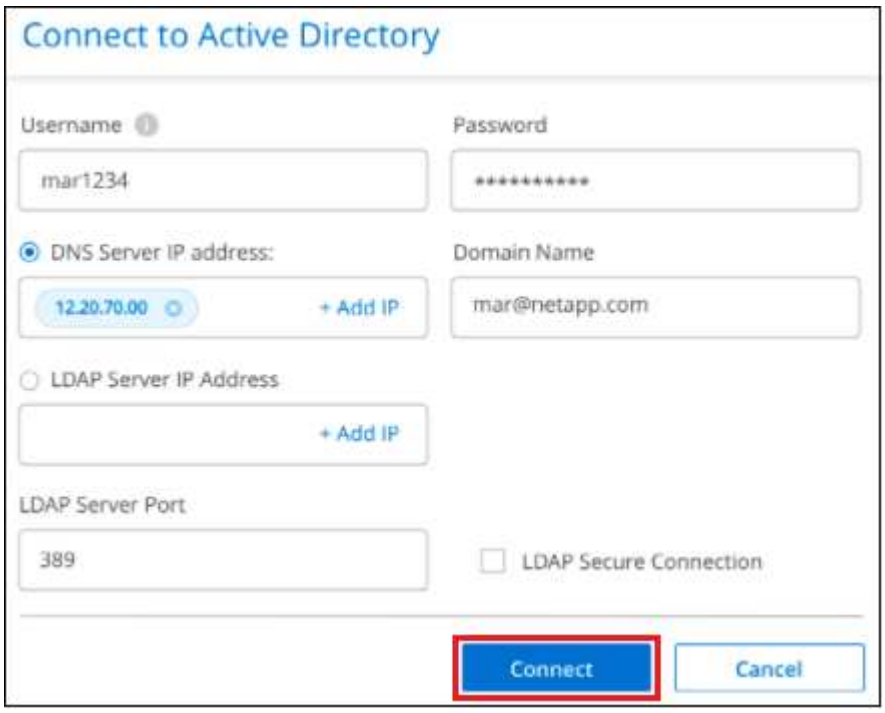
Fasi

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

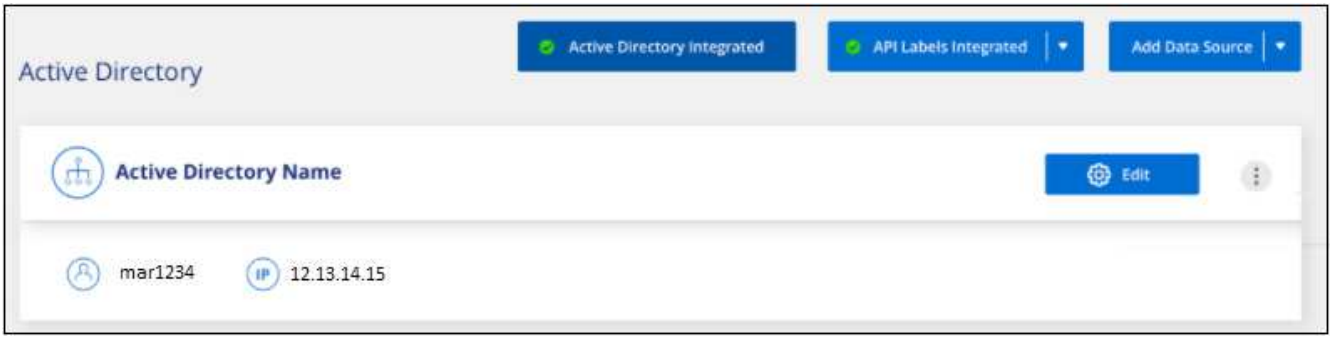


2. Nella finestra di dialogo connessione ad Active Directory, immettere i dettagli di Active Directory e fare clic su **Connetti**.

   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 se non è più necessaria facendo clic su E quindi **Rimuovi Active Directory**.

Impostare la licenza per la classificazione BlueXP

I primi 1 TB di dati che la classificazione BlueXP scansiona in un'area di lavoro BlueXP sono gratuiti per 30 giorni. Una licenza BYOL di NetApp, o un abbonamento dal mercato del tuo cloud provider, è necessario per continuare la scansione dei dati dopo tale data.

Alcune note prima di leggere ulteriori informazioni:

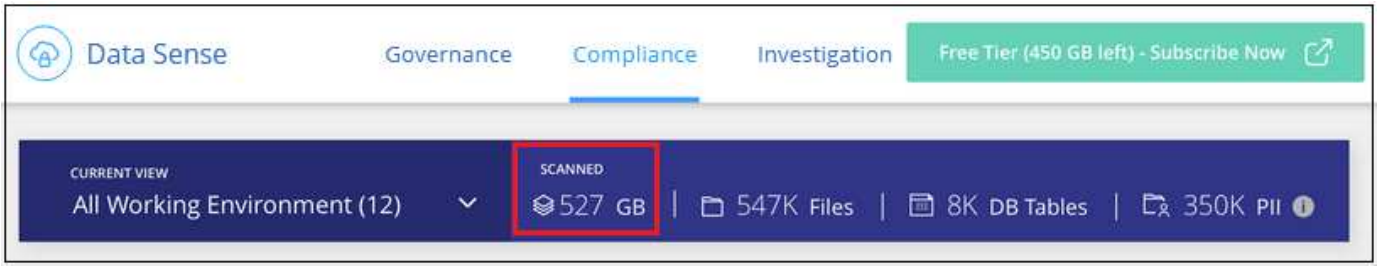
- Se hai già sottoscritto l'abbonamento BlueXP pay-as-you-go (PAYGO) nel mercato del tuo cloud provider, sarai automaticamente iscritto anche alla classificazione BlueXP. Non dovrai più iscriverti.
- La classificazione BlueXP (Data Sense) Bring-Your-Own-License (BYOL) è una licenza *floating* che è possibile utilizzare in tutti gli ambienti di lavoro e le origini dati nello spazio di lavoro che si intende sottoporre a scansione. Nel portafoglio digitale BlueXP viene visualizzato un abbonamento attivo.
- La quantità di dati sottoposti a scansione viene calcolata in base alle dimensioni del file logico senza efficienze dello storage.

"Scopri di più sulle licenze e sui costi relativi alla classificazione BlueXP".

prova gratuita di 30 giorni

È disponibile una prova gratuita di 30 giorni per un massimo di 1 TB di dati analizzati dalla classificazione BlueXP in un'area di lavoro BlueXP. Dovrai acquistare una licenza BYOL da NetApp o iscriverti a un abbonamento dal mercato del tuo cloud provider per continuare la scansione dei dati dopo quel momento.

Puoi iscriverti in qualsiasi momento e non ti verrà addebitato alcun costo fino al termine del periodo di prova di 30 giorni o fino a quando la quantità di dati non supera 1 TB. È sempre possibile visualizzare la quantità totale di dati sottoposti a scansione dalla dashboard di governance per la classificazione BlueXP. Inoltre, il pulsante *Iscriviti ora* semplifica l'iscrizione quando sei pronto.



Utilizza un abbonamento PAYGO per la classificazione BlueXP

Le iscrizioni pay-as-you-go dal marketplace del tuo cloud provider ti consentono di concedere in licenza l'uso dei sistemi Cloud Volumes ONTAP e di molti servizi BlueXP, come la classificazione BlueXP. Pagherai il tuo cloud provider per la quantità di dati che la classificazione BlueXP sta analizzando su base oraria in un singolo abbonamento.

L'iscrizione garantisce che il servizio non subisca interruzioni al termine della prova gratuita. Al termine del periodo di prova, verrà addebitato ogni ora il costo in base alla quantità di dati che si sta eseguendo la scansione. Non ti verrà addebitato alcun costo dal tuo abbonamento durante la prova gratuita.

Fasi

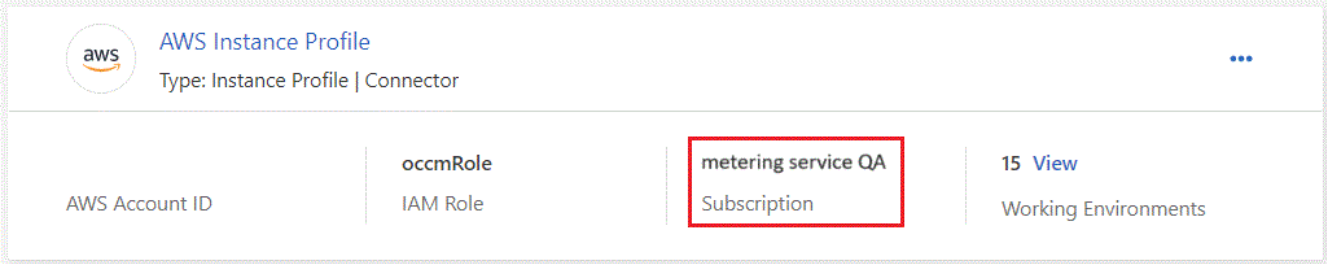
Questi passaggi devono essere completati da un utente che ha il ruolo di *account Admin*.

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

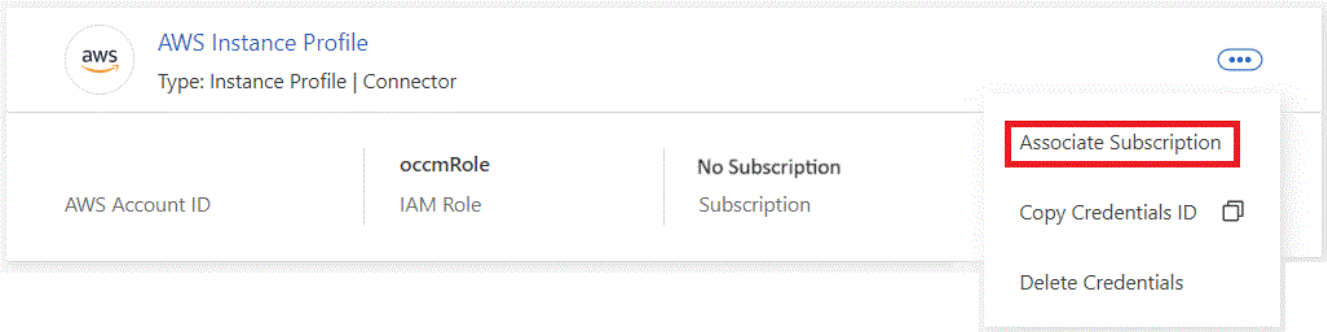
2. Fare clic su **credenziali** e individuare le credenziali per il profilo dell'istanza AWS, l'identità del servizio gestito Azure o Google Project.

   L'abbonamento deve essere aggiunto a Instance Profile, Managed Service Identity o Google Project. La ricarica non funziona altrimenti.

   Se disponi già di un abbonamento BlueXP (come mostrato di seguito per AWS), allora sei tutto impostato: Non devi fare altro.



3. Se non disponi ancora di un abbonamento, fai clic sul menu azione e su **Associa abbonamento**.



4. Selezionare un abbonamento esistente e fare clic su **associate** oppure fare clic su **Add Subscription** (Aggiungi abbonamento) e seguire la procedura.

   Il video seguente mostra come associare un "Mercato AWS" Iscrizione a un abbonamento AWS:

   ► https://docs.netapp.com/it-it/bluexp-classification//media/video_subscribing_aws.mp4 *(video)*

   Il video seguente mostra come associare un "Azure Marketplace" Iscrizione a un abbonamento Azure:

   ► https://docs.netapp.com/it-it/bluexp-classification//media/video_subscribing_azure.mp4 *(video)*

   Il video seguente mostra come associare a. "Google Cloud Marketplace" Iscrizione a un abbonamento GCP:

   ► https://docs.netapp.com/it-it/bluexp-classification//media/video_subscribing_gcp.mp4 *(video)*

Utilizzare un contratto annuale

Paga la classificazione BlueXP annualmente acquistando un contratto annuale. Sono disponibili in termini di 1, 2 o 3 anni.

Se disponi di un contratto annuale da un marketplace, tutta la scansione dei dati di classificazione BlueXP verrà addebitata in base al contratto. Non puoi combinare un contratto di mercato annuale con un BYOL.

- AWS: "Per informazioni sui prezzi, consulta l'offerta BlueXP Marketplace".
- Azure: "Per informazioni sui prezzi, consulta l'offerta BlueXP Marketplace".
- Cloud Google: Contatta il tuo commerciale NetApp per acquistare un contratto annuale. Il contratto è disponibile come offerta privata in Google Cloud Marketplace. Dopo che NetApp condividerà con te l'offerta privata, puoi selezionare il piano annuale effettuando l'iscrizione da Google Cloud Marketplace durante l'attivazione della classificazione BlueXP.

Utilizzare una licenza BYOL di classificazione BlueXP

Le licenze Bring-Your-Own di NetApp offrono termini di 1, 2 o 3 anni. La licenza di classificazione BYOL BlueXP (Data Sense) è una licenza *mobile* in cui la capacità totale è condivisa tra **tutti** gli ambienti di lavoro e le origini dati, semplificando il rinnovo e la licenza iniziale.

Se non disponi di una licenza di classificazione BlueXP, contattaci per acquistarne una:

- Mailto:ng-contact-data-sense@netapp.com?subject=Licensing[Invia e-mail per acquistare una licenza].
- Fare clic sull'icona della chat nell'angolo inferiore destro di BlueXP per richiedere una licenza.

Se si dispone di una licenza basata su nodo non assegnata per Cloud Volumes ONTAP che non si intende utilizzare, è possibile convertirla in una licenza di classificazione BlueXP con la stessa equivalenza in dollari e la stessa data di scadenza. "Fai clic qui per ulteriori informazioni".

USA il Digital Wallet di BlueXP per gestire le licenze BYOL di classificazione BlueXP. È possibile aggiungere nuove licenze, aggiornare le licenze esistenti e visualizzare lo stato della licenza dal portafoglio digitale BlueXP.

Ottenere il file di licenza per la classificazione BlueXP

Dopo aver acquistato la licenza di classificazione BlueXP (rilevamento dati), si attiva la licenza in BlueXP inserendo il numero seriale di classificazione BlueXP e l'account NSS (NetApp Support Site), o caricando il file di licenza NetApp (NLF). Se si prevede di utilizzare questo metodo, la procedura riportata di seguito mostra come ottenere il file di licenza NLF.

Se hai implementato la classificazione BlueXP su un host in un sito on-premise che non dispone di accesso a Internet, significa che hai implementato il connettore BlueXP "modalità privata", è necessario ottenere il file di licenza da un sistema connesso a internet. L'attivazione della licenza tramite il numero seriale e l'account NSS non è disponibile per le installazioni in modalità privata.

Prima di iniziare

Prima di iniziare, è necessario disporre delle seguenti informazioni:

- Numero di serie della classificazione BlueXP

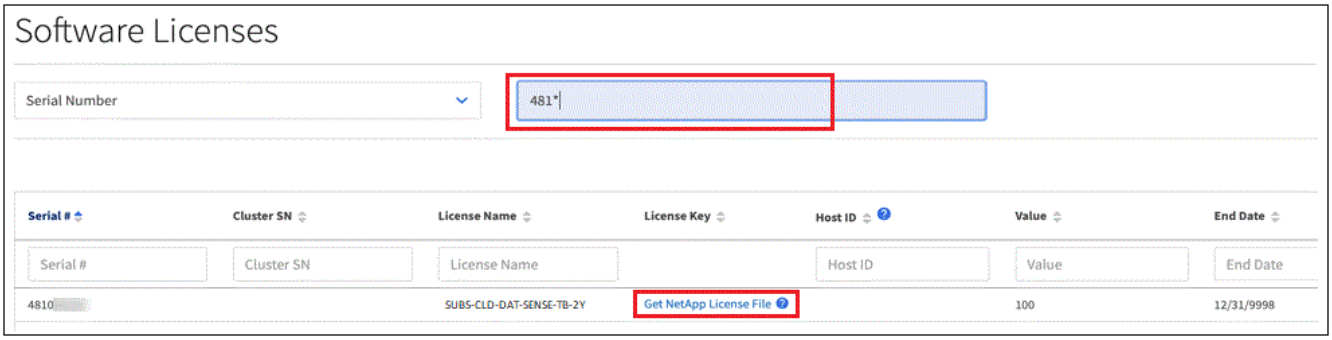
  Individua questo numero nell'ordine di vendita o contatta l'account team per ottenere queste informazioni.

- ID account BlueXP

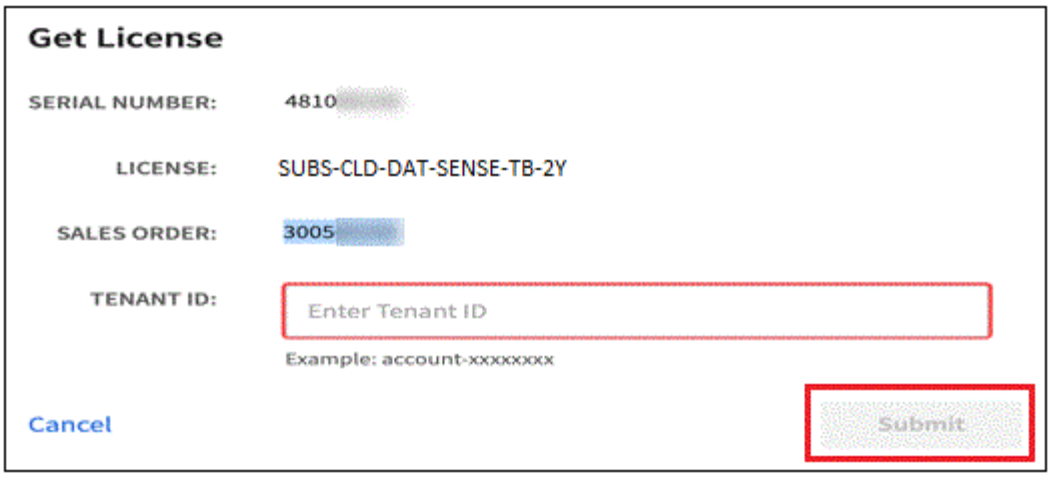
  Puoi trovare il tuo ID account BlueXP selezionando l'elenco a discesa **account** nella parte superiore di BlueXP, quindi facendo clic su **Gestisci account** accanto all'account. L'ID account si trova nella scheda Panoramica. Per i siti in modalità privata senza accesso a Internet, utilizzare **account-DARKSITE1**.

Fasi

1. Accedere a "Sito di supporto NetApp" E fare clic su **sistemi > licenze software**.
2. Inserire il numero di serie della licenza di classificazione BlueXP.



3. Nella colonna **chiave di licenza**, fare clic su **Ottieni file di licenza NetApp**.
4. Inserire l'ID account BlueXP (chiamato ID tenant sul sito di supporto) e fare clic su **Submit** (Invia) per scaricare il file di licenza.



Aggiungere le licenze BYOL di classificazione BlueXP al proprio account

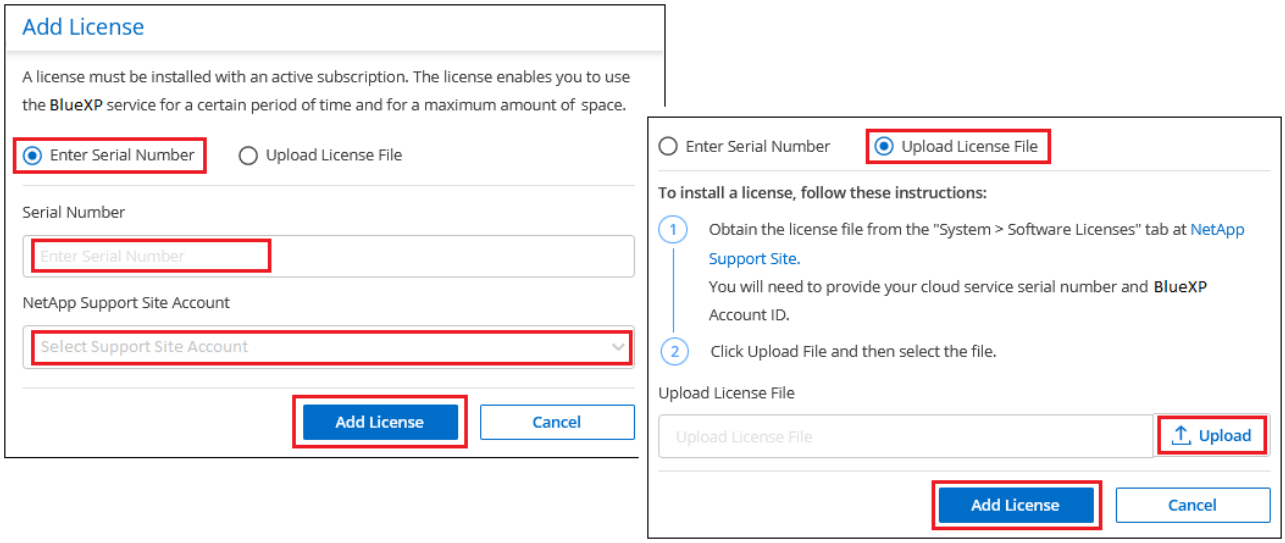
Dopo aver acquistato una licenza di classificazione BlueXP (Data Sense) per l'account BlueXP, è necessario aggiungere la licenza a BlueXP per utilizzare il servizio di classificazione BlueXP.

Fasi

1. Dal menu BlueXP, fare clic su **Governance > Digital wallet**, quindi selezionare la scheda **licenze servizi dati**.
2. Fare clic su **Aggiungi licenza**.
3. Nella finestra di dialogo *Add License*, inserire le informazioni sulla licenza e fare clic su **Add License**:
   - Se si dispone del numero di serie della licenza di classificazione BlueXP e si conosce il proprio account NSS, selezionare l'opzione **inserire il numero di serie** e immettere le informazioni desiderate.

     Se il tuo account NetApp Support Site non è disponibile nell'elenco a discesa, "Aggiungere l'account NSS a BlueXP".

   - Se si dispone del file di licenza di classificazione BlueXP (richiesto se installato in un sito buio), selezionare l'opzione **Upload License file** (carica file di licenza) e seguire le istruzioni per allegare il file.



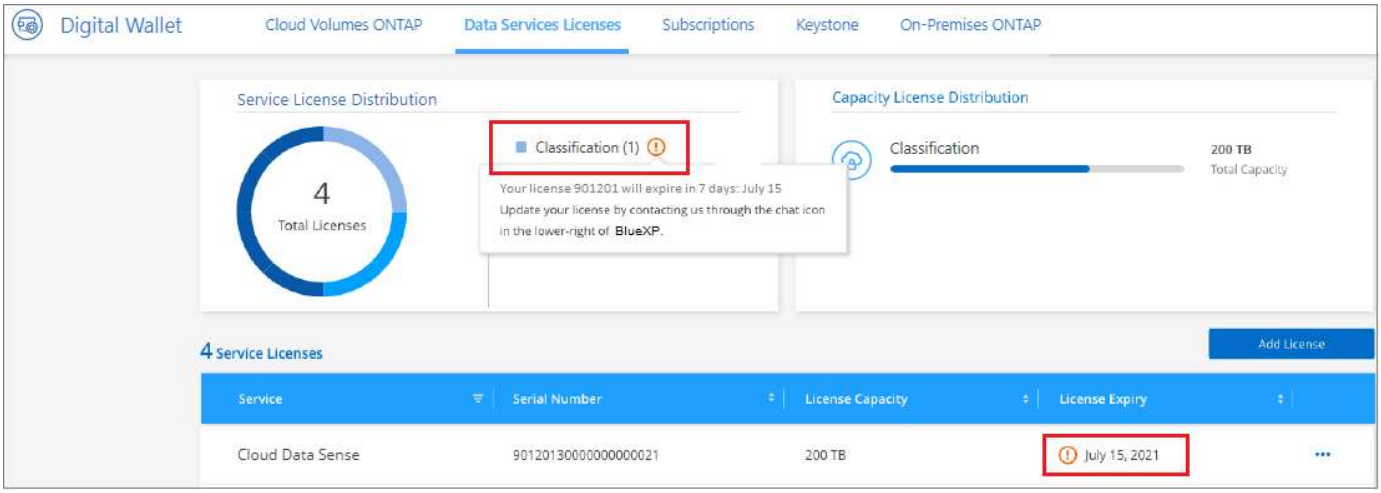
Risultato

BlueXP aggiunge la licenza in modo che il servizio di classificazione BlueXP sia attivo.

Aggiornare una licenza BYOL di classificazione BlueXP

Se il termine concesso in licenza si avvicina alla data di scadenza o se la capacità concessa in licenza raggiunge il limite, verrà inviata una notifica nell'interfaccia utente classificazione.

Questo stato viene visualizzato anche nel Digital Wallet di BlueXP e in "Notifiche".



È possibile aggiornare la licenza di classificazione BlueXP prima della scadenza, in modo da non interrompere l'accesso ai dati sottoposti a scansione.

Fasi

1. Fare clic sull'icona della chat in basso a destra in BlueXP per richiedere un'estensione del termine o una capacità aggiuntiva alla licenza Cloud Data Sense per il numero di serie specifico. È inoltre possibile inviare all'indirizzo inviare un'e-mail per richiedere un aggiornamento della licenza.

   Dopo aver pagato la licenza e averla registrata nel NetApp Support Site, BlueXP aggiorna automaticamente la licenza nel portafoglio digitale BlueXP e la pagina licenze servizi dati rifletterà la modifica tra 5 e 10 minuti.

2. Se BlueXP non riesce ad aggiornare automaticamente la licenza (ad esempio, se installata in un sito buio), sarà necessario caricare manualmente il file di licenza.

   a. È possibile Ottenere il file di licenza dal NetApp Support Site.

   b. Nella pagina del portafoglio digitale BlueXP della scheda *licenze servizi dati*, fare clic su ••• Per il numero di serie del servizio che si sta aggiornando, fare clic su **Aggiorna licenza**.

c. Nella pagina *Update License*, caricare il file di licenza e fare clic su **Update License** (Aggiorna licenza).

Risultato

BlueXP aggiorna la licenza in modo che il servizio di classificazione BlueXP continui ad essere attivo.

Considerazioni sulla licenza BYOL

Quando si utilizza una licenza BYOL di classificazione BlueXP (Data Sense), BlueXP visualizza un avviso nell'interfaccia utente di classificazione BlueXP e nell'interfaccia utente del portafoglio digitale BlueXP quando la dimensione di tutti i dati che si sta scansionando è prossima al limite di capacità o alla data di scadenza della licenza. Vengono visualizzati i seguenti avvisi:

- Quando la quantità di dati che si sta scansionando ha raggiunto il 80% della capacità concessa in licenza, e di nuovo quando si è raggiunto il limite
- 30 giorni prima della scadenza di una licenza e di nuovo alla scadenza della stessa

Utilizzare l'icona chat in basso a destra dell'interfaccia BlueXP per rinnovare la licenza quando vengono visualizzati questi avvisi.

Se la licenza scade o si è raggiunto il limite BYOL, la classificazione BlueXP continua a funzionare, ma l'accesso ai dashboard viene bloccato in modo da non visualizzare le informazioni relative ai dati sottoposti a scansione. Solo la pagina *Configuration* è disponibile nel caso in cui si desideri ridurre il numero di volumi sottoposti a scansione per portare potenzialmente l'utilizzo della capacità al di sotto del limite di licenza.

Una volta rinnovata la licenza BYOL, BlueXP aggiorna automaticamente la licenza nel portafoglio digitale BlueXP e fornisce l'accesso completo a tutti i dashboard. Se BlueXP non riesce ad accedere al file di licenza tramite una connessione Internet sicura (ad esempio, se installato in un sito buio), è possibile ottenere il file da soli e caricarlo manualmente su BlueXP. Per istruzioni, vedere Come aggiornare una licenza di classificazione BlueXP.

> Se l'account in uso dispone sia di una licenza BYOL che DI un abbonamento PAYGO, la classificazione BlueXP *non* passerà all'abbonamento PAYGO alla scadenza della licenza BYOL. È necessario rinnovare la licenza BYOL.

Domande frequenti sulla classificazione BlueXP

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

Servizio di classificazione BlueXP

Le seguenti domande forniscono una comprensione generale della classificazione BlueXP.

Che cos'è la classificazione BlueXP?

La classificazione BlueXP è un'offerta cloud che utilizza la tecnologia basata sull'intelligenza artificiale (ai) per aiutarti a comprendere il contesto dei dati e identificare i dati sensibili nei tuoi sistemi storage. I sistemi possono essere ambienti di lavoro aggiunti a BlueXP Canvas e molti tipi di origini dati a cui la classificazione BlueXP può accedere attraverso le reti. "Consulta l'elenco completo qui sotto".

La classificazione BlueXP fornisce parametri predefiniti (ad esempio tipi e categorie di informazioni sensibili) per soddisfare le nuove normative sulla conformità dei dati in materia di privacy e sensibilità, come GDPR, CCPA, HIPAA e altro ancora.

Come funziona la classificazione BlueXP?

La classificazione BlueXP implementa un altro livello di intelligenza artificiale insieme al sistema BlueXP e ai sistemi storage. Esegue quindi la scansione dei dati su volumi, bucket, database e altri account storage e indicizza le informazioni sui dati trovate. La classificazione BlueXP sfrutta sia l'intelligenza artificiale che l'elaborazione del linguaggio naturale, al contrario di soluzioni alternative che sono comunemente costruite intorno alle espressioni regolari e alla corrispondenza dei modelli.

La classificazione BlueXP utilizza l'ai per fornire una comprensione contestuale dei dati per un rilevamento e una classificazione accurati. È basato sull'ai perché è progettato per i moderni tipi di dati e la scalabilità. Inoltre, comprende il contesto dei dati per fornire un rilevamento e una classificazione efficaci e precisi.

"Scopri di più sul funzionamento della classificazione BlueXP".

Quali sono i casi di utilizzo più comuni per la classificazione BlueXP?

- Identificare le informazioni personali identificabili (PII).
- Individuare e creare report su dati specifici in risposta a soggetti interessati, come richiesto da GDPR, CCPA, HIPAA e altre normative sulla privacy dei dati.
- Rispettare le nuove e future normative sulla privacy dei dati.
- Rispettare le normative sulla privacy e sulla conformità dei dati.
- Migrazione dei dati dai sistemi legacy al cloud.
- Rispettare le policy di conservazione dei dati.

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

E l'architettura della classificazione BlueXP?

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. Ciò consente il supporto per ambienti multi-cloud, cross-cloud, cloud privato e on-premise.

Quali cloud provider sono supportati?

La classificazione BlueXP funziona come parte di BlueXP e supporta AWS, Azure e GCP. In questo modo, la tua organizzazione potrà ottenere una visibilità unificata della privacy tra diversi cloud provider.

La classificazione BlueXP dispone di un’API REST e funziona con strumenti di terze parti?

BlueXP supporta le funzionalità API REST per i propri servizi. Se BlueXP non è il punto di gestione preferito, i servizi come la classificazione BlueXP possono essere utilizzati anche tramite un’API REST. Ogni azione dell’utente dispone di un’API REST che può essere integrata con sistemi di terze parti. Vedere "API di classificazione BlueXP" per ulteriori informazioni.

La classificazione BlueXP è disponibile attraverso i mercati?

Sì, le classificazioni BlueXP e BlueXP sono disponibili nei mercati AWS, Azure e GCP.

Analisi e scansione della classificazione BlueXP

Le seguenti domande si riferiscono alle prestazioni di scansione della classificazione BlueXP e agli analytics disponibili per gli utenti.

Con quale frequenza la classificazione BlueXP esegue la scansione dei dati?

Mentre la scansione iniziale dei dati potrebbe richiedere un po' di tempo, le scansioni successive esaminano solo le modifiche incrementali, riducendo i tempi di scansione del sistema. La classificazione BlueXP scansiona continuamente i dati in modo round-robin, sei repository alla volta, in modo che tutti i dati modificati vengano classificati molto rapidamente.

"Scopri come funzionano le scansioni".

Nota: La classificazione BlueXP analizza i database solo una volta al giorno, pertanto non viene eseguita la scansione continua dei database come avviene per altre origini dati.

Le scansioni dei dati hanno un impatto trascurabile sui sistemi storage e sui dati. Tuttavia, se si è preoccupati anche di un impatto molto ridotto, è possibile configurare la classificazione BlueXP per eseguire scansioni "lente". "Scopri come ridurre la velocità di scansione".

Posso cercare i miei dati usando la classificazione BlueXP?

La classificazione BlueXP offre ampie funzionalità di ricerca che semplificano la ricerca di un file o di un dato specifico in tutte le origini connesse. La classificazione BlueXP consente agli utenti di effettuare ricerche più approfondite rispetto a quanto riflettono i metadati. Si tratta di un servizio indipendente dal linguaggio che può anche leggere i file e analizzare una moltitudine di tipi di dati sensibili, come nomi e ID. Ad esempio, gli utenti possono eseguire ricerche negli archivi di dati strutturati e non strutturati per trovare dati che potrebbero essere trapelati dai database ai file utente, in violazione delle policy aziendali. Le ricerche possono essere salvate in un secondo momento e le policy possono essere create per eseguire ricerche e azioni sui risultati a una frequenza impostata.

Una volta trovati i file di interesse, è possibile elencare le caratteristiche, inclusi tag, account dell’ambiente di lavoro, bucket, percorso file, categoria (dalla classificazione), dimensione del file, ultima modifica, stato delle autorizzazioni, duplicati, livello di sensibilità, dati personali, tipi di dati sensibili all’interno del file, proprietario, tipo di file, dimensione del file, tempo di creazione, hash di file, se i dati sono stati assegnati a qualcuno che cerca la loro attenzione, e altro ancora. I filtri possono essere applicati a caratteristiche non pertinenti. La classificazione BlueXP dispone inoltre di controlli RBAC per consentire lo spostamento o l’eliminazione dei file, se sono presenti le autorizzazioni corrette. Se non sono presenti le autorizzazioni corrette, è possibile assegnare le attività a un utente dell’organizzazione che dispone delle autorizzazioni appropriate.

Che tipo di analisi fornisce la classificazione BlueXP?

Le origini dati possono essere rappresentate visivamente e le relazioni possono essere definite e rappresentate graficamente. Ad esempio, gli amministratori possono visualizzare tutti i dati obsoleti, duplicati e non correlati al business tra le origini dati dell'intera azienda (sistemi on-premise, database, condivisioni di file, archivi S3, OneDrive, ecc.). Possono quindi copiare, spostare, eliminare e gestire i dati per ottimizzare i costi di storage e ridurre i rischi. Gli utenti possono ridurre i rischi osservando quali dati sensibili potrebbero essere esposti e possono creare lavori per gestire le autorizzazioni per una protezione dei dati efficace. La classificazione BlueXP classifica anche tutti i diversi tipi di dati, in modo che gli amministratori possano analizzare i dati per tipo e vedere quali azioni sono state intraprese sui dati e quando.

La classificazione BlueXP offre report?

Sì. Le informazioni offerte dalla classificazione BlueXP possono essere rilevanti per gli altri stakeholder della tua organizzazione, pertanto ti consentiamo di generare report per condividere le informazioni. Per la classificazione BlueXP sono disponibili i seguenti report:

Report sulla valutazione dei rischi per la privacy
: Fornisce informazioni sulla privacy dai dati e un punteggio di rischio per la privacy. "Scopri di più".

Report Data Subject Access Request
: Consente di estrarre un report di tutti i file che contengono informazioni relative al nome specifico o all'identificativo personale di un soggetto. "Scopri di più".

Report PCI DSS
: Consente di identificare la distribuzione delle informazioni sulla carta di credito nei file. "Scopri di più".

Report HIPAA
: Consente di identificare la distribuzione delle informazioni sanitarie tra i file. "Scopri di più".

Report Data Mapping
: Fornisce informazioni sulle dimensioni e sul numero di file negli ambienti di lavoro. Ciò include capacità di utilizzo, età dei dati, dimensioni dei dati e tipi di file. "Scopri di più".

Report Data Discovery Assessment
: Fornisce un'analisi di alto livello dell'ambiente sottoposto a scansione per evidenziare i risultati del sistema e mostrare le aree di preoccupazione e le potenziali fasi di risoluzione dei problemi. "Modalità di apprendimento".

Report su un tipo di informazioni specifico
: Sono disponibili report che includono dettagli sui file identificati che contengono dati personali e dati personali sensibili. È inoltre possibile visualizzare i file suddivisi per categoria e tipo di file. "Scopri di più".

Le prestazioni di scansione variano?

Le prestazioni di scansione possono variare in base alla larghezza di banda della rete e alle dimensioni medie dei file nell'ambiente in uso. Può anche dipendere dalle caratteristiche di dimensione del sistema host (nel cloud o on-premise). Vedere "L'istanza di classificazione BlueXP" e. "Implementazione della classificazione BlueXP" per ulteriori informazioni.

Quando si aggiungono inizialmente nuove origini dati, è anche possibile scegliere di eseguire solo una scansione di "mappatura" invece di una scansione di "classificazione" completa. Il mapping può essere eseguito sulle origini dati molto rapidamente perché non accede ai file per vedere i dati all'interno. "Vedere la differenza tra una scansione di mappatura e di classificazione".

Gestione e privacy della classificazione BlueXP

Le seguenti domande forniscono informazioni su come gestire le impostazioni di classificazione e privacy di BlueXP.

Come si attiva la classificazione BlueXP?

Innanzitutto, è necessario implementare un'istanza della classificazione BlueXP in BlueXP o in un sistema on-premise. Una volta eseguita l'istanza, è possibile attivare il servizio su ambienti di lavoro, database e altre origini dati esistenti dalla scheda **Configurazione** o selezionando un ambiente di lavoro specifico.

"Scopri come iniziare".

> Attivando la classificazione BlueXP su un'origine dati si ottiene una scansione iniziale immediata. I risultati della scansione vengono visualizzati subito dopo.

Come si disattiva la classificazione BlueXP?

È possibile disattivare la classificazione BlueXP dalla scansione di un singolo ambiente di lavoro, database, gruppo di condivisione file, account OneDrive o account SharePoint dalla pagina di configurazione della classificazione BlueXP.

"Scopri di più".

> Per rimuovere completamente l'istanza di classificazione BlueXP, è possibile rimuovere manualmente l'istanza di classificazione BlueXP dal portale del provider di cloud o dalla posizione on-premise.

Posso personalizzare il servizio in base alle esigenze della mia organizzazione?

La classificazione BlueXP offre informazioni pronte all'uso ai tuoi dati. Queste informazioni possono essere estratte e utilizzate per le esigenze della tua organizzazione.

Inoltre, la classificazione BlueXP offre diversi modi per aggiungere un elenco personalizzato di "dati personali" che la classificazione BlueXP identificherà nelle scansioni, fornendo un quadro completo della posizione dei dati potenzialmente sensibili in *tutti* i file delle organizzazioni.

- È possibile aggiungere identificatori univoci in base a colonne specifiche nei database che si sta eseguendo la scansione — questo viene chiamato **Data Fusion**.
- È possibile aggiungere parole chiave personalizzate da un file di testo.
- È possibile aggiungere modelli personalizzati utilizzando un'espressione regolare (regex).

"Scopri di più".

È possibile istruire il servizio per escludere la scansione dei dati in determinate directory?

Sì. Se si desidera che la classificazione BlueXP escluda la scansione dei dati che risiedono in determinate directory di origine dati, è possibile fornire tale elenco al motore di classificazione. Dopo aver applicato questa modifica, la classificazione BlueXP esclude la scansione dei dati nelle directory specificate.

"Scopri di più".

Vengono sottoposte a scansione copie snapshot che risiedono su volumi ONTAP?

No La classificazione BlueXP non scansiona gli snapshot perché il contenuto è identico al contenuto del volume.

Cosa succede se il tiering dei dati è attivato sui volumi ONTAP?

Quando la classificazione BlueXP esegue la scansione di volumi con dati cold a livelli per lo storage a oggetti, esegue la scansione di tutti i dati presenti sui dischi locali e sui dati cold a livelli per lo storage a oggetti. Ciò vale anche per i prodotti non NetApp che implementano il tiering.

La scansione non scalda i dati a freddo - rimane fredda e rimane nello storage a oggetti.

La classificazione BlueXP può inviare notifiche alla mia organizzazione?

Sì. In combinazione con la funzionalità Criteri, è possibile inviare avvisi e-mail agli utenti BlueXP (giornalmente, settimanalmente o mensilmente) o a qualsiasi altro indirizzo e-mail, quando un criterio restituisce risultati in modo da poter ricevere notifiche per proteggere i dati. Scopri di più "Policy".

È inoltre possibile scaricare i report sullo stato dalla pagina Governance e dalla pagina Investigation che è possibile condividere internamente all'organizzazione.

La classificazione BlueXP funziona con le etichette AIP incorporate nei file?

Sì. È possibile gestire le etichette AIP nei file che la classificazione BlueXP sta analizzando, se si è abbonati "Azure Information Protection (AIP)". È possibile visualizzare le etichette già assegnate ai file, aggiungere etichette ai file e modificare le etichette esistenti.

"Scopri di più".

Tipi di sistemi di origine e tipi di dati

Le domande seguenti riguardano i tipi di storage che è possibile sottoporre a scansione e i tipi di dati sottoposti a scansione.

Quali fonti di dati è possibile sottoporre a scansione con la classificazione BlueXP?

La classificazione BlueXP consente di eseguire la scansione dei dati da ambienti di lavoro aggiunti a BlueXP Canvas e da molti tipi di origini dati strutturate e non strutturate a cui la classificazione BlueXP può accedere attraverso le reti.

Ambienti di lavoro:

- Cloud Volumes ONTAP (implementato in AWS, Azure o GCP)
- Cluster ONTAP on-premise
- Azure NetApp Files
- Amazon FSX per ONTAP
- Amazon S3

Origini dati:

- File share non NetApp

- Storage a oggetti (che utilizza il protocollo S3)
- Database (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL SERVER)
- Account OneDrive
- Account SharePoint Online e on-premise
- Account Google Drive

La classificazione BlueXP supporta le versioni NFS 3.x e CIFS 1.x, 2,0, 2,1 e 3,0.

Esistono restrizioni quando viene implementato in un'area governativa?

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

- Impossibile eseguire la scansione di account OneDrive, SharePoint e Google Drive.
- La funzionalità dell'etichetta AIP (Microsoft Azure Information Protection) non può essere integrata.

Quali origini dati è possibile eseguire la scansione se si installa la classificazione BlueXP in un sito senza accesso a Internet?

La classificazione BlueXP può eseguire la scansione dei dati solo da origini dati locali al sito on-premise. Al momento, la classificazione BlueXP può eseguire la scansione delle seguenti origini dati locali in "modalità privata", nota anche come sito "scuro":

- Sistemi ONTAP on-premise
- Schemi di database
- Account SharePoint on-premise (SharePoint Server)
- Condivisioni di file NFS o CIFS non NetApp
- Storage a oggetti che utilizza il protocollo S3 (Simple Storage Service)

Quali tipi di file sono supportati?

La classificazione BlueXP esegue la scansione di tutti i file per informazioni su categorie e metadati e visualizza tutti i tipi di file nella sezione tipi di file della dashboard.

Quando la classificazione BlueXP rileva le informazioni personali identificabili (PII) o quando esegue una ricerca DSAR, sono supportati solo i seguenti formati di file:

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

Quali tipi di dati e metadati cattura la classificazione BlueXP?

La classificazione BlueXP consente di eseguire una scansione generale di "mappatura" o una scansione completa di "classificazione" sulle origini dati. La mappatura fornisce solo una panoramica di alto livello dei dati, mentre la classificazione fornisce una scansione di alto livello dei dati. Il mapping può essere eseguito sulle origini dati molto rapidamente perché non accede ai file per vedere i dati all'interno.

- Scansione di mappatura dei dati.

  La classificazione BlueXP esegue la scansione solo dei metadati. Questo è utile per la gestione e la

governance dei dati globali, l'ambito rapido dei progetti, le proprietà molto grandi e la prioritizzazione. La mappatura dei dati si basa sui metadati ed è considerata una scansione **rapida**.

Dopo una scansione rapida, è possibile generare un report di mappatura dei dati. Questo report offre una panoramica dei dati memorizzati nelle origini dati aziendali per aiutarti a prendere decisioni in merito all'utilizzo delle risorse, alla migrazione, al backup, alla sicurezza e ai processi di conformità.

- Scansione di classificazione dei dati (profonda).

  La classificazione BlueXP esegue la scansione utilizzando protocolli standard e autorizzazioni di sola lettura in tutti gli ambienti. I file selezionati vengono aperti e sottoposti a scansione per rilevare dati aziendali sensibili, informazioni private e problemi relativi al ransomware.

  Dopo una scansione completa, sono disponibili molte funzionalità di classificazione BlueXP aggiuntive che è possibile applicare ai dati, ad esempio visualizzare e perfezionare i dati nella pagina Data Investigation, cercare i nomi all'interno dei file, copiare, spostare ed eliminare i file di origine e molto altro ancora.

La classificazione BlueXP acquisisce metadati come nome del file, autorizzazioni, ora di creazione, ultimo accesso e ultima modifica. Sono inclusi tutti i metadati visualizzati nella pagina Dettagli analisi dati e nei rapporti analisi dati.

La classificazione BlueXP è in grado di identificare molti tipi di dati privati, come dati personali e dati personali sensibili. Per informazioni dettagliate sui dati privati, fare riferimento a. "Categorie di dati privati analizzate dalla classificazione BlueXP".

Posso limitare le informazioni di classificazione di BlueXP a utenti specifici?

Sì, la classificazione BlueXP è completamente integrata con BlueXP. Gli utenti di BlueXP possono visualizzare solo le informazioni relative agli ambienti di lavoro che possono visualizzare in base ai privilegi dell'area di lavoro.

Inoltre, se si desidera consentire a determinati utenti di visualizzare solo i risultati della scansione di classificazione di BlueXP senza avere la possibilità di gestire le impostazioni di classificazione di BlueXP, è possibile assegnare a tali utenti il ruolo Cloud Compliance Viewer.

"Scopri di più".

Qualcuno può accedere ai dati privati inviati tra il browser e la classificazione BlueXP?

No I dati privati inviati tra il browser e l'istanza di classificazione BlueXP sono protetti con una crittografia end-to-end che utilizza TLS 1,2, il che significa che NetApp e terze parti non possono leggerli. La classificazione BlueXP non condividerà dati o risultati con NetApp a meno che non venga richiesto e approvato l'accesso.

I dati sottoposti a scansione rimangono nell'ambiente in cui si opera.

Come vengono gestiti i dati sensibili?

NetApp non ha accesso ai dati riservati e non li visualizza nell'interfaccia utente. I dati sensibili vengono mascherati, ad esempio gli ultimi quattro numeri vengono visualizzati per le informazioni sulla carta di credito.

Dove sono memorizzati i dati?

I risultati della scansione sono memorizzati in Elasticsearch all'interno dell'istanza di classificazione BlueXP.

Come si accede ai dati?

La classificazione BlueXP accede ai dati archiviati in Elasticsearch tramite chiamate API, che richiedono autenticazione e sono crittografati tramite AES-128. L'accesso a Elasticsearch richiede direttamente l'accesso root.

Licenze e costi

Le seguenti domande riguardano licenze e costi per l'utilizzo della classificazione BlueXP.

Quanto costa la classificazione BlueXP?

Il costo per l'utilizzo della classificazione BlueXP dipende dalla quantità di dati che si sta eseguendo la scansione. I primi 1 TB di dati che la classificazione BlueXP scansiona in un'area di lavoro BlueXP sono gratuiti per 30 giorni. Dopo aver raggiunto uno dei due limiti, per continuare la scansione dei dati è necessario uno dei seguenti elementi:

- Un abbonamento all'elenco BlueXP Marketplace dal tuo provider cloud, o.
- Una BYOL (Bring-Your-Own-License) di NetApp

Vedere "prezzi" per ulteriori informazioni.

Cosa succede se è stato raggiunto il limite di capacità BYOL?

Se si raggiunge un limite di capacità BYOL, la classificazione BlueXP continua a funzionare, ma l'accesso ai dashboard viene bloccato in modo da non visualizzare le informazioni relative ai dati sottoposti a scansione. Solo la pagina di configurazione è disponibile nel caso in cui si desideri ridurre il numero di volumi sottoposti a scansione per portare potenzialmente l'utilizzo della capacità al di sotto del limite di licenza. È necessario rinnovare la licenza BYOL per ottenere l'accesso completo alla classificazione BlueXP.

Implementazione del connettore

Le seguenti domande si riferiscono a BlueXP Connector.

Che cos'è il connettore?

Il connettore è un software in esecuzione su un'istanza di calcolo all'interno del tuo account cloud o on-premise, che consente a BlueXP di gestire in modo sicuro le risorse cloud. È necessario implementare un connettore per utilizzare la classificazione BlueXP.

Dove deve essere installato il connettore?

- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in AWS, Amazon FSX per ONTAP o nei bucket AWS S3, si 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.
- Quando si esegue la scansione dei dati in Cloud Volumes ONTAP in GCP, si utilizza un connettore in GCP.
- Quando si eseguono scansioni di dati in sistemi ONTAP on-premise, condivisioni di file non NetApp, storage a oggetti S3 generico, database, cartelle OneDrive, account SharePoint e account Google Drive, è possibile utilizzare un connettore in una qualsiasi di queste posizioni cloud.

Quindi, se si dispone di dati in molte di queste posizioni, potrebbe essere necessario utilizzare "Connettori

multipli".

La classificazione BlueXP richiede l'accesso alle credenziali?

La classificazione BlueXP non recupera le credenziali di storage. Al contrario, vengono archiviati nel connettore BlueXP.

La classificazione BlueXP usa le credenziali del piano dati, ad esempio, le credenziali CIFS per montare le condivisioni prima della scansione.

È possibile implementare il connettore sul proprio host?

Sì. È possibile "Implementare il connettore on-premise" Su un host Linux nella rete o su un host nel cloud. Se si prevede di implementare la classificazione BlueXP on-premise, potrebbe essere necessario installare anche il connettore on-premise, ma non è necessario.

La comunicazione tra il servizio e il connettore utilizza il protocollo HTTP?

Sì, la classificazione BlueXP comunica con il connettore BlueXP tramite HTTP.

E i siti sicuri senza accesso a Internet?

Sì, anche questo è supportato. È possibile "Implementare il connettore su un host Linux on-premise che non dispone di accesso a Internet". "Questa funzione è nota anche come "modalità privata"". Quindi, è possibile individuare cluster ONTAP on-premise e altre origini dati locali e eseguire la scansione dei dati utilizzando la classificazione BlueXP.

Implementazione della classificazione BlueXP

Le seguenti domande si riferiscono all'istanza di classificazione BlueXP separata.

Quali modelli di implementazione supporta la classificazione BlueXP?

BlueXP consente all'utente di eseguire scansioni e report sui sistemi praticamente ovunque, inclusi ambienti on-premise, cloud e ibridi. La classificazione BlueXP viene normalmente implementata utilizzando un modello SaaS, in cui il servizio viene attivato tramite l'interfaccia BlueXP e non richiede alcuna installazione hardware o software. Anche in questa modalità di implementazione click-and-run, la gestione dei dati può essere eseguita indipendentemente dal fatto che gli archivi di dati siano on-premise o nel cloud pubblico.

Quale tipo di istanza o macchina virtuale è richiesto per la classificazione BlueXP?

Quando "implementato nel cloud":

- In AWS, la classificazione BlueXP viene eseguita su un'istanza m6i.4xlarge con un disco GP2 da 500 GiB. È possibile selezionare un tipo di istanza più piccolo durante la distribuzione.
- In Azure, la classificazione BlueXP viene eseguita su una macchina virtuale Standard_D16s_v3 con un disco da 500 GiB.
- In GCP, la classificazione BlueXP viene eseguita su una macchina virtuale n2-standard-16 con un disco persistente 500 GiB Standard.

Si noti che è possibile implementare la classificazione BlueXP su un sistema con meno CPU e meno RAM, ma ci sono delle limitazioni quando si utilizzano questi sistemi. Vedere "Utilizzando un tipo di istanza più piccolo" per ulteriori informazioni.

"Scopri di più sul funzionamento della classificazione BlueXP".

È possibile implementare la classificazione BlueXP sul proprio host?

Sì. È possibile installare il software di classificazione BlueXP su un host Linux con accesso a Internet nella rete o nel cloud. Tutto funziona allo stesso modo e si continua a gestire la configurazione e i risultati della scansione tramite BlueXP. Vedere "Implementazione della classificazione BlueXP on-premise" per i requisiti di sistema e i dettagli sull'installazione.

E i siti sicuri senza accesso a Internet?

Sì, anche questo è supportato. È possibile "Implementare la classificazione BlueXP in un sito on-premise che non dispone di accesso a Internet" per siti completamente sicuri.